FLUKE ®

68x Series

Enterprise LANMeter®

Users Manual

April 1999
Rev. 1, 1/2000

LIMITED WARRANTY AND LIMITATION OF LIABILITY

Each Fluke product is warranted to be free from defects in material and workmanship under normal use and service. The warranty period is one year and begins on the date of shipment. Parts, product repairs, and services are warranted for 90 days. This warranty extends only to the original buyer or end-user customer of a Fluke authorized reseller, and does not apply to fuses, disposable batteries, or to any product which, in Fluke's opinion, has been misused, altered, neglected, contaminated, or damaged by accident or abnormal conditions of operation or handling. Fluke 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 does not warrant that software will be error free or operate without interruption.

Fluke 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. Warranty support is available only if product is purchased through a Fluke authorized sales outlet or Buyer has paid the applicable international price. Fluke 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's warranty obligation is limited, at Fluke's option, to refund of the purchase price, free of charge repair, or replacement of a defective product which is returned to a Fluke authorized service center within the warranty period.

To obtain warranty service, contact your nearest Fluke 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 assumes no risk for damage in transit. Following warranty repair, the product will be returned to Buyer, transportation prepaid (FOB Destination). If Fluke determines that failure was caused by neglect, misuse, contamination, alteration, accident, or abnormal condition of operation or handling, including overvoltage failures caused by use outside the product's specified rating, or normal wear and tear of mechanical components, Fluke 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 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.

Fluke Corporation
P.O. Box 9090
Everett, WA 98206-9090
U.S.A.

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

11/99

Table of Contents

Appendices

List of Tables

List of Figures

Chapter 1
Introduction

Getting Started

Refer to the *Getting Started* manual, PN 1546949, for basic operating details of your LANMeter instrument. The *Getting Started* manual is supplied with your LANMeter instrument. Some of the information from *the Getting Started* manual is repeated in this chapter for your convenience.

Chapter Summary

1. **Introduction:** Introduces the Fluke Enterprise LANMeter™ (68x Series) instruments and lists the supplied equipment.
2. **Testing Cables and Connectors:** Provides information about running cable tests and interpreting test results.
3. **Monitoring the Network:** Provides information about running network monitor tests and interpreting test results.
4. **Testing Network Components:** Provides information about running network component tests and interpreting test results.
5. **Testing Novell NetWare:** Provides information about running Novell NetWare tests and interpreting test results.
6. **Testing TCP/IP Networks:** Provides information about running TCP/IP Network tests, TCP/IP Internetwork tests, and interpreting test results.
7. **SwitchWizard Option:** Provides information about running the SwitchWizard™ Option and interpreting test results.
8. **Testing Banyan VINES:** Provides information about running Banyan VINES tests and interpreting test results.

9. **Testing NetBIOS:** Provides information about running NetBIOS tests and interpreting test results.
10. **WideAreaWizard Option:** Provides information about running the WideAreaWizard™ Option and interpreting test results.
11. **Web Agent/WebRemote Control:** Provides information about using and configuring the LANMeter instrument as a web server so that it can be accessed and controlled using a web browser.
12. **File Manager:** Provides information about using File Manager for configuring the instrument, selecting previously saved files, and performing actions on the Reports & Graphics, Data Log, and Station List files.
13. **Terminal Emulator Option:** Provides information about using Terminal Emulator to inspect or change the configuration of network devices.
14. **Station List:** Provides information about the Station List Utility, which allows the use of symbolic names for alphanumeric, station addresses.

Appendices

A. **Troubleshooting Scenarios:** Provides specific examples of troubleshooting Ethernet and Token Ring networks.

B. **Specifications:** Provides the specifications for the LANMeter instruments.

C. **Maintenance:** Provides information about the LANMeter instrument maintenance and accessories.

D. **Utilities:** Provides information about using the Enterprise LANMeter Utilities.

E. **Glossary:** Provides definitions of terms used in this manual.

Fluke 68x Series Instruments

The Fluke Enterprise LANMeter (68x Series) instruments are versatile battery-operated handheld instruments used to isolate many problems that can occur on your Ethernet and Token Ring networks. The Fluke Enterprise LANMeter series consists of the Fluke 686, Fluke 685, Fluke 683, Fluke 682, and Fluke 680 LANMeter instruments.

Table 1-1. LANMeter Instrument Network Configuration

Model #	10 Mbps Ethernet	100 Mbps Ethernet	4 Mbps Token Ring	16 Mbps Token Ring
680			X	X
682	X			
683	X	X		
685	X		X	X
686	X	X	X	X

Equipment Supplied

The following equipment is supplied with the LANMeter instrument:

❒ Combination Wire Map and Cable Identifier #0 Remote Adapter
❒ Instrument Case
❒ Users Manual on CD-ROM
❒ Getting Started Manual
❒ AC Adapter/Battery Charger

Auto Test

You can use the Auto Test feature to automatically configure your LANMeter instrument with an IP address and start the Segment Discovery test. Auto Test uses DHCP Discover Mode to assign an IP address. Refer to Chapter 6, “Testing TCP/IP Networks” for more information on configuring your LANMeter instrument’s IP address and the Segment Discovery test.

Start Auto Test by pressing the ENTER RUN key from the top-level softkeys. You should allow the Segment Discovery test to run at least 20 minutes to get an accurate view of your network. You can stop Auto Test by pressing the EXIT STOP softkey.

Interface Mode Icons

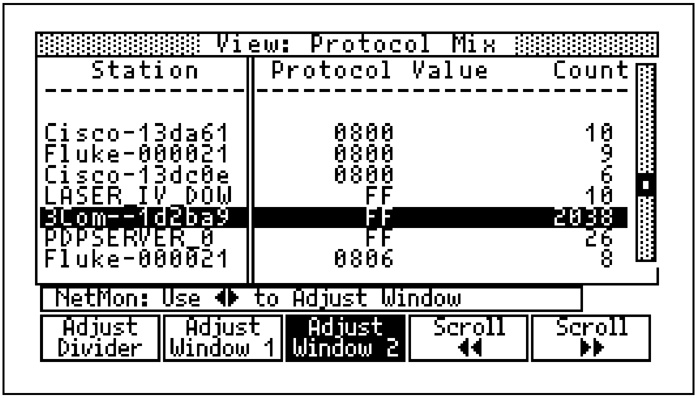
This icon is used in this manual to signify that the text that follows refers to the Ethernet interface only. The Fluke 683 and 682 have the Ethernet interface only and the Fluke 686 and 685 can be switched between the Ethernet and Token Ring interfaces.

This icon is used in this manual to signify that the text that follows refers to the Token Ring interface only. The Fluke 680 has the Token Ring interface only and the Fluke 686 and 685 can be switched between the Ethernet and Token Ring interfaces.

View All

The View All function is available from many tests and therefore its description is presented here rather than for each and every test.

View All allows you to look at text report results that take up more space than can be displayed on a single screen. The maximum number of nodes in a View All report is 512. After a test has stopped, you can select **View All**, after pressing MENU. This will display a report of up to 512 nodes. This capability is supported in any test that supports the Print All capability, such as Protocol Mix and Top MAC. View All also shows Active Monitor History information for the Ring Stations test. Figure 1-1 shows a View All example screen.



View: Protocol Mix

Station	Protocol Value	Count
Cisco-13da61	0800	10
Fluke-000021	0800	9
Cisco-13dc0e	0800	6
LASER_IV_DOW	FF	10
3Com--1d2ba9	FF	2038
PDPSERVER_0	FF	26
Fluke-000021	0806	8

NetMon: Use ◀▶ to Adjust Window

Figure 1-1. View All Example Screen

The View All display is split into two windows that stay synchronized keeping related data on the same horizontal lines. You can view the rest of the available results in Figure 1-1 by changing the location of the divider and scrolling left and right in either of the two windows.

You change the information shown by selecting the **Adjust Divider**, **Adjust Window 1**, or **Adjust Window 2** softkeys. Selecting **Adjust Divider** allows you to change the size of the two windows. Selecting **Adjust Window 1** or **Adjust Window 2** allows you to scroll left or right throughout the report. Pressing the **Adjust Divider**, **Adjust Window 1**, or **Adjust Window 2** softkey a second time displays the **Prev Page** and **Next Page** softkeys.

You can display MAC Address and Protocols, for example, by first selecting **Adjust Window 2**, scrolling to the left until the **`MAC Address`** and **`Protocols`** columns are displayed. Selecting **Adjust Window 2** again displays the **Prev Page** and **Next Page** softkeys.

Table 1-2 shows a printout of a View All report.

Table 1-2. View All Example Report

```
------------------------------------------------------------
  Station    MAC Address    Protocol   Protocol Value  Count
------------------------------------------------------------
Cisco-13da61 00000c13da61           IP      0800          10
Fluke-000021 00c017000021           IP      0800           9
Cisco-13dc0e 00000c13dc0e           IP      0800           6
LASER_IV_DOW 08000994aa86 NetWare802.3        FF          10
3Com--1d2ba9 0020af1d2ba9 NetWare802.3        FF        2038
PDPSERVER_0  00403200d5c6 NetWare802.3        FF          26
Fluke-000021 00c017000021          ARP      0806           8
Cisco-13da61 00000c13da61          ARP      0806           8
LAW          0020af67ffa1 NetWare802.3        FF          22
TLH          0000f4a02c47 NetWare802.3        FF         501
DEB          0020af68009b NetWare802.3        FF        1465
Cisco-13da61 00000c13da61     Loopback      9000           2
Cisco-13dc0e 00000c13dc0e     Loopback      9000           2
             001b21000000     Vines IP      0BAD           2
Cisco-13da61 00000c13da61     Vines IP      0BAD           1
JK           0020af68010a NetWare802.3        FF           3
Cisco-13dc0e 00000c13dc0e     Vines IP      0BAD           1
```

Chapter 2
Testing Cables and Connectors

Introduction

The Enterprise LANMeter offers an extensive range of cable testing features that allow you to isolate and repair physical layer problems that can impact your network's operation. The following standard cable tests are available on the Enterprise LANMeter:

- ❒ Cable Scan
- ❒ Wire Map
- ❒ Cable I.D.
- ❒ DC Continuity
- ❒ Find NVP

Fiber cable testing is available on the Enterprise LANMeter when using the Fiber Test Option, Part Number DSP-FTK. Refer to the "The Fiber Test Option" section in this chapter for more information on testing fiber cable.

100 MHz Category 5 cable testing is available on the Enterprise LANMeter when using the 100 MHz Cable Test Option (also called 100 MHz Remote), Part Number 68X-002. The following cable tests require the 100 MHz Cable Test Option. Refer to the "The 100 MHz Remote" section in this chapter for more information on the 100 MHz Cable Test Option.

- ❒ Cable Autotest
- ❒ Near-End Crosstalk (NEXT)
- ❒ Attenuation
- ❒ Calibrate Remote

Press the top-level **Cable Tests** softkey to access Cable Tests. Figure 2-1 shows the Cable Tests softkeys.

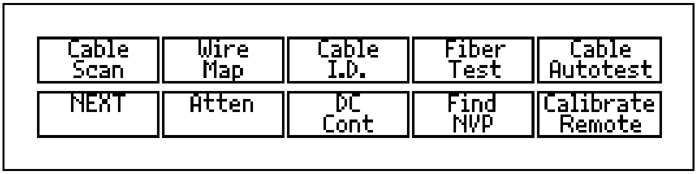


Figure 2-1. Cable Test Softkeys

The Fiber Test Option

The Fiber Test Option allows the Enterprise LANMeter to test fiber optic cable. You can measure optical loss and output power on multimode or singlemode cable.

The Fiber Test Option requires the Enterprise LANMeter software version 8.00, or later, and consists of the following:

❒ Fiber Optic Meter (Fluke DSP-FOM)
❒ Singlemode Fiber Optic Source (Optional—Fluke LS-1310/1550)
❒ Multimode Fiber Optic Source (Fluke DSP-FOS)
❒ Two Fiber Optic Patch Cables

Warning

Never look directly into the fiber optic source connector or attempt to adjust or modify the source. Doing so might expose you to hazardous LED radiation.

The following topics are covered in this section:

❒ Ensuring Accurate Measurements
❒ Setting a Reference
❒ Measuring Optical Loss
❒ Measuring Output Power
❒ Fiber Test Results

Refer to the instruction sheet that is provided with the Fiber Test Option for specifications and maintenance information for the fiber optic meter and sources.

Ensuring Accurate Measurements

Do the following to help ensure accurate fiber measurements:

❒ Clean all fiber connectors before testing.
❒ Before using the optical source, turn it on and let it stabilize for 2 minutes.

Setting a Reference

Use the following procedure, before measuring a cable's optical loss, to set a reference level by measuring the loss in the fiber patch cables and connectors:

1. Make the connections shown in Figure 2-2. Use the same type of cable as the cable to be tested.

   To test in singlemode, connect the optional Singlemode Fiber Optic Source (Fluke LS-1310/1550), for 1310 and 1550 wavelengths.. To test in multimode, connect the Multimode Fiber Optic Source (Fluke DSP-FOS), for 1300 and 850 wavelengths.

2. Press the top-level **Cable Tests** softkey.
3. Press the **Fiber Test** softkey two times. The LANMeter instrument detects the active fiber optic meter and the meter's wavelength setting and then displays the fiber test results, as shown in Figure 2-5.
4. Press the **Set Ref.** softkey from the fiber test display to set the reference level for the LANMeter instrument.

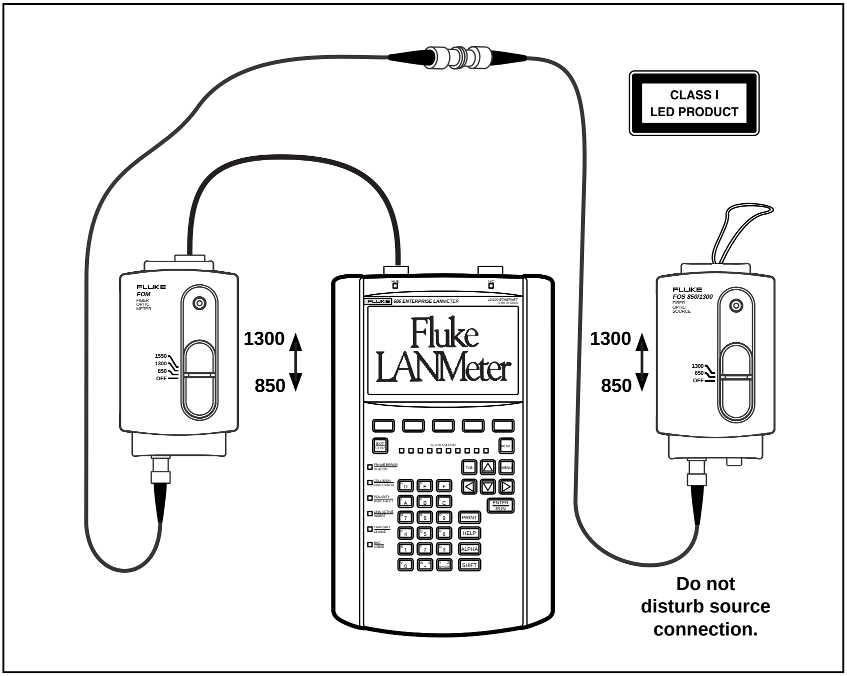
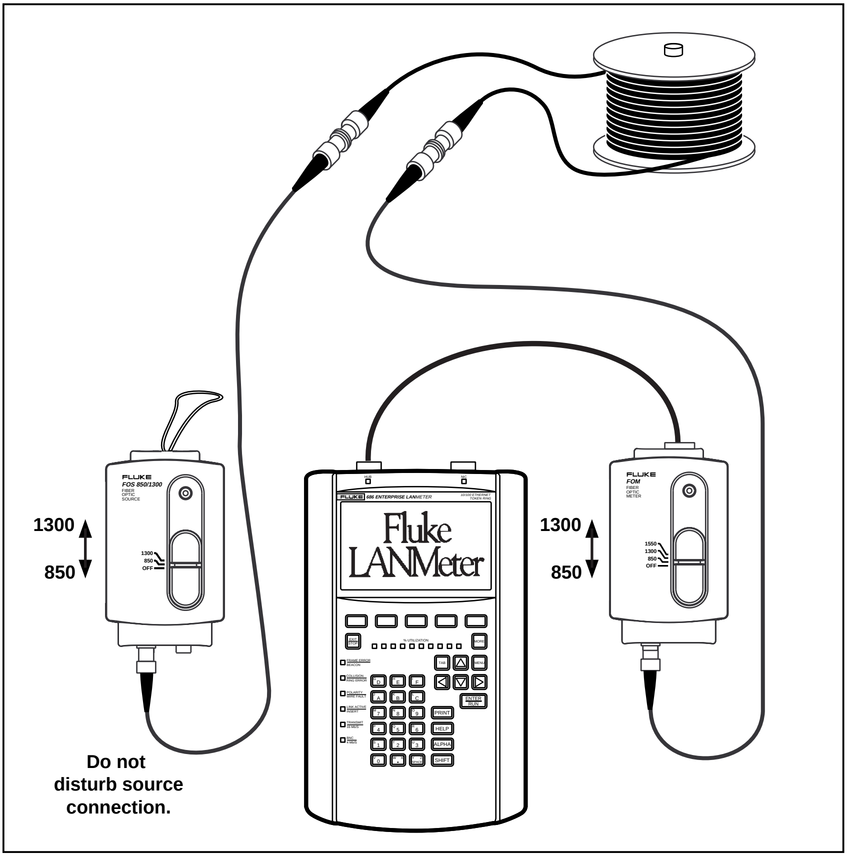


Figure 2-2. Connections for Setting a Reference Level

Measuring Optical Loss

After setting the reference, do not disturb the source connection as you make connections to measure optical loss, as shown in Figure 2-3. If the fiber test is not already running, press the top-level **Cable Tests** softkey and then press **Fiber Test** twice to start the test. The LANMeter instrument displays the fiber test results as shown in Figure 2-5.



Do not disturb source connection.

Figure 2-3. Connections for Measuring Optical Loss

Measuring Output Power

Make the connections shown in Figure 2-4 to measure the output power. If the fiber test is not already running, press the top-level **Cable Tests** softkey and then press **Fiber Test** twice to start the test. The LANMeter instrument displays the fiber test results as shown in Figure 2-5.

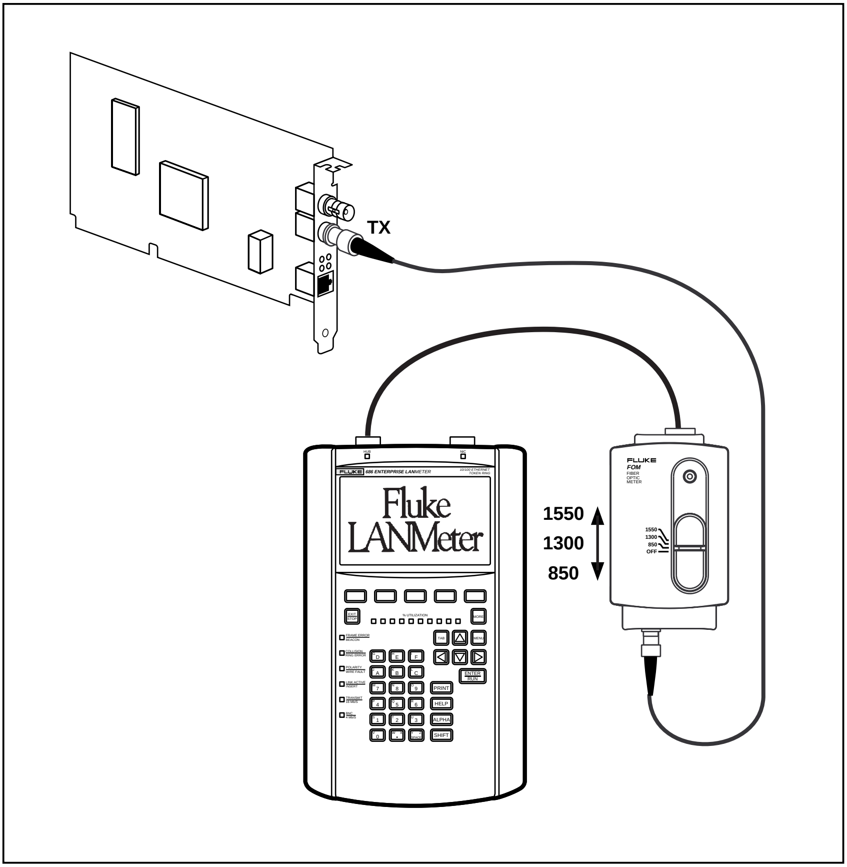
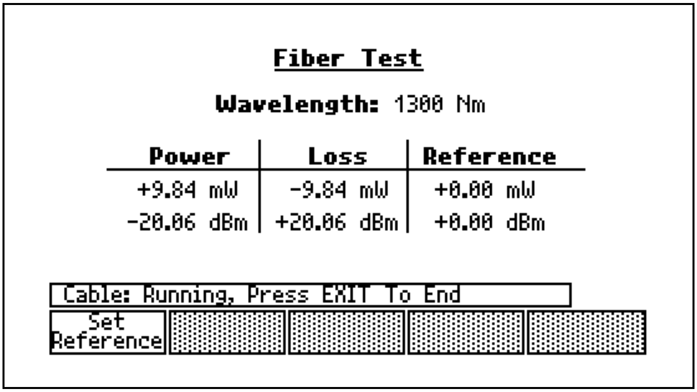


Figure 2-4. Connections for Measuring Output Power

Fiber Test Results

Output power, optical power loss, and the current reference level are shown in microwatts (µW) and decibels (dBm or dB). Figure 2-5 shows Fiber Test Option sample results. The power and loss measurements are updated continuously.



Fiber Test

Wavelength: 1300 Nm

Power	Loss	Reference
+9.84 mW	-9.84 mW	+0.00 mW
-20.06 dBm	+20.06 dBm	+0.00 dBm

Cable: Running, Press EXIT To End

Figure 2-5. Fiber Test Option Sample Results

The 100 MHz Remote

The optional 100 MHz Remote enhances the LANMeter instrument’s cable testing capabilities to include 100 MHz cable certification to TSB-67 Level I compliance.

The optional 100 MHz Remote is compatible with all Fluke 68x Series instruments except some Fluke 67x Series instruments upgraded to 68x Series. Your 67x instrument is compatible with the 100 MHz Remote if its serial number is as described in Table 2-1 or if your instrument displays **100 MHz Cable Test Compatible** in the power-on screen or in the top-level softkey screen.

Table 2-1. Valid Serial #s for Upgraded 67x Series

Model #	Valid Serial #s for Upgraded 67x Series 100 MHz Remote Compatibility
670	> 6311801
672	> 6296601
675	> 6281701

The 100 MHz Remote tests 100 ohm twisted pair cable only and measures attenuation, Near-End Crosstalk (NEXT) and Attenuation to Crosstalk Ratio (ACR) across a frequency range up to 100 MHz.

LEDs on the 100 MHz Remote indicate the current state of the remote and of the test in progress; refer to Figure 2-6 and Table 2-2. The following shows the LEDs and their meaning:

❒	Yellow	Test in progress
❒	Green	Test passed
❒	Red	Test failed

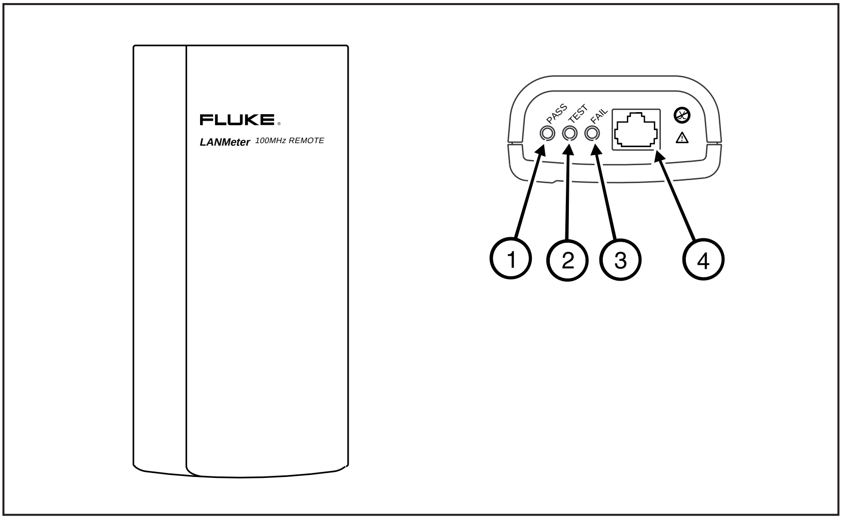


Figure 2-6. 100 MHz Remote

Table 2-2. 100 MHz Remote Features

Item	Feature	Description
1	Pass LED	A green LED that turns on at the end of a test if no faults were detected.
2	Test LED	A yellow LED that turns on when a test is in progress.
3	Fail LED	A red LED that turns on at the end of a test if one or more faults were detected.
4	RJ-45 Connector	A shielded 8-pin jack for shielded and unshielded twisted pair cable.

The 100 MHz Remote uses a standard 9 volt alkaline battery. The 100 MHz Remote remains in a sleep mode until it is turned on by the LANMeter instrument and it automatically returns to its sleep mode approximately 15 seconds after the end of the test.

Attaching Cables for the 100 MHz Remote

To run a cable test using the 100 MHz Remote, attach the Remote and the LANMeter instrument's **TO HUB/MAU** RJ-45 connector to opposite ends of the same cable.

If you set up and start the LANMeter instrument at one end of the cable, it will wait until the 100 MHz Remote is attached to the other end of the cable before starting the test.

The 100 MHz Remote tests 100 ohm twisted pair cable only.

Calibrate the 100 MHz Remote

You must calibrate the 100 MHz Remote using the supplied ScTP Cat 5 patch cable prior to running the Cable Autotest, NEXT, or Attenuation test. If you do not, the LANMeter instrument prompts you with a message to calibrate the 100 MHz Remote. Refer to the "Calibrate Remote" section at the end of this chapter for information on running this test.

Note

> *The LANMeter instrument stores the 100 MHz Remote calibration information in non-volatile memory so that you only have to run the Calibrate Remote test once per 100 MHz Remote. The LANMeter instrument can store calibration information on up to five 100 MHz Remotes.*
>
> *For re-calibration, run the Calibrate Remote test once per 100 MHz Remote every three months.*

100 MHz Remote Accessories

The 100 MHz Remote is documented in this chapter and comes with the following accessories:

- ❐ ScTP Cat 5 Patch Cable
- ❐ Soft Carrying Case

Attaching Cables

It is important to properly connect the LANMeter instrument to your network. Refer to the “Attaching Cables” section in the “*Getting Started*” manual for detailed information on attaching cables for all Cable Tests that do not require the Fiber Test Option or the 100 MHz Remote. For testing fiber cable, which requires the Fiber Test Option, refer to the previous “The Fiber Test Option” section for information on attaching cables. For Cable Tests that require the 100 MHz Remote, refer to the previous “The 100 MHz Remote” section for information on attaching cables.

Configuring Cable Tests

The two fields available for configuration in most of the Cable Tests are Specification and Cable Type. The network specification and cable type that you select determine which test standards are used and which tests are run during cable testing. The network specification should be selected first. Only the cable types that apply to the selected network specification are available in the Cable Type selection field. Refer to Table 2-3 for information on which cables are available for a given network specification. You can also configure additional parameters for each test by using the following procedure:

1. Press the top-level **Cable Tests** softkey.
2. Highlight the desired test by pressing its softkey once or by pressing MORE and then pressing the softkey once. (The first softkey in a test group is automatically highlighted.)
3. Press MENU, select the **Configure** option (it may already be selected), and then press ENTER RUN to access the configuration screen.
4. Configure the available parameters.

   a. Press ▽ or △ to highlight the desired field.

b. Press [SPACE], **Show Choices**, or use ◁ or ▷ to select any of the preprogrammed parameters for a given field or enter the desired value by using the numbers 0 through 9 as required.

To undo any configuration changes you made, press [MENU], select **Cancel Changes** in the Configuration Menu, and then press [ENTER RUN].

5. Press [EXIT STOP] to save your configuration to non-volatile memory and exit the configuration screen.

The following are all of the Cable Tests configuration parameters. The selected network specification and cable type define the default parameters.

□ Specification can be one of the Network Specifications shown in Table 2-3. Selecting the network specification is important because it determines the configurable cable types, the configuration default values, the tests to be run, and the measurement limits.

□ Cable is one of the Cable Types shown in Table 2-3 or 2-4. The cable types available depend upon the selected network specification. Only the appropriate cable types are available for a given network specification.

□ NVP (Nominal Velocity of Propagation) is a two digit number.

□ Test Pairs are defined by the selected Network Specification. Select a subset of the available pairs to be tested by pressing **Show Choices** or by using ◁ or ▷.

Note

To insure compliance with the Network Specification, the maximum number of pairs should be tested.

□ Ambient Temperature can be 20, 30, 40, or 50 °C. (Only available when a TIA specification is selected.) This parameter affects the limits measured against for the Attenuation test.

□ Test Speed as Fast or TIA Compliant. The Fast test speed uses 500 KHz steps for the NEXT test. TIA Compliant meets the requirements for TSB-67 Level 1 and uses 150 KHz steps for the 1 - 31.25 MHz range and 250 KHz steps for the 31.25 - 100 MHz range.

It is important to correctly set the network specification and cable type to obtain accurate results.

To restore all network specifications defaults and cable NVPs, press [MENU], select **Restore Defaults**, and press [ENTER RUN].

Table 2-3 shows the cable types that are available for the given network specification and which tests are run.

Table 2-3. Cable Types versus Network Specifications and Tests Run

For this Specification	These Cable Types are Available	These Tests are Run During Cable Autotest	On these Pairs
TIA Cat 5 Channel	UTP Cat 5, ScTP Cat 5	Wire Map, Length, Impedance, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
TIA Cat 5 Basic Link	UTP Cat 5, ScTP Cat 5	Wire Map, Length, Impedance, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
TIA Cat 4 Channel	UTP Cat 5, UTP Cat 4, ScTP Cat 5, ScTP Cat 4	Wire Map, Length, Impedance, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
TIA Cat 4 Basic Link	UTP Cat 5, UTP Cat 4, ScTP Cat 5, ScTP Cat 4	Wire Map, Length, Impedance, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
TIA Cat 3 Channel	UTP Cat 5, UTP Cat 4, UTP Cat 3, ScTP Cat 5, ScTP Cat 4, ScTP Cat 3	Wire Map, Length, Impedance, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
TIA Cat 3 Basic Link	UTP Cat 5, UTP Cat 4, UTP Cat 3, ScTP Cat 5, ScTP Cat 4, ScTP Cat 3	Wire Map, Length, Impedance, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
ISO/IEC Class C	UTP Cat 5, UTP Cat 4, UTP Cat 3, ScTP Cat 5, ScTP Cat 4, ScTP Cat 3	Wire Map, Length, Impedance, Prop. Delay, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
ISO/IEC Class D	UTP Cat 5, ScTP Cat 5	Wire Map, Length, Impedance, Prop. Delay, Attenuation, NEXT, ACR	1-2, 3-6, 4-5, and 7-8

Table 2-3. Cable Types versus Network Specifications and Tests Run (Cont)

For this Specification	These Cable Types are Available	These Tests are Run During Cable Autotest	On these Pairs
IEEE 10BASE2	RG-58 ThinLAN, RG-58 Foam, 10BASE2	Length, Impedance	BNC Coax
IEEE 10BASE5	RG-8 ThickLAN, 10BASE5	Length, Impedance	BNC Coax
10BASE-T	UTP Cat 5, UTP Cat 4, UTP Cat 3, ScTP Cat 5	Wire Map, Length, Impedance, Attenuation, NEXT	1-2 and 3-6
100BASE-TX	UTP Cat 5, ScTP Cat 5	Wire Map, Length, Impedance, Attenuation, NEXT, ACR	1-2 and 3-6
100BASE-T4	UTP Cat 5, UTP Cat 4, UTP Cat 3, ScTP Cat 5	Wire Map, Length, Impedance, Prop. Delay, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
100VG-AnyLAN	UTP Cat 5, UTP Cat 4, UTP Cat 3, ScTP Cat 5, ScTP Cat 4, ScTP Cat 3	Wire Map, Length, Impedance, Prop. Delay, Attenuation, NEXT	1-2, 3-6, 4-5, and 7-8
TokenRing, 4 Mb/s	UTP Cat 5, UTP Cat 4, UTP Cat 3, ScTP Cat 5, STP *****	Wire Map, Length, Impedance, Attenuation, NEXT, ACR	3-6 and 4-5
TokenRing, 16 Mb/s	UTP Cat 5, UTP Cat 4, UTP Cat 3, ScTP Cat 5, STP *****	Wire Map, Length, Impedance, Attenuation, NEXT, ACR	3-6 and 4-5
TP-PMD	UTP Cat 5, ScTP Cat 5	Wire Map, Length, Impedance, Attenuation, NEXT, ACR	1-2 and 7-8

***** Attenuation, NEXT, Wire Map, and ACR tests are not executed for 150 ohm STP cable.

Table 2-4. Cable Types, NVP, Impedance (Z) and Pairs

Cable Type	NVP	Z	100 MHz Remote Required
UTP Cat 5	69	100	Yes
UTP Cat 4	66	100	Yes
UTP Cat 3	62	100	Yes
STP	78	150	No
ScTP Cat 5	69	100	Yes
ScTP Cat 4	69	100	Yes
ScTP Cat 3	60	100	Yes
10BASE2	80	50	No
10BASE5	78	50	No
RG-58 ThinLAN	66	50	No
RG-58 Foam	78	50	No
RG-8 ThickLAN	84	50	No

Running Cable Tests

All Cable Tests are run in a similar manner. Use the following procedure to run all Cable Tests:

1. Press the top-level **Cable Tests** softkey.
2. Highlight the desired test by pressing its softkey once or by pressing MORE and then pressing the softkey once. (The first softkey in a test group is automatically highlighted.)
3. Connect the instrument as described in the "Attaching Cables" section in the *Getting Started* manual. If you are using the Fiber Test Option or the 100 MHz Cable Test Option, refer to the previous "The Fiber Test Option" or "The 100 MHz Cable Test Option" section for information on attaching cables.
4. Configure the instrument for the desired Cable Test. Refer to the "Configuring Cable Tests" section in this chapter for more information on configuring Cable Tests.
5. Run the desired test by pressing the test softkey again, or by pressing ENTER RUN.
6. Observe the View Summary test results (the default) or press **View Details** to display the details. Some tests require pressing △ or ▽ to view all of the results.

The Cable I.D. and DC Continuity tests require pressing EXIT STOP to end the test.

Refer to the following sections for a description of each of the Cable Tests.

Description of Cable Tests

The following sections describe each of the Cable Tests except for the Fiber Test. (Refer to “The Fiber Test Option” section for information on the Fiber Test.) Some tests require the 100 MHz Remote option. Refer to “The 100 MHz Remote” section for more information.

- ❒ Cable Scan
- ❒ Wire Map
- ❒ Cable I.D.
- ❒ Cable Autotest for 100 Ohm Twisted Pair Cable (requires the 100 MHz Remote option)
- ❒ Cable Autotest for Coax and 150 Ohm STP Cable
- ❒ NEXT (requires the 100 MHz Remote option)
- ❒ Attenuation (requires the 100 MHz Remote option)
- ❒ DC Continuity
- ❒ Find NVP
- ❒ Calibrate Remote (requires the 100 MHz Remote option)

Cable Scan

Cable Scan should be the first test run when a cable is suspected as the cause of a network failure. Cable Scan measures a cable’s length and characteristic impedance. In doing this, cable faults (such as excessive length, split-pairs) and other cable anomalies can be found. Cable Scan also compares its measurement results against the selected network specification and reports either **Cable OK** or **Suspected Cable Problem**. The LANMeter instrument also attempts to detect the Far End connection of the cable.

The Cable Scan test supports all of the LANMeter instrument configurable Cable Types and does not require the 100 MHz Remote.

Note

Similar types of cables from different vendors may have different NVP characteristics which can produce slightly different Cable Test results. If you desire highly accurate cable lengths results, you will need to run the Find NVP test first and enter your results into the appropriate test's NVP configuration parameter.

When testing 100 ohm twisted pair cabling, you can connect the Wire Map adapter (which properly terminates the cable) to the cable Far End, and then use the instrument to detect smaller impedance discontinuities, such as split pairs, that can occur at punchdown blocks.

Note

Cable Scan automatically detects a self-shorting IBM connector (Token Ring only) and correctly reports the cable length.

Note

For the most accurate cable length results, the cable should be open on the Far End. In the case of some 10BASE-T hubs, the hub can disable the port, which would require you to reset the hub.

After highlighting the **Cable Scan** softkey, you can configure the network specification and cable type for the cable you are about to test. You can also press MENU, select **Configure**, and press ENTER RUN to configure other parameters as needed. Refer to the "Configuring Cable Tests" section, for more information on configuring a Cable Test and to Table 2-3 for a listing of network specifications and their associated cable types.

When testing coaxial networks, you can use the following procedure to scan cable on a live coaxial network:

1. Configure the desired coaxial cable type as 10BASE2, 10BASE5, RG-58 ThinLAN, RG-58 Foam, or RG-ThickLAN.
2. Press MENU from the Cable Scan selection screen, select **BNC Term On** option, and then press ENTER RUN. The BNC LED starts flashing to indicate that the LANMeter instrument's internal 50 ohm termination is set.
3. Quickly remove the terminator at the end of the coaxial segment and attach the cable to your LANMeter instrument.
4. Press **Cable Scan** or ENTER RUN to run the test.

Caution

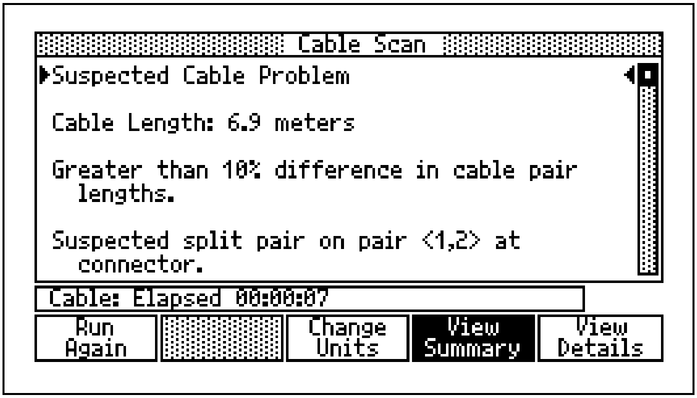
You can temporarily bring down your coaxial network if you exit Cable Scan while still connected to the network. This is because exiting Cable Scan causes the LANMeter instrument to automatically remove the internal 50 ohm termination, which is required for coaxial networks.

The instrument displays Cable Scan View Summary results at the end of the test. Figure 2-7 shows sample Cable Scan, View Summary results. The summary results include status of cable, Far-End connection, length, and impedance. The results may require that you scroll down to view all of the information.

You can then press **View Details** for information on pairs tested, length of the pair, impedance of the pair, and status of the pair (such as, split-pair or terminated).

A dash ("-") in the Length field implies that the LANMeter instrument could not measure the length of the cable. This is usually caused by the cable being terminated.

A dash ("-") in the Impedance field implies that the LANMeter instrument could not measure the cable's impedance. To make impedance measurements, the cable must be longer than 5 meters or terminated.



Cable Scan

Suspected Cable Problem

Cable Length: 6.9 meters

Greater than 10% difference in cable pair lengths.

Suspected split pair on pair <1,2> at connector.

Cable: Elapsed 00:00:07

Figure 2-7. Cable Scan Summary Results

Interpreting the Cable Scan Results

The primary use of the Cable Scan test is to measure a cable's characteristic impedance and length, and to test for any cable faults. To get the best results from the Cable Scan test, do the following:

1. Configure the network specification and cable type correctly.
    a. The network specification defines the pairs that are tested.
    b. The cable type determines the characteristic impedance and NVP.
2. Use the correct NVP (Nominal Velocity of Propagation).
    a. The Cable Scan test transmits a pulse on the cable and measures the time the pulse takes to travel down the cable and return to the instrument.
    b. For the instrument to accurately calculate the cable length, it is important to configure the correct NVP. The instrument is programmed with the standard NVP values supplied by cable manufacturers. These NVP values are generally worst case values. NVP variations are not uncommon between different batches of the same manufacturer's cable type.
    c. If you desire very accurate cable length tests, let the instrument calculate a precise NVP value by using the Find NVP test with a known length of cable. Store the new NVP value in any of the cable types for later use.
3. The instrument measures the actual length of the copper wires. Because wires are twisted within the cable, the measured length of the copper wires may be somewhat longer than the cable's physical length and the length of individual pairs within a cable may vary slightly.
4. Unlike most cable scanners, the LANMeter instrument measures the correct cable length for cables with self-shorting loopback hermaphroditic connectors (typically used with Token Ring Type 1 cable). **Do not** halve the reported length to get the actual cable length.

    The instrument length measurements have no dead zone, so you can measure right up to the connector. This is valuable in isolating connector and short-cable related problems.

5. An impedance test is used to detect split pairs that occur at the connector. There must be at least 5 meters of cable, or the cable must be terminated, to make a valid impedance measurement.
6. When the instrument reports a cable fault, it is likely due to one or more of the following:
   a. Punchdown block connection
   b. Connectors
   c. Cable kinks or cuts
7. If you use the Cable Scan test for testing cables plugged into MAUs (Token Ring only), the resulting cable lengths will be an approximation that depend upon the type of MAU used. Expect the best results with passive MAUs. Reported distances are always somewhat longer than the actual cable length due to the signal passing through the MAU. False faults may also be reported.
8. If you use the Cable Scan to test SILVER SATIN (flat telephone cable) or any other untwisted cable, it is likely that it will report a split pair on the cable. Due to the construction of flat telephone cable, it does not have twisted wire pairs. **You should never use untwisted cable for LAN applications.**

Wire Map

The Wire Map test checks for miswires on all eight conductors of twisted pair cabling. PASS/FAIL testing is only performed on the pairs required by the selected network specification.

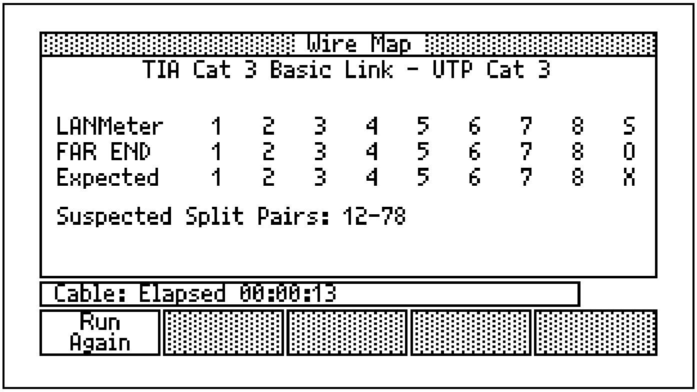
For the Wire Map test, you need to connect the near end of the test cable to the instrument **TO HUB/MAU** connector and attach the Wire Map adapter, or the 100 MHz Remote, to the Far End of the cable before running the test. The Wire Map adapter correctly terminates a UTP cable at 100 ohms. The 100 MHz Remote is required to test the shield continuity of a cable and to detect split pairs.

Note

> *Wire Map may not operate correctly with some IBM data connector-to-RJ adapters. For Wire Map to operate correctly, these adapters must not have impedance matching circuitry (baluns) and there must not be shield-to-lead connections. For the best results, the adapter must directly connect the Tx and Rx pairs without any other connections (use Fluke N6707).*

To run the **Wire Map** test, first highlight its softkey, configure the network specification and cable type for the cable you are about to test, and then press the **Wire Map** softkey again, or press ENTER RUN. You can also press MENU, select **Configure**, and press ENTER RUN to configure other parameters as needed. Refer to the “Configuring Cable Tests” section, for more information on configuring a Cable Test and to Table 2-3 for a listing of network specifications and their associated cable types.

The instrument displays Wire Map results at the end of the test. Use the arrow key functions to scroll through the results if the list is larger than can be displayed on the screen. Figure 2-8 shows Wire Map sample results.



```
                         Wire Map
         TIA Cat 3 Basic Link - UTP Cat 3

LANMeter    1   2   3   4   5   6   7   8   S
FAR END     1   2   3   4   5   6   7   8   O
Expected    1   2   3   4   5   6   7   8   X

Suspected Split Pairs: 12-78

Cable: Elapsed 00:00:13
```

Figure 2-8. Wire Map Sample Results

Interpreting the Wire Map Results

The following list describes the Wire Map results screen:

LANMeter Representation of LANMeter instrument wires. The **S** represents the cable shield.

FAR END Far End connection relative to the LANMeter instrument wires.

Expected Expected Far End connection. **X** indicates that the wire is not specified by the network specification.

The Expected row indicates the expected Far End connection as defined by the selected network specification. When Wire Map detects an open or a short, use Cable Scan to obtain a more detailed analysis.

If an **X** is displayed the wire is not specified by the network specification. If a split pair is suspected, **Suspected Split Pairs: <Pair>** is reported in the wire map results display. Split pairs will only be detected when the remote is used as the wire map adapter.

Use the following information while interpreting FAR-END measurement results:

N Where N is a wire, 1 through 8.

O Wire is open.

S Shield has continuity.

SS Wire is shorted to the shield.

SN Wire is shorted to another pin N (where N is 1 through 8).

? The LANMeter instrument could not determine the Far End connection.

Cable Identifier

Cable Identifier (I.D.) assists you in mapping cables to individual offices from the wiring closet. The instrument identifies unique Cable Identifier Remote Units and displays them in the order detected. Cable Identifier is for twisted pair cables only. Cable Identifier does not require configuration.

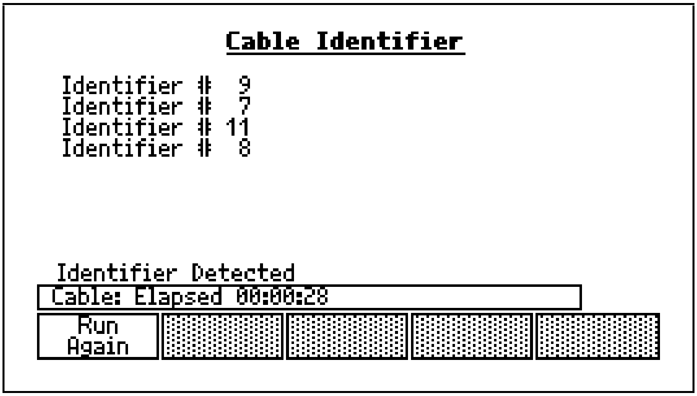
For the Cable I.D. test, you need to connect a Cable Identifier Remote Unit, 100 MHz Remote (#0), or Wire Map Adapter (#0) to the Far End of the cable that you wish to identify in the wiring closet and connect the cable near-end to the instrument **TO HUB/MAU** RJ-45 or DB-9 connector. You can also connect the optional RJ45-to-punchdown block adapter to the **TO HUB/MAU** connector (with an RJ-to-RJ cable) to quickly map cables to individual offices.

You can connect up to 12 Cable Identifier Remote Units (optional) that the instrument can uniquely identify from the wiring closet. The 100 MHz Remote and Wire Map adapter also functions as Cable Identifier Remote Unit 0 for this test.

Note

> *Cable Identifier may not operate correctly with some IBM data connector-to-RJ adapters. For Cable Identifier to operate correctly, these adapters must not have impedance matching circuitry (baluns) and there must not be shield-to-lead connections. For the best results, the adapter must directly connect the Tx and Rx pairs without any other connections (use Fluke N6707).*

The instrument displays Cable Identifier results as collected and displays a history of the last eight identified Cable Identifier Remote Units. Press EXIT STOP to stop the test. Figure 2-9 shows Cable Identifier sample results.



Cable Identifier

```
Identifier #  9
Identifier #  7
Identifier # 11
Identifier #  8
```

Identifier Detected

Cable: Elapsed 00:00:28

Figure 2-9. Cable Identifier Sample Results

Cable Autotest

Cable Autotest runs a series of tests to measure the electrical characteristics of a cable and compares the results with the network specification for the configured cable type. The tests run by Cable Autotest depend on the network specification and cable type you select.

Cable Autotest requires the 100 MHz Remote to test 100 ohm twisted pair cables. Cable Autotest can also be used to test 50 ohm coax or 150 ohm STP cable, but only a limited subset of the tests are executed. Refer to the following sections for more information.

After highlighting the **Cable Autotest** softkey, you should configure the network specification and cable type for the cable you are about to test. You can also press MENU, select **Configure**, and press ENTER RUN to configure other parameters as needed. Refer to the “Configuring Cable Tests” section, for more information on configuring a Cable Test and to Table 2-3 for a listing of network specifications and their associated cable types.

For all of the Autotest Results you can access the following functions or the Test Menu by pressing MENU:

Last Result — Restores the previous Autotest results for each measurement.

Configure — Lets you configure all of the available parameters, such as Specification, Cable, and NVP.

Print All — Prints a Cable Autotest Report. You will be prompted for a cable identification string for the report title.

This gives you a summary report of all the Cable Autotests run. For a report showing the specific test data, run the desired stand-alone test and execute a Print All.

View All — Lets you view the Cable Autotest Report. You will be prompted for a cable identification string for the report title.

The following is a portion of a sample Cable Autotest report:

```
                      Test Summary: Pass

Test Standard: TIA Cat 5 Channel          Cable Type: UTP Cat 5
  Standards Version: 1.0                  NVP: 69%
  Cable Temperature: 20C (68F)
LANMeter MAC ADDR: 00C017850025           Remote S/N: 1923

                      Wire Map Result
       LANMeter RJ-45 Pin:    1   2   3   4   5   6   7   8   S
         Remote RJ-45 Pin:    1   2   3   4   5   6   7   8   O
Expected Remote RJ-45 Pin:    1   2   3   4   5   6   7   8   X

Pair               1,2     3,6     4,5     7,8

Impedance(ohms)    108     106     108     104
Limit(ohms)        85-115  85-115  85-115  85-115
Result             Pass    Pass    Pass    Pass
```

100 Ohm Twisted Pair Cable Autotest

When testing 100 ohm twisted pair cable, Autotest can run the following tests as required by the specification:

❒ Wire Map (on all 4 pairs)
❒ Length
❒ Impedance
❒ Propagation Delay
❒ Attenuation
❒ NEXT (Near-End Crosstalk)
❒ ACR (Attenuation to Crosstalk ratio)

When testing 100 ohm twisted pair cable, the 100 MHz Remote must have been previously calibrated with the LANMeter instrument using the Calibrate Remote test.

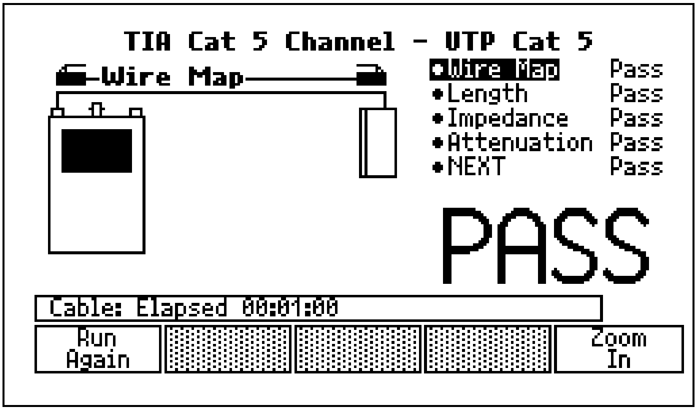
Note

The LANMeter instrument stores the 100 MHz Remote calibration information in non-volatile memory so that you only have to run the Calibrate Remote test once per 100 MHz Remote. The LANMeter instrument can store calibration information on up to five 100 MHz Remotes.

For re-calibration, run the Calibrate Remote test once per 100 MHz Remote every three months.

Cable Autotest Results

Cable Autotest results are displayed during the test; refer to Figure 2-10. Cable Autotest shows a Pass or Fail for each test run and then shows a Pass or Fail for compliance to the selected network specification.



TIA Cat 5 Channel - UTP Cat 5

•Wire Map	Pass
•Length	Pass
•Impedance	Pass
•Attenuation	Pass
•NEXT	Pass

PASS

Cable: Elapsed 00:01:00

Figure 2-10. Cable Autotest Sample Results

If the Wire Map Autotest fails the Cable Autotest stops the current test. You will need to correct the cable problem that caused the Wire Map failure and run the Cable Autotest again.

The selected network specification determines which tests must be run and passed by a cable to verify compliance. The LANMeter instrument reports the final results as specified by the TSB-67 specification; refer to Table 2-5.

Table 2-5. Autotest TSB-67 Reporting Requirements

Individual Test Results	**Overall Results**
All individual test results show PASS	PASS
One or more individual test results show PASS*. All others show PASS.	PASS
One or more individual test results show FAIL*. All others show PASS or PASS*.	FAIL
One or more individual test results show FAIL.	FAIL

Note

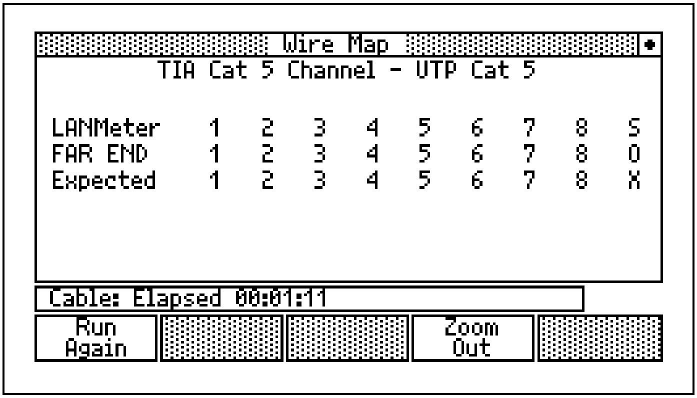
An asterisk (*) following a test result value indicates that the value is within the LANMeter instrument's accuracy specification.

You can select a result of interest and press **Zoom In** to view additional information on that result. You can then press **Zoom Out** to return to the Cable Autotest results screen.

Wire Map Autotest Results

For all measurements that require using the 100 MHz Remote, if the Wire Map Autotest fails the Cable Autotest stops testing. You will need to correct the cable problem that caused the Wire Map failure and run the Cable Autotest again.

Figure 2-11 shows Wire Map Autotest sample results.



TIA Cat 5 Channel - UTP Cat 5

LANMeter	1	2	3	4	5	6	7	8	S
FAR END	1	2	3	4	5	6	7	8	0
Expected	1	2	3	4	5	6	7	8	X

Cable: Elapsed 00:01:11

Figure 2-11. Wire Map Autotest Sample Results

The following list describes the Wire Map Autotest Results screen:

LANMeter Representation of LANMeter instrument wires. The **S** represents the cable shield.

FAR END Far End connection relative to LANMeter instrument Wires.

Expected Expected Far End connection. **X** indicates that the wire is not specified by the network specification.

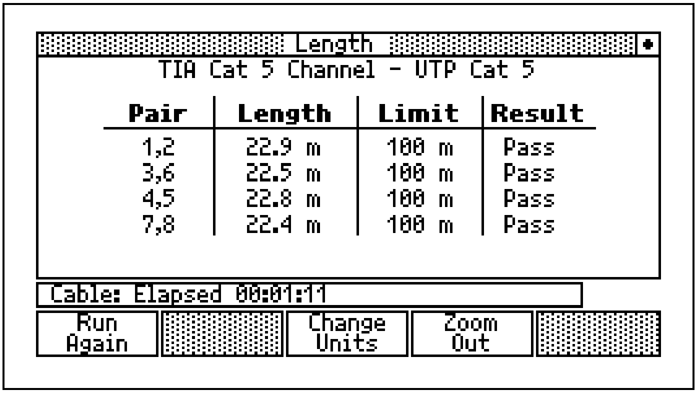
The Wire Map test checks for miswires on all eight conductors of twisted pair cabling plus the shield. PASS/FAIL testing is only performed on the pairs called out by the selected network specification. The Expected results indicates the expected Far End connection as defined by the selected network specification. If an **X** is displayed, the wire is not specified by the network specification.

The Autotest Summary results for Wire Map reports PASS/FAIL as a result of comparing the expected Far End connections with the measured result. Split pairs are detected by running NEXT at 10 MHz. If a split pair is suspected, **Suspected Split Pairs: <Pair>** is reported in the wire map results display.

For a more extensive interpretation of Wire Map results, refer to the stand-alone Wire Map test.

Length Autotest Results

Figure 2-12 shows Length Autotest sample results.



Length

TIA Cat 5 Channel - UTP Cat 5

Pair	Length	Limit	Result
1,2	22.9 m	100 m	Pass
3,6	22.5 m	100 m	Pass
4,5	22.8 m	100 m	Pass
7,8	22.4 m	100 m	Pass

Cable: Elapsed 00:01:11

Figure 2-12. Length Autotest Sample Results

The following list describes the Length Autotest Results screen:

Pair The measurement pair tested, defined by the selected network specification.

Length The measured length of the pair.

Limit The maximum acceptable length.

Result PASS/FAIL interpretation of the measured length compared to the network specification limits.

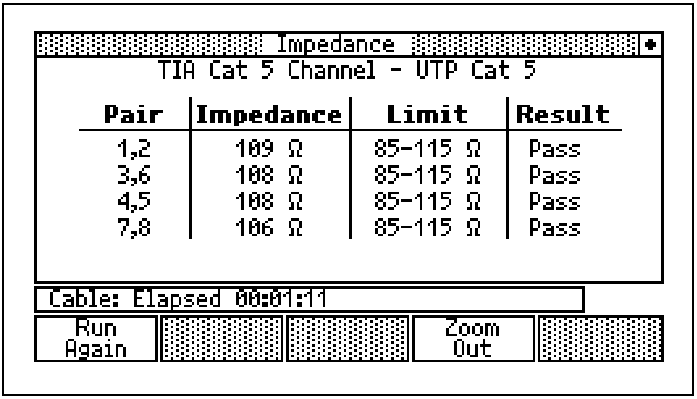
The number of wire pairs tested depends on the network specification selected. The length of a pair fails if the measured pair length is greater than the MAX link length +10 % NVP uncertainty. If any pair fails, the Autotest Summary results reports **FAIL**.

Note

A dash ("-") in the Length field implies that the LANMeter instrument could not measure the length of the cable. This is usually caused by the cable being terminated. Check the Far End to verify that the cable is connected to the 100 MHz Remote.

Impedance Autotest Results

Figure 2-13 shows Impedance Autotest sample results.



Impedance

TIA Cat 5 Channel - UTP Cat 5

Pair	Impedance	Limit	Result
1,2	109 Ω	85-115 Ω	Pass
3,6	108 Ω	85-115 Ω	Pass
4,5	108 Ω	85-115 Ω	Pass
7,8	106 Ω	85-115 Ω	Pass

Cable: Elapsed 00:01:11

Figure 2-13. Impedance Autotest Sample Results

The Impedance Autotest measures the characteristic impedance of the cable on each pair specified by the selected network standard. If the impedance of an individual pair fails, **WARN** is displayed in the Autotest summary results.

The following list describes the Impedance Autotest Results screen:

Pair — The measurement pair tested.

Impedance — The measured impedance.

Limit — The range of acceptable impedance.

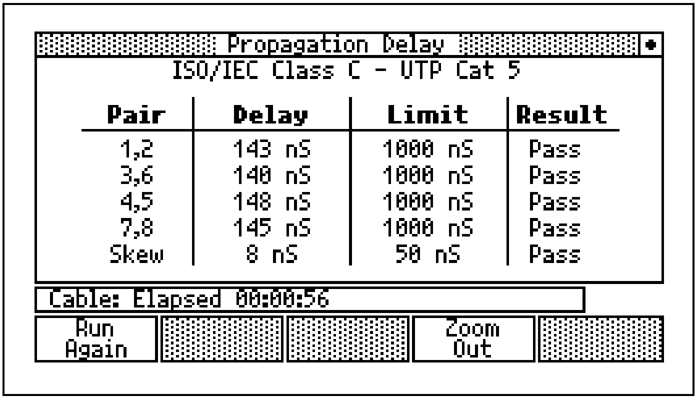
Result — PASS/FAIL interpretation of the measured impedance compared to the network specification limits.

Note

A dash "-" in the Impedance field implies that the LANMeter instrument could not measure the cable's impedance. To make impedance measurements, the cable must be longer than 5 meters. When a "-" is reported, the LANMeter instrument does not fail the Impedance test.

Propagation Delay Autotest Results

Figure 2-14 shows Propagation Delay Autotest sample results.



Propagation Delay

ISO/IEC Class C - UTP Cat 5

Pair	Delay	Limit	Result
1,2	143 nS	1000 nS	Pass
3,6	140 nS	1000 nS	Pass
4,5	148 nS	1000 nS	Pass
7,8	145 nS	1000 nS	Pass
Skew	8 nS	50 nS	Pass

Cable: Elapsed 00:00:56

Figure 2-14. Propagation Delay Autotest Sample Results

Propagation Delay Autotest measures the delay for one length of the cable and compares it to the selected network standard. Skew is the difference in propagation delay between pairs. The largest skew is reported.

The following list describes the Propagation Delay Autotest Results screen:

Pair — The measurement pair tested, defined by the selected network specification. The skew test result is also indicated in this column.

Delay — The measured propagation delay of the pair or the largest skew between any of the pairs.

Limit — The maximum acceptable delay.

Result — PASS/FAIL interpretation of the measured delay compared to the network specification limits.

The number of wire pairs tested depends on the network specification selected. If any pair fails or if the skew measurement fails, the Autotest Summary results reports **FAIL**.

Note

> *A dash ("-") in the Length field implies that the LANMeter instrument could not measure the length of the cable. This is usually caused by the cable being terminated. Check the Far End to verify that the cable is connected to the 100 MHz Remote.*

Propagation delay is only measured for certain cable specifications (100BASE-T4, 100VG-AnyLAN, and the ISO/IEC specifications). Refer to Table 2-3 for a complete list.

Attenuation Autotest Results

Refer to the stand-alone Attenuation test section for results information.

NEXT Autotest Results

Refer to the stand-alone NEXT test section for results information.

ACR Autotest Results

The ACR test calculates the Attenuation to Crosstalk Ratio (ACR) for each combination of cable pairs. ACR is expressed as the difference between the measured NEXT and attenuation values (in dB). The larger the ACR value the better it prevents the signal from being lost in the crosstalk noise.

ACR results are displayed as they are determined per individual sample run. The final results are then displayed as required; refer to Table 2-6.

Table 2-6. ACR Reporting Requirements

	If Pass	**If Marginal (* on test result)**	**If Fail**
Reported Results	Highest ACR, the frequency, and the test limit at that frequency.	Worst case ACR margin, the frequency, and the test limit at that frequency.	Worst case ACR margin, the frequency, and the test limit at that frequency.

Coax and 150 Ohm STP Cable Autotest

The 100 MHz Remote is not required for testing coax or 150 Ohm STP cables.

When testing coax cable and 150 Ohm STP cable, Autotest runs the following tests:

- ❒ Length
- ❒ Impedance

Note

> *To run an impedance test, the cable length must be greater than 5 meters. If the cable is too short to make a valid measurement, Cable Autotest will not fail the test.*

For a more comprehensive test on Coax and STP cable, run the Cable Scan test.

NEXT

NEXT (Near-End Crosstalk) is a measure of signal coupling from one pair to another pair. The measurement results are derived from stepped frequency voltage measurements. The configured specification dictates the pairs tested, the frequency step size, the measurement frequency range, and the acceptable limits.

NEXT is measured by applying a signal on one pair and measuring the crosstalk of the signal onto the other pairs one at a time as defined by the network specification. Since the proximity of the pairs to each other impacts the crosstalk, each pair combination (with one pair transmitting) needs to be tested. NEXT changes with frequency and is measured across a frequency range at specific frequency steps.

For example, the following shows the transmit and measurement pair combinations for a 4-pair cable:

Transmit on Pair	**1, 2**
Measure on Pair	**3, 6**
	4, 5
	7, 8
Transmit on Pair	**3, 6**
Measure on Pair	**4, 5**
	7, 8
Transmit on Pair	**4, 5**
Measure on Pair	**7, 8**
Across Frequency Range:	**1 MHz to 100 MHz**

Note

You can change the step size of the NEXT measurement. The two modes available are TIA Compliant mode, which meets the requirements for TSB-67 Level 1 and allows for 150/250 KHz steps; or Fast mode, which allows for 500 KHz steps. Refer to the Cable Configuration menu for changing the step size.

While the test is in progress, the LANMeter instrument reports NEXT measurements as the data at each frequency step is derived. NEXT measurements are made at the remote end of the LANMeter instrument.

To run the NEXT test, attach the LANMeter instrument to one end of the cable pair to be tested and attach the 100 MHz Remote to the other end of the cable pair. The LANMeter instrument measures NEXT at the remote end of the cable. **To test a cable pair for full compliance to the selected specification, NEXT must be measured from both ends of the cable.** To do this, a second measurement should be made after swapping the position of the LANMeter instrument and the 100 MHz Remote.

After highlighting the **NEXT** softkey, you can configure the network specification and cable type for the cable you are about to test. You can also press MENU, select **Configure**, and press ENTER RUN to configure other parameters as needed. Refer to the "Configuring Cable Tests" section for more information on configuring a Cable Test and to Table 2-3 for a listing of network specifications and their associated cable types.

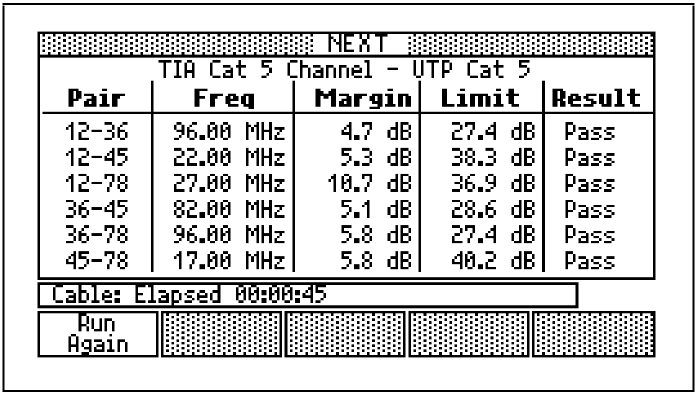
NEXT Results

The LANMeter instrument shows the amount of NEXT Margin available in the NEXT test results. This allows you to see how close all pairs are to the NEXT limit. NEXT results are displayed as they are determined per individual sample run. The final results are then displayed as required by the TSB-67 specification.

NEXT represents the difference between the test transmitted signal and the received crosstalk signal in another cable pair (represented in decibels (dB)). Since this is the difference, the larger the NEXT value, the better the results. (For example, a NEXT of 40 dB is much better than 20 dB.)

NEXT results for your network typically will not change after the installation, except where moves or changes are made.

Figure 2-15 shows NEXT sample results.



NEXT

TIA Cat 5 Channel - UTP Cat 5

Pair	Freq	Margin	Limit	Result
12-36	96.00 MHz	4.7 dB	27.4 dB	Pass
12-45	22.00 MHz	5.3 dB	38.3 dB	Pass
12-78	27.00 MHz	10.7 dB	36.9 dB	Pass
36-45	82.00 MHz	5.1 dB	28.6 dB	Pass
36-78	96.00 MHz	5.8 dB	27.4 dB	Pass
45-78	17.00 MHz	5.8 dB	40.2 dB	Pass

Cable: Elapsed 00:00:45

Figure 2-15. NEXT Sample Results

While the test is in progress, the LANMeter reports the NEXT margin as each frequency is tested. The NEXT margin is the difference between measured NEXT and the test limit. The results show the worst case frequency, NEXT margin, and the test limit at that frequency.

To view the measured NEXT values, run the stand alone NEXT measurement not the Cable Autotest which also runs NEXT. Use **Print All** or **View All** to view measurement results for every frequency tested. The test limit and NEXT values are reported for each pair combination.

The following list describes the NEXT results screen:

Pair
The tested pair combination defined by the selected network specification.

Freq
The NEXT Frequency of the event.

Margin
The difference between the measured NEXT and the test limit of the specification limit.

Limit
The test limit of the specification.

Result
PASS/FAIL/MARGINAL (*) test result interpretation of the NEXT compared to the acceptable specification range. An asterisk (*) following the test result indicates that the value is within the LANMeter instrument’s margin of accuracy.

You can access the following functions of the Test Menu by pressing MENU:

Last Result
Restores last measurement results.

Configure
Allows you to configure the cable.

Print All
Prints NEXT measurement results at each frequency for each pair.

This report shows the specific test data for the NEXT test. For summary information, run the Cable Autotest and execute a Print All from there.

View All
Displays the Frequency (in MHz) and measured NEXT on each pair.

Attenuation

Attenuation measures the loss of signal strength over the length of the cable.

The 100 MHz Remote applies a test signal to a specific cable pair and measures the attenuation across the link.

Attenuation changes with frequency and therefore is measured across a frequency range at specific frequency steps.

The configured specification dictates the pairs tested, the frequency step size, the measured frequency range, and the acceptable limits. While the test is in progress, the LANMeter instrument reports attenuation measurements as the data at each frequency step is derived.

To run the Attenuation test, attach the LANMeter instrument to one end of the cable pair to be tested and attach the 100 MHz Remote to the other end. The Remote must be calibrated to run the Attenuation test.

Note

> *The LANMeter instrument stores the 100 MHz Remote calibration information in non-volatile memory so that you only have to run the Calibrate Remote test once per 100 MHz Remote. The LANMeter instrument can store calibration information on up to five 100 MHz Remotes.*
>
> *For re-calibration, run the Calibrate Remote test once per 100 MHz Remote every three months.*

After highlighting the **Atten** softkey, you can configure the network specification and cable type for the cable you are about to test. You can also press MENU, select **Configure**, and press ENTER RUN to configure other parameters as needed. Refer to the "Configuring Cable Tests" section for more information on configuring a Cable Test and to Table 2-3 for a listing of network specifications and their associated cable types.

Attenuation Results

Attenuation results are displayed as they are determined. The TSB-67 specification calls out that reporting requirements of Table 2-7 be displayed by the test tool. Refer to your selected network specification for more detailed information on interpreting Attenuation results.

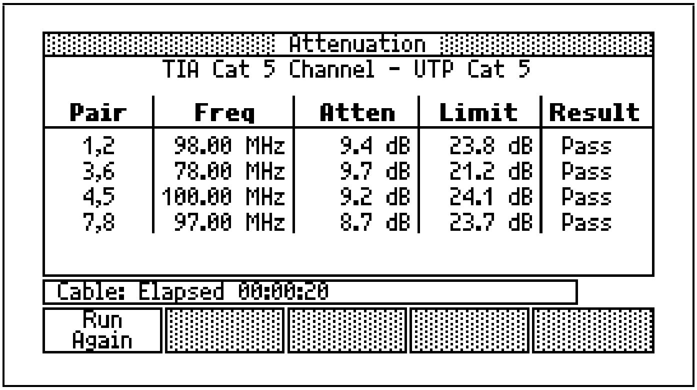
Table 2-7. Attenuation TSB-67 Reporting Requirements

	If Pass	**If Marginal** **(* on test result)**	**If Fail**
Reported Results	Highest measured attenuation, the frequency, and the test limit at that frequency.	Measured attenuation where marginal, the frequency, and the test limit at that frequency.	Measured attenuation at failure, the frequency, and the test limit at that frequency.

The Attenuation test is made across the frequency range and at the step size that is called out by the selected network specification. The lower the Attenuation value, represented in decibels (dB), the better the results. For example, an Attenuation of 10 dB is much better than 30 dB.

Attenuation results for your network typically will not change after the installation, except where moves or changes are made.

Figure 2-16 shows Attenuation sample results.



Attenuation

TIA Cat 5 Channel - UTP Cat 5

Pair	Freq	Atten	Limit	Result
1,2	98.00 MHz	9.4 dB	23.8 dB	Pass
3,6	78.00 MHz	9.7 dB	21.2 dB	Pass
4,5	100.00 MHz	9.2 dB	24.1 dB	Pass
7,8	97.00 MHz	8.7 dB	23.7 dB	Pass

Cable: Elapsed 00:00:20

Figure 2-16. Attenuation Sample Results

The following list describes the Attenuation results screen:

Pair
The tested pair. Defined by the selected network specification.

Freq
The Attenuation Frequency of the event. Refer to Table 2-7 for PASS/FAIL/MARGINAL (*****) interpretation.

Atten
The measured Attenuation. Refer to Table 2-7 for PASS/FAIL/MARGINAL (*****) interpretation.

Limit
The test limit of the specification.

Result
PASS/FAIL/MARGINAL (*****) test result interpretation of the measured Attenuation compared to the acceptable specification range.

Attenuation is a measure of signal loss along the cabling link. Attenuation changes with the frequency of the signal and is measured over the frequency range specified by the selected specification.

The configured specification dictates the pairs tested, the frequency step size, and the measurement frequency range. While the test is in process, the LANMeter instrument reports Attenuation measurements as the data at each frequency step is derived.

Note

An asterisk (*****) *following a test result value indicates that the value is within the LANMeter instrument's accuracy specification. All Cable Tests, except Wire Map, may produce results with an asterisk as required by the selected network specification.*

You can access the following functions or the Test Menu by pressing MENU:

Last Result
Restores previous measurement results.

Configure
Allows you to configure the cable.

Print All
Prints Attenuation measurement results at each frequency for each pair.

This report shows the specific test data for the Attenuation test. For summary information, run the Cable Autotest and execute a Print All from there.

View All	Displays the Frequency (in MHz) and measured Attenuation on each pair.

DC Continuity (Fluke 686, 685, 683, and 682 Only)

Use DC Continuity to test coax cables connected to the LANMeter instrument's BNC connector. You can test for missing and/or bad terminators.

The test attempts to draw some conclusions about the results. Table 2-8 shows some conclusion examples.

Table 2-8. DC Continuity BNC Conclusion Examples

Result	Conclusion
50Ω	Single 50-ohm terminator detected
25Ω	Two 50-ohm terminators detected
75Ω	Warning: Suspect a single 75-ohm terminator
93Ω	Warning: Suspect a single 93-ohm terminator
29 to 46Ω	Warning: Suspect bad or incorrect terminators. Test each terminator individually.
> 100Ω	Warning: Suspected missing terminator

Find NVP

Find NVP calculates NVP (Nominal Velocity of Propagation) for a cable of known length and, for twisted pair cabling, reports if the TX and RX leads differ in length by more than 10%, and optionally stores the value in any of the available cable types.

You can configure the following parameters for Find NVP:

❒ Cable Type
❒ Cable Length
❒ Units in Feet or Meters

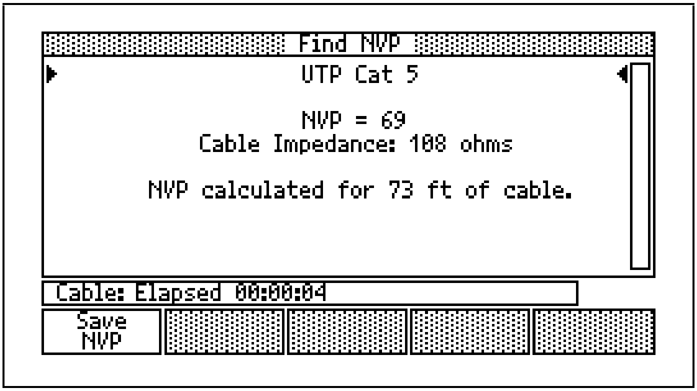
Note

> *Restoring defaults in any configuration menu restores all Cable test defaults, including NVP values.*

When you enter the actual cable length, the affect of the twist rate is included in the calculated NVP. Since the cable manufacturers have different twist rates for each cable, the measured length of the other calibrated pair varies around the nominal value.

The instrument displays Find NVP results at the end of the test. Results include whether a cable is too short, terminated, or too long (at the remote end) and the characteristic impedance and NVP values. Figure 2-17 shows Find NVP sample results.

Select **Save NVP** to store the results along with the Cable Types.



Find NVP

UTP Cat 5

NVP = 69
Cable Impedance: 108 ohms

NVP calculated for 73 ft of cable.

Cable: Elapsed 00:00:04

Figure 2-17. Find NVP Sample Results

Calibrate Remote

You must calibrate the 100 MHz Remote prior to using it in the Cable Autotest, Attenuation, or NEXT tests. If you do not, the LANMeter instrument will prompt you with a message telling you to calibrate the 100 MHz Remote. Use the following procedure to calibrate the 100 MHz Remote:

1. Attach the 100 MHz Remote to the Enterprise LANMeter's RJ-45 connector using the ScTP Cat 5 Patch Cable supplied with your 100 MHz Remote.
2. Press the top-level **Cable Tests** softkey.
3. Press MORE and then **Calibrate Remote**.

The LANMeter instrument stores the 100 MHz Remote calibration information in non-volatile memory so that you only have to run the Calibrate Remote test once per 100 MHz Remote. For re-calibration, run the Calibrate Remote test once per 100 MHz Remote every three months.

The LANMeter instrument can store calibration information on up to five 100 MHz Remotes. If you calibrate a sixth remote, remote number one is deleted from the LANMeter instrument's memory and replaced by the calibration information for the sixth remote.

Chapter 3
Monitoring the Network

Introduction

The Enterprise LANMeter monitors the general health of your network by measuring and reporting on key network parameters. Your Enterprise LANMeter has an Instant-on feature that starts to monitor the network as soon as the instrument is powered on and connected to the network. The Utilization, Frame Error, Collisions, and Link Active LEDs are active for the Instant-on feature.

Select the top-level **Network Monitor** softkey to access Network Monitor tests.

The Fluke 686 and 683 LANMeter instruments provide the additional capability for Network Monitor tests of running on Fast Ethernet (100 Mbps) networks.

The MAC Matrix, Protocol Mix, and Top MAC (Top Senders, Top Receivers, and Top Broadcasts) tests are the same for both the Ethernet and Token Ring interface modes.

It is important to properly connect the instrument to your network. Refer to the “Attaching Cables” section of the *Getting Starte* manual for detailed information on attaching cables.

Refer to Chapter 4 “Testing Network Components,” for information on the Traffic Generator test. All other Network Monitor tests are covered in this chapter.

Configuring Network Monitor Tests

All Network Monitor tests are configured in a similar manner. Use the following procedure to configure all Network Monitor tests:

1. Press the top-level **Network Monitor** softkey.
2. Highlight the desired test for configuration.

   The exact steps required to highlight a test depend on which test you want to configure. The first test is automatically highlighted. Otherwise, you press the test softkey once or press MORE, then press the test softkey once (for the second row of tests).
3. Press MENU. Press △ or ▽ to select the **Configure** option (if it is not already selected).
4. Press ENTER RUN and configure the test as desired.

   Refer to the individual test sections in this chapter for specific configuration parameter options.

   To undo any configuration changes you made, press MENU, select **Cancel Changes** in the Configuration Menu, and then press ENTER RUN.
5. Press EXIT STOP to save your configuration to non-volatile memory and exit the Configuration screen.

Running Network Monitor Tests

All Network Monitor tests are run in a similar manner. Use the following procedure to run all Network Monitor tests:

1. Verify that the correct connector type is selected under **Setup/Utils**, Network Configuration.
2. Press the top-level **Network Monitor** softkey.
3. Highlight the desired test to run.

   The exact steps required to highlight a test depend on which test you want to run. The first test is automatically highlighted. Otherwise, you either press the test softkey once or press MORE, then press the test softkey once (for the second row of tests).
4. Configure the instrument for the desired network configuration. Refer to the “Configuring Network Monitor Tests” section in this chapter, for more information on configuring Network Monitor tests.
5. Connect the instrument as described in the “Attaching Cables” section of the *Getting Started* manual.
6. Run the test by pressing the test softkey or by pressing ENTER RUN.

   For Fluke 686 and 683 instruments configured for 100 Mbps only, the test will stop if the link pulse is lost (for example, if you disconnect the instrument from the network).
7. Observe the test results. Refer to the individual test sections in this chapter for information on available results options.
8. Press EXIT STOP to end the test.

Ethernet Tests

The LANMeter instrument provides the following Network Monitor Ethernet tests:

- Network Statistics and Error Statistics tests form one group.
- MAC Matrix test
- Protocol Mix test
- Top MAC, which is composed of Top Senders, Top Receivers, and Top Broadcasts tests, form the second group.

All tests within a group run simultaneously. Therefore, the Network Statistics and Error Statistics tests run simultaneously, as do the Top MAC (Top Senders, Top Receivers, and Top Broadcasts) tests. The MAC Matrix and Protocol Mix tests run independently.

Select the **Top MAC** softkey to access the Top Senders, Top Receivers, and Top Broadcasts test group, or select either the **Network Stats** or **Error Stats** softkey to access the Network Statistics and Error Statistics test group. Figure 3-1 shows the Ethernet Network Monitor Softkeys.

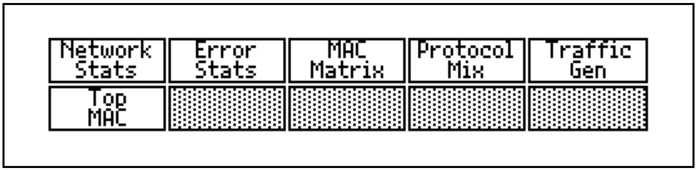


Figure 3-1. Ethernet Network Monitor Softkeys

After selecting one group of tests, you can view the results of a different test within the group by pressing its softkey. The group of tests must be running for you to switch between the different test results. For example, press **Network Stats** from the Network Monitor softkeys to access the Network Statistics and Error Statistics group of tests. The instrument displays Network Statistics information. Then press **Error Stats** without pressing EXIT STOP, to change the display to show the Error Statistics results on the same data sample.

Refer to Chapter 4 “Testing Network Components,” for information on the Traffic Generator test.

Network Statistics

Network Statistics monitors the general health of your network by calculating statistics for key network parameters. Network Statistics is the test where most troubleshooting scenarios begin. The instrument calculates all statistics at the same time for each 1-second sample period. Running Network Statistics simultaneously runs the Error Statistics test. To display the results of the Error Statistics test on the same data sample, either press **Error Stats** while the test is running, or press **Error Stats** after the test is stopped but prior to leaving the measurement.

Configuration Parameters

You can configure the following parameters for Network Statistics. The default parameter is underlined.

❒ Data Logging as <u>Off</u> or On. When you configure Data Logging as On, you also have the option of configuring one of the following Logging Periods. The first time interval is the test duration and the second interval (in parenthesis) is the sample period.

  ❒ 24 minutes (1 second)
  ❒ 2 hours (5 seconds)
  ❒ 12 hours (30 seconds)
  ❒ 24 hours (1 minute)
  ❒ 5 days (5 minutes)
  ❒ 5 days (1 minute)
  ❒ 7 days (1 minute)

  When you select the 7 day (1 minute) and 5 day (1 minute) logging periods, the LANMeter instrument actually saves seven one-day logs and five one-day logs, respectively. There is a short delay (about 4 minutes) in data collection between each day’s log.

  Data Logging captures Network Statistics and Error Statistics simultaneously.

Caution

Your LANMeter instrument notifies you if the oldest Data Log file will be lost when you run a new Data Log. Also, running the 7 day (1 minute) and 5 day (1 minute) Data Logs can cause currently saved Data Logs to be lost. This is because the 7 day (1 minute) and 5 day (1 minute) Data Logs actually save seven one-day logs and five one-day logs, respectively.

Your LANMeter instrument reminds you of the possibility of losing a Data Log when you start data logging. You then have the opportunity to cancel data logging, export any important Data Log files, or restart the measurement.

The LANMeter instrument displays **`DATA LOGGING Active!`** on the status line to provide a reminder that Data Logging is enabled and active.

Use the Data Logging feature to have the instrument run Network Stats for a period of time and then stop the test and log the results. These results can be analyzed at a later time. Refer to the "Configuring Network Monitor Tests" section for more information on configuration, and refer to the "Data Logging" section later in this chapter for more information on Data Logging.

Results

The instrument displays Network Statistics results after calculating the statistics for the first 1-second sample period and updates these results for each successive sample period.

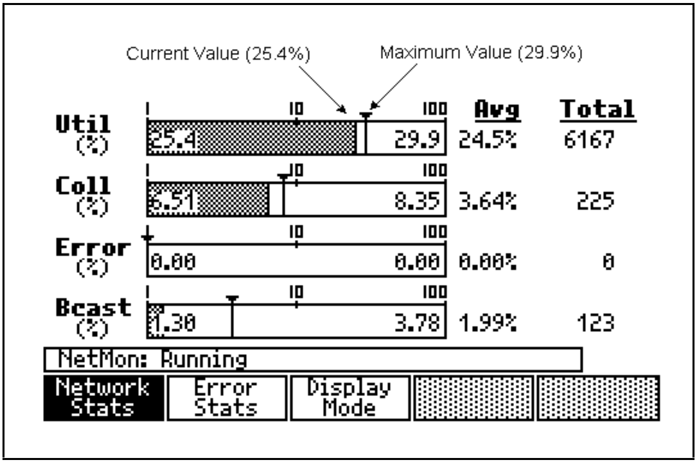
Network Statistics shows Utilization, Collisions, Errors, and Broadcasts as numerical values and as bar graphs. The bar graphs show current and maximum values. The current value is the shaded portion of the bar with its numerical value inside the bar on the left-hand side. The maximum value is indicated on the graph with a small triangle above the bar with its numerical value inside the bar on the right-hand side. The instrument also shows the average and total numerical values in a tabular format. Figure 3-2 shows a sample of the Ethernet Network Statistics results.

Press **Display Mode** and then select **Percents** or **Counts** as the display format. When percentages are chosen, the following are the results:

Utilization:	percentage of total network bandwidth used
Collisions:	percentage of frames that collided (sum of all collision types)
Errors:	percentage of frames that had errors (sum of all error types)
Broadcasts:	percentage of frames that are broadcasts

Note

Collision and error types are described in the next section on the Error Statistics test.



Current Value (25.4%)

Maximum Value (29.9%)

			Avg	Total
Util (%)	25.4	29.9	24.5%	6167
Coll (%)	6.51	8.35	3.64%	225
Error (%)	0.00	0.00	0.00%	0
Bcast (%)	1.30	3.78	1.99%	123

NetMon: Running

Figure 3-2. Ethernet Network Statistics Sample Results

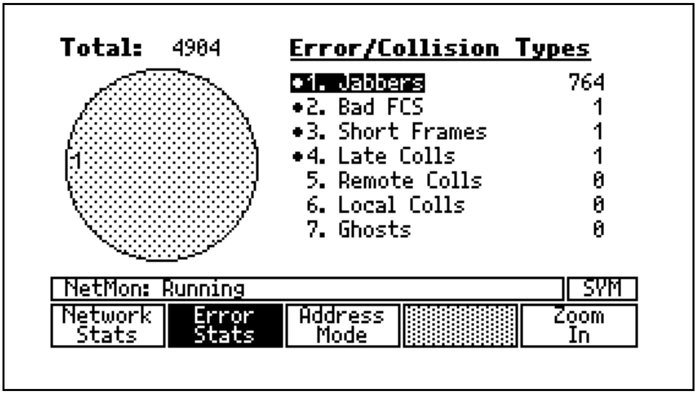
Error Statistics

Error Statistics monitors the types and sources of network errors and collisions. Running Error Statistics automatically runs the Network Statistics test. To display the results of the Network Statistics tests on the same data sample, simply press its softkey while the test is running.

Results

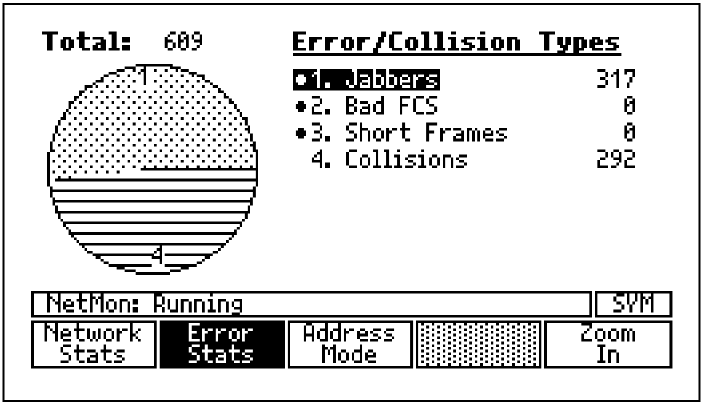
The instrument displays Error Statistics results after calculating the statistics for the first sample period and updates these results for each successive 1-second sample period. Error Statistics displays results in numerical format and in a pie chart that shows error distributions by error type. Remote Collisions, Local Collisions, and Ghosts are only reported at 10 Mbps.

For the source addresses of the specific Error Type, highlight the error type marked with the Zoom icon (•) and press the **Zoom In** softkey. Figure 3-3 shows 10 Mbps Error Statistics sample results and Figure 3-4 shows 100 Mbps Error Statistics sample results.



```
Total:   4904        Error/Collision Types
                     •1. Jabbers              764
                     •2. Bad FCS                1
                     •3. Short Frames           1
                     •4. Late Colls             1
                      5. Remote Colls           0
                      6. Local Colls            0
                      7. Ghosts                 0
NetMon: Running
```

Figure 3-3. Ethernet Error Statistics (10M) Sample Results



```
Total:  609        Error/Collision Types

                   •1. Jabbers             317
                   •2. Bad FCS               0
                   •3. Short Frames          0
                    4. Collisions          292

NetMon: Running                            SYM
```

Figure 3-4. Ethernet Error Statistics (100M) Sample Results

Description of Error Types

The instrument defines the following error and collision types for Error Statistics.

Collisions at 100 Mbps

At 100 Mbps, the LANMeter instrument counts the total number of short collisions, late collisions, and local collisions and reports them as Collisions.

Local Collision

A local collision occurs when two or more nodes transmit at the same time on the segment monitored by the instrument. Figure 3-5 shows a local collision. If two nodes collide on the other side of a repeater, the instrument counts this as a Remote Collision. Local Collisions and Remote Collisions are only reported at 10 Mbps.

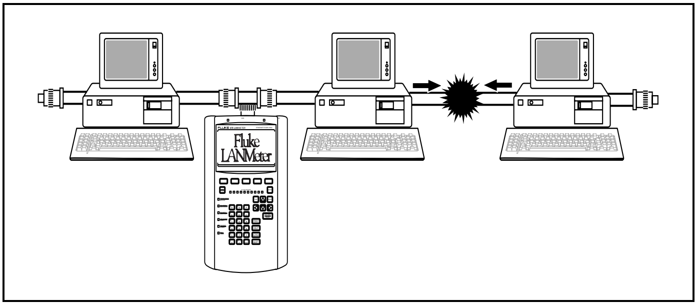


Figure 3-5. Local Collision

On a 10BASE-T network, the instrument must be transmitting in order to observe local collisions; otherwise, it only monitors remote collisions. Excessive collisions are most often caused by a physical media problem such as missing or incorrect terminators, impedance discontinuities (such as, defective connectors, cable stubs, crushed cables), or defective network interface cards.

Remote Collision

A remote collision is one that occurs on the other side of a repeater from the instrument. Remote Collisions are only reported at 10 Mbps. Figure 3-6 shows a remote collision. A 10BASE-T hub is essentially a multi-port repeater with a segment dedicated to each station. All collisions (unless the LANMeter instrument is transmitting) observed by the instrument are by definition remote collisions.

You may find that the instrument's remote collision count may not agree with some protocol analyzers. This is because most protocol analyzers are blind to collisions that occur in a frame's preamble. The LANMeter instrument is not blind to preamble collisions and sees the same collisions as 10BASE-T hubs.

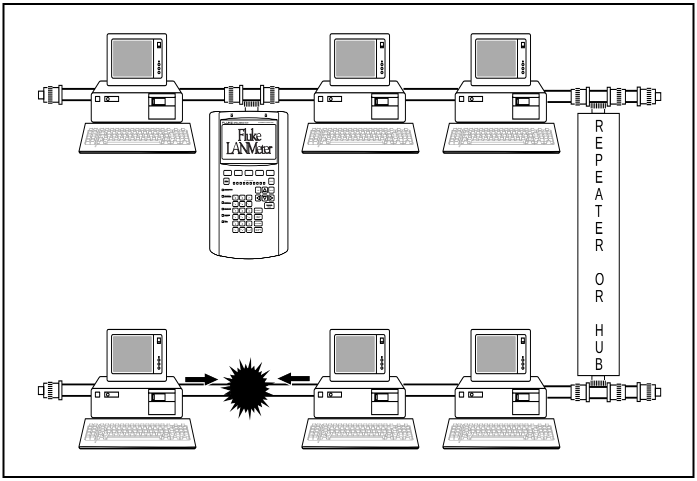


Figure 3-6. Remote Collision

Late Collision

A late collision is one that occurs after the first 64 bytes in a frame. The instrument generally can only observe a late collision on a coaxial segment. Late Collisions are reported at both 10 Mbps and 100 Mbps. To see a late collision on 10BASE-T networks, the instrument must be transmitting at the time. Late collisions in 10BASE-T networks, or late collisions that occur on the other side of a repeater, appear as a bad FCS frame when monitored by the instrument. Figure 3-7 shows late collisions.

Causes of Late Collisions are a faulty NIC card or a network that is physically too long. A network is physically too long if the end-to-end signal propagation time is greater than the time it takes to transmit the minimum legal sized frame (about 57.6 microseconds).

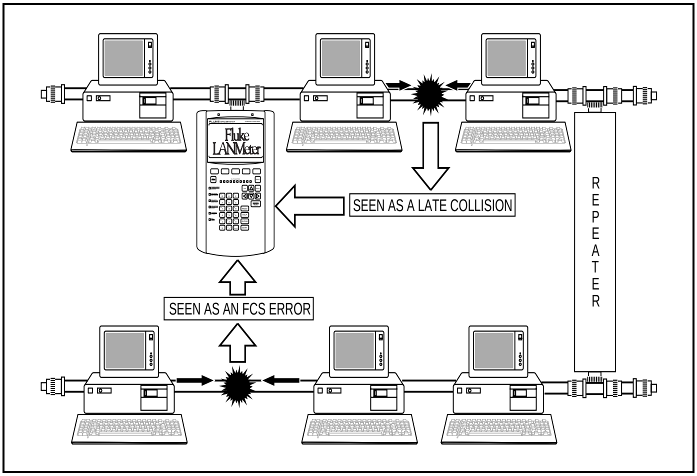


Figure 3-7. Late Collisions

Short Frame

A short frame is a frame that is less than the minimum legal size (less than 64 bytes) which has a good frame check sequence. In general you should not see short frames. The most likely cause of a short frame is a faulty NIC card, or its driver. Some protocol analyzers and network monitors call these frames Runts. Short Frames are reported at both 10 Mbps and 100 Mbps.

Jabber

A jabber is a frame that is greater than the maximum legal size (1518 bytes) which has a good or bad frame check sequence. In general you should not see jabbers. The most likely causes of jabbers are faulty NIC card (or its driver), cabling, or grounding problems. Jabbers are reported at both 10 Mbps and 100 Mbps.

Frame Check Sequence (FCS) Error

An FCS error is a legal sized frame with a bad frame check sequence. An FCS error can be caused by a faulty NIC or driver, cabling, hub or induced noise. If a late collision occurs that is also remote, the LANMeter instrument will indicate an FCS error. Bad FCSs are reported at both 10 Mbps and 100 Mbps.

Ghosts

Ghosts are energy on the cable that appears to be a frame, but does not have a valid beginning of frame pattern (that is, the start delimiter does not equal 10101011). This ghost frame must be at least 72 or more bytes long, otherwise it is classified as a remote collision. Because of the nature of ghost frames, the position of the instrument on the network can greatly influence test results. Ghosts are only reported at 10 Mbps.

Causes for Ghosts

Ground loops and other wiring problems cause some repeaters to believe that a frame is being received. Since the repeater is only reacting to an AC voltage riding on the cable, there is not a valid frame to pass along the network. The repeater, however, transmits this energy along the network. This may be a jam pattern or a very long preamble. Ghost events on a LAN consume bandwidth and can slow down a network. The LANMeter instruments are currently the only products that recognize these events.

Ghosts versus Noise

Ghosts are the result of network elements reacting to noise. The LANMeter instrument’s ability to measure ghosts is not the same thing as a noise measurement. There are many forms of noise that can exist on a network segment that do not hamper network throughput or functionality. Some types of noise fool nodes on a network segment into thinking they are receiving a frame. Each node can react differently. There are no standards defining how, or when, a node should react to a noisy LAN segment. The LANMeter instrument acts like a typical node on the network. Like any other node, some forms of noise on the network cause the instrument to believe the noise is data. Depending on the length of the event, the instrument either interprets this data as a ghost or a remote collision. The ghost measurements are most useful when a repeater transmits ghosts as a result of receiving noise on another port.

Runts

Many protocol analyzers and network monitors count runts. Unfortunately the term “runt” is not standardized and means different things in different products. For this reason the LANMeter instrument does not classify any network event as a runt. Instead the instrument classifies those frames typically called runts, as either Remote Collisions or Short Frames.

Unclassified

There are network events which will prevent the LANMeter instrument from being able to determine what kind of error condition occurred. These will be reported as Unclassified.

Unknown Type

Under very high error rate conditions, the instrument may register a count for unknown types. These are errors that occurred but the instrument could not determine the type of error due to the high error rate condition.

Ethernet Network Health Overview and Guidelines

The parameters that are acceptable for a healthy network are determined by many variables. These include worst case response time, the number of transmitting stations, the types of applications in use, the cabling systems, and the types of spanning devices (such as hubs, repeaters, bridges, and routers). No two networks, even within the same organization, are the same. For many networks, server and workstation throughput are more significant factors than the capacity of the physical media. For these reasons it is difficult to generalize as to what makes a healthy network. There are no magic numbers for good or bad network parameters. For example, the Utilization percent and the number and type of collisions, can not in itself indicate whether network performance is good or bad.

Keeping in mind the above considerations, the following list provides some guidelines for interpreting the health of an Ethernet network.

Recommendations for network health:

1. Utilization should average less than 40%. If you have extended peaks of greater than 70% you may want to investigate the causes and consider configuration changes to lower the average utilization. Generally, the greater the number of stations, the lower the acceptable utilization threshold.

2. The collision rate should be less than 5%. Be wary of large bursts of collisions (greater than 20%); this can be an indicator of a severe cabling or component problem.

3. Bad FCS errors, late collisions, jabbers, and short frames should be rare occurrences and should be investigated when they become repetitive. These error conditions are typically a result of some kind of problem with the cabling and/or network configuration. Refer to the previous "Description of Error Types" for information on which errors are reported at 10 Mbps and 100 Mbps.

4. Excessive broadcast traffic adversely affects all stations on the network. Investigate nodes that are transmitting many broadcasts and consider reconfiguring them. The average broadcast frame rate should be less than 5%.

Token Ring Tests

The instrument provides two groups of Token Ring Network Monitor tests and the Protocol Mix and Token Rotation tests. All tests within a group run simultaneously. The Network Statistics, Error Statistics, and Ring Stations tests run simultaneously, as do the Top MAC (Top Senders, Top Receivers, and Top Broadcasts) tests. The Protocol Mix, Token Rotation, and MAC Matrix tests run independently. Select the **Top MAC** softkey to access the Top Senders, Top Receivers, and Top Broadcasts test group, or select either the **Network Stats**, **Error Stats**, or **Ring Stations** softkey to access the Network Statistics, Error Statistics and Ring Stations test group. Figure 3-8 shows the Token Ring Network Monitor Softkeys.

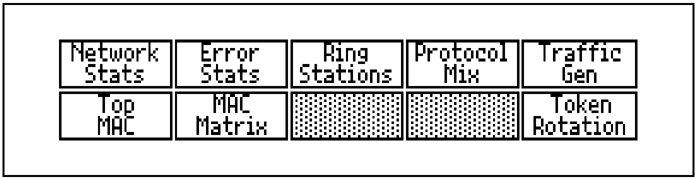


Figure 3-8. Token Ring Network Monitor Softkeys

After selecting one group of tests, you can view the results of a different test within the group by pressing its softkey. The group of tests must be running to switch between the different results. For example, press **Network Stats** from the Network Monitor softkeys to access the Network Statistics, Error Statistics, and Ring Stations group of tests. The instrument displays Network Statistics information. Then press **Error Stats** (or **Ring Stations**), without pressing EXIT STOP, to change the display to show the Error Statistics results on the same data sample.

Refer to Chapter 4 “Testing Network Components,” for information on the Traffic Generator test.

Network Statistics

Network Statistics monitors the general health of your network by calculating statistics for key network parameters. Network Statistics is the test where most troubleshooting scenarios begin. The instrument calculates all statistics at the same time for a 1-second sample period. Running Network Statistics simultaneously runs the Error Statistics and Ring Stations tests. To display the results of one of these other tests on the same data sample, simply press its softkey while the test is running.

If the ring is beaconing when you start the test, the instrument enters the ring after requesting verification and automatically reports the fault domain.

Configuration Parameters

You can configure the following parameters for Network Statistics. The default parameters are underlined.

❒ Utilization Display format as Percent or Frames/sec.

❒ Data Logging as Off or On and one of the following Logging Periods, when Data Logging is On. The first time interval is the test duration and the second interval (in parenthesis) is the sample period.

  ❒ 24 minutes (1 second)
  ❒ 2 hours (5 seconds)
  ❒ 12 hours (30 seconds)
  ❒ 24 hours (1 minute)
  ❒ 5 days (5 minutes)
  ❒ 5 days (1 minute)
  ❒ 7 days (1 minute)

  When you select the 7 day (1 minute) and 5 day (1 minute) logging periods, the LANMeter instrument actually saves seven one-day logs and five one-day logs, respectively. There is a short delay (about 4 minutes) in data collection between each day’s log.

  Data Logging captures Network Statistics and Error Statistics simultaneously.

Caution

> **Your LANMeter instrument notifies you if the oldest Data Log file will be lost when you run a new Data Log. Also, running the 7 day (1 minute) and 5 day (1 minute) Data Logs can cause currently saved Data Logs to be lost. This is because the 7 day (1 minute) and 5 day (1 minute) Data Logs actually save seven one-day logs and five one-day logs, respectively.**
>
> **Your LANMeter instrument reminds you of the possibility of losing a Data Log when you start data logging. You then have the opportunity to cancel data logging, export any important Data Log files, or restart the measurement.**

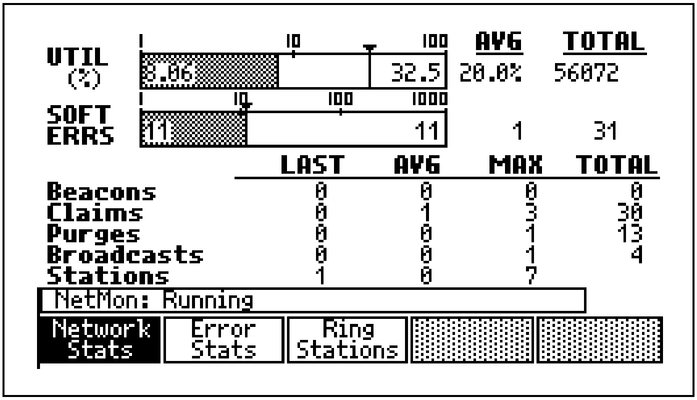
The LANMeter instrument displays **`DATA LOGGING Active!`** on the status line to provide a reminder that Data Logging is enabled and active.

Use the Data Logging feature to have the instrument run Network Stats for a period of time and then stop the test and log the results. These results can be analyzed at a later time. Refer to the “Configuring Network Monitor Tests” section for more information on configuration, and refer to the “Data Logging” section for more information on Data Logging.

Results

The instrument displays Network Statistics results after calculating the statistics for the first 1-second sample period and updates these results for each successive sample period.

Network Statistics shows Utilization and Soft Errors as numerical values and as a bar graph. The bar graph shows current and maximum values. The current value is the shaded portion of the bar with its numerical value inside the bar on the left-hand side. The maximum value is indicated on the graph with a small triangle above the bar with its numerical value inside the bar on the right-hand side. The instrument also shows the details of the Soft Errors as last, average, maximum, and total numerical values in a tabular format. Figure 3-9 shows Network Statistics sample results. The **Last** parameter is the most recent sample value.



	AVG	TOTAL
UTIL (%)	20.0%	56072
SOFT ERRS	1	31

	LAST	AVG	MAX	TOTAL
Beacons	0	0	0	0
Claims	0	1	3	30
Purges	0	0	1	13
Broadcasts	0	0	1	4
Stations	1	0	7	

NetMon: Running

Figure 3-9. Token Ring Network Statistics Sample Results

Error Statistics

Error Statistics monitors the types and sources of soft errors. Running Error Statistics automatically runs the Network Statistics and Ring Stations tests. To display the results of one of these other tests on the same data sample, simply press its softkey while the test is running. Error Statistics does not require configuration.

Use the Data Logging feature to have the instrument run a test for a period of time and then stop the test and log the results. These results can be analyzed at a later time. Data Logging is enabled in the Network Statistics configuration menu. Refer to the "Configuring Network Monitor Tests" section for more information on configuration, and refer to the "Data Logging" section for more information on Data Logging.

Results

The instrument displays Error Statistics results after calculating the statistics for the first sample period and updates these results for each successive 1-second sample period. Error Statistics displays results in numerical format and in a pie chart that shows error distributions by error type. For detailed information on a specific Error Type, highlight the error type marked with the Zoom icon (•) and press the **Zoom In** softkey. Refer to Table 3-1 for error type information and possible causes. Figure 3-10 shows Error Statistics sample results and Figure 3-11 shows Error Statistics Fault Domain sample results.

Determining the Fault Domain

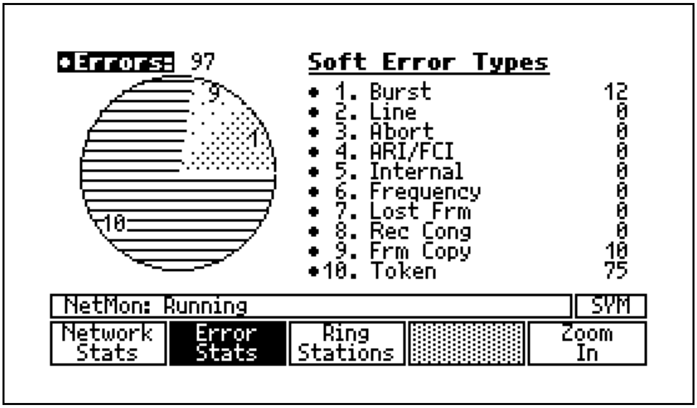
A Token Ring network will continue to operate in the presence of soft or recoverable errors. The station that detects a soft error transmits a Report Soft Error frame 2 seconds after detecting the soft error. Each Report Soft Error frame contains the number and type of errors detected by that station.

The soft error fault domain isolates the problem to two stations, their connecting cables, and any equipment (a MAU, for example) between the two stations. The two fault domain stations are the station reporting the error and its Nearest Active Upstream Neighbor (NAUN).

Under high traffic conditions, the LANMeter instrument may send Receiver Congestion soft errors. These soft errors do not affect network performance.

Table 3-1. Error Frame Types and Possible Causes

Error Frame	Transmitting Station and Reason	When to be Concerned	Possible Cause	Problem Isolation
Ring Purge	Transmitted by active monitor when a token is lost (No token transmitted for 10 ms).	When there are no station insertions or removals	- Usually caused when there are station insertions or removals - Noisy line - Faulty (or marginal) NIC	- Check stations reporting soft errors for problem location. - Check the active monitor as the source of the problem. Rebooting the active monitor forces another station to take over as active monitor.
Claim Token	Transmitted by active monitor when it fails to see the ring purges it sent. Error gets escalated to a beacon condition if active monitor continues not to receive claim tokens. Transmitted by a station when it detects an active monitor failure.	When there are no station insertions or removals	- Hard error (open transmit or receive cable, or stuck MAU port) - Active monitor failure	- Check stations reporting soft errors for problem location. - Check the active monitor as the source of the problem. Rebooting the active monitor forces another station to take over the active monitor functions.
Beacon	Transmitted by any station that detects a hard failure.	Always	- Hard failure (open transmit or receive cable, or stuck MAU port)	- Beacon Alert pop-up window gives the domain of the problem. Check the reporting station, its NAUN, or the cabling and equipment between the two stations.

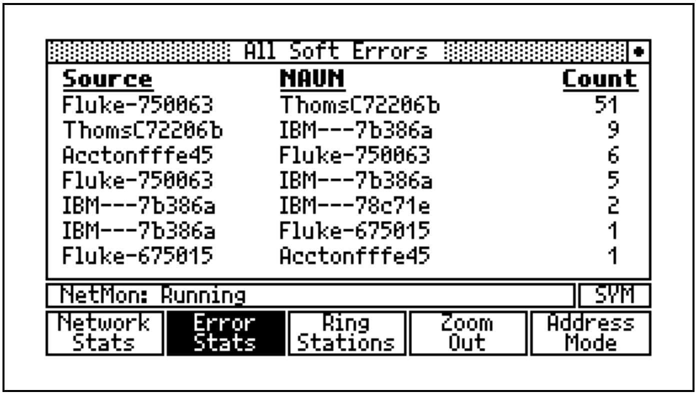


Errors: 97

Soft Error Types	
• 1. Burst	12
• 2. Line	0
• 3. Abort	0
• 4. ARI/FCI	0
• 5. Internal	0
• 6. Frequency	0
• 7. Lost Frm	0
• 8. Rec Cong	0
• 9. Frm Copy	10
•10. Token	75

NetMon: Running

Figure 3-10. Token Ring Error Statistics Sample Results



All Soft Errors

Source	NAUN	Count
Fluke-750063	ThomsC72206b	51
ThomsC72206b	IBM---7b386a	9
Acctonfffe45	Fluke-750063	6
Fluke-750063	IBM---7b386a	5
IBM---7b386a	IBM---78c71e	2
IBM---7b386a	Fluke-675015	1
Fluke-675015	Acctonfffe45	1

NetMon: Running

Figure 3-11. Token Ring Error Statistics Fault Domain Sample Results

Soft error types are either isolating or nonisolating. Isolating error types isolate the problem to a fault domain. Any station on the ring can cause nonisolating errors, but only the station detecting the error transmits the Report Soft Error frame. Table 3-2 lists the soft error types and their possible causes.

Table 3-2. Soft Error Types and Possible Causes

Error Frame	Transmitting Station and Reason	When to be Concerned	Possible Cause	Problem Isolation
Line	Transmitted by any station that detects an invalid character in a frame or token, or detects an error in the frame check sequence (FCS).	When there are no station insertions or removals	- Usually caused when there are station insertions or removals - Noisy line - Faulty (or marginal) NIC	- Check the reporting station, its NAUN, or the cabling and equipment between the two stations.
Internal	Transmitted by a station when it detects a recoverable internal error.	Always	- Faulty (or marginal) NIC	- Replace the reporting station's NIC.
Burst	Transmitted by any station that detects a lack of signal.	When there are no station insertions or removals	- Usually caused when there are station insertions or removals - Noisy line - Faulty (or marginal) NIC	- Check the reporting station, its NAUN, or the cabling and equipment between the two stations.
Abort Delimiter Transmitted	Transmitted by any station that transmits an abort delimiter as a result of an internal error or corrupted token.	When there are no station insertions or removals	- Noisy line - Faulty (or marginal) NIC	- Replace the reporting station's NIC. - Check the reporting station, its NAUN, or the cabling and equipment between the two stations.

Table 3-2. Soft Error Types and Possible Causes (Cont)

Error Frame	Transmitting Station and Reason	When to be Concerned	Possible Cause	Problem Isolation
A/C	Transmitted by any station that detects a failure in the neighbor notification protocol.	When there are no station insertions or removals	- Noisy line	- Check the reporting station, its NAUN, or the cabling and equipment between the two stations.
Lost Frame	Transmitted by any station that detects a lost frame.	When there are no station insertions or removals	- Usually caused when there are station insertions or removals - Noisy line - Faulty (or marginal) NIC	- Check the reporting station, its NAUN, or the cabling and equipment between the two stations.
Receiver Congestion	Transmitted by any station that recognizes a frame addressed to it, but does not have buffer space available for the frame.	When a station regularly reports congestion	- Station is overloaded - Station network drivers are not loaded	- This problem is common when you warmboot a station, but the network drivers have not been loaded. If the reporting station is a workstation, the problem is most likely not serious. - If the reporting station is a server or a bridge, check the configuration for a small receive buffer size.
Frame Copied	Transmitted by any station that detects, through the AC bits, that there is a possible duplicate address.	Always	- Misconfigured or faulty bridge - Duplicate remote or local station address	- Check bridges for old software revision or misconfiguration. - If the network uses locally administrated addresses, verify that there are no other stations on the network with the same address as the reporting station.

Table 3-2. Soft Error Types and Possible Causes (Cont)

Error Frame	Transmitting Station and Reason	When to be Concerned	Possible Cause	Problem Isolation
Frequency Error	Transmitted by any station that receives a signal of the wrong frequency.	Always	- Faulty (or marginal) NIC	- Replace the reporting station’s, or the NAUN’s, NIC.
Token	Transmitted by the active monitor when it detects a token has been lost.	When there are no station insertions or removals	- Usually caused when there are station insertions or removals - Noisy line - Faulty (or marginal) NIC	- Check the reporting station, its NAUN, or the cabling and equipment between the two stations.

Ring Stations

The Ring Stations test monitors the network and compiles an ordered list of stations inserted into the ring. This list of stations is in the correct physical order around the ring, starting with the active monitor.

Running Ring Stations simultaneously runs the Network Statistics and Error Statistics tests. To display the results of one of these other tests, simply press its softkey while the test is running.

Ring Stations does not require configuration.

The instrument displays Ring Stations results after it has compiled the list and updates the list every 7 seconds.

The instrument displays markers to indicate changes in ring station status; refer to Table 3-3.

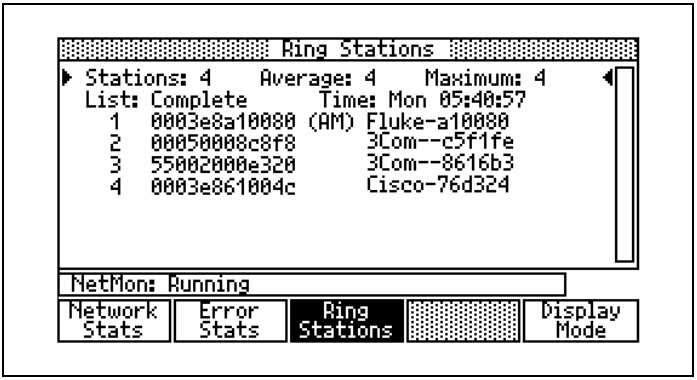
Table 3-3. Ring Stations Status Markers

Marker	Meaning
?	Previously active station that is now removed from the ring
!	Active station, new since test began
*	Active station, once removed and now reinserted on the ring
• • •	Grouping markers (these three markers are used together to mark a valid group of stations)

The Ring Stations test relies on complete neighbor notification to build the Station List. The instrument suspends updates to the Ring Stations results as long as it detects that the station lists are incomplete. During this time the instrument produces grouping markers; refer to Table 3-3. These markers group portions of the station list known to be valid. The gaps between these groups indicate a missing station (or stations). The order in which stations appear in the list may not be valid outside of the marked groups or between the groups. The instrument resumes Ring Stations result updates when it is able to produce a complete station list.

You can use the LANMeter instrument to map stations to MAU ports. To do this, run the Ring Stations test and successively remove and replace ring stations by unplugging their connectors from the MAU. If you remove a station from the ring, the instrument places a question mark beside its listing after the next neighbor notification sequence.

The first line of the results display shows the current, minimum, and maximum number of stations detected since the start of the test. The second line shows the time that the last sample period ended. The remainder of the results display lists the stations on the ring with the active monitor listed first. The remaining stations are shown in the correct physical order of active stations as plugged into the MAUs. Figure 3-12 shows Ring Stations sample results.



```
                     Ring Stations
▶ Stations: 4    Average: 4    Maximum: 4  ◀
  List: Complete      Time: Mon 05:40:57
    1   0003e8a10080 (AM) Fluke-a10080
    2   00050008c8f8      3Com--c5f1fe
    3   55002000e320      3Com--8616b3
    4   0003e861004c      Cisco-76d324

 NetMon: Running
```

Figure 3-12. Ring Stations Sample Results

The instrument lists stations only if they are inserted into the ring and if they are participating in the MAC layer protocol. The instrument lists stations that are inserted into the ring, even if they are not currently logged in to the server.

Ring Stations can display more than a full screen of information, depending on the quantity of stations on the ring. You can display stations that are beyond the screen by using △ or ▽. You can pause the display by pressing ▽ and then scrolling through this window to view the data while running this test. Press ENTER RUN to resume updating the display. Ring Stations then displays the results of the most recent Neighbor Notification process. The instrument displays the beacon pop-up window if it detects a beacon frame while the test is running.

Press and release MENU, then select **Print All**, and press ENTER RUN to print the entire ring station list (in ASCII form).

Merging New Stations into Station List

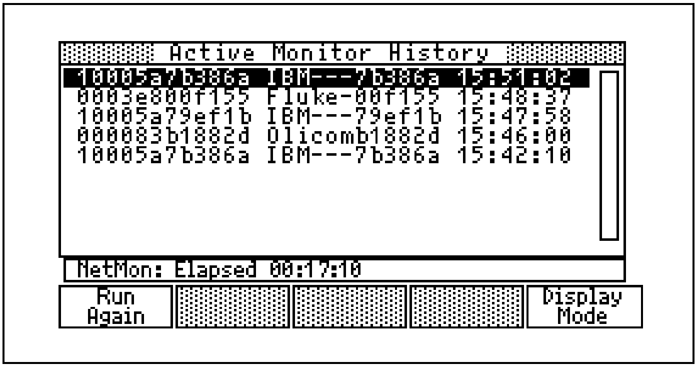
To merge the stations discovered by Ring Stations into the current Station List, press MENU, then select **Merge Stations**.

Note

> *After you use* MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.*

Viewing the Active Monitor History

From the Ring Stations screen, you can view the Active Monitor History by pressing **Display Mode** and then selecting **Active Monitor History**. Figure 3-13 shows the Active Monitor History sample results. The active monitor history is helpful when you are trying to identify problems with stations trying to become the active monitor. You can press **Display Mode** and then select **Ring Stations** to return to the Ring Stations screen.



Active Monitor History

```
10005a7b386a IBM---7b386a 15:51:02
0003e800f155 Fluke-00f155 15:48:37
10005a79ef1b IBM---79ef1b 15:47:58
000083b1882d Olicomb1882d 15:46:00
10005a7b386a IBM---7b386a 15:42:10
```

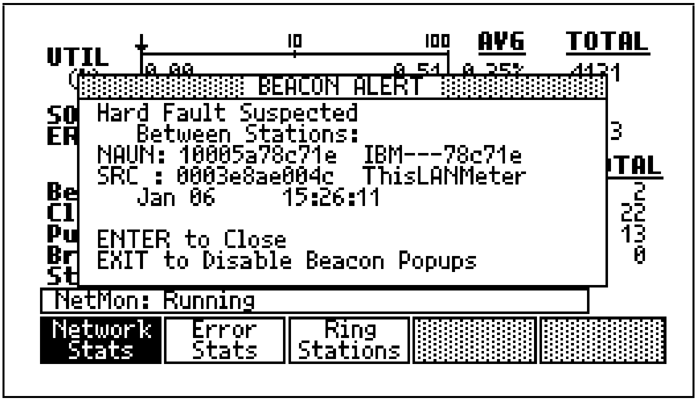
NetMon: Elapsed 00:17:10

Figure 3-13. Active Monitor History Sample Results

Beacon Alert Pop-Up Window

The instrument displays a Beacon Alert pop-up window when it detects beacon frames on your network. This window alerts you that your network has a beacon condition and indicates the fault domain.

In the Beacon Alert pop-up window, the instrument also indicates whether it suspects a hard failure or if the ring has recovered, as shown in Figure 3-14. If the ring has recovered, press ENTER RUN to continue or press EXIT STOP to ignore beacon alerts during the rest of this test. In the case of a persistent hard fault, use the fault domain information to resolve the problem. Refer to Appendix A "Troubleshooting Scenarios," for details in resolving a beaconing ring.



```
BEACON ALERT
Hard Fault Suspected
   Between Stations:
NAUN: 10005a78c71e  IBM---78c71e
SRC : 0003e8ae004c  ThisLANMeter
   Jan 06     15:26:11

ENTER to Close
EXIT to Disable Beacon Popups

NetMon: Running
```

Figure 3-14. Beacon Alert Pop-Up Window

Token Rotation Time

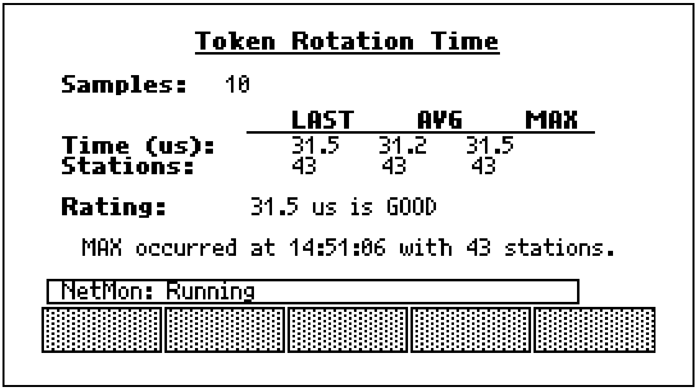
Token Rotation calculates the time for the token to travel completely around the ring.

Token Rotation Time is similar to, but not the same as Token Availability. The instrument measures true Token Rotation Time, which is independent of traffic load. Token Availability is subject to traffic load. You may find that the Token Rotation Time measurement disagrees with some protocol analyzer measurements. This is because these protocol analyzers are measuring Token Availability not Token Rotation Time.

Token Availability measures the time between free tokens. This is an indication of how often a station can transmit.

Token Rotation does not require configuration.

Token Rotation shows the last, average, and maximum values for token rotation time (in microseconds) along with the number of active stations. Figure 3-15 shows Token Rotation sample results. The instrument also reports when token rotation time is outside the normal range.



```
               Token Rotation Time

   Samples:   10
                      LAST     AVG     MAX
   Time (us):         31.5    31.2    31.5
   Stations:          43      43      43

   Rating:           31.5 us is GOOD

    MAX occurred at 14:51:06 with 43 stations.

  NetMon: Running
```

Figure 3-15. Token Rotation Sample Results

Token rotation time should be less than 150 microseconds for proper network operation, although the IEEE 802.5 standard permits token rotation times as long as 2000 microseconds. The token rotation time for your network depends first on the number of inserted stations, and second on the length of all the cables. You can use Token Rotation Time (not Token Availability) to calculate the ring Adjusted Ring Length (ARL). Refer to the Token Rotation help text for an example on calculating ARL. Highlight the Token Rotation softkey and press HELP to view Token Rotation help text.

Token Ring Network Health Overview and Guidelines

The following list provides some guidelines for interpreting the health of a Token Ring network:

1. Utilization should average less than 50%. You may want to investigate extended peaks of greater than 70%. Average Utilization above 50% suggests the need to plan network changes for improving traffic capacity.
2. Ring Purges are normal during station insertion and removal. If Ring Purges occur other than during station insertions and removals, they are abnormal and should be investigated.
3. Claim Tokens are caused by a problem or by a change in the active monitor or by a hard fault condition. A change in the active monitor includes turning it off.
4. Excessive Broadcast traffic adversely affects all stations on the network. Investigate stations that send many all-routes broadcasts.
5. Beacons are the result of a hard error condition. The network can recover from some beacons automatically. Recoverable errors that cause beacons include broken Transmit or Receive wires and stations inserting at the wrong speed. If the ring does not recover by itself, it is necessary to fix the problem manually.

Interpreting Results

The most common cause of ring purges and certain soft errors is the insertion or removal of a station from the network. This is inevitable due to the speed relationship between MAU relay operation when physically inserting or removing a station, and that of data transmission on a network. It takes about 20 milliseconds for a MAU relay to open or close. This is relatively slow compared to Token Ring data transmission speeds on a 4 Mbps network. For example, ten 500-byte frames transmit in about 10 milliseconds on a 4 Mbps network. Inserting one station onto the ring can eliminate or distort many frames. You can safely ignore these error types whenever topology changes occur. You can verify that topology changes have occurred by checking the minimum and maximum number of stations before and after running the test.

If ring purges and certain soft error types occur while the ring topology is unchanged, a problem exists. The magnitude of the problem is proportional to the magnitude of the error frame rate. Ring purges disrupt normal traffic flow, because the ring resets itself to recover from the error. This causes a loss in effective network bandwidth. This lower effective network bandwidth may manifest itself to network users as poor response time.

If these problems occur with some regularity, your network most likely has some physical problem. Refer to Table 3-1 or 3-2 for information on specific errors.

Data Logging

The Data Logging feature stores Network Statistics and Error Statistics information, for a user-specified time period, to non-volatile memory. Use Data Logging to track your network performance over time, not just a snapshot of your network health as the Network Statistics and Error Statistics screens display. Data Logging turns the instrument into a proactive tool to help anticipate problems before they become critical.

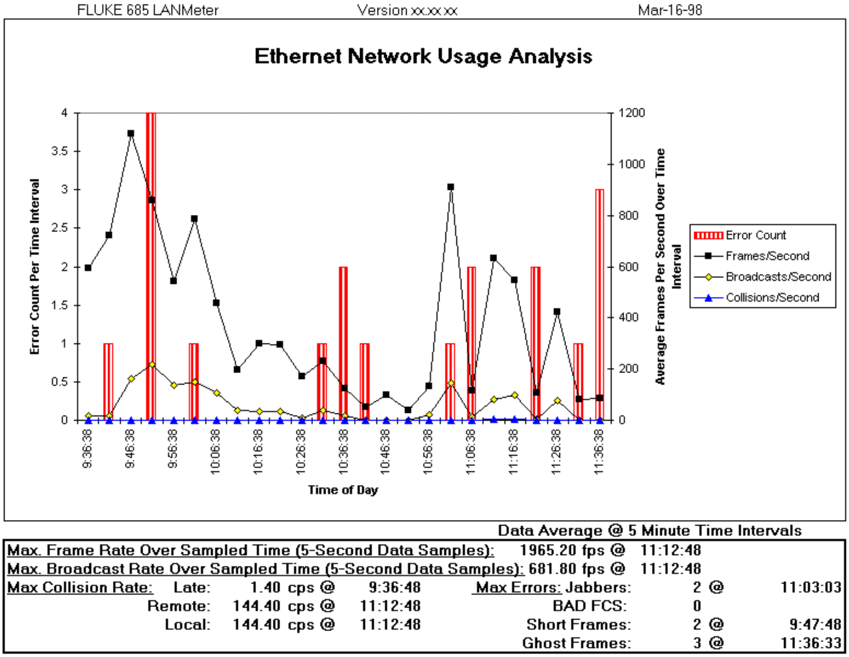
You can use HealthScan™, Network Inspector LANMeter Edition, or a spreadsheet program to view data log results. For information on HealthScan refer to Appendix D "Utilities." In North America you can call 1-800-44-FLUKE to order Network Inspector LANMeter Edition or you can access the FLUKE Networks home page (refer to the section "Useful Networking Links" in chapter 11).

Each Log File stores up to 1440 sample points. Each sample point logs the current counts of the Network Statistics or Error Statistics events as listed in Table 3-4. The following two procedures describe how to enable Data Logging and how to export its results to a PC.

Table 3-4. Network Stats and Error Stats Data Logging Events

Ethernet	Token Ring
Percent Utilization	Percent Utilization or Frame Count
Frame Count	Broadcasts
Broadcasts	Beacons
Jabbers	Ring Purges
Bad FCS frames	Claim Tokens
Short Frames	Line Errors
Late Collisions (at 10 Mbps only)	Burst Errors
Remote Collisions (at 10 Mbps only)	Receiver Congestion Errors
Collisions	Frame Copied Errors
Ghosts (at 10 Mbps only)	Lost Token Errors
	Other Soft Errors

Figure 3-16 shows a Fluke Network HealthScan sample report for 10 Mbps.



Data Average @ 5 Minute Time Intervals

Max. Frame Rate Over Sampled Time (5-Second Data Samples): 1965.20 fps @ 11:12:48
Max. Broadcast Rate Over Sampled Time (5-Second Data Samples): 681.80 fps @ 11:12:48

Max Collision Rate:	Late:	1.40 cps @	9:36:48	Max Errors: Jabbers:	2	@	11:03:03
	Remote:	144.40 cps @	11:12:48	BAD FCS:	0		
	Local:	144.40 cps @	11:12:48	Short Frames:	2	@	9:47:48
				Ghost Frames:	3	@	11:36:33

Figure 3-16. Ethernet Network Usage Analysis Chart and Result Data

Enabling Data Logging

Use the following procedure to enable Data Logging:

1. Press the top-level **Network Monitor** softkey. This also highlights the **Network Statistics** softkey.

2. Press MENU.

3. Select the **Configure** option (it may already be selected) and press ENTER RUN.

4. Set the Data Logging field to **On** by pressing ◁ or ▷.

5. Select the Logging Period field by pressing ▽.

6. Select the desired logging period by pressing ◁ or ▷, or by pressing **Show Choices** and then selecting the logging period. The sample period is shown in parenthesis.

   To undo any configuration changes you made, press MENU, select **Cancel Changes** in the Configuration Menu, and then press ENTER RUN.

7. Press EXIT STOP to save your configuration to non-volatile memory and exit the Network Statistics Configuration screen.

Caution

Your LANMeter instrument notifies you if the oldest Data Log file will be lost when you run a new Data Log. Also, running the 7 day (1 minute) and 5 day (1 minute) Data Logs can cause currently saved Data Logs to be lost. This is because the 7 day (1 minute) and 5 day (1 minute) Data Logs actually save seven one-day logs and five one-day logs, respectively.

Your LANMeter instrument reminds you of the possibility of losing a Data Log when you start data logging. You then have the opportunity to cancel data logging, export any important Data Log files, or restart the measurement.

Once data logging is enabled and Network Statistics is running, the instrument logs the event counts for each sample period. The LANMeter instrument also displays **`DATA LOGGING Active!`** on the status line to provide a reminder that Data Logging is enabled and active. At the end of the logging period the test stops automatically and stores the logged data to non-volatile memory. Pressing EXIT STOP before the logging period is over causes the logged counts to be saved to non-volatile memory.

Caution

The instrument does not write Data Log data to non-volatile memory until the Logging Period is over or until you press EXIT STOP. Loss of power during this period causes all data to be lost.

Exporting Results to a PC

Refer to Appendix D "Utilities," for information on how to export (or upload) Data Logging results to your PC.

MAC Matrix

Use the MAC Matrix test to display frame counts for the top conversations between local MAC addresses.

Configuration Parameters

You can configure the following parameters for MAC Matrix (the defaults are underlined):

❒ Conversations with a single station as Off or On. If you selected **On**, then also configure the following parameter.

❒ Filter Address of single station.

When filtering is on, displayed conversations are limited to those that are to or from the filtered address. With filtering off, the test tracks the first 512 conversing station pairs seen on the network, displaying the busiest eight.

Results

The instrument displays MAC Matrix results after monitoring network traffic for the first 1-second sample period and updates these results for each successive sample period. The MAC Matrix test displays the frame counts for both directions of the top conversations between local MAC addresses. Figure 3-17 shows MAC Matrix sample results.

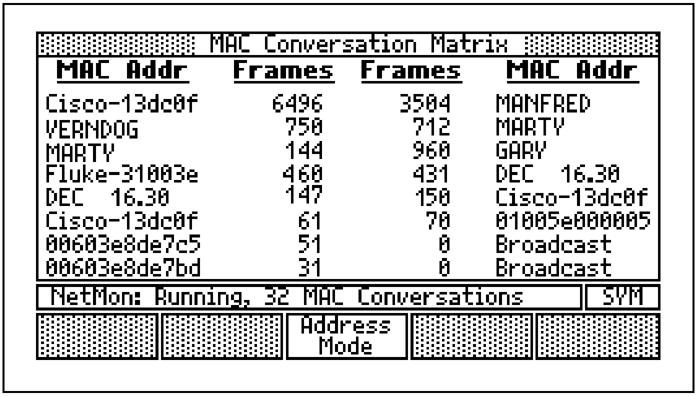
Press MENU, select **Print All**, and then press ENTER RUN (from the MAC Matrix results screen) for an ASCII printout of the Top MAC Conversation Matrix. You can use **View All** to display all of the results without printing.

Press the **Address Mode** softkey to display a menu of alternatives for switching the address format between hexadecimal, manufacturers prefix, or symbolic name.

To merge the stations discovered by MAC Matrix into a Station List, press MENU, then select **Merge Stations**.

Note

> *After you use* MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.*



MAC Conversation Matrix

MAC Addr	Frames	Frames	MAC Addr
Cisco-13dc0f	6496	3504	MANFRED
VERNDOG	750	712	MARTY
MARTY	144	960	GARY
Fluke-31003e	460	431	DEC 16.30
DEC 16.30	147	150	Cisco-13dc0f
Cisco-13dc0f	61	70	01005e000005
00603e8de7c5	51	0	Broadcast
00603e8de7bd	31	0	Broadcast

NetMon: Running, 32 MAC Conversations SYM

Figure 3-17. MAC Matrix Sample Results

Protocol Mix

The Ethernet Protocol Mix test tracks ETHERTYPE, 802.2 SAP, and 802.2 SNAP encapsulation methods. The Token Ring Protocol Mix test tracks 802.2 SAPs, SNAP encapsulation, and the sum of all MAC frame types. For NetWare protocols, Protocol Mix explicitly displays the different frame types as different protocols. This helps you identify configuration problems related to frame type methods. Protocol Mix runs as a separate test and has a 1-second sample period.

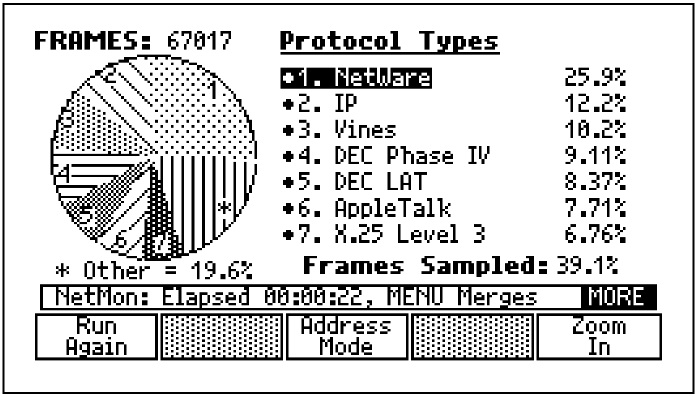
For information on running Protocol Mix on networks running Cisco ISL protocol, refer to the following “Protocol Mix with Mirror Ports” topic.

If Protocol Mix identifies a SAP or Ethertype not defined, the number or SAP is shown (for example, 8045 or SAP 05).

Protocol Mix shows the top eight protocols in a pie chart, numerically, and as a percentage of total traffic. Figure 3-18 shows sample Protocol Mix results.

You can press ▽ or △ to select one of the protocols marked with the Zoom icon (●), then press the **Zoom In** softkey to display a list containing the top senders of the selected protocol type. The top senders are identified by counting frames sent. After stopping the test, press and release MENU, select **Print All**, and then press ENTER RUN to print the entire list in ASCII format.

Press the **Address Mode** softkey to display a menu for selecting the protocol type as a hexadecimal value or protocol name.



```
FRAMES: 67017   Protocol Types
                ●1. NetWare           25.9%
                ●2. IP                12.2%
                ●3. Vines             10.2%
                ●4. DEC Phase IV      9.11%
                ●5. DEC LAT           8.37%
                ●6. AppleTalk         7.71%
                ●7. X.25 Level 3      6.76%
* Other = 19.6%   Frames Sampled: 39.1%
NetMon: Elapsed 00:00:22, MENU Merges   MORE
```

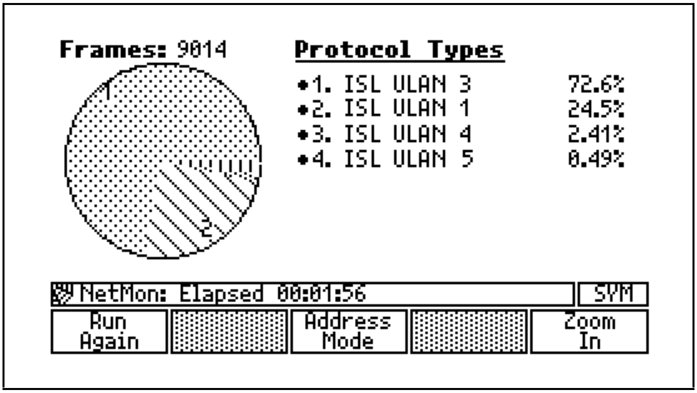
Figure 3-18. Protocol Mix Sample Results

Cisco ISL VLAN Protocol Mix

A virtual LAN (VLAN) VLAN on a Cisco switch is essentially a broadcast domain; it allows the transmission of traffic that belong to it and blocks traffic from other stations in other VLANs.

VLANs can be extended from one Cisco switch to another using physical links called trunk lines. Any Fast Ethernet port can be configured as a trunk and trunks can use the Inter-Switch Link (ISL) protocol to support multiple VLANs. An ISL trunk is like a continuation of the switching backplane. ISL trunks provide a means for a Cisco switch to multiplex up to 1000 VLANs between switches and routers.

After you plug the LANMeter instrument into a port on a Cisco switch that mirrors the ISL trunk line, you can then run Protocol Mix to report the bandwidth consumed by each VLAN running over that ISL trunk line.



Frames: 9014

Protocol Types

•1.	ISL VLAN 3	72.6%
•2.	ISL VLAN 1	24.5%
•3.	ISL VLAN 4	2.41%
•4.	ISL VLAN 5	0.49%

NetMon: Elapsed 00:01:56

Figure 3-19. Protocol Mix (VLANs) Sample Results

Press **Address Mode** to display a menu of alternatives for switching the data format between counts and percentages.

You can highlight a VLAN and then press **Zoom In** to drill down to display a list of MAC source addresses encapsulated within ISL. Conversely, you can press **Zoom Out** to return to the Protocol Mix screen.

Top MAC

Use the **Top MAC** softkey to access the Top Senders, Top Receivers, and Top Broadcasters test group. Top Senders, Top Receivers, and Top Broadcasts tests run simultaneously. To display the results of one of these other tests, simply press its softkey.

Top Senders and Top Receivers

Top Senders and Top Receivers tests monitor the busiest transmitting nodes, by MAC address, on your network. The instrument determines top senders and receivers by sampling the network as specified by your configuration setup.

Configuration Parameters

You can configure the following parameters for Top Senders or Top Receivers (the defaults are underlined):

❒ Senders to a single station as Off or On. If you selected **On**, then also configure the following parameter.

❒ Filter MAC Address of the single station

Note

Address filtering is based upon the destination address and results reflect traffic to and from the filtered station.

If you would like to determine which stations are sending the most traffic to a particular station, such as a server, set the filter address to the server's MAC address and run the Top Senders test. The instrument prompts you to enter this address when you set the **Senders to a single stn** field to **On**. Press Y Z SPACE to select an address from the Station List, or enter the address directly using the numbers 0 through 9 and the letters A through F.

The configuration parameters for Top Senders and Top Receivers also affects the Top Broadcasts test.

Results

The instrument displays Top Senders or Top Receivers results after monitoring network traffic for the first 1-second sample period and updates these results for each successive sample period. The Top Senders and Top Receivers tests display results in percent of total traffic and in a pie chart that identifies the senders, or receivers, and shows the quantity of traffic transmitted. Figure 3-19 shows Top Senders sample results. The Top Receivers results are similar to that of Top Senders.

The **Frames sampled** field shows the percentage of the total frames used to calculate the results. The total frame count is shown in the top left-hand corner of the display.

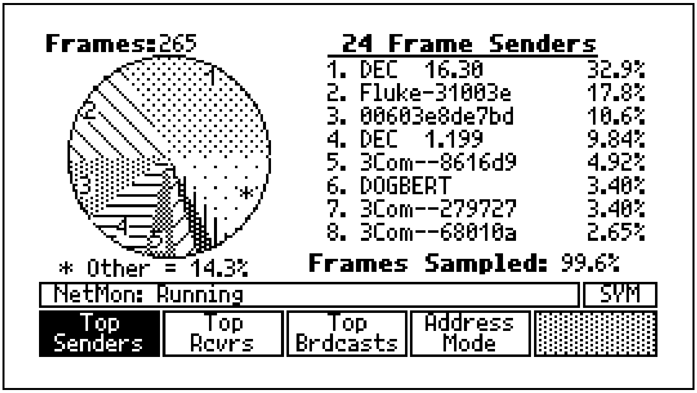
Press and release MENU, select **Print All**, and then press ENTER RUN (from the Top Senders or Top Receivers results screen) for an ASCII printout of all top senders or top receivers. You can use **View All** to display all of the results without printing.

Press the **Address Mode** softkey to display a menu of alternatives for switching the address format between hexadecimal, manufacturers prefix, or symbolic name.

To merge the stations discovered by Top Senders or Top Receivers into a Station List, press MENU, then select **Merge Stations**.

Note

> *After you use* MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.*



```
Frames:265              24 Frame Senders
                        1. DEC   16.30         32.9%
                        2. Fluke-31003e        17.8%
                        3. 00603e8de7bd        10.6%
                        4. DEC   1.199         9.84%
                        5. 3Com--8616d9        4.92%
                        6. DOGBERT             3.40%
                        7. 3Com--279727        3.40%
                        8. 3Com--68010a        2.65%
* Other = 14.3%         Frames Sampled: 99.6%
NetMon: Running                                 SYM
```

Figure 3-20. Network Monitor Top Senders Sample Results

Top Broadcasters

Top Broadcasts monitors the type and source of broadcasts on your network. Running Top Broadcasts simultaneously runs Top Senders and Top Receivers tests. To display the results of one of these other tests, simply press its softkey while the test is running.

For Ethernet networks, Top Broadcasts can show traffic as Broadcast Mix or Broadcast Sources. Press **Display Mode** and then select **Broadcast Mix** or **Broadcast Sources**. Broadcast Mix categorizes traffic as Broadcast, Multicast, and Non-Broadcast. Broadcast Sources displays the top broadcasting addresses.

For Token Ring networks, Top Broadcasts can show traffic as Broadcast Mix or Broadcast Sources. Press **Display Mode** and then select **Broadcast Mix** or **Broadcast Sources**. Broadcast Mix categorizes traffic as All Routes, Single Routes, and Non-Broadcast. Broadcast Sources displays the top broadcasting addresses.

Configuration Parameters

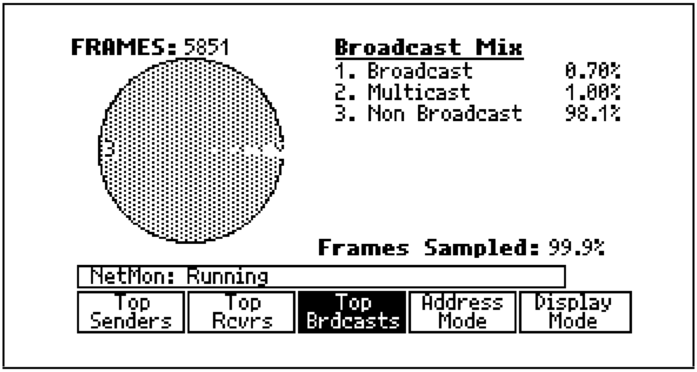
You can configure the following parameters for Top Broadcasts (the defaults are underlined):

- ❒ Senders to a single station as <u>Off</u> or On. If you selected **On**, then also configure the following parameter.
- ❒ Filter Address of single station

The configuration parameters for this test also affect the Top Senders and Top Receivers tests.

Results

The instrument displays Top Broadcasts results after monitoring network traffic for the first 1-second sample period and updates these results for each successive sample period. Top Broadcasts displays results in numerical format and in a pie chart that shows types and sources of broadcasts. Figure 3-20 shows Ethernet Top Broadcasts sample results.



FRAMES: 5851

Broadcast Mix

1. Broadcast 0.70%
2. Multicast 1.00%
3. Non Broadcast 98.1%

Frames Sampled: 99.9%

NetMon: Running

Figure 3-21. Ethernet Top Broadcasts Sample Results

The **Frames sampled** field shows the percentage of the total frames used to calculate the results. The total frame count is shown in the top left-hand corner of the display.

Chapter 4
Testing Network Components

Introduction

The Enterprise LANMeter can test your network components by using one of the following groups of tests. Select the appropriate top-level softkey to access the desired group of tests.

Ethernet	**Token Ring**
NIC/Hub Tests	NIC/MAU Tests Network Tests

You can also use the Traffic Generator for testing network components in Ethernet and Token Ring networks. The Traffic Generator test is available in the Network Monitor group of tests.

It is important to properly connect the LANMeter instrument to your network. Refer to the “Attaching Cables” section in the *Getting Started* manual for detailed information on attaching cables.

Configuring Network Component Tests

All network components tests are configured in a similar manner. Use the following procedure to configure all network components tests:

1. Press the top-level softkey of the desired test category. (Pressing MORE may be necessary.) Network component tests can be accessed by using one of the following softkeys:

   ❐ **NIC/Hub Tests** (Ethernet only)
   ❐ **NIC/MAU Tests** (Token Ring only)
   ❐ **Network Tests** (Token Ring only)
   ❐ **Network Monitor** (Ethernet and Token Ring)

2. Highlight the desired test for configuration.

   The exact steps required to highlight a test depend on which test you want to configure. The first test is automatically highlighted. Otherwise, you either press the test softkey once or press MORE, then press the test softkey once (for the second row of tests).

3. Press MENU (this also selects the **Configure** option); then press ENTER/RUN. Some tests allow some or all of the configuration parameters to be set, without using the MENU key, by just selecting the test's softkey. Tests that have no configuration parameters display **(no choices)** or **Save Config** in place of the **Configure** option.

4. Configure the desired parameters.

   Some network components tests do not require configuration and other network components tests have different configuration parameters. Refer to the individual test sections in this chapter for available configuration parameters.

   To undo any configuration changes you made, press MENU, select **Cancel Changes** in the Configuration Menu, and then press ENTER/RUN.

5. Press EXIT/STOP to save your configuration to non-volatile memory and exit the Configuration screen.

Running Network Component Tests

All Network component tests are run in a similar manner. For the Fluke 686 and 685, when the instrument is in the Ethernet mode, NIC/Hub Tests are available, and when the instrument is in the Token Ring mode, NIC/MAU Tests are available. Use the following procedure to run all Network component tests:

1. Press the top-level softkey of the desired test category. (Pressing MORE may be necessary.)
2. Highlight the desired test to run.

   The exact steps required to highlight a test depend on which test you want to run. The first test is automatically highlighted. Otherwise, you either press the test softkey once or press MORE, then press the test softkey once (for the second row of tests).
3. Configure the instrument parameters for the selected test. Refer to the “Configuring Network component tests” section in this chapter for more information.
4. Connect the instrument as described in the “Attaching Cables” section of the *Getting Started* manual.
5. Run the desired test by pressing the test softkey or by pressing ENTER RUN.
6. Observe the test results. Refer to the individual test sections in this chapter for information on available results options.
7. Press EXIT STOP to end the test, if required.

NIC/MAU and NIC/Hub Tests

NIC/Hub (Ethernet) Tests and NIC/MAU (Token Ring) Tests are used to test network components. The following list shows which tests are available for each topology. Select the top-level **NIC/Hub Tests** or **NIC/MAU Tests** softkey to access these tests. Figure 4-1 shows Ethernet NIC/Hub Tests softkeys and Figure 4-2 shows Token Ring NIC/MAU Tests softkeys.

Ethernet	**Token Ring**
Hub Autotest	MAU Autotest
NIC Autotest	NIC Autotest
Expert-T Autotest	Expert-T Autotest
	Lobe Test
	MAU Reset

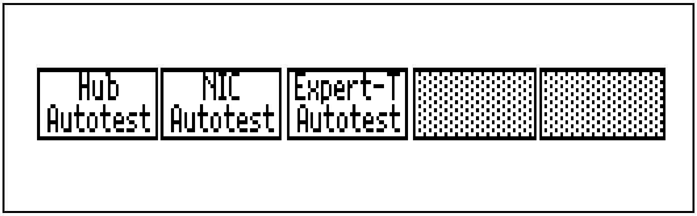


Figure 4-1. Ethernet NIC/Hub Tests Softkeys

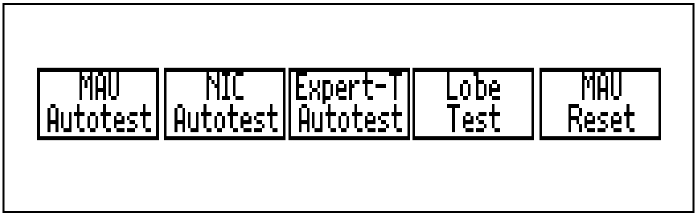


Figure 4-2. Token Ring NIC/MAU Tests Softkeys

Ethernet NIC/Hub Tests

Detecting port configurations

Using your 686 or 683 model LANMeter instrument, you can identify port speed and duplex configurations quickly, which in many cases will lead to immediate application performance improvements.

When you run the Enterprise LANMeter Hub-Autotest, NIC-Autotest and Expert-T measurements, you can detect the speed and duplex configuration of the attached hub port or NIC. The Enterprise LANMeter will automatically sense if the other port is using Auto-Negotiation and which speeds and duplex configurations are being offered. If 100Megabit link pulses are detected, these measurements will test an incoming frame so that you can tell if the attached port or NIC is configured for Full or Half Duplex. Using specially designed hardware, the 686 and 683 will wait up to 30 seconds for an incoming frame. As that frame is received, data is then transmitted on the segment. Subsequently, if the incoming frame has a good FCS, then the other port is Full Duplex. If the incoming frame has a bad FCS, then the other port is Half Duplex, which sent an Ethernet jam signal in response to the LANMeter's transmission. If the other port is a 100BASE-TX hub, a single collision will be seen within the collision domain. No data is lost however, as the MAC chip sets will automatically retransmit the collided frame.

NIC/Hub Tests:

❒ Hub Autotest
❒ NIC Autotest
❒ Expert-T Autotest

Hub Autotest

Use Hub Autotest to perform a functional test of a hub. Hub Autotest verifies that a hub can correctly send and receive traffic. Use Hub Autotest to test hubs for new installations or when you suspect a faulty hub or wiring. Hub Autotest does not certify a hub to 10BASE-T or 100BASE-TX standards.

Hub Autotest performs some (depending on the situation) or all of the following functions:

❒ Checks the Link Pulse state. If the Link Pulse is inactive, verify that the instrument is correctly connected to the hub and run the test again. If the

Hub Autotest does not see a link pulse, it tests the cable for faults after prompting you to accept this operation.

Note

Some equipment that was developed prior to the 10BASE-T standard may not implement the Link Pulse function.

- Checks the transmit (TX) polarity from the hub. If the polarity is incorrect (that is, the TX+ and TX- leads are reversed) the connection may not operate. The LANMeter instrument turns on the Polarity LED when the polarity is reversed. Most newer equipment automatically compensates for reversed polarity.
- Checks the receive (RX) signal level from the hub. For Hub Autotest to get an accurate reading of the transmit signal level, the instrument must be connected within 20 feet of the hub. If the signal level is low, verify that the instrument is connected within 20 feet of the hub.
- Verifies that the instrument can receive frames from the network. The instrument also logs the protocols it monitors and the encapsulation methods used.
- Pings or ARPs for some of the devices found (NetWare and TCP/IP networks only). This is done to verify that a station connected to this hub port can successfully talk to a server.

Configuration

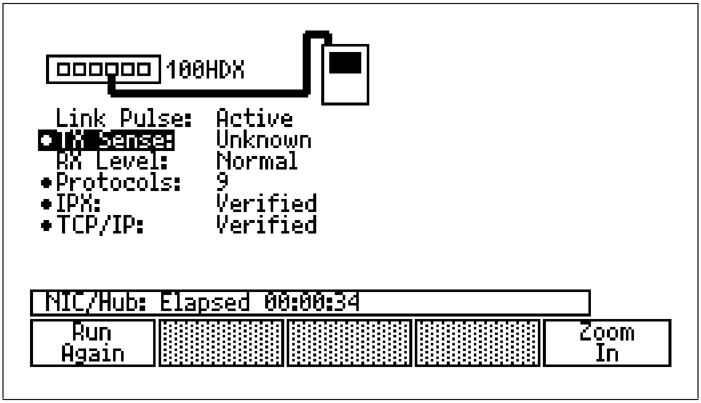
The following configuration parameters are available for Hub Autotest:

- Cable Type as shown in Table 2-3.
- Cable Units as feet or meters.

It is not necessary to configure Hub Autotest unless you want to change the default conditions.

Results

The instrument displays Hub Autotest results at the end of the test. These results are shown in summary form. Figure 4-3 shows Ethernet Hub Autotest sample results. You can get more detailed information for the items marked with the Zoom icon (●), by highlighting the item and then pressing the **Zoom In** softkey.



```
100HDX
  Link Pulse:   Active
● TX Sense:     Unknown
  RX Level:     Normal
● Protocols:    9
● IPX:          Verified
● TCP/IP:       Verified

NIC/Hub: Elapsed 00:00:34
```

Figure 4-3. Ethernet Hub Autotest Sample Results

For TCP/IP networks, do not be concerned if some of the nodes do not respond. If these nodes are on the other side of a router, the router may not respond for the target node.

Note

> *Some IP devices, mostly routers, may not respond even if the LANMeter instrument is on the same segment. Running the TCP/IP Tests, with a valid local IP configuration, can test connectivity.*

If Hub Autotest measures a low signal level, verify that the instrument is connected within 20 feet of the hub and run the test again.

NIC Autotest

Use NIC Autotest to perform a functional test of a 10BASE-T, 100BASE-TX, or ThinLAN NIC card. For NetWare clients and TCP/IP nodes, NIC Autotest verifies that a NIC card can correctly send and receive traffic. Use the NIC Autotest to verify new NIC card installations or to test a suspected faulty NIC card or wiring. The NIC Autotest does not certify a NIC card to 10BASE-T or 10BASE2 standards.

Note

> *For ThinLAN coaxial networks, the instrument and the NIC under test must be the only devices on the network. The connection should be a relatively short coaxial cable (less than 20 feet) with a single terminator at the network interface card. (The instrument will automatically terminate its end of the cable.)*

NIC Autotest prompts you to load the network drivers (such as, **For Novell networks run IPX**). Once the adapter card starts transmitting, NIC Autotest captures and displays the NIC card's MAC address, protocol driver, and Frame Type method (such as, Ethertype, Novell 802.3, or SNAP).

NIC Autotest performs some (depending on the situation) or all of the following functions:

❐ Checks the Link Pulse state. If the Link Pulse is inactive, verify that the instrument is correctly connected to the NIC card and run the test again. If the NIC Autotest does not see a link pulse, it tests the cable for faults after prompting you to accept this operation.

Note

Some equipment that was developed prior to the 10BASE-T standard may not implement the Link Pulse function.

❐ Checks the transmit (TX) polarity from the NIC. If the polarity is incorrect (that is, the TX+ and TX- leads are reversed) the connection may not operate. Most newer equipment automatically compensates for reversed polarity.

❐ Checks the receive (RX) signal level from the NIC. For NIC Autotest to get an accurate reading of the transmit signal level, the instrument must be connected within 20 feet of the NIC card. If the signal level is low, verify that the instrument is connected within 20 feet of the NIC card.

❐ Verifies the correct protocol driver and the adapter card’s MAC address. Once the adapter card starts transmitting, the instrument captures and displays the NIC card’s MAC address, protocol driver and Frame Type method (such as, Ethertype, Novell 802.3, or SNAP).

❐ Pings the NIC card to verify that it can correctly send and receive frames (for NetWare and TCP/IP systems only).

Configuration

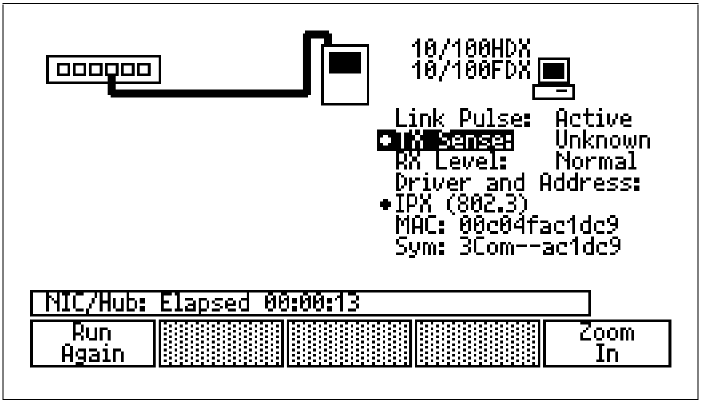
The following configuration parameters are available for NIC Autotest:

- ❒ Cable Type as shown in Table 2-3.
- ❒ Cable Units as <u>feet</u> or meters.

It is not necessary to configure NIC Autotest unless you want to change the default conditions.

Results

The instrument displays NIC Autotest results at the end of the test. These results are shown in summary form. Figure 4-4 shows Ethernet NIC Autotest sample results. You can get more detailed information for the items marked with the Zoom icon (●), by highlighting the item and then pressing the **Zoom In** softkey.



```
10/100HDX
10/100FDX
 Link Pulse:  Active
●TX Sense:    Unknown
 RX Level:    Normal
 Driver and Address:
●IPX (802.3)
 MAC: 00c04fac1dc9
 Sym: 3Com--ac1dc9
NIC/Hub: Elapsed 00:00:13
```

Figure 4-4. Ethernet NIC Autotest Sample Results

If NIC Autotest measures a low signal level, verify that the instrument is connected within 20 feet of the NIC card and run the test again.

For coaxial networks, make sure that a terminator is connected only at the NIC-card end of the network.

Expert-T Autotest

Use Expert-T Autotest to diagnose a station’s difficulty in gaining access to the network. Expert-T Autotest automates the tests performed by the individual NIC Autotest and Hub Autotest. Expert-T Autotest attempts to isolate the problem to the hub, cabling, or NIC card. Expert-T Autotest works with 10BASE-T and 100BASE-TX networks.

Expert-T Autotest performs the following functions:

- ❐ Automatically runs the Hub Autotest. If Expert-T Autotest fails to sense the 10BASE-T or 100BASE-TX link pulse it optionally tests the cable for faults.
- ❐ Electrically disconnects itself from the hub.
- ❐ Automatically runs the NIC Autotest. Expert-T Autotest prompts you to load the network drivers (for example, **For Novell networks run IPX**). Once the adapter card starts transmitting, Expert-T Autotest captures and displays the NIC card’s MAC address, protocol driver, and Frame Type method (such as, Ethertype, Novell 802.3, or SNAP).
- ❐ Electrically connects the NIC card directly to the hub, electrically bypassing the LANMeter instrument monitoring circuits and stopping its analysis.

Configuration

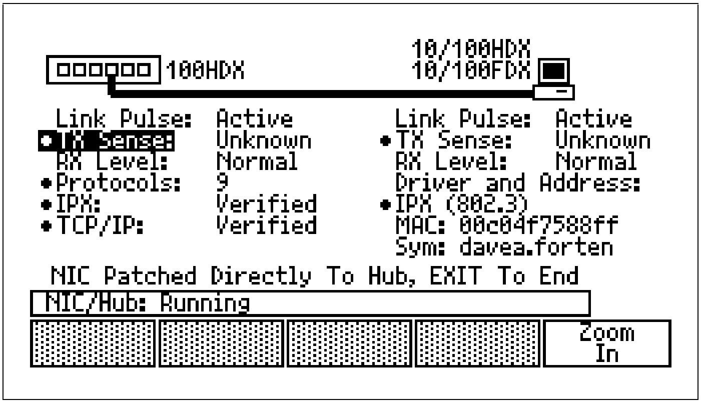
The following configuration parameters are available for Expert-T Autotest:

- ❐ Cable Type as shown in Table 2-3.
- ❐ Cable Units as feet or meters.

It is not necessary to configure Expert-T Autotest unless you want to change the default conditions.

Results

The instrument displays Expert-T Autotest results after completion of the test. Figure 4-5 shows Ethernet Expert-T Autotest sample results. These results are shown in summary form. You can get more detailed information for the items marked with the Zoom icon (•), by highlighting the item and then pressing the **Zoom In** softkey.



```
                                10/100HDX
        100HDX                  10/100FDX

 Link Pulse:  Active        Link Pulse:  Active
•TX Sense:    Unknown      •TX Sense:    Unknown
 RX Level:    Normal        RX Level:    Normal
•Protocols:   9             Driver and Address:
•IPX:         Verified     •IPX (802.3)
•TCP/IP:      Verified      MAC: 00c04f7588ff
                            Sym: davea.forten
 NIC Patched Directly To Hub, EXIT To End
 NIC/Hub: Running
                                                 Zoom
                                                  In
```

Figure 4-5. Ethernet Expert-T Autotest Sample Results

Token Ring NIC/MAU Tests

You can run the following NIC/MAU Tests:

- ❒ MAU Autotest
- ❒ NIC Autotest
- ❒ Expert-T Autotest
- ❒ Lobe Test
- ❒ MAU Reset

MAU Autotest

Use the MAU Autotest to test a new or suspected faulty MAU port for correct operation.

The MAU Autotest automatically performs some (depending on the situation) or all of the following functions:

❒ Attempts insertion into the ring
❒ Reports if it is the only station in the ring
❒ Reports the ring speed
❒ Indicates the presence of network activity and ring state
❒ Runs cable tests when a cable fault is suspected

Press MENU, select **Configure**, and use **Show Choices** or the arrow keys to select the Cable Type.

Note

> *If the LANMeter instrument is configured for a DB-9 connector, the Cable Type is fixed at STP and you cannot change the Cable Type parameter. If you change the Cable Type to RJ-45, you can reconfigure the Cable Type parameter.*

The instrument displays MAU Autotest results at the end of the test. The MAU Autotest reports the ring speed and the Nearest Active Upstream Neighbor (NAUN).

NIC Autotest

Use the NIC Autotest to test a new or suspected faulty station NIC card for correct operation. The NIC Autotest executes a set of tests and reports their results.

Note

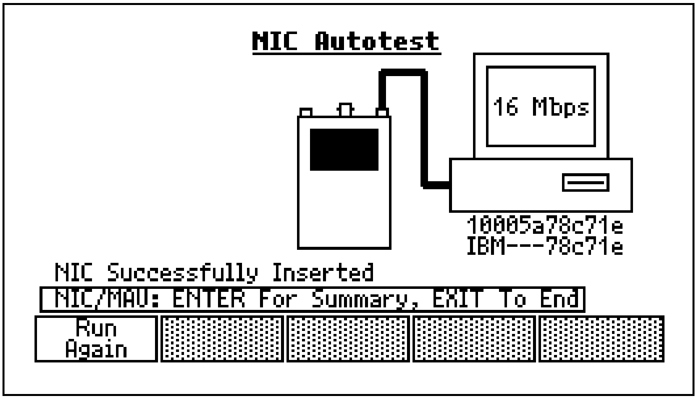
> *Token Ring NIC Autotest and Expert-T Autotest can have difficulties with some Token Ring NIC cards if they change speeds during their own auto-speed detection.*

NIC Autotest performs some (depending on the situation) or all of the following functions:

- ❐ Reports the results of the lobe test.
- ❐ Checks the Transmit and Receive leads for cable and connector faults, if the lobe test fails.
- ❐ Reports the speed of the NIC.
- ❐ Reports the MAC address of the NIC.
- ❐ Reports if NIC phantom voltage is applied and within specification.

Press MENU, select **Configure**, and press ◁ or ▷ to select the Cable Type.

The instrument displays NIC Autotest results at the end of the test. Figure 4-6 shows Token Ring NIC Autotest sample results.



NIC Autotest

NIC Successfully Inserted

NIC/MAU: ENTER For Summary, EXIT To End

Figure 4-6. Token Ring NIC Autotest Sample Results

Expert-T Autotest

Use the Expert-T Autotest to diagnose a station's difficulty in gaining access to the network. This problem may exist somewhere between the station and the MAU connecting it to the network.

Note

Token Ring NIC Autotest and Expert-T Autotest can have difficulties with some Token Ring NIC cards if they change speeds during their own auto-speed detection.

Expert-T Autotest performs the following functions:

- ❒ Attempts to insert into the ring. If insertion fails, the lobe cabling and MAU port are tested.
- ❒ Determines the ring speed and automatically sets itself to that speed and reports the NAUN.
- ❒ Displays the **Waiting for NIC to Insert** message in a pop-up window, and waits for the NIC to respond. At this point you should load the appropriate network driver on the station where the NIC is installed. For best results, power off the station until the LANMeter instrument displays the **Waiting for NIC to Insert** message.
- ❒ Monitors and reports results of the lobe test by the NIC and reports any suspected lobe wiring faults between the instrument and the NIC.
- ❒ Detects the NIC speed and verifies that the ring and NIC speeds match. If there is a mismatch in speeds, the NIC is prevented from inserting into the ring.
- ❒ Detects and reports the MAC address for the NIC.
- ❒ Detects and reports if phantom voltage is applied by the NIC and, if applied, reports if phantom voltage is out of specification.
- ❒ Monitors and reports the state of the ring (normal, beaconing, etc.).
- ❒ Monitors and reports the results of the station's Duplicate Address Test (DAT).

Note

When you select the **Auto** *ring speed, the 16 Mb/s LED is lit while the instrument is waiting for the NIC to insert.*

Configuration

When you highlight the **Expert-T Autotest** softkey, the instrument prompts you to configure the **End Mode**. The End Mode parameter determines how the instrument connects to the network under test after completing the Expert-T Autotest. The two options are **Release NIC Connection After Run** (the default) or **Maintain NIC Connection After Run**.

With the End Mode field set to **Release NIC Connection After Run**, the instrument breaks the **TO NIC** attached station connection to the network before running any additional network tests.

With the End Mode field set to **Maintain NIC Connection After Run**, the instrument maintains the **TO NIC** attached station connection after running Expert-T Autotest. This allows you to run other network tests, such as Network Statistics or Error Statistics, with the **TO NIC** attached station still inserted into the ring. This connection mode allows you to continue network testing without disturbing your setup, and it has the added benefit of not using an additional MAU port. If the **Maintain NIC Connection After Run** mode is selected, and no station is attached to the **TO NIC** connector, the instrument displays a **Waiting for NIC to Insert** pop-up window after attempting to run a network test.

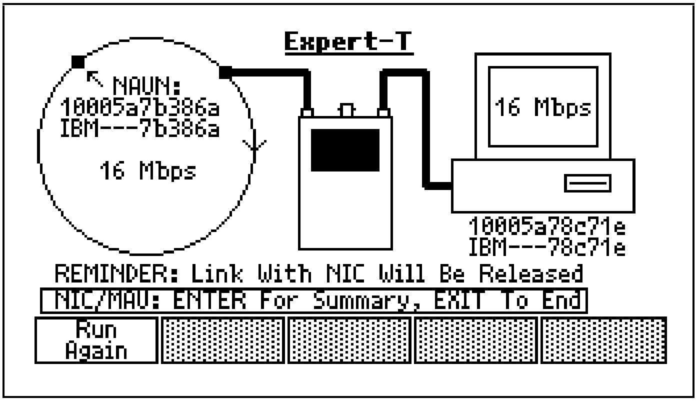
The following configuration parameters are available for Expert-T Autotest:

❒ Cable Type as shown in Table 2-3.
❒ Cable Units as <u>feet</u> or meters.

It is not necessary to configure Expert-T Autotest unless you want to change the default conditions.

Results

The instrument displays Expert-T Autotest results after completion of the test. These results are shown in summary form. Figure 4-7 shows Token Ring Expert-T Autotest sample results.



REMINDER: Link With NIC Will Be Released

NIC/MAU: ENTER For Summary, EXIT To End

Figure 4-7. Token Ring Expert-T Autotest Sample Results

Lobe Test

Lobe Test verifies that a cable can successfully pass 4 Mbps and/or 16 Mbps network traffic. This test does not disrupt an operational ring and does not cause the MAU relay to open.

The Lobe Test is not affected by the presence or absence of baluns and media filters. The Lobe Test can be used to ensure that baluns and media filters are not disrupting communications for the station connection.

Configuration

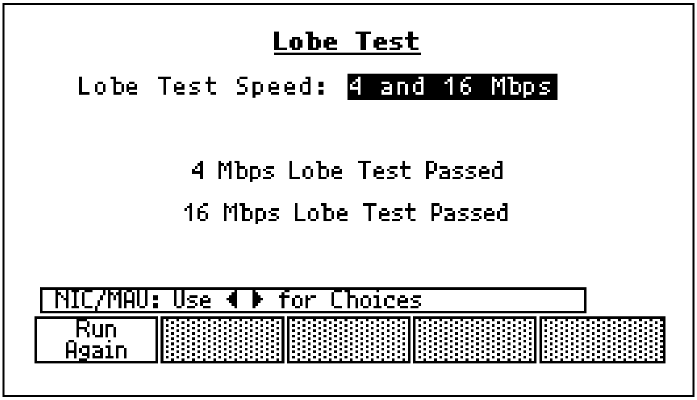
When you highlight the **Lobe Test** softkey, the instrument prompts you to configure the **Lobe Test Speed**. The Lobe Test Speed parameter determines the speed at which the instrument attempts to test the cable.

You can configure the Lobe Test Speed field for both 4 Mbps and 16 Mbps (the default), 4 Mbps, or 16 Mbps. With the Lobe Test Speed field set to both 4 Mbps and 16 Mbps, the instrument attempts to test the cable at one speed and then the other.

It is not necessary to configure Lobe Test unless you want to change the default conditions.

Results

The instrument displays Lobe Test results at the end of the test. Figure 4-8 shows Token Ring Lobe Test sample results.



Lobe Test

Lobe Test Speed: 4 and 16 Mbps

4 Mbps Lobe Test Passed

16 Mbps Lobe Test Passed

NIC/MAU: Use ◀ ▶ for Choices

Figure 4-8. Token Ring Lobe Test Sample Results

MAU Reset

MAU Reset attempts to unstick the relay in the attached MAU port and monitors network activity to verify correct relay operation.

MAU Reset does not require configuration.

The instrument displays a message if the MAU does not reset properly after running MAU Reset. If a MAU port cannot be reset after several attempts, the port may be faulty.

If the instrument has already inserted into the ring it will display a message stating that it is unlikely that the MAU port needs resetting. You can press the **MAU Reset** softkey or ENTER RUN to reset the MAU port or press EXIT STOP to exit the test.

Network Tests

Network Tests are a collection of tests that measure Token Ring network characteristics and poll network devices for information. Select the top-level **Network Tests** softkey to access one of the following tests. Figure 4-9 shows the Network Tests softkeys.

❒ Station Ping
❒ Phase Jitter
❒ Adapter Status
❒ Remove Station

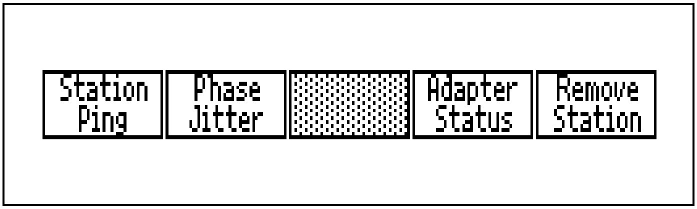


Figure 4-9. Network Tests Softkeys

Station Ping

Station Ping verifies connectivity to a given station. When you highlight the **Station Ping** softkey, the instrument prompts you for a **Target** station address. You can either enter a hexadecimal address (by using the numbers 0 through 9 and letters A through F) or select a symbolic name from the station list.

You can configure the Target station address after highlighting the **Station Ping** softkey or by using the configuration procedure.

Use the following procedure to select a symbolic name from the station list:

1. Press Y Z SPACE to display the current station list in a list window.
2. Press △ or ▽ to select the station of your choice.
3. Press ENTER RUN to select the symbolic name or press EXIT STOP to remove the list window and to enter the address in hexadecimal.

Configuration Parameters

You can configure the following parameters for Station Ping from the Configuration Menu. The default parameters are underlined.

❒ Target station address
❒ Broadcast Type as Single Route or All Routes
❒ Timeout as 1 second, 5 seconds, or 30 seconds

The Timeout period is the amount of time the instrument waits for a response.

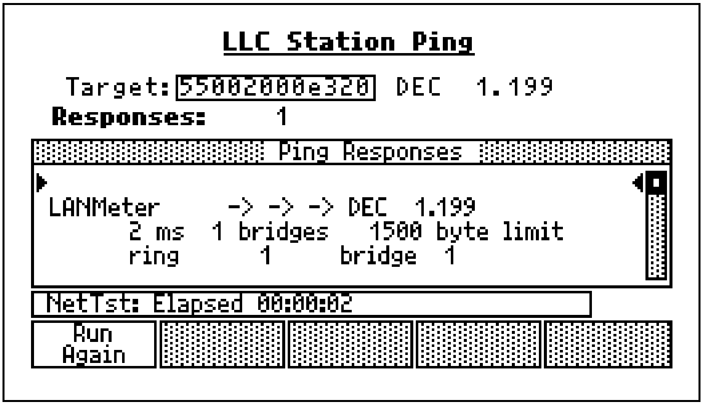
It is not necessary to configure Station Ping unless you want to change the default conditions.

Results

The instrument displays Station Ping results after the targeted station responds and updates this information after each response of the target station. If the target station does not respond within the configured Timeout period, the instrument displays the message **No response from station**. Figure 4-10 shows Token Ring Station Ping sample results.

Note

If the source routing is not enabled on the target station, the target station may not respond to a source-routed LLC station ping.



```
               LLC Station Ping

  Target:55002000e320  DEC   1.199
 Responses:     1
              Ping Responses
 LANMeter     -> -> -> DEC  1.199
       2 ms  1 bridges   1500 byte limit
       ring      1     bridge  1
NetTst: Elapsed 00:00:02
```

Figure 4-10. Token Ring Station Ping Sample Results

If you use source-routed bridges, you can use the Station Ping test to determine and display the route from the instrument to the target station.

Phase Jitter

The Phase Jitter test measures cumulative, uncorrelated phase jitter, which is an indication of noise on the network. The Phase Jitter test is best used to help you track the effects of changes that you make when troubleshooting or when making additions to your network.

The LANMeter instrument performs this test by first becoming the Active Monitor, which makes the instrument the source of the network clock, and then measuring the phase jitter while it transmits frames with all zeros and all ones. The instrument measures the amount of jitter between the incoming signal and its output signal. **The Phase Jitter test can give erroneous results if run on networks using retiming circuits or reclocking “Jitter Busters” because the instrument must source the network clock to run this test.**

Caution

> **To measure Phase Jitter, the instrument will become the Active Monitor. This process can occasionally cause a few beacons to occur on the ring. These beacons will not seriously affect network operation.**

Phase Jitter does not require configuration.

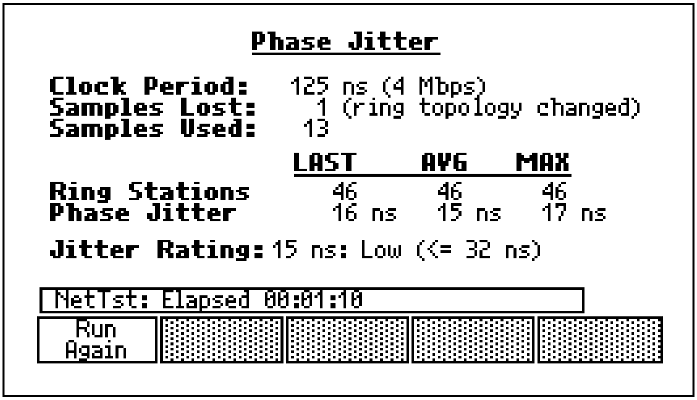
Results

Phase Jitter reports the following information. Figure 4-11 shows Token Ring Phase Jitter sample results.

❒ Number of Ring Stations
❒ Total amount of uncorrelated Phase Jitter
❒ Qualitative rating of the jitter

Caution

To measure Phase Jitter, the instrument transmits non-source routed frames. These frames may be forwarded by Token Ring transparent bridges to other LAN segments, increasing traffic. Source routed bridges ignore this traffic.



```
                  Phase Jitter

Clock Period:   125 ns (4 Mbps)
Samples Lost:     1 (ring topology changed)
Samples Used:    13

                LAST     AVG    MAX
Ring Stations     46      46     46
Phase Jitter      16 ns   15 ns  17 ns

Jitter Rating: 15 ns: Low (<= 32 ns)

NetTst: Elapsed 00:01:10
```

Figure 4-11. Token Ring Phase Jitter Sample Results

Interpreting Phase Jitter Results

Press HELP to get on-line assistance with interpreting phase jitter results. The Phase Jitter measurement is not identical to that defined by the IEEE 802.5 standard.

Uncorrelated phase jitter is one measure of the amount of noise on a Token Ring network. If a Token Ring network has an excessive amount of phase jitter, then network performance seriously degrades. Excessive phase jitter may manifest itself as slow response time, dropped connections, the inability to attach to a server, or stations can report an unusually high number of lost token, frame, and line soft errors. Refer to Appendix A “Troubleshooting Scenarios,” for information on how to use the Phase Jitter test to isolate a defective network component.

Generally, the lower the value of phase jitter the better. However, more important than the absolute value of phase jitter is the difference in phase jitter from before and after changing your network’s configuration.

If the Phase Jitter test reports jitter in the Inconclusive Region, you must interpret this result in light of existing network errors. For example, if your network has a lot of errors (such as ring purges and token, line, and burst soft error types) that are not associated with normal station insertions and removals, then refer to the “Error Statistics” section in Chapter 3 and to the “Tracking Down Sources of Phase Jitter” section in Appendix A to resolve the inconclusive phase jitter results. If the reported phase jitter is in the Inconclusive Region and there are no other network errors, then it is likely that the network is experiencing some low frequency phase jitter, which the Active Monitor’s elastic buffer is designed to accommodate. Low frequency phase jitter can be caused by bad or marginal network interface cards and network interface card interoperability problems.

Phase jitter results in the inconclusive region may also indicate the presence of a retiming device, which invalidates the test results.

Adapter Status

Adapter Status reports on the status of a target station’s network adapter.

When you highlight the **Adapter Status** softkey, the instrument prompts you for a **Target** station address. You can either enter a hexadecimal address (by using the numbers 0 through 9 and letters A through F) or select a symbolic name from the station list.

You can configure the Target station address after highlighting the **Adapter Status** softkey or by using the configuration procedure.

Use the following procedure to select a symbolic name from the station list:

1. Press Y Z SPACE to display the current station list in a list window.
2. Press △ or ▽ to select the station of your choice.
3. Press ENTER RUN to select the symbolic name or press EXIT STOP to remove the list window and to enter the address in hexadecimal.

Configuration Parameters

You can configure all of the following Adapter Status parameters by using the Configuration Menu. The default parameters are underlined.

❒ Target station address
❒ To Run a <u>Once</u> or Continuous

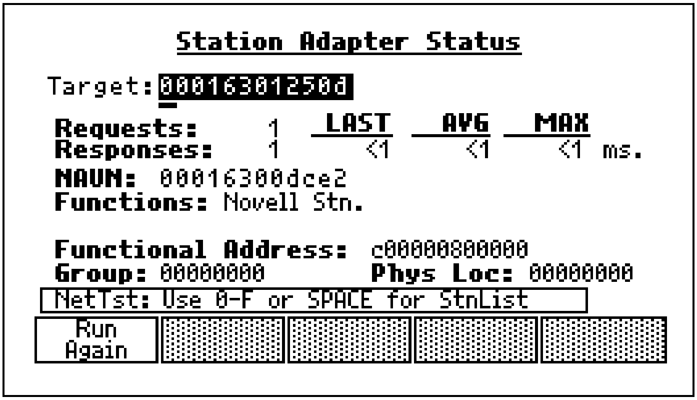
❒ Timeout period as 1 second, 5 seconds, or 30 seconds

The Timeout period is the amount of time the instrument waits for a response. When configuring Adapter Status to run continuously, set the repetition rate with the Timeout Period field.

It is not necessary to configure Adapter Status unless you want to change the default conditions.

Results

The instrument displays Adapter Status results after the targeted station responds and, if configured to run continuous, updates this information after each response of the targeted station. If the targeted station does not respond within the configured Timeout period, the instrument displays the message **No response from station**. Figure 4-12 shows Token Ring Adapter Status sample results.



```
              Station Adapter Status

   Target:00016301250d

    Requests:     1   LAST   AVG   MAX
    Responses:    1     <1    <1    <1  ms.
    MAUN:  00016300dce2
    Functions: Novell Stn.

    Functional Address:  c00000800000
    Group: 00000000      Phys Loc: 00000000
```

Figure 4-12. Token Ring Adapter Status Sample Results

In addition to providing a station response time, Adapter Status also reports the queried station's functional address (or addresses), group, and physical location. The functional address defines the logical function that the adapter card is performing. The group and physical location fields are set by the Local Configuration Report Server and are rarely used.

It is common for a device to perform more than one function and, therefore, to have more than one functional address. For example, an IBM Bridge can provide the following functions:

- ❒ Ring Error Monitor
- ❒ Ring Parameter Server
- ❒ Configuration Report Server
- ❒ Bridge
- ❒ LAN Manager

Remove Station

Remove Station removes a local station from the network by sending a Remove Ring Station frame to the specified station.

Caution

Remove Station causes the target station to lose its network connection. The user of the target station may lose work or data. Setting the target address to a functional broadcast address may cause all stations to be removed from the network.

When you highlight the **Remove Station** softkey, the instrument prompts you for a **Target** station address. You can either enter a hexadecimal address (by using the numbers 0 through 9 and letters A through F) or select a symbolic name from the station list.

Use the following procedure to select a symbolic name from the station list:

1. Press Y Z SPACE to display the current station list in a list window.
2. Press △ or ▽ to select the station of your choice.
3. Press ENTER RUN to select the symbolic name or press EXIT STOP to remove the list window and to enter the address in hexadecimal.

You can configure Remove Station, after highlighting its softkey, by entering the target address.

After verifying the removal of the targeted station, the instrument displays the Remove Station results. Remove Station reports the address of the removed station.

Not all stations will remove themselves from the ring after receiving the remove station command. Stations that are sending congested receiver soft errors and file servers can ignore the remove station command.

Traffic Generator

You can use Traffic Generator to stress test your network. Many problems, especially those related to cabling and network components (such as, hubs, bridges, adapter cards, and routers) only appear while the network is under heavy traffic load. You can also use Traffic Generator to simulate the affect of adding new users and services to your network.

Traffic Generator repetitively transmits a single frame. You can configure this frame and its transmission rate in the configuration screen. The Traffic Generator does not require you to construct protocol headers to send traffic through bridges and routers. When you select IPX or IP packet types, you simply fill in the appropriate MAC and network layer destination and source addresses and then Traffic Generator automatically builds the frame and calculates all header checksums.

When running, Traffic Generator attempts to add the amount of traffic specified in the configuration screen. At times, due to network conditions, the instrument may not be able to add all of the specified traffic.

In addition to running Traffic Generator by itself, you can configure Traffic Generator to operate in the background of some tests. This is done by pressing the top-level **Network Monitor** softkey, highlighting the **Traffic Generator** softkey, and using ◁ or ▷ to select **Run in Background** or **Respond to IP Ping**. The following tests can be run with Traffic Generator in the background:

Ethernet

Network Statistics
Error Statistics

Token Ring

Network Statistics
Error Statistics
Ring Stations

For the **Respond to IP Ping** selection, the LANMeter instrument’s IP stack will run with the traffic generator, allowing the instrument to respond to ICMP pings while sending traffic. This is particularly useful to test the impact of additional traffic loads over WAN links. As added traffic is routed over the WAN links, remote LANMeter instruments or network stations can look at the impact on ping response times by pinging the LANMeter instrument sending the traffic.

Configuring Traffic Generator

Use the following procedure for configuring Traffic Generator:

1. Press the top-level **Network Monitor** softkey.
2. Highlight the **Traffic Gen** softkey by pressing it once.
3. Press MENU and select **Configure**.
4. Press ENTER RUN and configure the desired parameters.

Note

> *If you have a Fluke 686, 685, 683, or 682 instrument, you can generate up to 10 Mbps traffic in the 10 Mbps mode and if you have a Fluke 686 or 683 instrument, you can generate up to 100 Mbps traffic in the 100 Mbps mode with Traffic Generator.*

You can configure the following parameters (the defaults are underlined):

- ❒ Frame rate transmitted (100 fr/s is the default) up to a maximum of 2500 fr/s for 10 Mbps or 25,000 fr/s for 100 Mbps.
- ❒ Size of each frame from 30 to 6000 bytes (400 bytes is the default). The frame size includes the frame check sequence.
- ❒ Type of packets generated as IPX, IP, and LLC Only. The following additional parameters are configurable depending on the Type field selection:
    - ❒ When IPX is selected, enter the appropriate source and destination addresses, network number, and the encapsulation type (Ethernet only).
    - ❒ When IP is selected, enter the appropriate source and destination addresses.

      To send traffic through an IP router, the destination MAC address must be set to the MAC address of the router and the destination IP address must be for a valid address within the subnet beyond that router.
    - ❒ When LLC Only is selected, enter the MAC destination address and the contents of the data field.

  Enter Source and Destination Addresses in hexadecimal or press Y Z SPACE to make a station list entry.

For the **Respond to IP Ping** selection, configure the LANMeter instrument’s IP stack first. The IP stack uses the configuration currently set for the Internet TCP/IP tests, which can be different from the Traffic Generator configuration. Refer to Chapter 6 “Testing TCP/IP Networks,” for additional information.

Running Traffic Generator

Use the following procedure to run Traffic Generator:

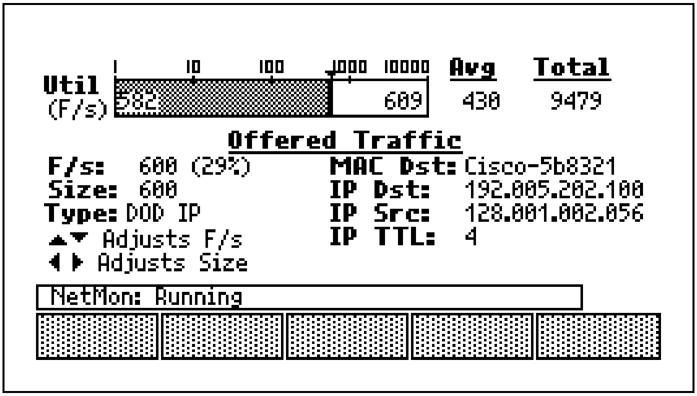
1. Press the top-level **Network Monitor** softkey.
2. Highlight the **Traffic Gen** softkey by pressing it once.
3. Press ◁ or ▷ to configure Traffic Generator for background or IP stack operation, as desired.

   The default is **Do Not Run in Background**. This field can not be stored in non-volatile memory, which means that cycling power results in this field being reset to **Do Not Run in Background**.
4. Press MENU and select **Configure** to access the Traffic Generator Configuration menu. Configure traffic parameters as desired. Refer to the "Configuring Traffic Generator" section for more information.
5. Connect the instrument as described in the "Attaching Cables" section of the *Getting Started* manual.
6. Press the **Traffic Gen** softkey, or press ENTER RUN, to run Traffic Generator. You can also start Traffic Generator while running a compatible test.

Note

While Traffic Generator is running you can adjust the frame rate by pressing △ or ▽, or adjust the frame size by pressing ◁ or ▷. Press and release SHIFT and then press the appropriate arrow key once to increment the frame size or frame rate by one. Take this action with care; the instrument allows you to transmit illegal sized frames.

7. Observe the results. Traffic generator displays a summary of how the traffic is configured along with a horizontal bar chart showing network utilization. Figure 4-13 shows a Traffic Generator sample results.
8. Press EXIT STOP to end the test.



```
       Util  582                609   Avg    Total
      (F/s)                           430    9479
                  Offered Traffic
 F/s:   600 (29%)       MAC Dst: Cisco-5b8321
 Size:  600             IP Dst:  192.005.202.100
 Type: DOD IP           IP Src:  128.001.002.056
 ▲▼ Adjusts F/s         IP TTL:  4
 ◀ ▶ Adjusts Size
 NetMon: Running
```

Figure 4-13. Traffic Generator Sample Results

Chapter 5
Testing Novell NetWare

Introduction

The Enterprise LANMeter can test your NetWare LANs by using the following Novell NetWare tests. The Novell NetWare tests diagnose problems on Novell networks and are accessed by selecting the **Novell NetWare** top-level softkey. Figure 5-1 shows the Novell NetWare softkeys.

❒ Server List
❒ NetWare Ping
❒ NetWare Stats
❒ Routing Analysis
❒ Top NetWare

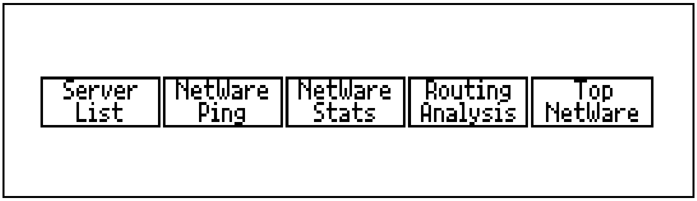


Figure 5-1. Novell NetWare Softkeys

The Novell NetWare tests verify client and server connectivity across IPX routers, compile a list of local or all servers, and identify the attached IPX network number.

It is important to properly connect the instrument to your network. Refer to the "Attaching Cables" section of the *Getting Started* manual for detailed information on attaching cables.

Configuring Novell NetWare Tests

All Novell NetWare tests are configured in a similar manner. It is not necessary to configure a Novell NetWare test unless you want to change the default condition. Use the following procedure to configure all Novell NetWare tests:

1. Press MORE, then press the **Novell NetWare** top-level softkey.
2. Highlight the desired test for configuration.

   The exact steps required to highlight a test depend on which test you want to configure. The first test in a group is automatically highlighted. Otherwise you press the test softkey once.
3. Press MENU. This also selects the **Configure** option.
4. Press ENTER/RUN.
5. Configure the desired parameters.

   Novell NetWare tests have different configuration parameters. Refer to the specific test section for available configuration parameters.

   To undo any configuration changes you made, press MENU, select **Cancel Changes** in the Configuration Menu, and then press ENTER/RUN.
6. Press EXIT/STOP to save your configuration to non-volatile memory and exit the Configuration screen.

Running Novell NetWare Tests

All Novell NetWare tests are run in a similar manner. Use the following procedure to run all Novell NetWare tests:

1. Press [MORE], then press the top-level **Novell NetWare** softkey.
2. Highlight the desired test to run.

   The exact steps required to highlight a test depend on which test you want to run. The first test in a group is automatically highlighted. Otherwise you press the test softkey once.
3. Configure the instrument parameters for the selected test. Refer to the specific test section for information on available configuration parameters.
4. Connect the instrument as described in the “Attaching Cables” section of the *Getting Started* manual.
5. Run the desired test by pressing the test softkey or by pressing [ENTER RUN].
6. Observe the test results. Refer to the individual test sections for information on available results options.
7. Press [EXIT STOP] to end the test.

Description of the Novell NetWare Tests

The following sections describe each Novell NetWare Test:

❒ Server List
❒ NetWare Ping
❒ NetWare Stats (File and Packet Stats)
❒ Routing Analysis
❒ Top NetWare (Top Senders and Top Receivers)

Server List

Server List either displays all servers, file servers, or just the nearest servers on the network, depending on configuration. Server List displays the nearest server for all supported frame types (if the Frame Type is **Auto**) and then displays a list of selected NetWare server types. This information is obtained by requesting the information from NetWare servers.

Configuration Parameters

You can configure the following parameters for Server List (the defaults are underlined):

❐ Timeout parameter as <u>1 second</u> or 5 seconds, 30 seconds.

❐ Ethernet Frame Type as <u>Auto</u>, 802.3, 802.2, Ethernet II, or SNAP (Ethernet only).

Configuring to Auto attempts all Ethernet frame types. It acquires server information from the first Nearest Server listed.

❐ Find All Servers, <u>File Servers</u>, or the Nearest Server.

All Servers lists all of the servers and services in the Novell NetWare network, such as NetWare Loadable Modules (NLMs). File Servers lists all file servers in the Novell NetWare network. Nearest Server emulates the "Nearest Server" request of a workstation login showing which servers are available for login.

If LANMeter can obtain a server list, the list is displayed under Available Servers.

Results

The instrument displays Server List results as the network servers respond. Server List results show the following information. Figure 5-2 shows Server List sample results.

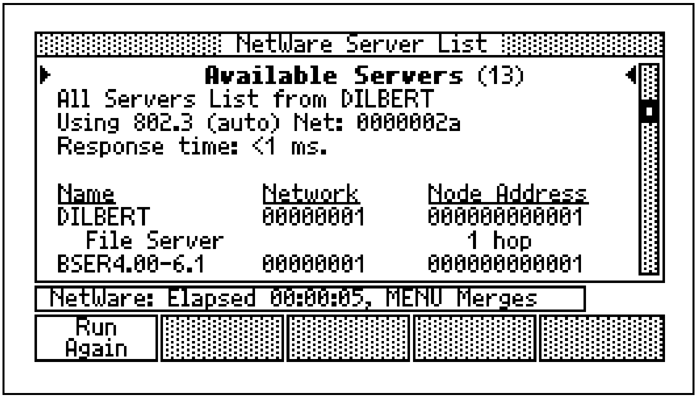
- ❒ Frame Type for Nearest Server (Ethernet only)
- ❒ Local Server Name (Ethernet only)
- ❒ Server Name
- ❒ IPX addresses
- ❒ Address and network number
- ❒ Response time
- ❒ Hops to server

Novell defines a **Hop** as a network. For example, Servers that are one hop away are on the same IPX network as the LANMeter instrument.

You can merge any file servers found into Station List by pressing MENU, then selecting **Merge Stations**.

Note

> *After you use* MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.*



```
NetWare Server List
▶           Available Servers (13)            ◀
  All Servers List from DILBERT
  Using 802.3 (auto) Net: 0000002a
  Response time: <1 ms.

  Name              Network       Node Address
  DILBERT           00000001      000000000001
    File Server                      1 hop
  BSER4.00-6.1      00000001      000000000001
 NetWare: Elapsed 00:00:05, MENU Merges
```

Figure 5-2. Server List Sample Results

Server List often displays more than a full screen of information. You can display servers that are beyond the screen by using △ and ▽.

NetWare Ping

NetWare Ping is a quick way to prove network connectivity to a specific NetWare server or user.

When you highlight the **NetWare Ping** softkey, the instrument prompts you for a **Target** server or workstation address. You can either enter a hexadecimal address (by using the numbers 0 through 9 and letters A through F) or choose a symbolic name from the station list by pressing Y Z SPACE.

NetWare Ping defaults to 802.3 Frame Type for Ethernet networks. If your network uses an Frame Type other than 802.3, you must configure NetWare Ping appropriately, otherwise packets sent by the instrument will not be recognized by the target station, or intermediate routers.

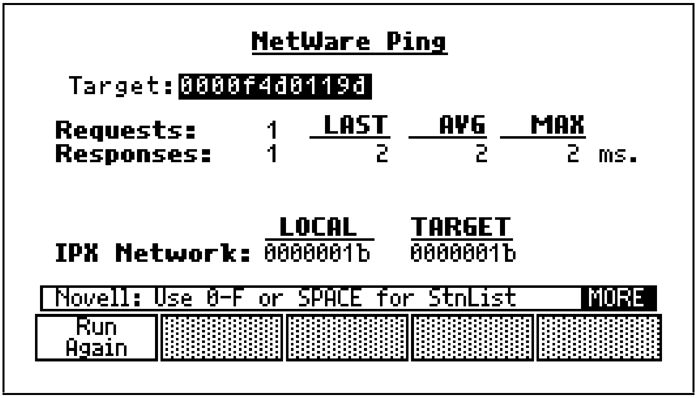
Configuration Parameters

You can configure the following parameters for NetWare Ping (the defaults are underlined):

- ❐ Target address in Hex or press Y Z SPACE to select from Station List. You can also configure the Target address from the NetWare Ping screen.
- ❐ Define the IPX Network. If set to all 0’s, the local IPX number is used.
- ❐ Run as Once or Continuous. When configuring NetWare Ping to run continuously, set the repetition rate with the Timeout Period field.
- ❐ Ethernet Frame Type as 802.3, 802.2, Ethernet II, or SNAP.
- ❐ Timeout as 1 second or 5 seconds.

Results

The instrument displays NetWare Ping results as the network stations respond. NetWare Ping results show the response time to the server or station. Figure 7-3 shows NetWare Ping sample results.



```
                 NetWare Ping
  Target:0000f4d0119d
 Requests:      1   LAST     AVG     MAX
 Responses:     1      2       2       2  ms.

                  LOCAL     TARGET
 IPX Network:  0000001b   0000001b
```

Figure 5-3. NetWare Ping Sample Results

NetWare Stats (File and Packet Statistics)

The **NetWare Stats** softkey accesses the File Statistics and Packet Statistics tests, which identify and isolate the sources of slow performance on a NetWare LAN and quantify the general health of a Novell Server. It automatically recognizes all NetWare IPX frame types. The instrument calculates all statistics at the same time with a 1-second sample period. File Statistics and Packet Statistics test run simultaneously. To display the results of the other test on the same data sample, simply press its softkey while the test is running.

File Statistics and Packet Statistics tests monitor the NetWare traffic for frame types that indicate an overloaded server, and for workstation traffic that indicate server loading (such as, File Requests and Routed traffic).

You can configure the following parameters for File Statistics and Packet Statistics (the defaults are underlined):

Configuration Parameters

❒ To/From a single Server as Off or On. If you select On, then also configure the following parameters:

❒ Filter address in Hex or press Y Z SPACE to select from Station List.

❒ Filter IPX Network address

Results

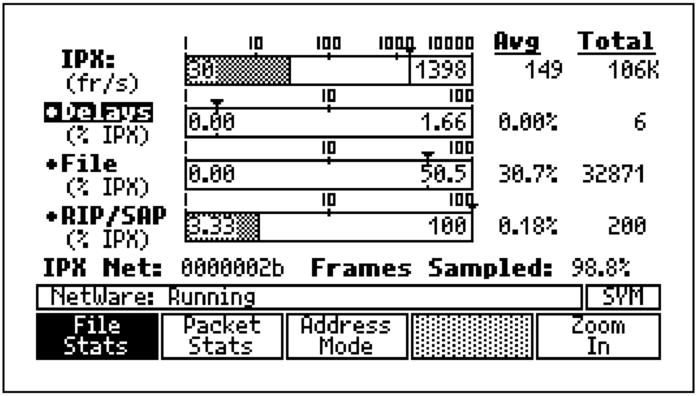
The instrument displays File Statistics and Packet Statistics results after calculating the statistics for the first 1-second sample period and updates these results for each successive sample period.

File Statistics and Packet Statistics tests show IPX frames per second, Delays, and File frames as numerical values and as a bar graph. The bar graph shows current and maximum values. The current value is the shaded portion of the bar with its numerical value inside the bar on the left-hand side. The maximum value is indicated on the graph with a small triangle above the bar with its numerical value inside the bar on the right-hand side. The instrument also shows the details of these measurements as average, and total numerical values in a tabular format. Figure 5-4 shows sample results of the File Statistics test. Packet Statistics test results are similar to the File Statistics test results.

The IPX bar graph displays the total number of IPX (NetWare) frames. The second bargraph displays the number of Delay Packets (also called Request Being Processed packets). Delay packets are transmitted by Novell Servers when they are becoming overloaded. Highlight the Delay packets category and press the **Zoom In** softkey to display a sorted list of the Servers transmitting the most delay packets. Generally, you should see less than 1% delay packets on a NetWare LAN.

The File bargraph tracks the total number of File Requests. Use △ or ▽ to select the File category and press the **Zoom In** softkey to display a sorted list of the clients making the most requests. Identifying a correlation between Delay packets and an excessive number of File Requests helps to track the sources of slow network performance.

The RIP/SAP bargraph track the total number of IPX RIP and IPX SAP packets on the network. Highlight the RIP/SAP category and press the **Zoom In** softkey to view the sources for these packets.



```
                1    10   100  1000 10000   Avg    Total
IPX:
 (fr/s)       30              1398          149    106K
•Delays
 (% IPX)      0.00            1.66          0.00%     6
•File
 (% IPX)      0.00            50.5          30.7%  32871
•RIP/SAP
 (% IPX)      3.33             100          0.18%    200
IPX Net: 0000002b  Frames Sampled: 98.8%
NetWare: Running                              SYM
```

Figure 5-4. File Statistics Sample Results

Routing Analysis

Routing Analysis presents a graphical representation of the source and destination nature of the monitored ring or segment. This test helps identify overloaded segments or rings and allow load balancing of NetWare traffic.

Results

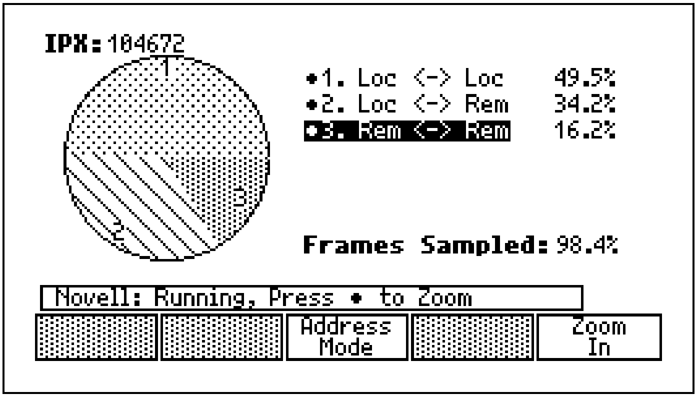
Routing Analysis displays classification results of all Novell traffic into one of the following three categories, as the traffic is monitored. Figure 5-5 shows Routing Analysis sample results.

Local <----> Local — The source and destination IPX addresses are on the IPX network being monitored. None of the traffic travels across a router. In Token Ring networks the traffic may cross source-routed bridges.

Local <----> Remote — Either the source or destination IPX address, but not both, is on another IPX network. That is, one or more routers is crossed.

Remote <----> Remote — Both the source and destination IPX addresses are not on the same network as the network being monitored. This means that this segment, or ring, is being used as a pass-through.

To find out what stations are sending and receiving traffic in each category, highlight the desired category by pressing △ or ▽ and press the **Zoom In** softkey.



```
IPX: 104672
•1. Loc <-> Loc    49.5%
•2. Loc <-> Rem    34.2%
•3. Rem <-> Rem    16.2%

Frames Sampled: 98.4%
Novell: Running, Press • to Zoom
```

Figure 5-5. Routing Analysis Sample Results

Interpreting Routing Analysis Results

Routing Analysis is most useful if you know your network topology. You should know the relative locations of the segment or ring being monitored and of the busy servers or workstations to properly interpret the results. The results can vary greatly from segment to segment.

For example, if you are monitoring a backbone segment, or ring, most of the traffic should be Remote to Remote. This should not be true if you are monitoring a workgroup LAN. Workgroup LANs normally have Local to Local traffic.

Top NetWare (Top Senders and Top Receivers)

The **Top NetWare** softkey accesses the Top Senders and Top Receivers tests, which track the top senders and receivers of Novell NetWare (IPX) traffic. Top Senders and Top Receivers tests run simultaneously. Once you run Top Senders or Top Receivers, you can observe the results of the other test simply by pressing its softkey.

Novell NetWare Top Senders and Top Receivers track stations by their IPX network number and address, while Network Monitor Top Senders and Receivers track stations by their MAC address. Novell NetWare Top Senders and Receivers looks beyond the MAC addresses (of intermediate routers) to the network layer and observes the actual client and server network addresses.

Note

When a network passes a packet through a NetWare router, the router retransmits the packet using its own MAC address. This leaves the network layer addresses untouched. The instrument gets an accurate picture of the end-to-end traffic by observing network layer addresses.

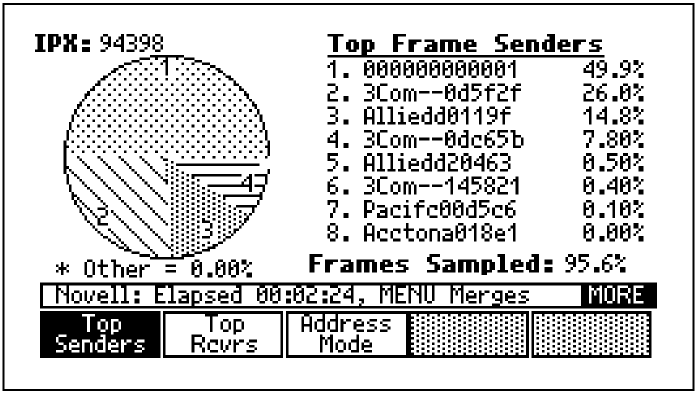
Configuration Parameters

You can configure the following parameters for Top Senders and Top Receivers (the defaults are underlined):

- ❒ Senders to a single station as <u>Off</u> or On. If you select On, then also configure the following parameters:
- ❒ Filter address in Hex or press Y Z SPACE to select from Station List.
- ❒ IPX Number in Hex.

Results

The instrument displays Top Senders and Top Receivers results as Novell sending or receiving stations are monitored on the network. The Top Senders and Top Receivers tests display results in percent of Novell traffic and in a pie chart that identifies the senders, or receivers, and shows the quantity of Novell traffic transmitted. Figure 5-6 shows Top Senders sample results and Top Receivers results are similar to that of Top Senders.



```
IPX: 94398                    Top Frame Senders
                              1. 000000000001     49.9%
                              2. 3Com--0d5f2f     26.0%
                              3. Alliedd0119f     14.8%
                              4. 3Com--0dc65b     7.80%
                              5. Alliedd20463     0.50%
                              6. 3Com--145821     0.40%
                              7. Pacifc00d5c6     0.10%
                              8. Acctona018e1     0.00%
 * Other = 0.00%             Frames Sampled: 95.6%
Novell: Elapsed 00:02:24, MENU Merges         MORE
```

Figure 5-6. Novell NetWare Top Senders Sample Results

You can press **Address Mode**, while the results are displayed, to access a menu for presenting the station address as symbolic name, hexadecimal address, or IPX network number.

After you stop the test by pressing EXIT STOP, you can view the last results by pressing MENU, then selecting **Last Result**. Also, after stopping the test, you have the option to merge any discovered IPX addresses into the IPX Station List by pressing MENU, then selecting **Merge Stations**.

Note

You must run the Station List measurement and exit to save the merged stations into non-volatile memory. You can also select `Save List` *from the* **MENU** *key selection in the Station List measurement to permanently save the merged stations.*

To print (or save a print file of) all NetWare Senders and Receivers in ASCII form, press SHIFT, then PRINT after the test has stopped.

Chapter 6
Testing TCP/IP Networks

Introduction

The Fluke Enterprise LANMeter (68x Series) can test and diagnose problems on your TCP/IP networks by using one of the following Internet TCP/IP tests:

- IP Auto Config
- Segment Discovery
- MultiPort Stats *
- Trace Route
- Internet Toolkit
- Scan Host
- ICMP Monitor
- ICMP Ping
- Top IP (Top Senders and Top Receivers)
- IP Matrix

* Optional, see Chapter 7 “SwitchWizard Option”

The Internet TCP/IP tests are accessed by selecting the **Internet TCP/IP** top-level softkey. Figure 6-1 shows the softkey selections.

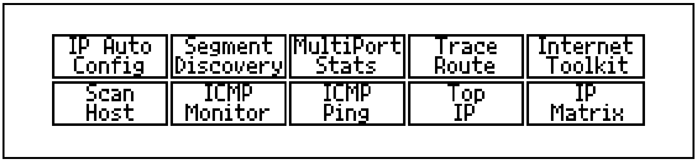


Figure 6-1. Enterprise LANMeter Internet TCP/IP Softkeys

Refer to the appropriate section in this chapter for more information on the desired test. The SwitchWizard option and MultiPort Statistics test are covered in the “SwitchWizard’s MultiPort Statistics Test” section in Chapter 7 “SwitchWizard Option.”

You can use Internet TCP/IP Enterprise LANMeter tests to determine which IP networks you are connected to and to obtain important network and host information. This is done by sending queries and by monitoring network activity.

The Internet TCP/IP tests launch an IP stack that enables the LANMeter instrument to respond to other stations on the network. The IP stack remains running after the Internet TCP/IP tests are run (except IP Auto Config). A LANMeter instrument will respond to Ping, Trace Route, and SNMP queries while its IP stack is running. This enables the instrument to be used with other LANMeter instruments or network management applications. The IP stack is turned off when you run any test other than the Internet TCP/IP tests or the Traffic Generator when configured for Respond to IP Ping.

For the Segment Discovery, Trace Route, and Scan Host tests, you can select any available IP host and then press **Use Toolkit** to gain access to more detailed information. Refer to the “Using Hyperlink Tests” topic in this chapter for an example of using the Toolkit via hyperlinks.

For all Internet TCP/IP tests, the Enterprise LANMeter can display device names by accessing DNS servers or by using the Station List.

Attaching Cables

It is important to properly connect the instrument to your network. For connecting your LANMeter instrument to your network, refer to the “Attaching Cables” section in the “*Getting Started*” manual for detailed information on attaching cables.

Configuring Enterprise LANMeter’s IP Parameters

The Enterprise LANMeter’s current IP address parameters are displayed when the **IP Auto Config** softkey is highlighted. It is not necessary to configure the instrument’s IP parameters unless you want to change the currently displayed settings. For the most complete and accurate results, it is recommended that the LANMeter instrument’s IP configuration be correct for the network you plan to access. If some parameters are not correct the Enterprise LANMeter could provide incomplete results.

The LANMeter instrument can assist you in configuring its IP parameters by running the IP Auto Config test or you can manually configure these parameters by using the following procedure. Refer to the "IP Auto Config" topic in the "Description of Internet TCP/IP Tests" section for more information on automatic configuration.

Manually Configuring Enterprise LANMeter

Use the following procedure to manually configure the LANMeter instrument:

1. Press the **Internet TCP/IP** top-level softkey.
2. Highlight the desired test for configuration.

   The exact steps required to highlight a test depend on which test you want to configure. The first test is automatically highlighted. Otherwise, either press the test softkey once, or press MORE, then press the test softkey once (for the second row of tests).
3. Press MENU and select **Configure**.
4. Press ENTER/RUN and then configure the desired parameters.

   Refer to the specific test section for available configuration parameters.

   To undo any configuration changes you make but haven't saved, press MENU, select **Cancel Changes**, and then press ENTER/RUN.
5. Press EXIT/STOP, or ENTER/RUN, to save the configuration to non-volatile memory and exit the configuration screen.
6. To restore a configuration to its default values, select the desired test, press MENU, select **Configure**, press ENTER/RUN, press MENU again, and then select **Restore Defaults** and press ENTER/RUN again.

The following are the Enterprise LANMeter’s IP configuration parameters:

- ❒ Source IP address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).
- ❒ Default Router address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).
- ❒ Default Mask as dotted decimal (press the **Show Choices** softkey to select from a list of legal masks).
- ❒ Use DNS as <u>Yes</u> or No. (Use ◁ or ▷ to toggle.) When you select Yes you can configure the DNS address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).
- ❒ Enter your SNMP Community name by using the alphanumeric keys. It is case sensitive and the default is **public**. You can use the softkeys to enter a special character or to edit your entry.

  A blank community string will disable SNMP queries in the Segment Discovery and Scan Host tests.

Configuring Internet TCP/IP Test Targets

To use the Scan Host, Trace Route, and Internet Toolkit tests, you need to configure a target IP address. You can configure this target address as dotted decimal, after highlighting the desired test. You can select the target address from the current Station List after pressing Y Z SPACE.

Running Internet TCP/IP Tests

All Internet TCP/IP tests are run in a similar manner. Use the following procedure to run all Internet TCP/IP tests.

1. Verify that the LANMeter instrument is connected properly.
2. Press the top-level **Internet TCP/IP** softkey.
3. Configure the Enterprise LANMeter's IP parameters, if needed, by running **IP Auto Config** or manually by using the procedure in the "Configuring Enterprise LANMeter's IP Parameters" section earlier in this chapter.
4. Highlight the desired test to run.

   The exact steps required to highlight a test depend on which test you want to run. The first test is automatically highlighted. Otherwise, you either press the test softkey once or press MORE, then press the test softkey once (for the second row of tests).
5. Configure the target IP address (if needed).
6. Run the desired test by pressing the test softkey or by pressing ENTER RUN.
7. Observe the test results. Refer to the individual test sections for information on available results options. The LANMeter instrument displays information on the Status Line to indicate activity.
8. Press EXIT STOP to end the test (if needed).

Note

Some IP hosts may not respond to an Internet TCP/IP test (such as Ping or Trace Route) the very first time. If this occurs, it is most likely due to the LANMeter instrument not yet being in the other host's Address Resolution Protocol (ARP) cache. If this is the case, run the test again.

Whenever the LANMeter instrument starts to run an Internet TCP/IP test, it first checks to see if the currently configured Source IP address is already in use by another IP host (i.e. a duplicate IP address). If your LANMeter instrument is using a duplicate IP, the instrument aborts the current test and displays an error message.

Using Hyperlink Tests

This section covers how to use hyperlink tests and shows an example test using the hyperlink functions:

Hyperlink Tests

Hyperlink tests provide the LANMeter instrument with the ability to jump to additional tests which provide a greater detail of information on a particular point of interest. Refer to the following example to see how hyperlinks can be used.

The LANMeter instrument provides access to hyperlink tests from Internet TCP/IP tests by providing links to the Internet Toolkit. Use the following procedure to execute a hyperlink test:

1. Highlight the desired hyperlink field from one of the Internet TCP/IP test results screens by using TAB. You can identify the hyperlink fields because they are underlined.
2. Press **Use Toolkit**, or ENTER RUN.
3. Select the desired Internet Toolkit tool. Refer to the "Internet Toolkit" section for more information.
4. Configure the tool if needed. Refer to the "Internet Toolkit" section for more information.
5. Press **Run Tool**, or ENTER RUN.
6. Press **Leave View** and then press **Exit Toolkit** to return back to the original Internet TCP/IP test screen.

When you are running a hyperlink test in Toolkit, you can press EXIT STOP repeatedly to return to the calling test and then stop the test. Pressing EXIT STOP more will return you to the top-level softkeys.

Whenever you press **Use Toolkit** the currently running test is suspended until you exit the Toolkit.

Example Test Using Hyperlink Tests

You can utilize LANMeter instrument hyperlinks to "drill-down" into a troubleshooting problem. This example shows how hyperlinks into the Internet Toolkit provide a powerful troubleshooting capability.

In the network scenario shown in Figure 6-2, a user has reported a performance problem between Server #1 and PC #2. The end-user's PC is at a remote site to yours, but since the server is at your site, you are responsible for troubleshooting problems involving that machine.

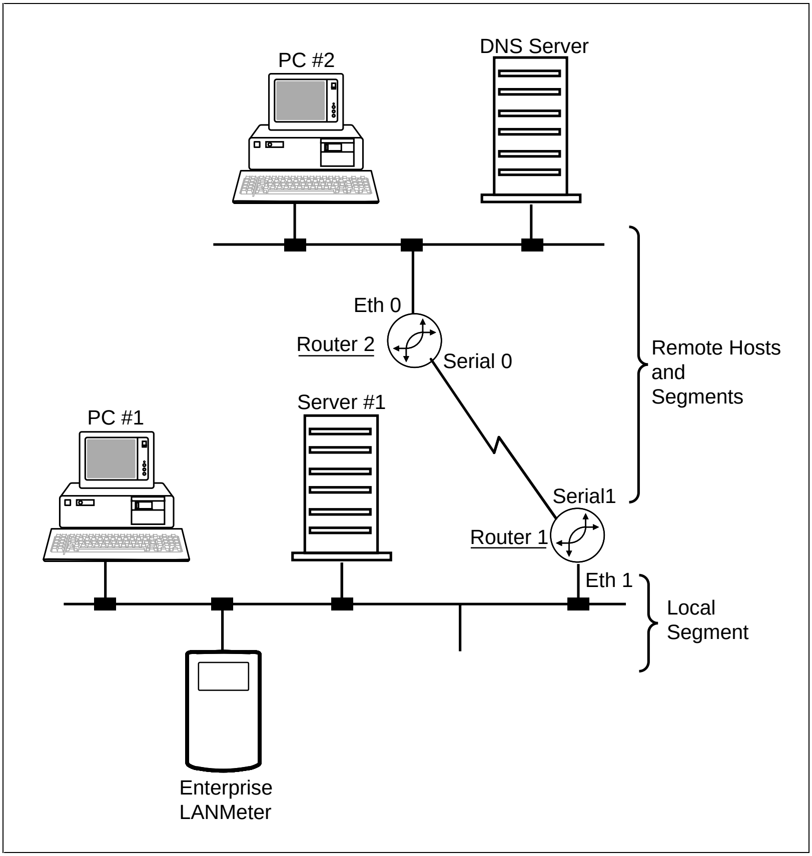
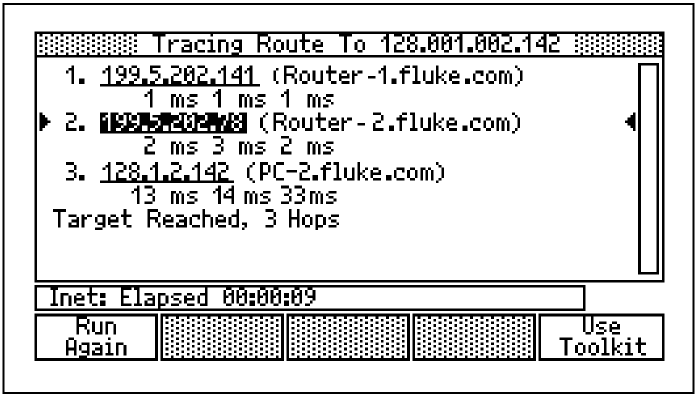


Figure 6-2. Hyperlinks Example Network

You can quickly determine that the local segment is healthy by connecting the LANMeter instrument onto the local Ethernet segment and running the Network Monitor test. You can then use the Internet TCP/IP's Trace Route test to see if there are any problems from the local segment to the end-user's PC.

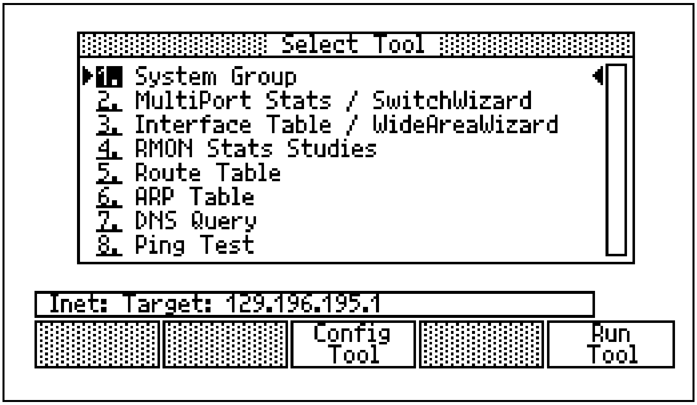
The Trace Route test results, shown in Figure 6-3, show that there is a large response time delay between the end-user's PC (PC #2) and the remote Router #2.



```
Tracing Route To 128.001.002.142
  1. 199.5.202.141 (Router-1.fluke.com)
        1 ms 1 ms 1 ms
▶ 2. 199.5.202.78 (Router-2.fluke.com)          ◀
        2 ms 3 ms 2 ms
  3. 128.1.2.142 (PC-2.fluke.com)
       13 ms 14 ms 33ms
 Target Reached, 3 Hops
Inet: Elapsed 00:00:09
```

Figure 6-3. Trace Route Results

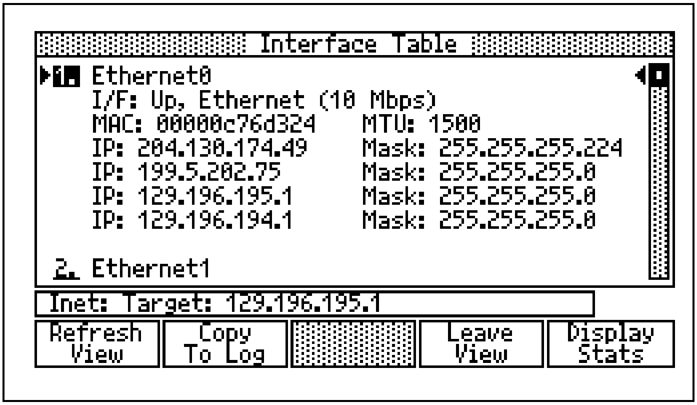
The performance to Router #2 is acceptable, so you need to see what information Router #2 can provide about the Ethernet interface on the other side of the router. Use the arrow keys to select the Router #2 hop and then press **Use Toolkit**. Figure 6-4 shows the Toolkit Menu.



```
Select Tool
▶1. System Group                            ◀
 2. MultiPort Stats / SwitchWizard
 3. Interface Table / WideAreaWizard
 4. RMON Stats Studies
 5. Route Table
 6. ARP Table
 7. DNS Query
 8. Ping Test
Inet: Target: 129.196.195.1
```

Figure 6-4. Toolkit Menu

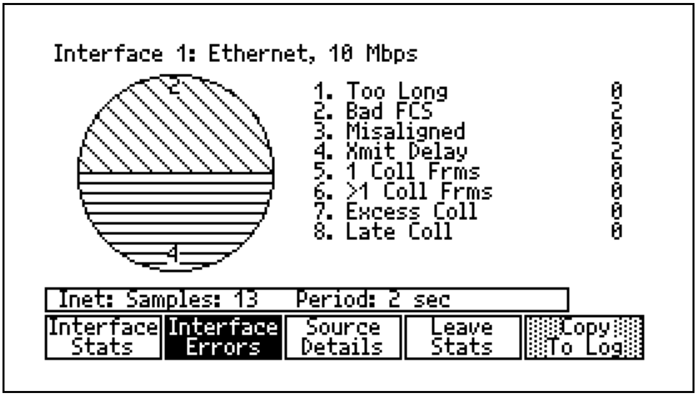
You can select the remote interface for analysis by selecting **Interface Table (SNMP)** from the Toolkit menu and pressing ENTER RUN; refer to Figure 6-5.



```
Interface Table
1. Ethernet0
   I/F: Up, Ethernet (10 Mbps)
   MAC: 00000c76d324     MTU: 1500
   IP: 204.130.174.49    Mask: 255.255.255.224
   IP: 199.5.202.75      Mask: 255.255.255.0
   IP: 129.196.195.1     Mask: 255.255.255.0
   IP: 129.196.194.1     Mask: 255.255.255.0

2. Ethernet1
Inet: Target: 129.196.195.1
```

Figure 6-5. Interfaces on Router

Interface Table displays a combination of the MIB II Interface table and the MIB II IP Address table. Shown together, you can see which interface you want to analyze. Pressing **Display Stats** starts the SNMP polled statistics for that device and interface; refer to Figure 6-6.



```
Interface 1: Ethernet, 10 Mbps
1. Too Long          0
2. Bad FCS           2
3. Misaligned        0
4. Xmit Delay        2
5. 1 Coll Frms       0
6. >1 Coll Frms      0
7. Excess Coll       0
8. Late Coll         0
Inet: Samples: 13   Period: 2 sec
```

Figure 6-6. Interface Statistics via SNMP

The interface statistics errors for Router #2 shows that many frames that were sent by Router #2 became collisions (especially Late Collisions). Late Collisions are often an indication of cable problems due to signal attenuation (or loss) because of cable faults. You can now troubleshoot the cause of the problem on the affected LAN segment.

Description of Internet TCP/IP Tests

The following sections describe the Internet TCP/IP LANMeter instrument tests:

- IP Auto Config
- Segment Discovery
- MultiPort Stats *
- Trace Route
- Internet Toolkit
- Scan Host
- ICMP Monitor
- ICMP Ping
- Top IP (Top Senders and Top Receivers)
- IP Matrix

* Optional, see Chapter 7 “SwitchWizard Option”

IP Auto Config

The current LANMeter instrument IP configuration is listed on the information tag that is shown on the screen when you highlight **IP Auto Config**. You can use IP Auto Config in one of the following discover Modes:

- Assisted
- Use BOOTP
- Use DHCP

Use the following procedure to run IP Auto Config:

1. Press the top-level **Internet TCP/IP** softkey. This also highlights the **IP Auto Config** softkey.
2. Press **IP Auto Config**, or ENTER RUN.
3. Use ◁ or ▷ to select the desired discover Mode (from the configuration popup menu).

4. Use ▽ to move down to the Timeout field. Use ◁ or ▷ to select the desired Timeout period (from the configuration popup menu).

5. Press ENTER RUN to run the test.

   Refer to the following sections for information on running the different discover modes.

6. Press **Save Config** or EXIT STOP to save the displayed configuration parameters, press **Edit Config** to modify the displayed parameters, or press **Cancel Config** to cancel the discovered configuration.

Assisted Discover Mode

Use the Assisted Discover Mode to have the LANMeter instrument help you configure its IP parameters. The IP Auto Config test first assists you in selecting an IP address for your LANMeter instrument and then it searches for the remainder of its network configuration parameters:

❒ The correct IP subnet mask
❒ A usable IP default router
❒ A usable Domain Name Service (DNS) server

Figure 6-7 shows the IP Auto Config results screen.

Note

> *For ease of configuration, you may want to always use the same host number for your LANMeter instrument's IP address. For example, host numbers 81 and 82 could be reserved on all networks for your LANMeter instrument.*

For Assisted Discover Mode, all of the IP network traffic addresses (local and non-local) are displayed as they are discovered. You can wait for the timeout period to expire or you can press ENTER RUN to skip the remaining time and proceed to the next step. The most frequently observed local IP network address is displayed for your selection. Use the following procedure to continue:

1. Select the desired IP network for your LANMeter instrument from the available list by pressing **Show Choices**. Select the IP network and then press ENTER RUN.

The LANMeter instrument displays **`(Local)`** next to the networks that are on the local segment.

2. Enter the host octet portion(s) of the IP address for your LANMeter instrument to use and press [ENTER RUN]. The LANMeter instrument then checks to see if the configured IP address is already in use by another host. If there is a duplicate IP address, you will be prompted to enter a different host octect.

   Your LANMeter instrument continues to search for the remainder of its network configuration parameters for the timeout period.

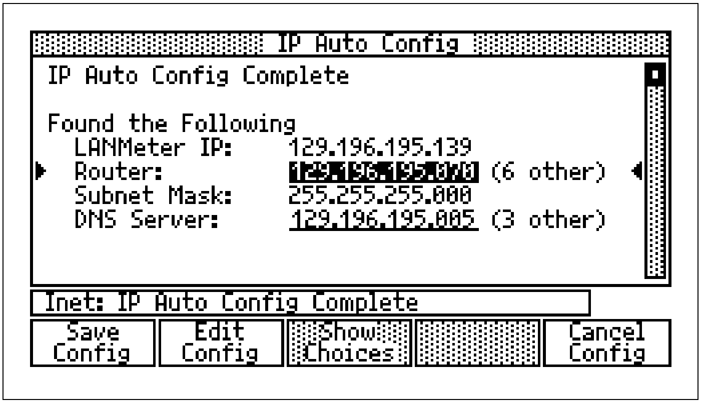
3. Select and accept the remaining discovered router, subnet mask, and DNS server parameters.

   Again, you can wait until the timeout period expires or you can press [ENTER RUN] to stop the discovery process.

4. Use [△] or [▽] to select one of the desired parameters if more than one choice is available (such as, **Router**) by pressing **Show Choices,** or [Y Z SPACE], select the parameter value, and then press [ENTER RUN].

5. Repeat step 4 for all parameters that you want to change.

6. Press **Save Config** or [EXIT STOP] to save and accept the displayed configuration parameters, press **Edit Config** to save the displayed configuration and to modify the desired parameters, or press **Cancel Config** to cancel the discovered configuration.



```
IP Auto Config

IP Auto Config Complete

Found the Following
  LANMeter IP:    129.196.195.139
▶ Router:         129.196.195.070 (6 other)  ◀
  Subnet Mask:    255.255.255.000
  DNS Server:     129.196.195.005 (3 other)

Inet: IP Auto Config Complete
```

Figure 6-7. IP Auto Config (Assisted Mode) Results Screen

Use BOOTP Discover Mode

The Use BOOTP Discover Mode is a simple process that requests the LANMeter instrument’s IP configuration from a preconfigured BOOTP server.

The following is a sample BOOTP configuration file:

```
allhost:\
        :ds=199.5.202.100:\
        :sm=255.255.255.192:\
        :gw=199.5.202.73:
lanmeter:ht=1:ha=0x00C017760003:ip=199.5.202.120:tc=allhost
```

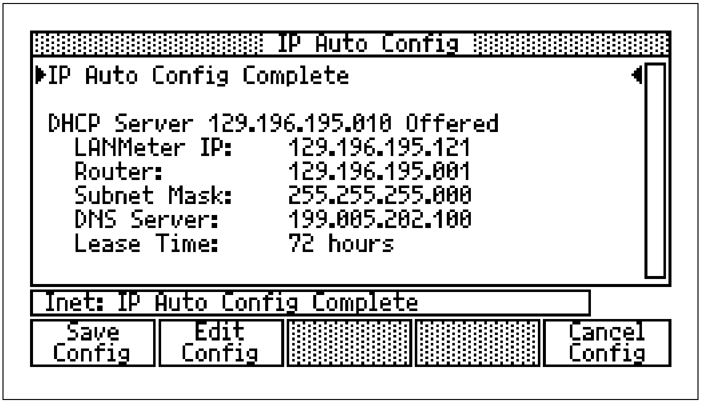
The following information defines the variables you need to modify in a sample BOOTP configuration file:

ds = Domain Name Server
sm = subnet mask
gw = default gateway
ha = LANMeter’s MAC address
ip = the IP address to assign to LANMeter

Use DHCP Discover Mode

A Dynamic Host Configuration Protocol (DHCP) server can provide the LANMeter instrument with a source IP address, default router, subnet mask, and DNS server. Select `Use DHCP` for the Discover Mode parameter and the LANMeter instrument’s IP configuration will be provided by a configured DHCP server. The LANMeter instrument automatically renews the DHCP lease any time the instrument’s IP stack is running. Figure 6-8 shows the results of IP Auto Config using DHCP discovery mode.

The LANMeter instrument is unable to renew the lease if a) the DHCP server is down or b) the LAN connection to the server is lost. In either case a warning popup will be displayed indicating that the measurement has been stopped. This is to prevent a possible duplicate IP situation from occurring.



```
▶IP Auto Config Complete

 DHCP Server 129.196.195.010 Offered
   LANMeter IP:    129.196.195.121
   Router:         129.196.195.001
   Subnet Mask:    255.255.255.000
   DNS Server:     199.005.202.100
   Lease Time:     72 hours

Inet: IP Auto Config Complete
```

Figure 6-8. IP Auto Config (DHCP Mode) Results Screen

Segment Discovery

Segment Discovery analyzes the attached IP network and catalogs the key IP network attributes and key systems while it searches for network problems (such as duplicate IP addresses and advertised services that are not available). The Segment Discovery test transmits various frames to solicit responses from hosts on the network in addition to passively monitoring traffic. The Key Devices feature of Segment Discovery is a quick mechanism for verifying connectivity and up/down status of important devices (e.g. servers or routers) even if they are not on your intranet. You can designate up to twenty key devices.

The Segment Discovery test requires that an appropriate LANMeter instrument IP address be configured. If you wish to designate and monitor key devices on your network then they must be configured. No other configuration is necessary for Segment Discovery.

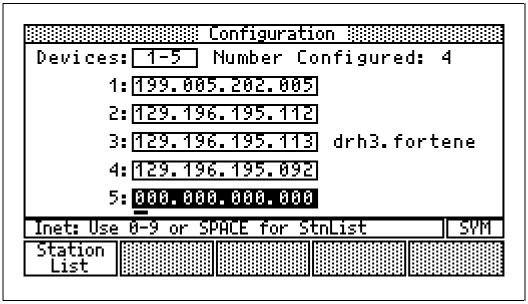
Note

If IP connectivity problems exist you may need to reconfigure your LANMeter instrument to the same IP subnetwork as the target host in order to use the Toolkit's SNMP tests.

Configuring Key Devices

Use the following procedure to configure Key Devices:

1. Press the top-level **Internet TCP/IP** softkey.
2. Press the **Segment Discovery** softkey, then press MENU.
3. Use the up and down arrow keys to select **Key Devices** and then press ENTER/RUN. Figure 6-9 shows a sample configuration menu.



```
Configuration
Devices: 1-5   Number Configured: 4
        1: 199.005.202.005
        2: 129.196.195.112
        3: 129.196.195.113  drh3.fortene
        4: 129.196.195.092
        5: 000.000.000.000
Inet: Use 0-9 or SPACE for StnList    SYM
Station
 List
```

Figure 6-9. Key Devices Sample Configuration Display

4. Use the **Show Choices** softkey or ◁ or ▷ to select the block of device numbers to configure. Use △ or ▽ to select a particular device to configure. Up to twenty key devices may be designated.
5. Configure the device address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).
6. Press EXIT/STOP, or ENTER/RUN, to save your configuration to non-volatile memory and exit the Configuration screen.
7. If any of your designated key devices are RMON agents then Segment Discovery will report them as such as long as SNMP discovery is turned on. SNMP discovery is turned on when the SNMP Community String is configured. Verify that the SNMP community string is configured by pressing the MENU key again. The SNMP community string is used for SNMP discovery and by the Internet Toolkit. **Key Devices** always uses the **`rmon`** community string for RMON discovery.
8. Use the arrow keys to select the **Configure** option and then press ENTER/RUN.

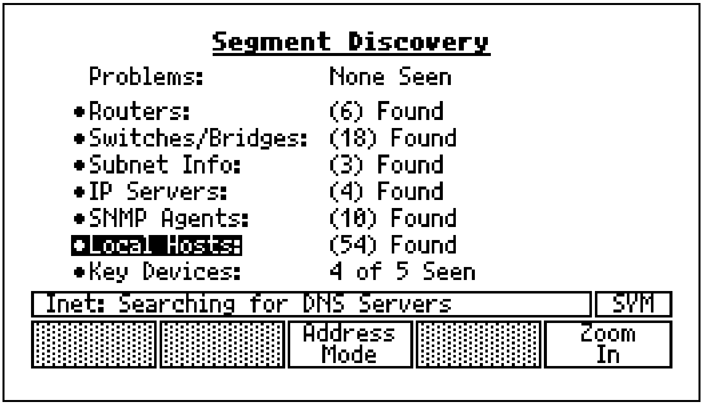
9. Verify that the SNMP Community string is enabled. In order to change the string, use the arrow keys to highlight the string and then either use the **Show Choices** softkey or enter from the keyboard a new community string. You can use the softkeys to enter a special character or to edit your entry.

10. Press EXIT STOP, or ENTER RUN, to save your configuration to non-volatile memory and exit the configuration screen.

11. Press ENTER RUN or the **Segment Discovery** softkey to run Segment Discovery.

Results

The Segment Discovery test results are displayed as they are discovered. Your LANMeter instrument uses a combination of traffic monitoring and active queries in its discovery process. Figure 6-10 shows the Segment Discovery Results Screen.



```
             Segment Discovery
  Problems:           None Seen
 •Routers:            (6) Found
 •Switches/Bridges:   (18) Found
 •Subnet Info:        (3) Found
 •IP Servers:         (4) Found
 •SNMP Agents:        (10) Found
 •Local Hosts:        (54) Found
 •Key Devices:        4 of 5 Seen
Inet: Searching for DNS Servers     SYM
```

Figure 6-10. Segment Discovery Results Screen

Note

If your Segment Discovery results include ***Switches/Bridges*** *your LANMeter instrument has SwitchWizard capabilities. Refer to Chapter 7 “SwitchWizard Option,” for information on SwitchWizard for Segment Discovery.*

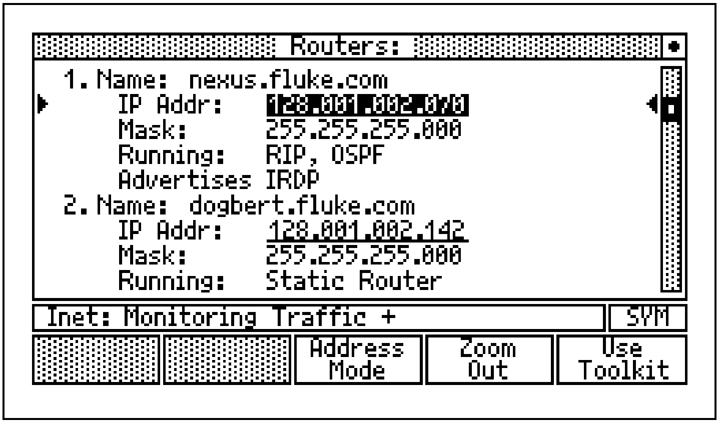
The Status Line shows an activity symbol when the Segment Discovery test is running. The following are the results that the Segment Discovery test can show:

1. A list of identified problems with hosts on the attached network. These problems include, hosts with duplicate IP addresses and misconfigured subnet masks. Problem reporting is suppressed for about the first 30 seconds while the LANMeter instrument attempts to verify any detected problem or problems. After this time, problems are reported when detected.

2. A list of IP routers on this LAN.

   This includes the IP routing protocols they run on this segment and subnet mask (if discovered).

   Figure 6-11 shows an example Routers Information Screen.



```
Routers:
 1. Name:  nexus.fluke.com
     IP Addr:    128.001.002.070
     Mask:       255.255.255.000
     Running:    RIP, OSPF
     Advertises IRDP
 2. Name:  dogbert.fluke.com
     IP Addr:    128.001.002.142
     Mask:       255.255.255.000
     Running:    Static Router
Inet: Monitoring Traffic +                SVM
```

Figure 6-11. Routers Information Screen

Segment Discovery finds routers by monitoring and analyzing routing protocols, by monitoring automatic discovery mechanisms (such as IRDP), and by analyzing off-network traffic going through a host (for static routers).

If the Name field is blank, your LANMeter instrument was unable to resolve the address to name translation.

3. A list of discovered Switches and Bridges. This is only available if you have purchased the SwitchWizard Option. Refer to Chapter 9 "SwitchWizard Option," for more information.

4. A list of IP subnets in use on this IP broadcast domain.

   This includes the subnet number and address class (A, B, or C), the legal host address range for this subnet, the proper IP broadcast address and the subnet mask in use.

5. A list of accessible servers on this LAN, which can include DHCP servers, BOOTP servers, WINS servers and DNS name servers.

   DHCP servers and BOOTP servers can provide automatic configuration data for end-nodes. Details from DHCP queries include host IP configuration options.

   DNS name servers can provide domain names for given IP addresses or IP addresses for domain names. WINS servers can provide the IP address associated with a given NetBIOS name.

6. A list of SNMP agents on this LAN. Segment Discovery attempts the default community string of "public" in addition to the community string that you have configured. Reported agents have either responded to the LANMeter instrument queries, or were observed transmitting SNMP data to some other host.

   SNMP discovery mode must be enabled for Segment Discovery to query potential SNMP agents. If discovery mode is not enabled then Segment Discovery will only passively discover SNMP agents. SNMP discovery mode is enabled when the SNMP Community String is enabled. Refer to the previous "Configuring Enterprise LANMeter's IP Parameters" section in this chapter.

7. A list of local hosts. Local hosts are hosts that are identified as being part of the same IP broadcast domain as your LANMeter instrument.

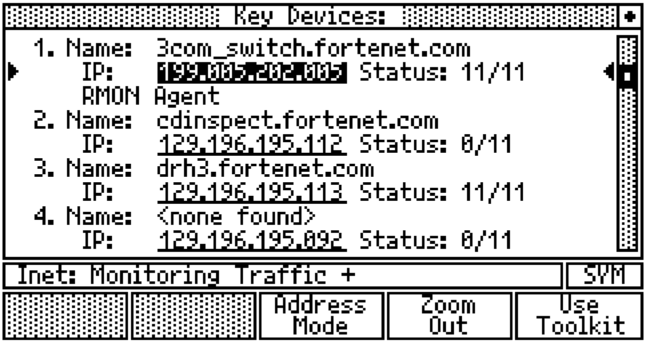
   Segment Discovery monitors and prompts local IP hosts to identify themselves. By using the **Zoom In** softkey you can view the IP and MAC addresses for these local IP hosts, even if their IP address is incorrect for the connected segment. You can highlight any discovered IP address and then press **Use Toolkit** to obtain information on that host.

8. A list of key devices and how many are reachable. **Key Devices** is a list of user specified stations that are designated as important. Up to twenty

devices may be designated. You must configure your key devices prior to running Segment Discovery. Refer to the previous section “Configuring Key Devices.”

Key Devices reports how many of these stations respond to an ICMP ping. If a station responds to the ping, then Key Devices will query it to determine if it is an RMON agent. Key Devices also indicates whether a device is a server, router, or switch if the device is local to the segment that the LANMeter instrument is connected. SNMP discovery mode must be enabled for Key Devices to determine if a station is an RMON agent. Refer to the previous section “Configuring Key Devices” for information on enabling SNMP discovery.

Figure 6-12 shows an example Key Devices results display.



```
                 Key Devices:
  1. Name:  3com_switch.fortenet.com
     IP:    199.005.202.005 Status: 11/11
     RMON Agent
  2. Name:  cdinspect.fortenet.com
     IP:    129.196.195.112 Status: 0/11
  3. Name:  drh3.fortenet.com
     IP:    129.196.195.113 Status: 11/11
  4. Name:  <none found>
     IP:    129.196.195.092 Status: 0/11
Inet: Monitoring Traffic +                SYM
```

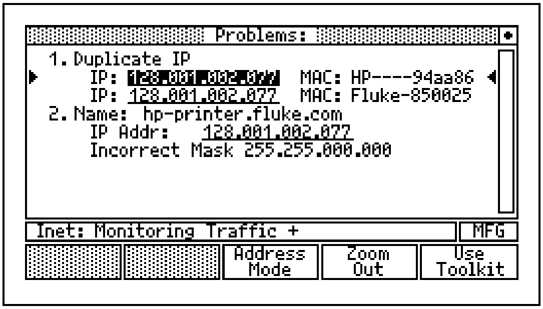
Figure 6-12. Key Devices Sample Result

The status line in the display shows the number of times that each device responded to the ICMP pings over the number of pings sent. The 0/11 status in Figure 6-13 indicates that the device is down or unreachable. Devices acting as RMON agents have the `RMON Agent` identifier on the line after the IP address. You can highlight the IP address of any responding device and then press the **Use Toolkit** softkey to obtain information on that station.

Problem Solving

One feature of the Segment Discovery test is to discover hosts which have duplicate IP addresses. Using the Internet Toolkit you can then make directed SNMP queries at each host, using the unique MAC address to communicate with each host. You can then analyze each host with SNMP to identify the problem host.

Figure 6-13 shows an example Segment Discovery Problems screen.



```
  1. Duplicate IP
▶     IP: 128.001.002.077  MAC: HP----94aa86 ◀
      IP: 128.001.002.077  MAC: Fluke-850025
  2. Name:  hp-printer.fluke.com
      IP Addr:    128.001.002.077
      Incorrect Mask 255.255.000.000
Inet: Monitoring Traffic +
```

Figure 6-13. Segment Discovery Problems Screen

Merging Stations

After your LANMeter instrument has found new stations and you have stopped the test, you can merge these stations along with their DNS names (if available) into the Station List by using MENU, **Merge Stations**. To save the new Station List into non-volatile memory you must enter and then exit the Station List measurement by pressing **Setup/Utils**, **Station List**, and then EXIT STOP. This merges IP addresses into the IP list and MAC addresses into the MAC list. DNS lookups are performed as a background process and it may take several minutes for DNS names to appear on large subnetworks.

MultiPort Stats

The MultiPort Statistics test is an optional feature and is described in Chapter 7 “SwitchWizard Option”.

Trace Route

Trace Route determines the path that IP packets take from the LANMeter instrument to a specified destination host and reports each router encountered.

The instrument traces the IP packet's route using low values for the IP protocol Time-to-Live parameter to elicit an ICMP TIME_EXCEEDED response from each router encountered. Each hop is tested three times to help identify changing routes within a path.

Trace Route also provides hyperlink access to the devices along the path from the LANMeter instrument to the test target.

This information can be instrumental in identifying problem areas on your IP internetwork. For more information on interpreting results, refer to the "Interpreting Trace Route Results" section in this chapter.

You can use Trace Route to diagnose the cause of serious performance or connectivity problems in IP networks (such as identifying potential performance bottlenecks).

Each of the discovered IP addresses along the path has a link to the Internet Toolkit test. You can select an IP address and press **Use Toolkit** to see more details on that host.

One specific use of the Trace Route test is to determine the location of a large increase in response time over one particular path segment.

Configuration Parameters

You can configure the following parameters for Trace Route by pressing MENU, selecting **Configure**, and pressing ENTER RUN:

❒ Target IP address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).

❒ Source IP address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).

❒ Default Router IP address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).

❒ Domain Name Server (DNS) IP Address. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).

❒ Start Hop Count. (The default is 1.)

❒ Maximum Hop Count. (The default is 30.)

❒ Use DNS as Yes or No. (Use ◁ or ▷ to toggle.)

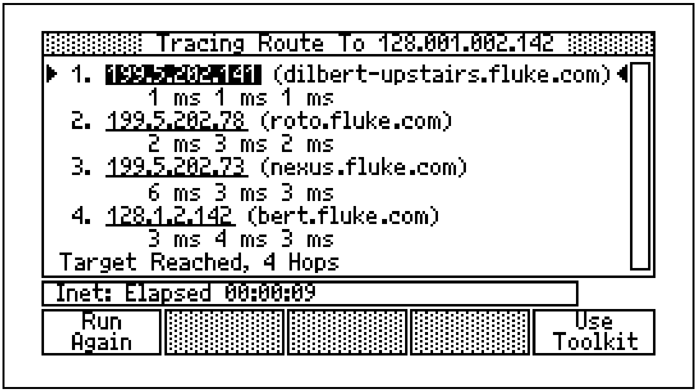
Prior to running Trace Route you must configure the Target IP address and the Source IP address. The Domain Name Server (DNS) server is optional and the local Router IP address is required in most environments.

Results

The Trace Route results are displayed as they become available. Figure 6-14 shows Trace Route sample results. You can run the test again by pressing **Run Again**.

Three round-trip times are displayed after each router's DNS name (if available) or dotted decimal address. If a router fails to respond, an asterisk (*****) is displayed. Press ▽ to view any additional results.

If results from any of the Internet Toolkit tools were previously copied to the Toolkit Log (by pressing **Copy to Log** in the Toolkit), those results can be observed by pressing **View Log**. This softkey is only available when there are results in the Toolkit log.



```
Tracing Route To 128.001.002.142
▶ 1. 199.5.202.141 (dilbert-upstairs.fluke.com)◀
        1 ms 1 ms 1 ms
  2. 199.5.202.78 (roto.fluke.com)
        2 ms 3 ms 2 ms
  3. 199.5.202.73 (nexus.fluke.com)
        6 ms 3 ms 3 ms
  4. 128.1.2.142 (bert.fluke.com)
        3 ms 4 ms 3 ms
 Target Reached, 4 Hops
Inet: Elapsed 00:00:09
```

Figure 6-15. Trace Route Sample Results

Interpreting Trace Route Results

You may see some of these results:

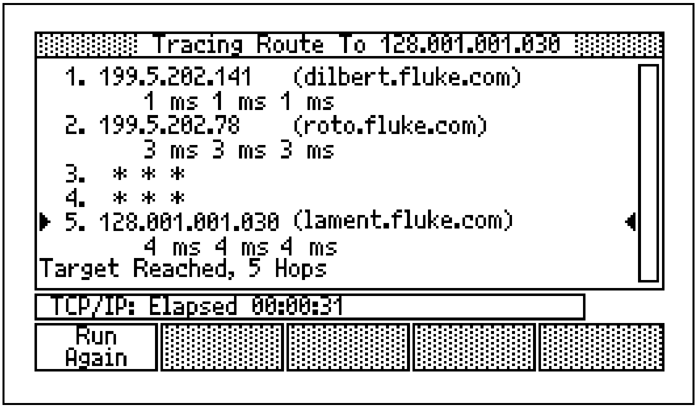
- ❒ No Response to UDP Query
- ❒ No Response from Router
- ❒ No Response from Target
- ❒ DNS Server not Reachable
- ❒ Different Routes Used

No Response to UDP Query

You will see a popup titled "No Response". Prior to running the Trace Route test, the LANMeter instrument sends an OSI Layer 4 (UDP) query to the target. If it fails then three possibilities exist. First, the target is not present or may not be powered on, therefore nothing is answering. Second, the target is not answering that UDP port, even though the message reached it. Third, there is a problem along the path, and that is why you are running the Trace Route test in the first place – to discover where the problem is in the path.

No Response from Router

Figure 6-15 shows an example of no response from router (this is shown as failed hops, *** * ***, but the target responds.) This condition can be due to a problem in the path, to the presence of a firewall, or to machines that do not support sending back ICMP packets (could be indicated if Trace Route provides good results at a later time).

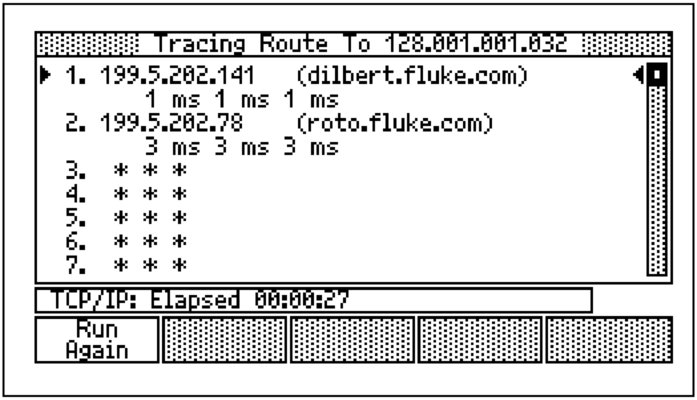


```
Tracing Route To 128.001.001.030
  1. 199.5.202.141   (dilbert.fluke.com)
        1 ms 1 ms 1 ms
  2. 199.5.202.78    (roto.fluke.com)
        3 ms 3 ms 3 ms
  3.  * * *
  4.  * * *
▶ 5. 128.001.001.030 (lament.fluke.com)
        4 ms 4 ms 4 ms
Target Reached, 5 Hops
TCP/IP: Elapsed 00:00:31
```

Figure 6-16. No Response from Router

No Response from Target

Figure 6-16 shows an example of no response from target. For a local target (on the same LAN), the results show the routers in the instrument’s configuration as the first hop, and then shows failures as asterisks (*****). For a remote target, the results can display Host Unreachable if a remote router sends that ICMP message, or it can display successive failures (as: *** * ***). If there is a broken path, you could confirm this by running the ICMP Ping test. For information on running the ICMP Ping test, refer to the “ICMP Ping” section of this chapter.



```
Tracing Route To 128.001.001.032
▶ 1. 199.5.202.141    (dilbert.fluke.com)
        1 ms 1 ms 1 ms
  2. 199.5.202.78     (roto.fluke.com)
        3 ms 3 ms 3 ms
  3.  * * *
  4.  * * *
  5.  * * *
  6.  * * *
  7.  * * *
TCP/IP: Elapsed 00:00:27
```

Figure 6-17. No Response from Target

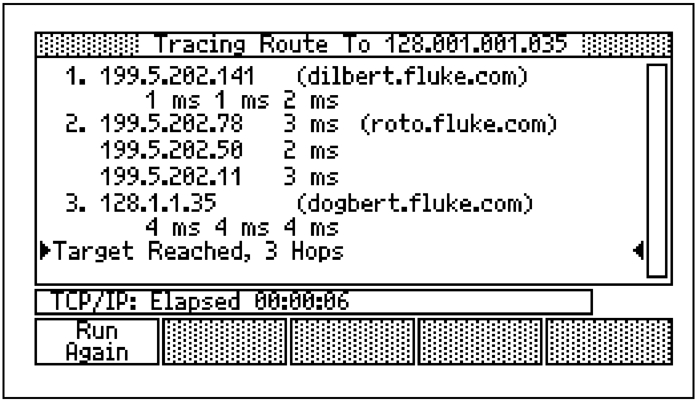
DNS Server not Reachable

The message **Name Query . . . Enter Cancels** is displayed on the Status Line if the instrument cannot contact the DNS server. Pressing ENTER RUN suspends DNS queries for this run of the test.

If there is no DNS server present on the network under test, you may use IP Auto Config to turn off the Use DNS feature. Select the **IP Auto Config** softkey, then MENU, **Configure**. Use ◁ or ▷ to toggle Use DNS to No.

Different Routes Used

Figure 6-17 shows an example of different routes used (for hop # 2). This condition can be due to load balancing, equal cost routes, or route flapping. Load balancing and equal cost routes are not problems and can often be identified with similar round-trip times. Route flapping is a problem caused by bad or unstable router tables and is often represented by very different round-trip times.

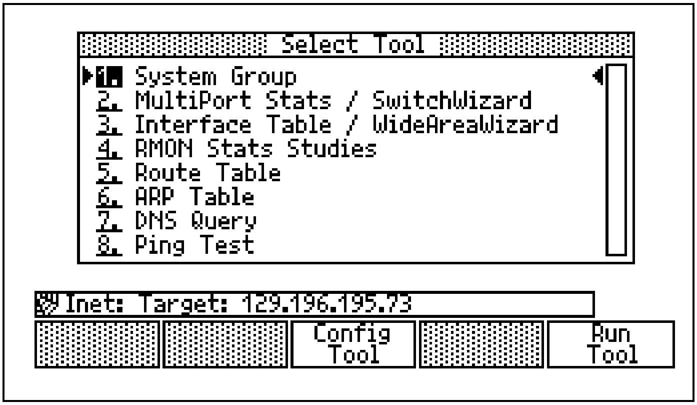


```
Tracing Route To 128.001.001.035
  1. 199.5.202.141   (dilbert.fluke.com)
        1 ms 1 ms 2 ms
  2. 199.5.202.78   3 ms  (roto.fluke.com)
     199.5.202.50   2 ms
     199.5.202.11   3 ms
  3. 128.1.1.35      (dogbert.fluke.com)
        4 ms 4 ms 4 ms
▶Target Reached, 3 Hops
TCP/IP: Elapsed 00:00:06
```

Figure 6-18. Different Routes Used

Internet Toolkit

The Internet Toolkit tests are a set of test tools that can be selected from the **Internet Toolkit** softkey or from a hypertext link from another of the Internet TCP/IP tests. Internet Toolkit tests provide more detailed analysis of the selected IP host. Figure 6-19 shows the Internet Toolkit Select Tool screen.



```
Select Tool
▶1. System Group
 2. MultiPort Stats / SwitchWizard
 3. Interface Table / WideAreaWizard
 4. RMON Stats Studies
 5. Route Table
 6. ARP Table
 7. DNS Query
 8. Ping Test
Inet: Target: 129.196.195.73
```

Figure 6-19. Internet Toolkit Select Tool Screen

You can select the desired tool by pressing the number, or △ or ▽, and then press **Run Tool** to run the test. You can press **Refresh View**, only while in a tool, to rerun the test.

When an Internet Toolkit tool is running the Status Line indicates the target address.

You can press **Leave View** or EXIT STOP to close a tool from the Toolkit. Tests that were running before you execute a hyperlink jump are suspended while you are in Toolkit and then resume after you exit Toolkit.

Configuration

You can configure an Internet Toolkit tool by first selecting a tool and then pressing **Config Tool**.

Each Internet Toolkit test tool has its own configuration screen. For the System Group, RMON Statistics Studies, Router Table, and ARP Table tools the following configuration parameters are available:

❐ Target address
❐ SNMP Community string

For the Interface Table tool the following configuration parameters are available:

❐ Target address
❐ SNMP Community string
❐ Data Source
❐ Rate

Note

If the target does not support SNMP, or is not accessible, the query may report the destination as unreachable.

If the community string is not configured correctly, the query may time out.

If the SNMP community string is blank (disabled) the Internet Toolkit will use "public".

If a custom community string is selected and the query times out, a community string of "public" is attempted.

Some devices, such as routers, may have an access list which specifies which devices it can communicate with using SNMP. If the LANMeter instrument's IP address is not in this list, the SNMP request may time out. Other security features may also cause a timeout.

For the DNS Query tool the following configuration parameters are available (the defaults are underlined):

- Search method by Address or by Name
- Target address or Name
- DNS default server

For the Ping Test tool the following configuration parameters are available (the defaults are underlined):

- Target address
- Run tool as Once or Continuous
- Rate of query as 1 per second to 1 per 60 seconds (default is 1 per 2 seconds).
- Ping Data Size (size of ICMP data) from 18 to 1472 bytes for Ethernet and 18 to 944 bytes for Token Ring

Description of the Internet Toolkit Tools

All SNMP information displayed by the LANMeter instrument is reported by querying SNMP agents. If the SNMP agents report information incorrectly then the LANMeter instrument passes along the same information. For example, WAN links that utilize an external clock can run at a speed other than what is reported.

Note

The LANMeter instrument only performs SNMP GET operations.

System Group

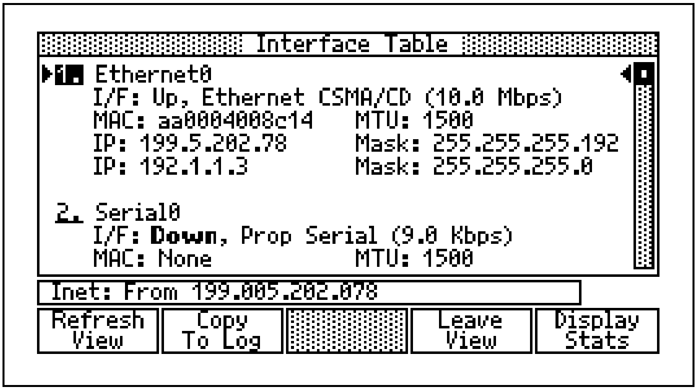
Use the System Group for MIB II system group information. The following information can be displayed:

- Name
- Description
- Up Time
- Contact
- Location
- Services
- Object ID

Interface Table

Use the Interface Table tool to determine interface configuration and statistics information. The Interface Table tool communicates with a machine using SNMP to collect interface and IP address information.

Figure 6-19 shows a sample Interface Table results screen.



```
Interface Table
1. Ethernet0
   I/F: Up, Ethernet CSMA/CD (10.0 Mbps)
   MAC: aa0004008c14    MTU: 1500
   IP: 199.5.202.78     Mask: 255.255.255.192
   IP: 192.1.1.3        Mask: 255.255.255.0

2. Serial0
   I/F: Down, Prop Serial (9.0 Kbps)
   MAC: None            MTU: 1500
Inet: From 199.005.202.078
```

Figure 6-20. Interface Table Results Screen

The following information can be displayed:

- The kind of interfaces on the target device
- Interface Reported as Up or Down
- Speed of Interfaces
- Interface Index or Slot and Port numbers*
- Virtual LAN (VLAN) number*
- MAC addresses
- Maximum Transmission Unit (MTU)
- Interface IP addresses and associated subnet mask

* Refer to Chapter 7 “SwitchWizard Option,” for supported devices (for slot, port, and VLAN).

If the FDDI Transmission MIBs are fully supported, the following FDDI entries are also shown:

- FDDI Port Status
- FDDI Ring State

For supported chassis switches with plug-in modules, Interface Table reports the slot and port numbers as labeled on the device. The slot and port numbers are obtained from the private MIB. If private MIB information is not available, the port number is obtained from the Bridge MIB and the interface number is obtained from the Interface Table.

If Interface Table detects a virtual LAN (VLAN) configuration, the VLAN number for the port is also displayed. A VLAN is a group of ports configured into one broadcast domain (or logical LAN). VLANs can only be detected by using private MIBs that are supported by the LANMeter instrument.

The individual statistics displayed depends on the MIB used. Refer to Table 6-1 for a listing of the individual statistics that are displayed for each MIB.

You can obtain SNMP information on the targeted interface by pressing **Display Stats**. The resulting statistics represent the performance of the targeted interface only. It does not represent the performance of the entire segment where the interface is attached, but of the errors and traffic sent from and to that interface. Table 6-2 shows MIB II, Ethernet, Token Ring, and FDDI Transmission MIB errors.

Table 6-1. Statistics Displayed per Source MIB

	Source MIBs			
Statistic	**MIB II**	**MIB II (WAN)**	**RMON**	**Transmission MIBs**
Util%	X		X	X
Util% (In)		X		
Util% (Out)		X		
Collisions			X	X
Errors	X	X	X	X
Broadcasts	X	X	X	X

Table 6-2. MIB II and Transmission MIB Errors

	Errors
MIB II **RFC 1213**	MIB II shows errors reported by lower layers but provides no detail.
Ethernet-Like Transmission MIB **RFC 1643**	Too Long Bad FCS Misaligned Transmit Delay 1 Collision Frames >1 Collisions Frames Excess Collisions Late Collisions
Token Ring Transmission MIB **RFC 1231** **RFC 1239**	Burst Line Abort ARI/FCI Internal Frequency Lost Frame Rx Congest Frame Copy Token
FDDI **Transmission MIB** **RFC 1285** **RFC 1512**	Frame Errors Lost Frames TVX Expire Not Copied TRT Expire Ring Ops Link Error Rate (LER)

If the LANMeter instrument detects a serial (WAN) interface, it still uses MIB II variables but displays **Util % (IN)**, **Util % (OUT)**, **Errors (IN)**, and **Errors (OUT)**.

Refer to Chapter 10, “WideAreaWizard Option” for more information about diagnostic capabilities for Frame Relay, ISDN, and T1/E1(DS1) interfaces discovered on routers, switches, and bridges.

If the LANMeter instrument determines that a Transmission MIB is supported for a given interface, that MIB is used to provide detailed information on the interface. Otherwise, only MIB II information is used to provide less detailed information, refer to Table 6-2.

The default configuration for the Interface Table tool uses the Ethernet or Token Ring RMON MIB as the source for statistics. The RMON MIB is used if it references the Interface Table directly without any filters.

For all links, the LANMeter instrument is dependent on the reported speed of the link to report statistics. If this speed is reported wrong, the percentage results can be significantly in error.

The display of the FDDI information shown depends on the target’s support of the FDDI MIB, including some optional groups.

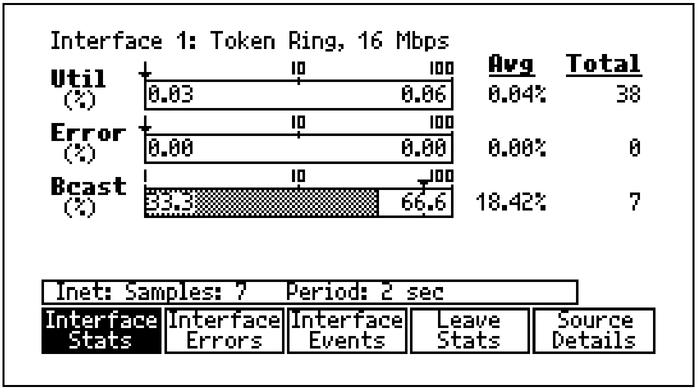
RMON Statistics Studies

The RMON Statistics Studies tool allows you to gather Ethernet or Token Ring segment statistics remotely. RMON agents can be standalone RMON probes on remote segments, RMON agents that are part of hubs or switches, or software-based RMON agents on UNIX or Novell servers. The RMON Statistics Studies tool supports Ethernet and Token Ring MIBs.

Note

The description on the RMON statistics studies that the LANMeter instrument reports comes from the RMON device and its description may not always be meaningful.

While the RMON Statistics Studies tool is running, it polls continually for information. Polling stops when you press **Leave Stats**. Figure 6-20 shows an example RMON Statistics Studies results screen.



```
Interface 1: Token Ring, 16 Mbps
                                                Avg      Total
Util     0.03                       0.06       0.04%       38
(%)
Error    0.00                       0.00       0.00%        0
(%)
Bcast    33.3                       66.6      18.42%        7
(%)

Inet: Samples: 7    Period: 2 sec
```

Figure 6-21. RMON Statistics Studies Results Screen

Use the following procedure to use the RMON Statistics Studies tool:

1. Target an IP address that has an RMON agent by using a hyperlink or by using the Internet Toolkit.

   This could be the same address as a hub, but some vendors will have a separate IP address for the RMON agent.

2. Run the tool to display the available studies.
3. Select the desired study and press **Display Stats**, or press ENTER RUN, to access the information in the study.

If the targeted RMON agent is several hops away, you can decrease the polling rate, by using **Config Tool**, to reduce the amount of traffic placed on the network by your LANMeter instrument.

RMON statistics group information has read-only capability. The LANMeter instrument does not create RMON studies, it will only read RMON studies that are already created and running. Creating an RMON study requires an SNMP Set operation, and the LANMeter instrument will not issue that command.

If the source for the RMON study is the RMON Filter Group and not the device's interface table entry, the name of the RMON Filter group entry is shown. Statistics studies from the RMON Filter group will reflect the traffic passed through the filter and may not reflect the traffic for the entire segment.

For Token Ring RMON there are two kinds of studies. One study shows Token Ring error and event statistics and the other study shows utilization statistics for all frame types.

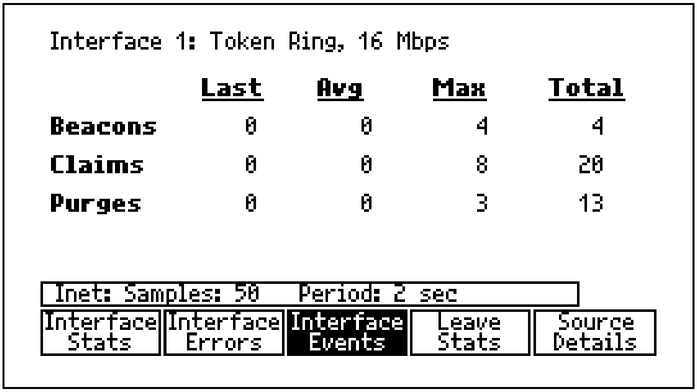
Table 6-3 shows Ethernet and Token Ring RMON errors available from the different MIBs.

Table 6-3. Ethernet and Token Ring RMON Errors

	Errors	**Statistics**
RMON Ethernet **RFC 1271**	<u>Ethernet Errors</u> CRC Align Undersize Oversize Fragments Jabbers Collisions	<u>Ethernet Util</u> Utilization Broadcasts Multicasts Collisions
RMON Token Ring **RFC 1513**	<u>Token Ring Errors</u> Burst Line Abort ARI/FCI Internal Frequency Lost Frame Rx Congestion Frame Copy Token	<u>Token Ring Util</u> Utilization Broadcasts Multicasts

Interface Events

The Interface Events softkey is only available when the source of data is the Token Ring RMON MIB. The Interface Events display shows the event details for the selected port as shown in Figure 6-21.



Interface 1: Token Ring, 16 Mbps

	Last	Avg	Max	Total
Beacons	0	0	4	4
Claims	0	0	8	20
Purges	0	0	3	13

Inet: Samples: 50 Period: 2 sec

Figure 6-22. MultiPort Statistics Interface Events

Beacons are the counts for frames on Token Ring networks that are transmitted when the token is lost and the normal error recovery methods, such as ring purging and token claiming, have failed. Purges are the counts for purging the network of any tokens prior to starting token claiming and Claims are the counts for initiating token claiming.

Route Table

Use the Route Table for MIB II Route Table information. The following information is displayed for each router:

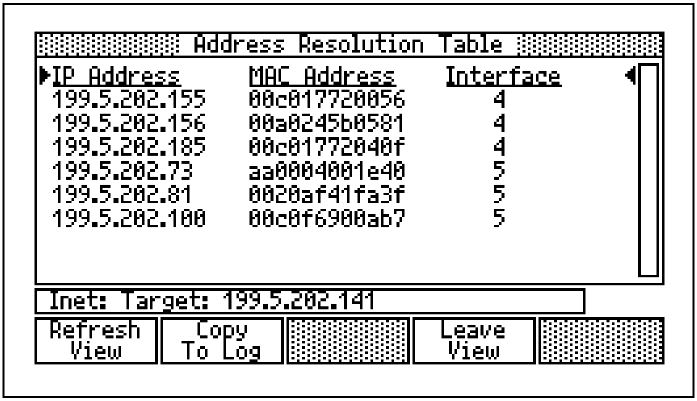
1. Destination network or host
2. Interface or next hop router to get to the destination
3. Destination mask

Destinations that are bound for an attached network segment are indicated on the display.

ARP Table

Use the ARP (Address Resolution Protocol) Table to analyze the IP and MAC address pairs being used by the target. The Interface number can be resolved in the Interface Table tool.

Figure 6-22 shows a sample ARP Table results screen.



Address Resolution Table

IP Address	MAC Address	Interface
199.5.202.155	00c017720056	4
199.5.202.156	00a0245b0581	4
199.5.202.185	00c01772040f	4
199.5.202.73	aa0004001e40	5
199.5.202.81	0020af41fa3f	5
199.5.202.100	00c0f6900ab7	5

Inet: Target: 199.5.202.141

Figure 6-23. ARP Table Results Screen

DNS Query

The Domain Name Server Query tool is used to perform name and address lookups as well as to verify that the IP address and name match in the DNS server. This is automatically done by the Domain Name Server Query tool.

The following information can be displayed:

- ❒ Name
- ❒ Address
- ❒ Reverse lookup
- ❒ Mail exchange records

In the case of a multi-homed machine (a device that has more than one interface), you could have multiple IP addresses shown if that information is in the DNS server.

You can discover the IP address of a host if you know the host name. With the DNS Query tool selected, press **Config Tool** and use ◁ or ▷ in the Search field to switch between By Name or By Address lookup functions. The name lookup must be fully qualified (for example, **`node.test.org`**).

Ping Tests

Use the Ping Tests to quickly verify connectivity with the target IP address while using a user configurable frame size. You can get response times by using the standalone ICMP Ping test in the standard TCP/IP tests.

A specific usage for changing the frame size is to test for congestion on the network. For example, if you identify a problem between two routers while using the Trace Route test, you could test for congestion by sending large packets through the routers.

The ICMP Monitor test can be used to resolve ICMP errors.

Internet Toolkit Results

The LANMeter instrument displays the results for the selected Internet Toolkit test tool as they are available. The actual results depend on the tool that you have selected.

When available, pressing **Refresh View** resends the SNMP queries.

Results from Internet Toolkit tools can be copied to the Toolkit Log by pressing **Copy to Log**. If anything is currently in the log, pressing **Copy to Log** appends the additional results to the end of the log file. You can display the log by pressing **View Log**. When there is information in the log, the **View Log** softkey is also available from Segment Discovery, Scan Host, and Trace Route tests.

You can print the log by stopping the current test, pressing MENU, selecting **Print All**, and pressing ENTER RUN. If the Toolkit was accessed through a hyperlink jump from another test, the log will be appended to that test's Print All report.

Scan Host

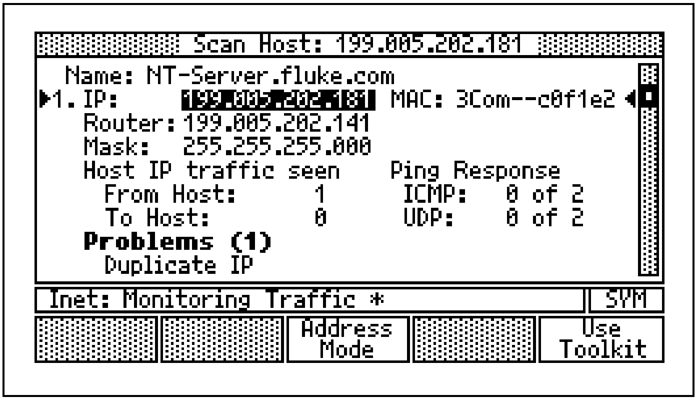
Use the Scan Host test to verify configuration and connectivity of a local IP host. The host being tested must be a local host, which is one that is on the same logical IP network segment as the LANMeter instrument.

One specific use of the Scan Host test and its Toolkit functions are to test hosts which are suspected of having problems with duplicate IP addresses. You can make directed SNMP queries at each host, specifically by MAC addresses, so that the problem host can be identified.

Results

Scan Host results are displayed as they are discovered. Figure 6-23 shows Scan Host Sample Results. Scan Host tests for and can display the following result information:

1. Target host being local to this segment. (**If not, the test stops.**)
2. ICMP Echo and UDP connectivity.
3. Target host's subnet mask, DNS name, and whether it uses a default router or utilizes routing protocols.
4. A sampling of IP packets sent from and to the target host to indicate IP activity.



```
Scan Host: 199.005.202.181
  Name: NT-Server.fluke.com
▶1. IP:      199.005.202.181 MAC: 3Com--c0f1e2 ◀
    Router: 199.005.202.141
    Mask:   255.255.255.000
    Host IP traffic seen     Ping Response
      From Host:      1       ICMP:   0 of 2
      To Host:        0       UDP:    0 of 2
    Problems (1)
      Duplicate IP
Inet: Monitoring Traffic *                    SYM
```

Figure 6-24. Scan Host Sample Results

If results from any of the Internet Toolkit tools were previously copied to the Toolkit Log (by pressing **Copy to Log** in the Toolkit), those results can be observed by pressing **View Log**. This softkey is only available when there are results in the Toolkit log.

ICMP Monitor

ICMP Monitor reports on ICMP packets. ICMP packets are the error reporting and recovery mechanisms for the TCP/IP protocol suite. These packets identify such problems as overloaded devices, incorrect routes, and unreachable destinations. The ICMP Monitor test monitors a network for these ICMP packets, decodes the relevant information (such as packet type, source, destination and target IP addresses) and displays them in an easy to understand format.

Configuration Parameters

You can configure the following parameters for ICMP Monitor:

- ❒ To/From Filter as On or Off. Configure the following parameter when this field is set to On.
- ❒ To/From address as a dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).

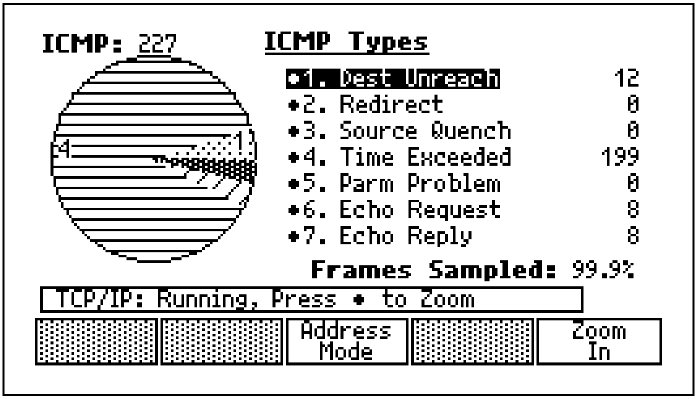
Your LANMeter instrument's IP address does not have to be configured to run the ICMP Monitor test.

Results

The instrument displays ICMP Monitor results as they become available. ICMP Monitor displays results as counts of various types of ICMP packets in a pie chart. Figure 6-24 shows ICMP Monitor sample results. Table 6-4 provides some guidance on how to interpret the results.

The following are monitored IP error packets:

1. Destination Unreachable
2. Redirect
3. Source Quench
4. Time Exceeded
5. Parameter Problem
6. Echo Request
7. Echo Reply



```
ICMP: 227        ICMP Types
                 •1. Dest Unreach        12
                 •2. Redirect             0
                 •3. Source Quench        0
                 •4. Time Exceeded      199
                 •5. Parm Problem         0
                 •6. Echo Request         8
                 •7. Echo Reply           8
                   Frames Sampled: 99.9%
TCP/IP: Running, Press • to Zoom
```

Figure 6-25. ICMP Monitor Sample Results

You can highlight an ICMP error result marked with the Zoom icon (•) and press the **Zoom In** softkey to display more details about that error (such as, source and destination IP addresses).

Press the **Address Mode** softkey to display a menu of alternatives for switching the address format between symbolic name or hexadecimal and/or decimal.

Table 6-4. ICMP Packet Information

ICMP Packet Type	Causes	Sent by (Source address)	Addressed to (Destination address)	Target Address
Redirect	A host is using a non-optimal route.	Gateway/router that detects the non-optimal route being used.	Host that originated the packet with a non-optimal route	Destination IP address of packet with a non-optimal route
Source Quench	A device is congested and is requesting the sending device stop sending packets.	The congested device. This may be either the target device or an intermediate router / gateway.	The device sending data.	Destination address of the packets that are causing congestion.
Destination Unreachable *****	The destination IP address or service cannot be found. Most often this is a misconfiguration. It may be an indication of an attempted security breech.	Device detecting the address or service is unreachable.	Host originating the misaddressed packet.	Unreachable destination IP address.
Parameter Problem	Something is wrong with the packet being sent.	Device detecting the problem.	Device originating the incorrectly formed packet.	Destination IP address of incorrectly formed packet.

Table 6-4. ICMP Packet Information (Cont.)

ICMP Packet Type	Causes	Sent by (Source address)	Addressed to (Destination address)	Target Address
Time Exceeded	Packet has passed through too many routers, causing its rejection. This may be an indication of a routing loop, misconfigured host, or perhaps someone running *Traceroute*.	Router/gateway that detected the TTL field is zero.	Device originating the rejected packet.	Destination IP address of rejected packet.
Echo Request	Echo request (ICMP Ping) packet.	Device originating the ping.	IP address to be pinged.	N/A
Echo Reply	Reply to a echo request.	Device being pinged.	IP address that originated the ping.	N/A
* Some devices may return a destination unreachable (port unreachable or network unreachable) incorrectly to Enterprise LANMeter discovery processes.				

ICMP Ping

ICMP Ping tests the network layer for connectivity. Ethernet ICMP Ping uses Ethertype frame types and Token Ring ICMP Ping uses SNAP frame types.

For each ping sent by the ICMP Ping test, the instrument first obtains the local physical address of the target IP address by performing an ARP for the target IP address. If this fails, the instrument executes an ARP for the default router address. Then, using the acquired MAC address the instrument takes the supplied dotted decimal IP address and sends an ICMP echo request, and then monitors for the ICMP Reply. If you have an Enterprise LANMeter, you can ping each other when properly configured.

Configuration Parameters

You can configure the following parameters for ICMP Ping:

❒ Destination IP address as dotted decimal or Station List entry (press Y Z SPACE to select from the IP station list)

❒ Source IP address as dotted decimal or Station List entry (press Y Z SPACE to select from the IP station list)

❒ Default Router address as dotted decimal or Station List entry (press Y Z SPACE to select from the IP station list)

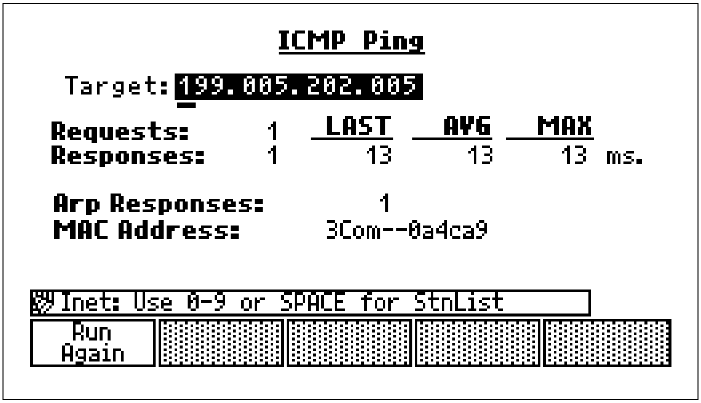
❒ Run as once or continuous

❒ Timeout as 1 second, 5 seconds, 30 seconds

Results

The instrument displays ICMP Ping results as they become available. Figure 6-25 shows ICMP Ping sample results. ICMP Ping displays the following result parameters:

❒ Target IP address
❒ Local MAC (target or router)
❒ Number of requests
❒ Number of responses
❒ Response time



```
                ICMP Ping
  Target: 199.005.202.005

 Requests:      1    LAST     AVG     MAX
 Responses:     1      13      13      13  ms.

 Arp Responses:        1
 MAC Address:       3Com--0a4ca9

 Inet: Use 0-9 or SPACE for StnList
```

Figure 6-26. ICMP Ping Sample Results

For continuous operation the minimum, average, and maximum response times are also displayed.

Top IP (Top Senders and Top Receivers)

Top Senders and Top Receivers tests track the busiest senders and receivers of TCP/IP traffic. Top Senders and Top Receivers run simultaneously. To display the results of the other test, simply press its softkey while the test is running or after the test has been stopped.

TCP/IP Top Senders and Receivers track stations by their IP address, while Network Monitor Top Senders and Receivers track stations by their MAC address. TCP/IP Top Senders and Receivers looks beyond the MAC addresses (of intermediate routers) to the network layer and observes the actual source and destination IP addresses.

Note

When a network passes a packet through a TCP/IP router, the router retransmits the packet with its own MAC address. This leaves the network layer addresses untouched. The instrument gets an accurate picture of the end-to-end traffic by observing network layer addresses.

Configuration Parameters

You can configure the following parameters for Top Senders or Top Receivers:

❒ Senders to a single station as Off or On. Configure the following parameter when this field is set to **On**.

❒ Filter Address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).

Your LANMeter instrument’s IP address does not have to be configured to run the TCP/IP Top Senders and Top Receivers test.

Results

The instrument displays Top Senders or Top Receivers test results after monitoring network traffic for the first 1-second sample period and updates these results for each successive sample period. The Top Senders and Top Receivers tests display results in percent of total traffic and in a pie chart that identifies the top senders, or top receivers, and shows the quantity of traffic transmitted. Figure 6-26 shows Top Senders sample results. The Top Receivers test results are similar to that of Top Senders.

The Top Senders/Top Receivers test will record the first 512 stations seen and will display the busiest 8 stations. The test will continue to count frames for the first 512 stations.

The **Frames sampled** field shows the percentage of the total frames used to calculate the results.

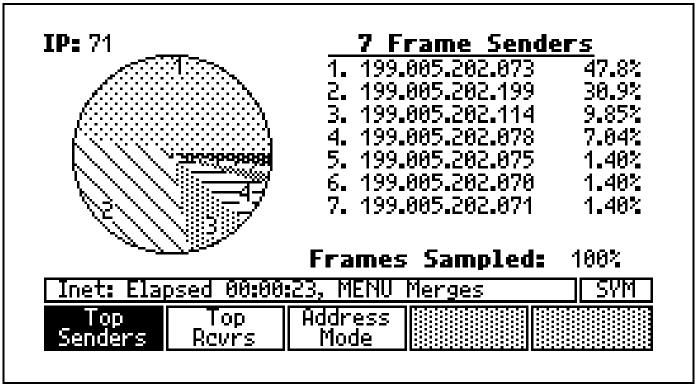
To print all TCP/IP Senders and Receivers results, press MENU, select **Print All**, and then press ENTER/RUN after the test has stopped.

You can merge any discovered IP addresses into the station list, after the test has stopped, by pressing MENU, then selecting **Merge Stations**.

Note

> *After you merge IP addresses into the station list, you will be reminded to use the* **Station List** *utility (from Setup/Utils) if you want to save the merged stations into non-volatile memory.*

Press the **Address Mode** softkey to display a menu of alternatives for switching the address format between symbolic name or hexadecimal and/or decimal.



```
IP: 71                      7 Frame Senders
                        1. 199.005.202.073    47.8%
                        2. 199.005.202.199    30.9%
                        3. 199.005.202.114    9.85%
                        4. 199.005.202.078    7.04%
                        5. 199.005.202.075    1.40%
                        6. 199.005.202.070    1.40%
                        7. 199.005.202.071    1.40%

                       Frames Sampled:  100%
Inet: Elapsed 00:00:23, MENU Merges           SYM
```

Figure 6-27. IP Top Senders Sample Results

IP Matrix

Use the IP Matrix test to display frame counts for the top conversations between local IP addresses.

Configuration Parameters

You can configure the following parameters for IP Matrix (the defaults are underlined):

- ❒ Conversations with a single station as <u>Off</u> or On. If you selected **On**, then also configure the following parameter.
- ❒ Filter Address as dotted decimal. The IP address may be obtained from a Station List entry (press the **Station List** softkey to select from the IP station list).

When filtering is on, displayed conversations are limited to those that are to or from the filtered address. The test will continue to count frames for the first 512 stations.

Results

The instrument displays IP Matrix results after monitoring network traffic for the first 1-second sample period and updates these results for each successive sample period. The IP Matrix test displays the frame counts for both directions of the top conversations between local IP addresses. Figure 6-27 shows IP Matrix sample results.

With filtering off, the test tracks the first 512 conversing station pairs seen on the network, displaying the busiest eight.

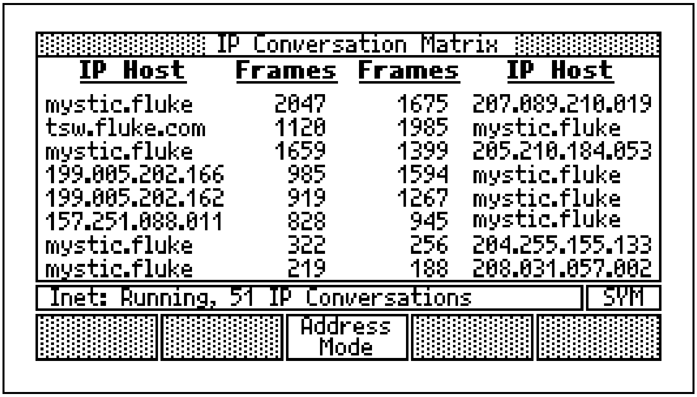
Press MENU, select **Print All**, and then press ENTER RUN (from the IP Matrix results screen) for an ASCII printout of the top IP Conversation Matrix. You can use **View All** to display all of the results without printing.

Press the **Address Mode** softkey to display a menu of alternatives for switching the address format between symbolic name or hexadecimal and/or decimal.

To merge the stations discovered by IP Matrix into a Station List, press MENU, then select **Merge Stations**.

Note

> *After you use* MENU *and* **Merge Stations** *you will be reminded to use the* **Station List** *utility (from Setup/Utils) if you want to save the merged stations into non-volatile memory.*



IP Conversation Matrix

IP Host	Frames	Frames	IP Host
mystic.fluke	2047	1675	207.089.210.019
tsw.fluke.com	1120	1985	mystic.fluke
mystic.fluke	1659	1399	205.210.184.053
199.005.202.166	985	1594	mystic.fluke
199.005.202.162	919	1267	mystic.fluke
157.251.088.011	828	945	mystic.fluke
mystic.fluke	322	256	204.255.155.133
mystic.fluke	219	188	208.031.057.002

Inet: Running, 51 IP Conversations

Figure 6-28. IP Matrix Sample Results

Chapter 7
SwitchWizard Option

Introduction

SwitchWizard™ is an optional feature supported in the Fluke Enterprise LANMeter (68x Series) instrument Software Version 7.00 and later. SwitchWizard enhances Segment Discovery and adds the SwitchWizard MultiPort Statistics test. SwitchWizard gives you the ability to discover and diagnose problems on the other side of Ethernet, Token Ring, and FDDI switches.

You can obtain version 7.0 or greater, software either by ordering a new Enterprise LANMeter instrument with option 68X-SW or by ordering the SwitchWizard software upgrade kit (option 68X-SWK) for your Enterprise LANMeter. The SwitchWizard option also includes the Terminal Emulator option (see Chapter 13 “Terminal Emulator). If you order the upgrade kit, you must first install the software as described in “Software Upgrade,” Appendix D, before you can enable it.

The SwitchWizard option comes configured in a trial usage mode. For more information on trial usage or if you have purchased the option, refer to the “Enabling the SwitchWizard Option” section of this chapter for information on how to make it permanently enabled.

You can determine if SwitchWizard is installed on your Enterprise LANMeter by running Manage Options (found by pressing **Setup/Utils** and then MORE). If the option is enabled, or if trial uses are still available, the SwitchWizard name appears on the top-level screen as well as on the Segment Discovery and Internet Toolkit screens. The MultiPort Statistics test is also available.

This chapter contains the following sections on SwitchWizard and Figure 7-1 shows the Enterprise LANMeter Internet TCP/IP softkeys.

❒ Enabling the SwitchWizard Option
❒ SwitchWizard for Segment Discovery
❒ SwitchWizard's MultiPort Statistics Test
❒ SwitchWizard for the Internet Toolkit

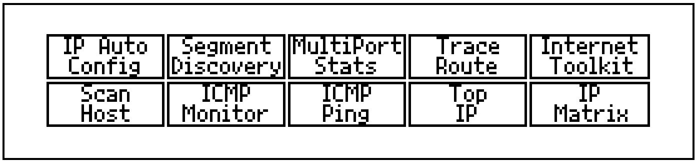


Figure 7-1. Enterprise LANMeter Internet TCP/IP Softkeys

Enabling the SwitchWizard Option

The SwitchWizard option comes configured in a trial usage mode. You can use SwitchWizard for a predefined number of days before your LANMeter instrument reverts back to an Enterprise LANMeter without the SwitchWizard option. A trial day is used when you run Segment Discovery's Switches and Bridges, MultiPort Statistics, or Toolkit MultiPort Statistics any number of times in one day. You can run **Manage Options**, from **Setup/Utils**, to view the number of trial days remaining.

If you have purchased the SwitchWizard option, you can permanently enable it by performing the following steps:

1. Complete the supplied FAX-back form including your Enterprise LANMeter's Ethernet or Token Ring MAC address and FAX it to Fluke to receive your enabling key.

   The Ethernet or Token Ring MAC address is available on the back of Enterprise LANMeter and from the Enable Option softkey screen (Figure 7-2).

2. Press the top-level **Setup/Utils** softkey.

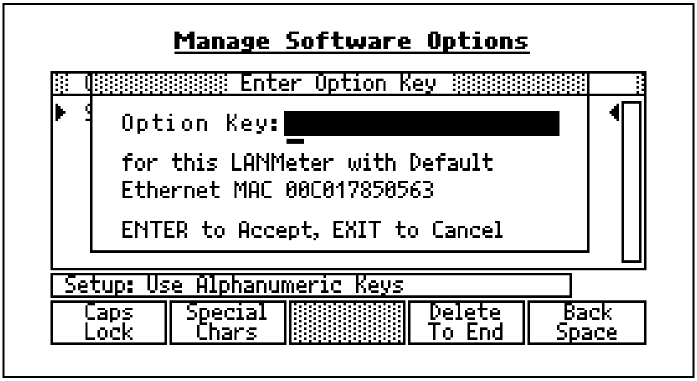
3. Press MORE, **Manage Options**, and then ENTER RUN to list your LANMeter instrument's enabled options. Each option can be enabled or disabled. This procedure assumes that your SwitchWizard option is disabled.

If you are using the SwitchWizard option in the trial usage mode, the number of remaining trial days is shown here.

4. Select the SwitchWizard option and press **Enable Options** to display the Enter Option Key screen, shown in Figure 7-2.

5. Enter your enabling key and then press ENTER RUN to enable the SwitchWizard option.

6. After the key is enabled, place the SwitchWizard Label onto the back of your Enterprise LANMeter. The SwitchWizard Label is included in the option 68X-SW and 68X-SWK kits. This label will help identify units that have the option enabled.



Manage Software Options

Enter Option Key

Option Key:

for this LANMeter with Default
Ethernet MAC 00C017850563

ENTER to Accept, EXIT to Cancel

Setup: Use Alphanumeric Keys

Figure 7-2. Enabling the SwitchWizard Option

SwitchWizard for Segment Discovery

SwitchWizard enhances Segment Discovery for troubleshooting switched networks by adding the discovery of switches and bridges. Switches and bridges found by the Segment Discovery test are reported in the Segment Discovery screen, as shown in Figure 7-3.

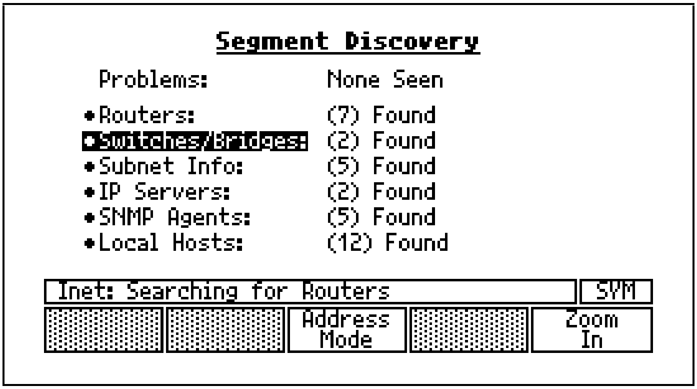
The following are used to discover switches and bridges:

❒ IEEE 802.1d Spanning Tree Protocol
❒ DEC Spanning Tree Protocol
❒ SNMP Requests (Bridge MIB)
❒ Cisco Systems' Cisco Discovery Protocol (CDP)

There should only be one device on the attached segment sending Spanning Tree frames. This device, the Root Bridge or Designated Bridge, will be the root device of the Spanning Tree or it will be the bridge closest (lowest cost) to the root bridge on the attached LAN. SwitchWizard shows the bridge or switch that is sending Spanning Tree Bridge Protocol Data Unit (BPDU) frames. Detection of more than one Designated Bridge is reported in **Problems** of the Segment Discovery screen.

The Spanning Tree protocol is encapsulated over 802.2 and is non-routable. The Bridge ID, used to uniquely identify that bridge or switch, is a 48 bit MAC address with a unique value. It may not reflect the same MAC address that is used by the bridge or switch's IP stack and SNMP agent. If the Enterprise LANMeter cannot show an IP/MAC address pair, it only shows the sending MAC address from the Spanning Tree frame. It is often possible to identify the bridge MAC address for TCP/IP by looking for very similar MAC addresses in Local Hosts.

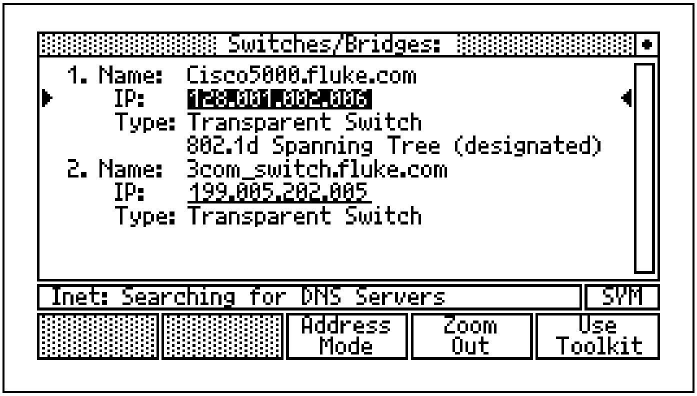
The Cisco Discovery Protocol (CDP) is used to support the discovery of selected Cisco devices that use virtual LANs (VLANs). If the IP "interface" of a Cisco switch is configured on another VLAN than what the LANMeter instrument is connected to, CDP is used to discover the IP address of that switch. It is possible for a CDP discovered switch to be reported, yet not be in the same broadcast domain or VLAN as the LANMeter instrument.



```
                 Segment Discovery
      Problems:          None Seen

     •Routers:           (7) Found
     •Switches/Bridges:  (2) Found
     •Subnet Info:       (5) Found
     •IP Servers:        (2) Found
     •SNMP Agents:       (5) Found
     •Local Hosts:       (12) Found

 Inet: Searching for Routers                SVM
```

Figure 7-3. Segment Discovery Results

The Switches/Bridges details (shown in Figure 7-4) indicate which discovery method (SNMP or Spanning Tree) found the device.



```
                Switches/Bridges:                    •
   1. Name:  Cisco5000.fluke.com
▶     IP:    128.001.002.006                        ◀
      Type:  Transparent Switch
             802.1d Spanning Tree (designated)
   2. Name:  3com_switch.fluke.com
      IP:    199.005.202.005
      Type:  Transparent Switch

 Inet: Searching for DNS Servers               SVM
```

Figure 7-4. Switches and Bridges Results

A bridge or switch device will be shown as a **Switch** if the retrieved SNMP Bridge MIB reports more than 2 ports. Otherwise the device will be shown as a **Bridge**.

For more information on the Segment Discovery test, refer to Chapter 6 “Testing TCP/IP Networks.”

SwitchWizard’s MultiPort Statistics Test

MultiPort Statistics allows you to diagnose hard-to-analyze switched LAN segments. It provides a graphical, multi-port view of segment utilization and health. Also, you can obtain detailed error information and port-by-port bridge forwarding table information. The MultiPort Statistics test is also available using hyperlinks in the Internet Toolkit.

Configuring the MultiPort Statistics Test

You configure the MultiPort Statistics test the same way as any Internet test. First by selecting the test and then pressing MENU and selecting **Configure**.

Each Internet test has its own configuration screen. For the MultiPort Statistics test the following configuration parameters are available (the defaults are underlined):

- Target address
- SNMP Community String
- Polling Rate as 2, 5, or 10 seconds
- Use RMON as Yes or No
- Interface (I/F) Start number from 1 to 999
- Interface (I/F) Count from 1 to 150

The Interface Start number is the number of the interface that you want the MultiPort Statistics test to begin displaying. If the Interface Start number is larger than the last interface on the device, an error message is displayed and you are prompted to change the configuration.

The Interface Count is the number of interfaces that you want available to scroll through. Only the remaining interfaces are displayed if the Interface Count is larger than the remaining interfaces on the device.

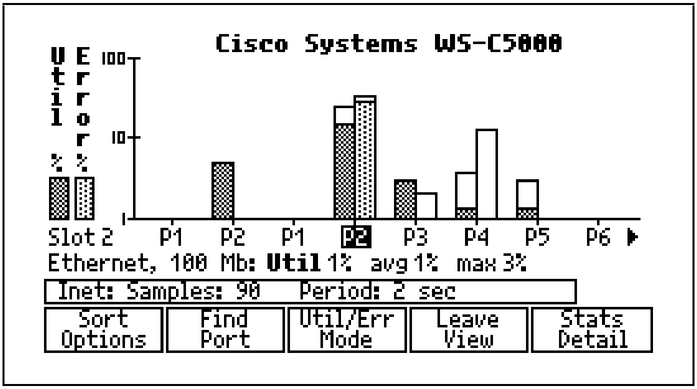
MultiPort Statistics Test Features

The MultiPort Statistics test has the following features:

- Sort Options
- Find Port
- Util/Err Mode
- Leave View
- Stats Detail

Figure 7-5 shows an example of MultiPort Statistics. It shows the current and maximum values for percent Utilization and percent Error. This screen can display up to eight ports simultaneously. Additional ports can be displayed by using the arrow keys or the **Find Port** softkey. Refer to the Find Port section in this chapter for more information.

The ports or interfaces shown will have utilization and error statistics updated every polling period (the default is 2 seconds). The port or interfaces not displayed will have maximum and average utilization and error values updated when a manual re-sort is selected or automatically about every 60 seconds. WAN interfaces will show the highest value of **DCE(IN)** or **DTE(OUT)**.



Ethernet, 100 Mb: **Util** 1% avg 1% max 3%

Inet: Samples: 90 Period: 2 sec

Figure 7-5. MultiPort Statistics

The Port Detail line, as shown in Figure 7-5, indicates the technology (for example, Ethernet), speed, and the current, average, and maximum Utilization, or Error, for the selected port. You can toggle the Port Detail line between Utilization and Error information by selecting **Util/Err Mode**. The Port Detail line indicates **DOWN** if statistics information is not available for the selected port.

MultiPort Statistics reports port numbers from the Bridge MIB. Due to the possibility of non-bridge ports in the Interface Table, the reported port number (**P1**, for example) may not be in the first Interface Table entry, but will often reflect the labeled port number on that device. When MultiPort Statistics can determine the port number it reports a **P** and the number (for example **P1**) and can provide Bridge Forwarding Table addresses under Stats Detail. When MultiPort Statistics can not determine the port number it reports the Interface

Table index number as an **I** (for interface) and the number (for example **I1**) and can not provide Bridge Forwarding Table addresses under Stats Detail.

For supported chassis switches with plug-in modules, MultiPort Statistics can report the slot and port numbers as labeled on the device if that vendor's private MIB is supported by the Enterprise LANMeter. The slot and port numbers are obtained from the private MIB. Refer to Figure 7-5. If private MIB information is not available or not supported, the port number is obtained from the Bridge MIB and the interface number is obtained from the Interface Table.

You can navigate through the main MultiPort Statistics display by using the keys listed in Table 7-1.

Table 7-1. MultiPort Statistics Key Navigation

Key	Function
△	Selects the port to the far-left on the display. Pressing a second time scrolls the display to the left by one full screen (if available).
▽	Selects the port to the far-right on the display. Pressing a second time scrolls the display to the right by one full screen (if available).
◁	Selects the next port to the left (same as SHIFT, then TAB).
▷	Selects the next port to the right (same as TAB).
SHIFT, then ◁	Selects the first port of the list.
SHIFT, then ▷	Selects the last port of the list.

Source of Data

SwitchWizard MultiPort Statistics shows the best information possible for the target device. Many switches support the RMON MIB, which reflects the health and performance of the entire LAN segment. On many switches, port-by-port MIB II statistics often reflect LAN segment values also. Some switches support RMON, MIB II only, or MIB II with an associated Transmission Error MIB. Some RMON implementations, from some devices, may be less reliable than MIB II data sources if they perform software-only statistics analysis. You can turn off RMON and analyze only MIB II data in those cases. For Token Ring RMON data sources, the MAC Layer and Promiscuous statistics groups must be present.

For other devices, such as routers and computer systems, the MIB II counters reflect the traffic in and out of that interface only. For example, the LAN segment may be very busy with over 60% utilization, but if little data is going through that router's interface, it may report only 4 or 5% utilization.

MultiPort Statistics relies upon the MIB II Interface Table and supported private MIBs for configuration data. If those tables do not contain entries for the switch's LAN ports, statistics for that device's ports will not be available. Other devices, such as routers and computer systems, can also be analyzed using SwitchWizard's MultiPort Statistics depending upon the level of MIB support.

The following is the source of the statistics data:

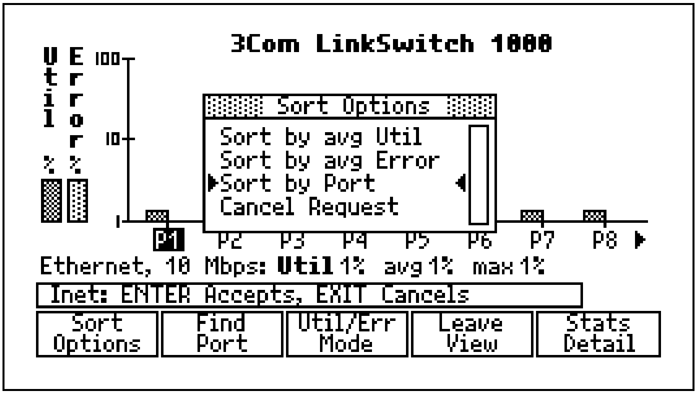
- ❒ Private (or Proprietary) MIB specifications (As of LANMeter instrument software version 7.50, SwitchWizard supports private MIBs for selected Bay Networks and Cisco Systems devices.)
- ❒ RMON Statistics Group, if available (default)
- ❒ MIB II Interface Table with Ethernet, Token Ring, or FDDI Transmission MIB (error information only)
- ❒ MIB II Interface Table only

Sort Options

You can select **Sort Options** to sort the ports by one of the following criteria, also shown in Figure 7-6. Pressing **Sort Options** also shows the current sort method.

❒ Sort by average Utilization
❒ Sort by average Error
❒ Sort by Port number (the default)

There will be a slight delay every time you perform a sort. This is because the non-displayed ports must be polled again prior to executing the sort. If you are sorting by utilization or by error, ports will automatically be re-sorted every 60 seconds.



3Com LinkSwitch 1000

Ethernet, 10 Mbps: **Util** 1% avg 1% max 1%

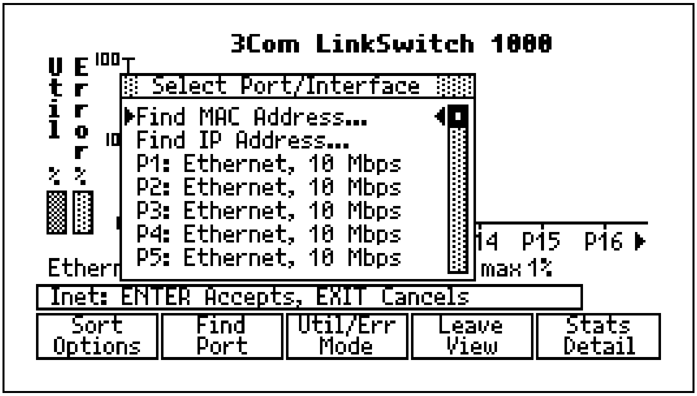
Inet: ENTER Accepts, EXIT Cancels

Figure 7-6. MultiPort Statistics Sort Options

Find Port

You can select **Find Port** to display an ordered list of ports from which you can then select a port for viewing, as shown in Figure 7-7. You can also search the target device for a specific port or interface by one of the following ways. After finding a port, that port or interface is highlighted on the screen.

- By location of MAC address
- By location of IP address
- By port or interface number



Inet: ENTER Accepts, EXIT Cancels

Figure 7-7. MultiPort Statistics Find Port

If the target supports the Bridge MIB Forwarding Table, you can find the port where a certain station resides. If you are running hyperlinked from the Segment Discovery test, you can also find ports based upon IP address. MultiPort Statistics will query the Bridge MIB for the MAC address shown in Segment Discovery's "Local Hosts" for the entered IP address.

After selecting **Find MAC Address** or **Find IP Address** you can use the **Station List** softkey to choose a MAC or IP address already merged into the Enterprise LANMeter's Station List.

You can also scroll the list of ports and interfaces to select one particular port for viewing.

Stats Detail

Pressing **Stats Detail** zooms into the details for the selected port or interface. Port information, including that port's MAC forwarding table from the Bridge MIB (if available), is displayed. You can also view more detailed errors and utilization frame counters. The error details shown will be determined by the MIB support for the agent and the port. If the RMON MIB or a detailed Transmission MIB (Ethernet, Token Ring, or FDDI) is available, then detailed error information will be reported.

Selecting **Stats Detail** provides access to the following information:

❐ Source Details
❐ Interface Stats
❐ Interface Errors
❐ Interface Events

Source Details

Selecting Source Details displays information on the selected interface, as shown in Figure 7-8. Source Details show MAC, IP, and FDDI information for that port's interface (if available). If the target supports the Transparent Bridge Forwarding table from the bridge MIB, the associated MAC addresses are displayed showing which devices are active on that LAN segment.

Note

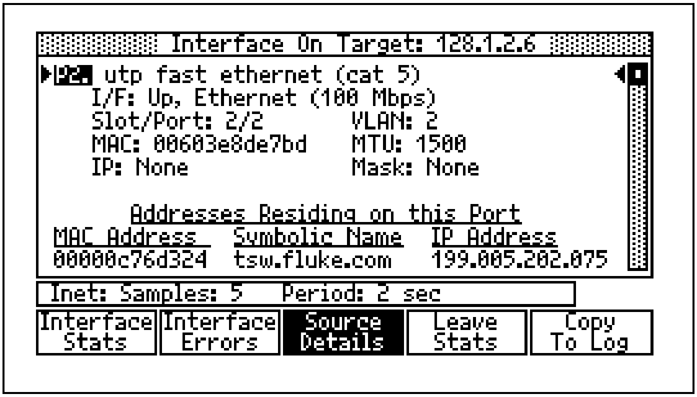
> *If the Toolkit was run from Segment Discovery, IP addresses and DNS names are shown if Segment Discovery has discovered those stations in "Local Hosts" and has found DNS names for those hosts.*

MAC addresses are collected from the Bridge Forwarding Table of the switch, or bridge, which has entries of all MAC addresses active on that port.

For supported chassis switches with plug-in modules, MultiPort Statistics can report the slot and port numbers as labeled on the device if that vendor's private MIB is supported by the Enterprise LANMeter. The slot and port numbers are obtained from the private MIB. If private MIB information is not available or not supported, the port number is obtained from the Bridge MIB and the interface number is obtained from the Interface Table.

If MultiPort Statistics detects a virtual LAN (VLAN) configuration, the VLAN number for the port is also displayed. A VLAN is a group of ports configured into one broadcast domain (or logical LAN). VLANs can only be detected by using private MIBs that are supported by the Enterprise LANMeter.

The MIBs used as the source of data are listed at the bottom of the scroll window.



```
Interface On Target: 128.1.2.6
▶P2. utp fast ethernet (cat 5)
    I/F: Up, Ethernet (100 Mbps)
    Slot/Port: 2/2        VLAN: 2
    MAC: 00603e8de7bd     MTU: 1500
    IP: None              Mask: None

        Addresses Residing on this Port
 MAC Address    Symbolic Name   IP Address
 00000c76d324   tsw.fluke.com   199.005.202.075
Inet: Samples: 5   Period: 2 sec
```

Figure 7-8. MultiPort Statistics Source Details

You can press **Copy To Log** to save the bridge forwarding table (the addresses that reside on this Port) to the Toolkit log. If anything is currently in the log, pressing **Copy to Log** appends the additional results to the end of the log file. The **Copy to Log** softkey is grayed out after it is used.

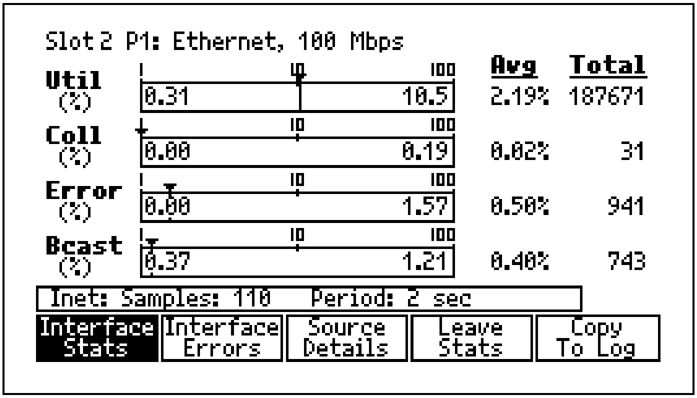
Interface Stats

The Interface Stats display shows the percentages for Utilization, Error, Broadcasts, and Collisions for the selected port as shown in Figure 7-9.

You can press **Copy To Log** to save statistics to the Toolkit log. If anything is currently in the log, pressing **Copy to Log** appends the additional results to the end of the log file. The **Copy to Log** softkey is grayed out after it is used.

The individual statistics displayed depends on the MIB used. Refer to Table 7-2 for a listing of the individual statistics that are displayed for each MIB.

For a detailed listing of Interface and Error Statistics based upon data source and interface type, refer to Table 7-3 and 7-4.



```
Slot 2 P1: Ethernet, 100 Mbps
                1        10        100    Avg     Total
Util           0.31               10.5    2.19%   187671
(%)
                         10        100
Coll           0.00               0.19    0.02%       31
(%)
                1        10        100
Error          0.00               1.57    0.50%      941
(%)
                1        10        100
Bcast          0.37               1.21    0.40%      743
(%)
 Inet: Samples: 110   Period: 2 sec
```

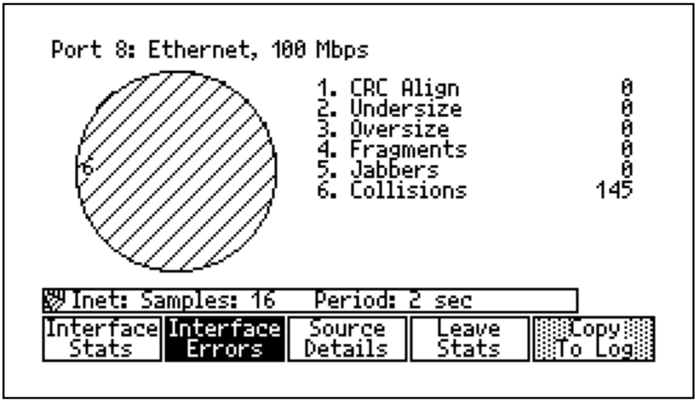
Figure 7-9. MultiPort Statistics Interface Stats

Table 7-2. Statistics Displayed per Source MIB

	Source MIBs			
Statistic	**MIB II**	**MIB II (WAN)**	**RMON**	**Transmission MIBs**
Util%	X		X	X
Util% (In)		X		
Util% (Out)		X		
Collisions			X	X
Errors	X	X	X	X
Broadcasts	X	X	X	X

Interface Errors

The Interface Errors display shows the error details for the selected port as shown in Figure 7-10. This information is not available if the data source was only the MIB II Interface Table and no Transmission MIBs were available.



```
Port 8: Ethernet, 100 Mbps

1. CRC Align            0
2. Undersize            0
3. Oversize             0
4. Fragments            0
5. Jabbers              0
6. Collisions         145

Inet: Samples: 16   Period: 2 sec
```

Figure 7-10. MultiPort Statistics Interface Errors

Note

For end-nodes and routers, utilization and error statistics represent the performance of the targeted interface only. It does not represent the performance of the entire segment where the interface is attached, but of the errors and traffic sent to and from that interface. For most Ethernet and Token Ring switches, these statistics represent the performance and errors for the port's segment. RMON Statistics in MultiPort Stats should always represent segment-wide statistics, as indicated in Table 7-3. Table 7-4 shows MIB II, Ethernet, Token Ring, and FDDI Transmission MIB errors.

Table 7-3. Ethernet and Token Ring RMON Errors

	Errors	Statistics
RMON Ethernet RFC 1271	CRC Align Undersize Oversize Fragments Jabbers Collisions	Utilization Broadcasts Multicasts Collisions
RMON Token Ring RFC 1513	Token Ring Errors Burst Line Abort ARI/FCI Internal Frequency Lost Frame Rx Congestion Frame Copy Token	Token Ring Util Utilization Broadcasts Multicasts

Table 7-4. MIB II and Transmission MIB Errors

	Errors
MIB II **RFC 1213**	MIB II shows errors reported by lower layers but provides no detail.
Ethernet-Like **Transmission MIB** **RFC 1643**	Too Long Bad FCS Misaligned Transmit Delay 1 Collision Frames >1 Collisions Frames Excess Collisions Late Collisions
Token Ring **Transmission MIB** **RFC 1231** **RFC 1239**	Burst Line Abort ARI/FCI Internal Frequency Lost Frame Rx Congest Frame Copy Token
FDDI **Transmission MIB** **RFC 1285** **RFC 1512**	Frame Errors Lost Frames TVX Expire Not Copied TRT Expire Ring Ops Link Error Rate (LER)

If Enterprise LANMeter detects a serial (WAN) interface, it still uses MIB II variables but displays **Util % (IN)**, **Util % (OUT)**, **Errors (IN)**, and **Errors (OUT)**.

If Enterprise LANMeter determines that a Transmission MIB is supported for a given interface, that MIB is used to provide detailed information on the interface. Otherwise, only MIB II information is used to provide less detailed information, refer to Table 7-3.

For all links, Enterprise LANMeter is dependent on the reported speed of the link to report statistics. If this speed is reported wrong, the percentage results can be significantly in error.

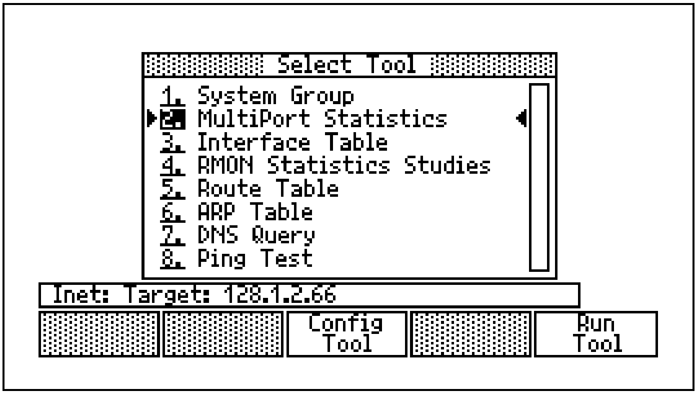
The accuracy of the FDDI information shown depends on the target's support of the FDDI MIB, including some optional groups.

You can press **Leave Stats** or EXIT STOP to return to the main MultiPort Statistics screen and then, if you desire, press **Leave View** or EXIT STOP to close the MultiPort Statistics test and return to the Internet TCP/IP test screen (or Toolkit, if that was your method of entering MultiPort Statistics).

SwitchWizard for the Internet Toolkit

SwitchWizard enhances the Internet Toolkit for troubleshooting switched networks by adding the MultiPort Statistics test as a tool. This tool provides the ability to analyze the health and performance of remote switched LAN segments on switched networks.

You can access the MultiPort Statistics tool from the MultiPort Statistics Test, the **Internet Toolkit** softkey, or a hypertext link from another of the Internet TCP/IP tests. Internet TCP/IP tests, including the Internet Toolkit, are covered in Chapter 6 “Testing TCP/IP Networks.” Figure 7-11 shows the Toolkit Menu.



Inet: Target: 128.1.2.66

Figure 7-11. Toolkit Menu

Chapter 8
Testing Banyan VINES

Introduction

The Enterprise LANMeter can test your Banyan VINES for Ethernet or Token Ring networks using the VINES Internet Protocol (VIP), by using one of the following Banyan tests. The Banyan tests diagnose problems on Banyan VINES networks and are accessed by selecting the **Banyan VINES** top level softkey. Figure 8-1 shows the Banyan VINES top level softkeys.

Refer to Chapter 6 “Testing TCP/IP Networks,” for VINES networks using TCP/IP.

❐ Address Server
❐ Server Discovery
❐ Top VINES

The Banyan VINES tests verify client and server connectivity across VINES Internet Protocol (VIP) routers, compile a list of servers, and identify the top senders and receivers of Banyan VINES traffic.

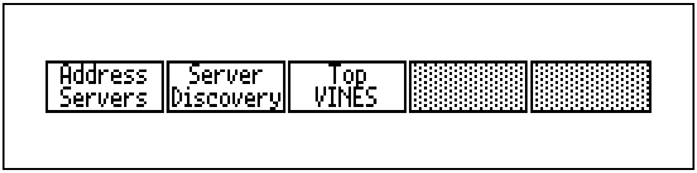


Figure 8-1. Banyan VINES Top-Level Softkeys

It is important to properly connect the instrument to your network. Refer the “Attaching Cables” section in the *“Getting Started”* manual for detailed information on attaching cables.

Configuring Banyan VINES Tests

All Banyan VINES tests are configured in a similar manner. It is not necessary to configure a Banyan VINES test unless you want to change the default condition. Use the following procedure to configure all Banyan VINES tests:

1. Press MORE, then press the **Banyan VINES** top level softkey.
2. Highlight the desired test for configuration.

   The exact steps required to highlight a test depend on which test you want to configure. The first test in a group is automatically highlighted. Otherwise you press the test softkey once.
3. Press MENU, select the **Configure** option (it may already be selected), and press ENTER RUN.
4. Configure the desired parameters.

   Banyan VINES tests have different configuration parameters. Refer to the specific test section for available configuration parameters.

   To undo any configuration changes you made, select **Cancel Changes** in the Configuration Menu, and then press ENTER RUN.
5. Press EXIT STOP to save your configuration to non-volatile memory and exit the Configuration screen.

Running Banyan VINES Tests

All Banyan VINES tests are run in a similar manner. Use the following procedure to run all Banyan VINES tests:

1. Press MORE, then press the top level **Banyan VINES** softkey.
2. Highlight the desired test to run.

   The exact steps required to highlight a test depend on which test you want to run. The first test in a group is automatically highlighted. Otherwise you press the test softkey once.
3. Configure the instrument parameters for the selected test. Refer to the specific test section for information on available configuration parameters.
4. Connect the instrument as described in the "Attaching Cables" section in the "*Getting Started*" manual.
5. Run the desired test by pressing the test softkey or by pressing ENTER RUN.
6. Observe the test results. Refer to the individual test sections for information on available results options.
7. Press EXIT STOP to end the test.

Description of the Banyan VINES Tests

The following sections describe each Banyan VINES Test:

❒ Address Server
❒ Server Discovery
❒ Top VINES (Top Senders and Top Receivers)

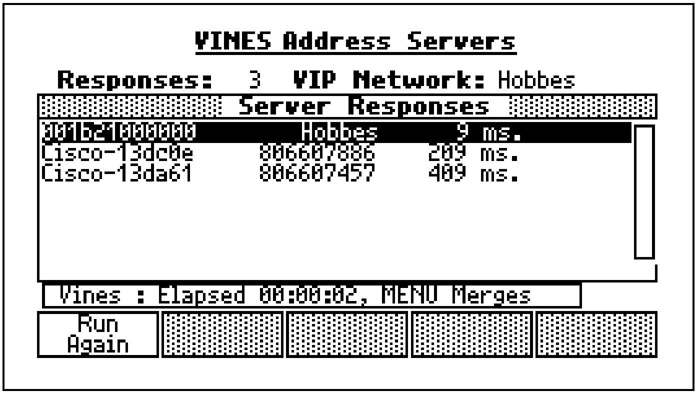
Address Server

Address Server displays local VINES servers and routers that provide clients with dynamic VINES Internet Protocol (VIP) addresses. When a client comes on-line, it requires a dynamic VIP address from a VINES address server to complete its boot process. There are no configurable options for Address Server.

Results

The VINES address servers are displayed in the order that they respond to the initial VINES ARP request. Address Server results show the following information. Figure 8-2 shows Address Server sample results.

- ❒ MAC address
- ❒ Server or Router VINES IP addresses
- ❒ Response time



```
VINES Address Servers

Responses:  3  VIP Network: Hobbes
             Server Responses
001b21000000         Hobbes         9 ms.
Cisco-13dc0e       806607886      209 ms.
Cisco-13da61       806607457      409 ms.

Vines : Elapsed 00:00:02, MENU Merges
```

Figure 8-2. VINES Address Server Sample Results

The VIP Network address indicates the network number of the server or router that responded first to provide the LANMeter instrument with a dynamic VIP address. You can add any Address Servers found to the Station List by pressing MENU and selecting **Merge Stations**.

Note

After you use MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.If no* ***VINES*** *Address Servers respond, then a client cannot boot on this network for Banyan VINES.*

Server Discovery

Server Discovery attempts to find all VINES servers on the network up to the configured Hop Count limit. Server Discovery displays servers that respond to a VINES StreetTalk broadcasts by their VINES IP addresses.

Configuration Parameters

You can configure the following parameters for Server Discovery (the defaults are underlined):

❒ Timeout parameter as 1 second, 5 seconds, or 30 seconds.
❒ Hop Count of 0 to 15, to place a limit on the search.

Note

The LANMeter instrument sends a StreetTalk broadcast that solicits multiple responses from all servers within the configured hop count. These responses may impact the performance of slow serial links. To minimize this effect, start testing with relatively small hop counts.

Results

The instrument displays Server Discovery results after the configured timeout. Server Discovery results show the following information. Figure 8-3 shows Server Discovery sample results.

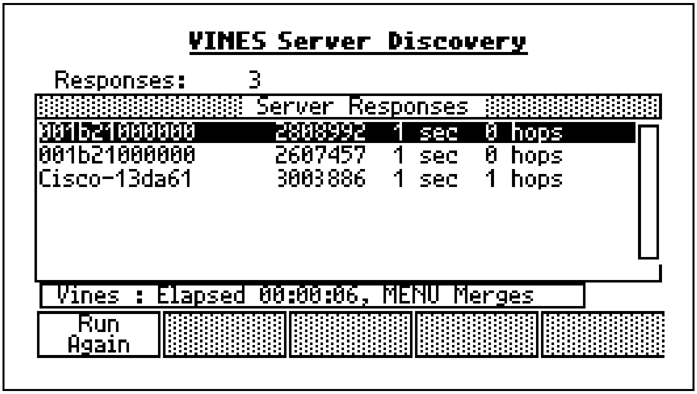
❒ MAC address, Ethernet or Token Ring
❒ VINES IP addresses
❒ Hops to server
❒ Response time (in seconds)

VINES servers that are measured to be zero hops away are on the same local area network as the LANMeter instrument. VINES servers that are one or more hops away are on the other side of a VINES router or router-server.

You can merge any servers found into the VINES Station List and into the Ethernet or Token Ring MAC Station List by pressing MENU and selecting **Merge Stations**. The instrument only merges MAC addresses that are local to the LAN where it is attached (that is, zero hops away). This is because packets going through routers use the local router’s MAC address. This is valid for Ethernet or Token Ring networks.

Note

> *After you use* MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.*



```
VINES Server Discovery

Responses:     3
Server Responses
001b21000000      2808992  1 sec  0 hops
001b21000000      2607457  1 sec  0 hops
Cisco-13da61      3003886  1 sec  1 hops

Vines : Elapsed 00:00:06, MENU Merges
```

Figure 8-3. VINES Server Discovery Sample Results

Server Discovery can display more than a full screen of information, depending on the quantity of servers on the network. You can display servers that are beyond the screen by using △ and ▽.

Top VINES (Top Senders and Top Receivers)

Use the **Top VINES** softkey to access the Top Senders and Top Receivers tests which track the top senders and receivers of Banyan VINES traffic. Top Senders and Top Receivers tests run simultaneously like all other Top Senders and Top Receivers tests but do not show results in a pie chart. Once you run Top Senders or Top Receivers, you can observe the results of the other test by pressing its softkey.

Banyan VINES Top Senders and Top Receivers track servers and end-nodes by their VINES IP address. End-nodes (or client addresses) are tracked, but are not merged into the Station List (like the servers are) when you select that option. This is because VINES end-nodes use dynamic addresses (which change often).

Note

> *When a network passes a packet through a Banyan VINES router, the router transmits the packet using its own MAC address. This leaves the network layer addresses untouched. The instrument gets an accurate picture of the end-to-end traffic by observing network layer addresses.*

Configuration Parameters

You can configure the following parameters for Top Senders and Top Receivers (the defaults are underlined):

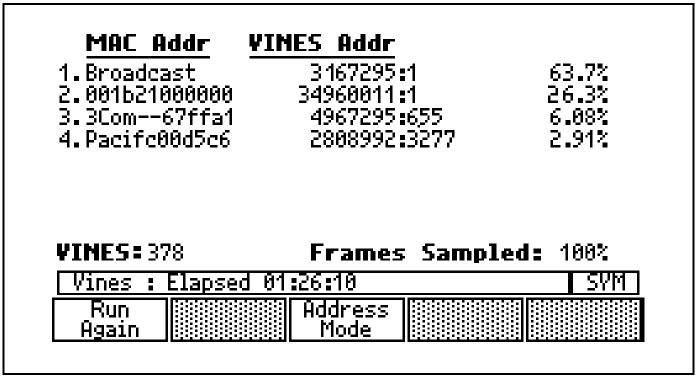
- ❒ Senders to a single station as Off or On. If you select On, then also configure the following parameter:
- ❒ Filter address in VINES IP address (in decimal) or press SPACE to select from Banyan VINES Servers in Station List. Only server addresses (i.e. ending in **1**) can be filtered.

Results

The instrument displays Top Senders and Top Receivers results while VINES sending or receiving stations are monitored on the network. The Top Senders and Top Receivers tests correlate the MAC and VIP addresses by displaying the following results. Figure 8-4 shows VINES Top Receivers sample results.

- ❒ Ethernet and Token Ring MAC address
- ❒ VINES IP address
- ❒ Percent of VINES traffic
- ❒ Total frames sampled

The Top Senders test results are similar to that of Top Receivers.



```
   MAC Addr    VINES Addr
1.Broadcast        3167295:1          63.7%
2.001b21000000    34960011:1          26.3%
3.3Com--67ffa1     4967295:655        6.08%
4.Pacifc00d5c6     2808992:3277       2.91%




VINES:378         Frames Sampled: 100%
 Vines : Elapsed 01:26:10              SYM
```

Figure 8-4. VINES Top Receivers Sample Results

You can press the **Address Mode** softkey, while the results are displayed, to access a menu for you to select the addresses displayed for VINES as symbolic or decimal and for MAC as symbolic, manufacturer, and Hex. After you stop the test by pressing EXIT STOP, you can view the last results by pressing MENU, then selecting **Last Result**. VINES Top Senders and Top Receivers support the View All feature like all Top Senders and Top Receivers.

The VIP address is in the form of **`network#:subnet#`**, where the network number is provided by the server. The network number for any end-node is the network number of its server. VINES servers always have a subnet number of 1.

You can merge all VINES network addresses found into the VINES Station List by pressing MENU and then selecting **Merge Stations**. The Merge Stations feature also adds MAC addresses into the Ethernet (or Token Ring) MAC Station List.

Note

After you use MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.*

The instrument only merges network addresses and only those MAC addresses that are local to the LAN where it is attached. This is because packets going through a router use that router’s MAC address. This is valid for Ethernet or Token Ring networks.

Station List

Vines addresses can be merged into the Station List. When this happens, the address is put into the VIP (Vines IP) list as well as the MAC list. Only servers are merged. This is because client addresses are dynamic and change frequently.

An address merged into the VIP list will be in the form **`network#:1`**. The network# comes from the server and the 1 indicates a server. In the MAC list, a name will automatically be given in the form **`VN network#.`** The VN indicates Vines and the network# is given to help identify the MAC address with the Vines Network # when it was found.

Chapter 9
Testing NetBIOS (Microsoft and IBM PC Networks)

Introduction

The Enterprise LANMeter can test your Network Basic Input/Output System (NetBIOS) networks and diagnose problems by using one of the following NetBIOS tests. The NetBIOS tests are accessed by pressing MORE and then selecting the **NetBIOS** top-level softkey.

❐ IP Auto Config
❐ NetBIOS Discovery
❐ NetBIOS Ping
❐ Top NetBIOS

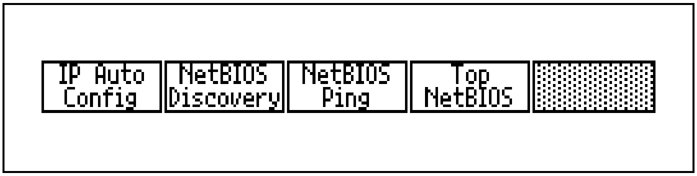


Figure 9-1. NetBIOS Test Softkeys

NetBIOS is used on top of three encapsulated protocols; 802.2 (NetBEUI, NetBIOS Extended User Interface), IPX/SPX, and TCP/IP. These protocols are used by various operating systems and peer-to-peer workstations including; Microsoft's NT Server, NT Workstation, Windows for Workgroups, Windows 95, and LAN Manager; IBM's LAN Server, IBM OS/2; and Novell NetWare's NetBIOS.

NetBIOS is a protocol that supports the Server Message Block (SMB) protocol. SMB is encapsulated on NetBIOS and carries the application data. Microsoft's NT Server, NT Workstation, and Windows 95, and IBM's LAN Server (for example) are all SMB servers. The protocol stacks are comprised of SMB, then NetBIOS, and then whatever is underneath NetBIOS (such as NetBEUI, IPX/SPX, or TCP/IP).

NetBIOS tests are driven by node names within an administrative domain. Each domain handles security and is administered locally.

Note

A NetBIOS domain is different than a TCP/IP Domain Name Service (DNS).

The LANMeter instrument supports RFC 1001 and 1002 for NetBIOS over TCP/IP.

It is important to properly connect the instrument to your network. Refer to the "Attaching Cables" section in the "*Getting Started*" manual for detailed information on attaching cables.

The LANMeter instrument can test NetBIOS communications that occur over either the TCP/IP or IPX/SPX and 802.2 protocols. For additional TCP/IP testing refer to Chapter 6 "Testing TCP/IP Networks." For additional IPX/SPX testing refer to Chapter 5 "Testing Novell NetWare."

Configuring Instrument IP Parameters

Refer to the "Configuring Enterprise LANMeter's IP Parameters" section in Chapter 6 for information on this topic.

The NetBIOS tests requires some configuration information in order to test networks with different NetBIOS encapsulations. Running the IP Auto Config or manually configuring the IP information is required to test NetBIOS over TCP/IP. This configuration information is shared with the Internet TCP/IP tests described in Chapter 6. If the LANMeter instrument has already been configured for your network under TCP/IP, you do not have to reconfigure the instrument.

The NetBIOS Ping test using IPX/SPX requires you to select a Frame Type (Ethernet only).

Running NetBIOS Tests

All NetBIOS tests are run in a similar manner. Use the following procedure to run all NetBIOS tests.

1. Verify that the LANMeter instrument is connected properly.
2. Press [MORE] and then the top-level **NetBIOS** softkey.
3. Configure the LANMeter instrument's IP parameters if your network supports NetBIOS over TCP/IP (not required for Top NetBIOS).
4. Configure the desired parameters for the NetBIOS test that you are going to run.
5. Run the desired test by pressing the test softkey or by pressing [ENTER RUN].
6. Observe the test results. Refer to the individual test sections for information on available results options. The LANMeter instrument displays a changing symbol on the Status Line to indicate activity.
7. Press [EXIT STOP] to end the test.

Whenever the LANMeter instrument runs an Internet TCP/IP or a transmitting NetBIOS test it determines if it is using another host's IP address. If the LANMeter instrument is using a duplicate IP address, the instrument displays an error message.

Description of the NetBIOS Tests

The following sections describe each NetBIOS test:

❒ IP Auto Config
❒ NetBIOS Discovery
❒ NetBIOS Ping
❒ Top NetBIOS (Top Senders and Top Receivers)

IP Auto Config

Refer to the "IP Auto Config" section in Chapter 6 for information on this topic.

NetBIOS Discovery

NetBIOS Discovery analyzes the attached network and catalogs the key NetBIOS network attributes (such as name to address information) while it searches for network problems (such as Duplicate Machine Names.) The NetBIOS Discovery test depends on information obtained from some initial traffic to use for querying the network for additional information.

NetBIOS Discovery is an active test. The LANMeter instrument sends queries to devices on the network to obtain detailed information. The speed at which this information is discovered varies with the current network traffic. For example, the NetBIOS name servers are discovered when a name server responds to a name request.

Configuration Parameters

You can configure the following parameters for NetBIOS Discovery (the defaults are underlined):

❒ Send IP Frames as Yes or <u>No</u>. If you select Yes for the Send IP Frames parameter, you can then select the following. If the IP Auto Config test functioned successfully, this parameter is automatically set to Yes.

❒ Source Address

❒ Router Address

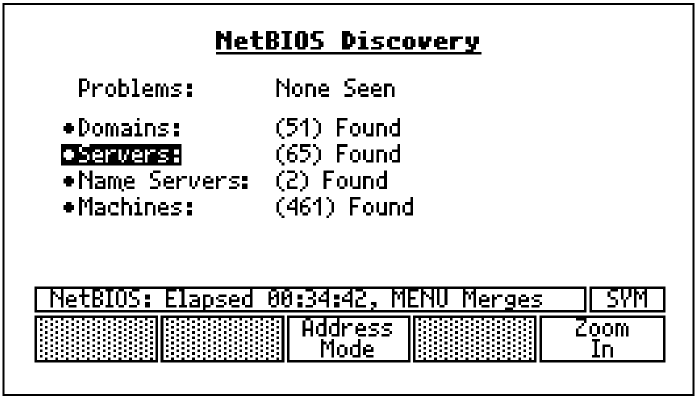
❒ Mask

Results

NetBIOS Discovery test results are displayed as they are discovered. The Status Line shows an activity symbol when the NetBIOS Discovery test is running. The following are some of the problems that the NetBIOS Discovery test can show:

1. Name in Conflict (Duplicate Name)
2. Registration Error
3. Default router not responding to ARP

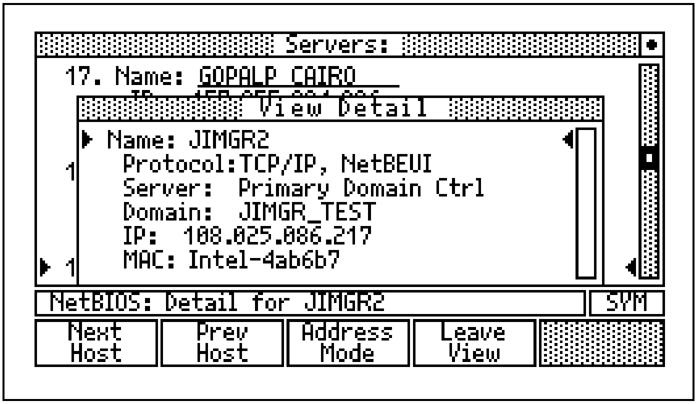
The NetBIOS Discovery test transmits NetBIOS requests onto the network to run its test. Figure 9-2 shows a sample NetBIOS Discovery results screen.



```
NetBIOS Discovery

 Problems:      None Seen

•Domains:       (51) Found
•Servers:       (65) Found
•Name Servers:  (2) Found
•Machines:      (461) Found

NetBIOS: Elapsed 00:34:42, MENU Merges
```

Figure 9-2. NetBIOS Discovery Results Screen

You can press **Zoom In** to view additional information. Figure 9-3 shows a sample NetBIOS servers result screen using **Zoom In**.



```
Servers:
 17. Name: GOPALP CAIRO
View Detail
▶ Name: JIMGR2
   Protocol:TCP/IP, NetBEUI
   Server:  Primary Domain Ctrl
   Domain:  JIMGR_TEST
   IP:  108.025.086.217
   MAC: Intel-4ab6b7
NetBIOS: Detail for JIMGR2
```

Figure 9-3. NetBIOS Servers Results Screen

After the test is stopped, you can view or print the NetBIOS Discovery results by pressing MENU, select **View All** or **Print All** as desired, and then press ENTER RUN.

After the LANMeter instrument has found new stations you can merge these stations into the appropriate Station List by pressing MENU and selecting **Merge Stations**. This allows NetBEUI addresses with the discovered machine names to merge into the MAC list, IPX/SPX nodes to merge into the IPX/SPX list, and IP addresses to merge into the IP list.

Note

After you use MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.*

NetBIOS Ping

NetBIOS Ping allows you to test the network layer connectivity by pinging a node by name.

NetBEUI traffic will be local to the attached segment and is not routable. The configured name for NetBEUI must be local. NetBIOS over IP traffic can cross IP routers and the NetBIOS over IPX/SPX can also cross IPX/SPX routers.

NetBIOS over IP can ping nodes that are local or nodes that are on the other side of routers. The LANMeter instrument queries a NetBIOS Name Server (NBNS) to obtain the IP address information required to ping NetBIOS over IP. The address of the name server must be manually entered into the configuration. If the IP node is not local and is not registered with a NetBIOS name server, the IP address in the LANMeter instrument’s Station List is used.

Some NetBIOS over TCP/IP implementations cannot use NetBIOS Name Servers or may not respond to a local Broadcast. You can use NetBIOS Ping with these nodes by merging or entering the target name and IP address into the Station List before running the Ping.

Configuration Parameters

You can configure the desired Target Name after you highlight the NetBIOS Ping softkey or you can configure the following parameters by pressing MENU, selecting **Configure**, and pressing ENTER/RUN (the defaults are underlined):

❐ Target Name up to 16 characters

❐ Protocol as NetBEUI, Over IPX/SPX, or Over TCP/IP

Selecting **Over IPX/SPX** provides the following additional configuration parameters:

❐ Frame Type as 802.2, 802.3, Ethernet II, or SNAP (Ethernet only)

Selecting **Over TCP/IP** provides the following additional configuration parameters:

❐ Source address

❐ Router address

❐ NetBIOS Name Server address

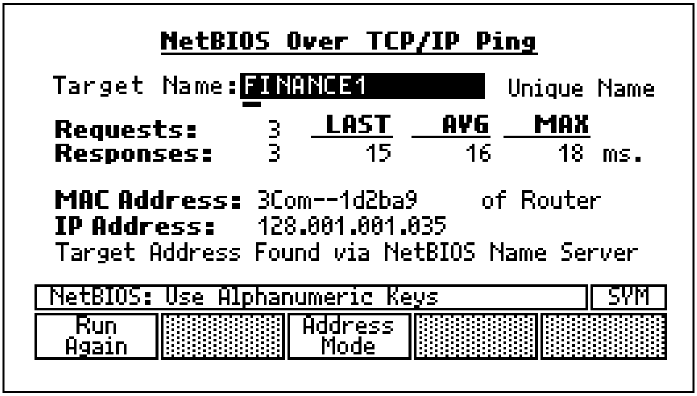
❐ Mask

❐ Run Once or Continuous

❐ Timeout as 1, 5, or 30 seconds

Results

The Status Line shows an activity symbol when the NetBIOS Ping test is running. Figure 9-4 shows a sample NetBIOS Ping results screen.



```
              NetBIOS Over TCP/IP Ping

 Target Name:FINANCE1                Unique Name

 Requests:     3   LAST    AVG    MAX
 Responses:    3     15     16     18  ms.

 MAC Address: 3Com--1d2ba9     of Router
 IP Address:  128.001.001.035
 Target Address Found via NetBIOS Name Server

 NetBIOS: Use Alphanumeric Keys              SYM
```

Figure 9-4. NetBIOS Ping Results Screen

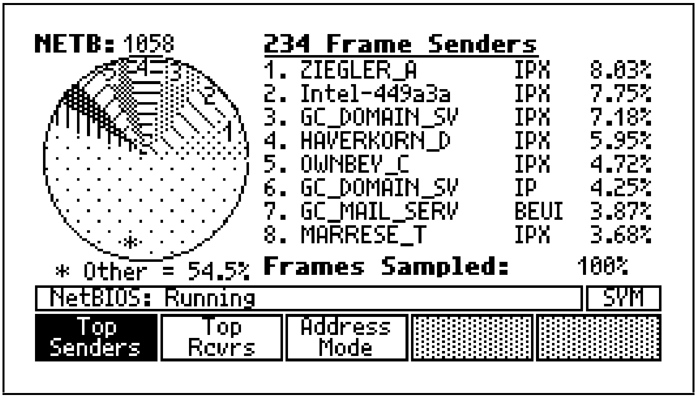
Top NetBIOS (Top Senders and Top Receivers)

Use the **Top NetBIOS** softkey to access the Top Senders and Top Receivers tests which track the top senders and receivers of NetBIOS traffic. Top Senders and Top Receivers tests run simultaneously. Once you run Top Senders or Top Receivers, you can observe the results of the other test simply by pressing its softkey.

There are no configuration parameters for NetBIOS Top Senders and Top Receivers.

Results

The instrument displays Top Senders and Top Receivers results as NetBIOS sending or receiving stations are monitored on the network. The Top Senders and Top Receivers tests display results as source address, encapsulation protocol, percent of NetBIOS traffic, and a pie chart that identifies the senders, or receivers, and shows the quantity of NetBIOS traffic transmitted. Figure 9-5 shows Top Senders sample results. Top Receivers results are similar to that of Top Senders.



```
NETB: 1058        234 Frame Senders
                  1. ZIEGLER_A        IPX    8.03%
                  2. Intel-449a3a     IPX    7.75%
                  3. GC_DOMAIN_SV     IPX    7.18%
                  4. HAVERKORN_D      IPX    5.95%
                  5. OWNBEY_C         IPX    4.72%
                  6. GC_DOMAIN_SV     IP     4.25%
                  7. GC_MAIL_SERV     BEUI   3.87%
                  8. MARRESE_T        IPX    3.68%
 * Other = 54.5%  Frames Sampled:            100%
NetBIOS: Running                              SVM
```

Figure 9-5. NetBIOS Top Senders Sample Results

Note

NetBIOS machines can run with multiple protocols. It is possible for a node to appear three times based upon protocols in use.

You can press the **Address Mode** softkey, while the results are displayed, to access a menu for you to select the station addresses as symbolic name, hexadecimal address, and IPX/SPX network number (Net). These results show IPX/SPX network numbers not MAC addresses.

After the LANMeter instrument has found new stations you can merge these stations into the appropriate Station List by pressing MENU and selecting **Merge Stations**. This allows IP addresses to merge into the IP list, IPX/SPX nodes to merge into the IPX/SPX list, and NetBEUI addresses to merge into the MAC list. These addresses are merged with blank names. You can use the NetBIOS Discovery test for name (address) discovery.

Note

> *After you use* MENU *and* **Merge Stations** *you will be reminded to use the LANMeter* **Station List** *(from Setup/Utils) if you want to save the merged stations into non-volatile memory.*

After the test is stopped, you can view or print all NetBIOS Top Senders and Receivers results by pressing MENU, selecting **View All** or **Print All** as desired, and then pressing ENTER RUN.

Chapter 10
WideAreaWizard Option

Introduction

The WideAreaWizard™ is an optional feature supported in the Fluke Enterprise LANMeter (68x Series) instrument Software Version 8.00 and later. The WideAreaWizard enhances the Internet Toolkit's Interface Table by adding reporting capabilities for discovered WAN interfaces. The WideAreaWizard gives you the ability to discover and diagnose problems on Frame Relay, ISDN, and T1/E1 interfaces on routers, switches, and bridges. The WideAreaWizard also allows you to display virtual circuit information for appropriate technologies.

You can obtain the latest version of LANMeter software either by ordering a new Enterprise LANMeter instrument with option 68X-WW or by ordering the WideAreaWizard software upgrade kit (option 68X-WWK) for your Enterprise LANMeter instrument. The WideAreaWizard option also includes the Terminal Emulator option (see Chapter 13 "Terminal Emulator). If you order the upgrade kit, you must first install the software as described in Appendix D "Software Upgrade," before you can enable it.

The WideAreaWizard option comes configured in a trial usage mode. For more information on trial usage or if you have purchased the option, refer to the "Enabling the WideAreaWizard Option" section of this chapter for information on how to make it permanently enabled.

You can determine if the WideAreaWizard is installed on your Enterprise LANMeter by running **Manage Options**, from **Setup/Utils**, and then pressing ENTER RUN. If the option is enabled, or if trial uses are still available, the WideAreaWizard name appears on the top-level screen as well as on the Internet Toolkit screens.

This chapter contains the following sections on the WideAreaWizard and Figure 10-1 shows the Enterprise LANMeter Internet TCP/IP softkeys.

❐ Enabling the WideAreaWizard Option
❐ WideAreaWizard for the Internet Toolkit

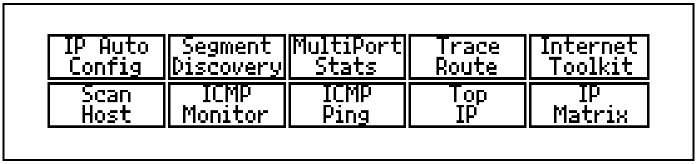


Figure 10-1. Enterprise LANMeter Internet TCP/IP Softkeys

Enabling the WideAreaWizard Option

The WideAreaWizard option comes configured in a trial usage mode. You can use the WideAreaWizard for a predefined number of days before your Enterprise LANMeter reverts back to an instrument without the WideAreaWizard option. A trial day is used when you run Toolkit's Interface Table any number of times in one day. You can run **Manage Options**, from **Setup/Utils**, to view the number of trial days remaining.

If you have purchased the WideAreaWizard option, you can permanently enable it by performing the following steps:

1. Complete the supplied FAX-back form including your Enterprise LANMeter's Ethernet or Token Ring MAC address and serial number, and FAX it to Fluke to receive your enabling key.

   The Ethernet or Token Ring MAC address and serial number are available on the back of Enterprise LANMeter or from the Enable Option softkey screen (Figure 10-2).

2. Press the top-level **Setup/Utils** softkey.

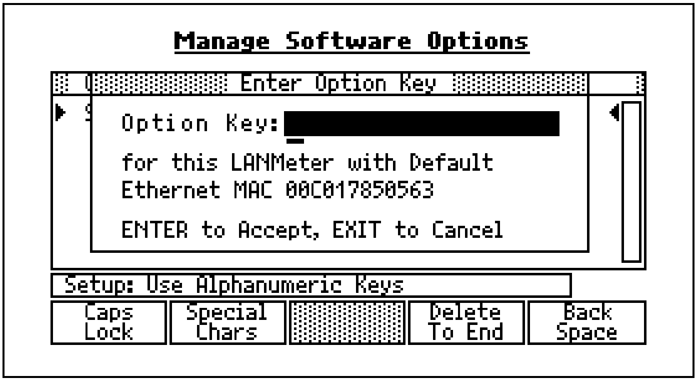
3. Press **Manage Options**, and then ENTER RUN to list your LANMeter instrument's enabled options. Each option can be enabled or disabled. This procedure assumes that your WideAreaWizard option is disabled.

   If you are using the WideAreaWizard option in the trial usage mode, the number of remaining trial days is shown here.

4. Select the WideAreaWizard option and press **Enable Options** to display the Enter Option Key screen, shown in Figure 10-2.

5. Enter your enabling key and then press ENTER RUN to enable the WideAreaWizard option.

6. After the key is enabled, the LANMeter instrument will display a popup message indicating that it needs to reboot in order to implement the change. While it is rebooting, place the WideAreaWizard Label onto the back of your Enterprise LANMeter. The WideAreaWizard Label is included in the option 68X-WW and 68X-WWK kits. This label will help identify units that have the option enabled.



Manage Software Options

Enter Option Key

Option Key:

for this LANMeter with Default
Ethernet MAC 00C017850563

ENTER to Accept, EXIT to Cancel

Setup: Use Alphanumeric Keys

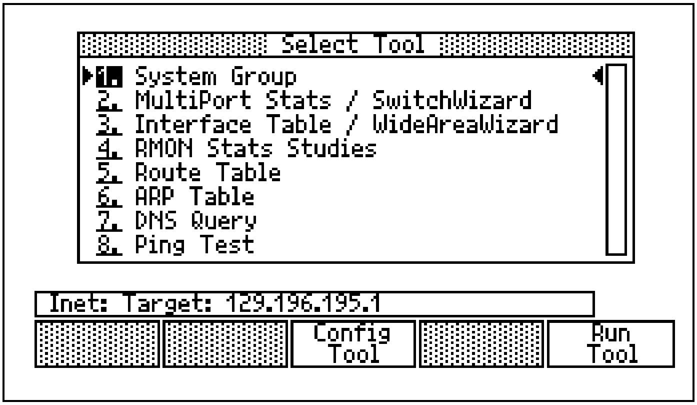
Figure 10-2. Enabling the WideAreaWizard Option

WideAreaWizard for the Internet Toolkit

The WideAreaWizard provides diagnostic information capabilities for Frame Relay, ISDN and T1/E1 (DS1) interfaces on discovered routers, switches and bridges. The WideAreaWizard is accessed through the Interface Table tool in the Internet Toolkit.

Interface Table

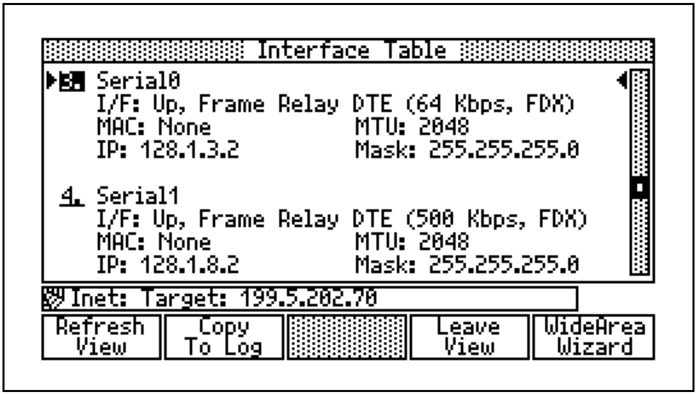
You can access the Interface Table tool from the **Internet Toolkit** softkey, or a hypertext link from another of the Internet TCP/IP tests. Internet TCP/IP tests, including the Internet Toolkit, are covered in Chapter 6 “Testing TCP/IP Networks.” Figure 10-3 shows the Toolkit Menu.



Inet: Target: 129.196.195.1

Figure 10-3. Toolkit Menu

Select the Interface Table to report the detected devices. Figure 10-4 shows Interface Table sample results for Frame Relay. The ISDN and T1/E1 have similar Interface Table result screens.



```
                    Interface Table
3. Serial0
   I/F: Up, Frame Relay DTE (64 Kbps, FDX)
   MAC: None            MTU: 2048
   IP: 128.1.3.2        Mask: 255.255.255.0

4. Serial1
   I/F: Up, Frame Relay DTE (500 Kbps, FDX)
   MAC: None            MTU: 2048
   IP: 128.1.8.2        Mask: 255.255.255.0
Inet: Target: 199.5.202.70
```

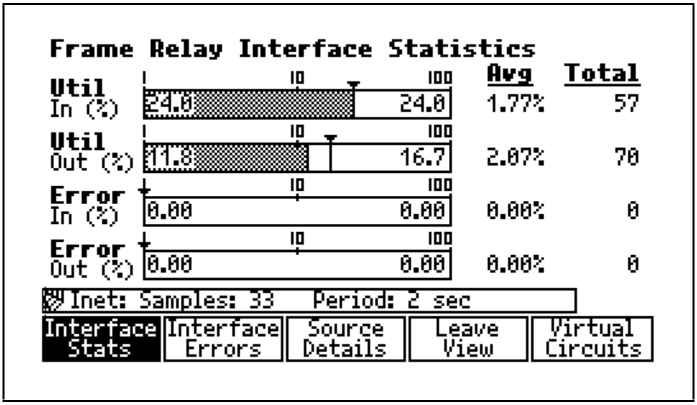
Figure 10-4. Frame Relay Interface Table Sample Results

You can scroll through the Interface Table results to display the discovered interfaces. When you select an interface that is a LAN interface the **Display Stats** softkey is available and when it is a supported WideAreaWizard interface (Frame Relay, ISDN, or T1/E1) the **WideAreaWizard** softkey is available.

Interface Statistics and Errors

Pressing the **WideAreaWizard** softkey displays the Interface Statistics screen for the selected WAN interface. Refer to the “Source Details” section in this chapter for more information.

Figure 10-5 shows sample Interface Statistics results for Frame Relay.



Frame Relay Interface Statistics

			Avg	Total
Util In (%)	24.0	24.0	1.77%	57
Util Out (%)	11.8	16.7	2.07%	70
Error In (%)	0.00	0.00	0.00%	0
Error Out (%)	0.00	0.00	0.00%	0

Inet: Samples: 33   Period: 2 sec

Figure 10-5. Frame Relay Interface Statistics Sample Results

The sample Interface Statistics display shows the percentages for Utilization In, Utilization Out, Error In, and Error Out for the selected interface.

For Frame Relay interfaces, you can select **Interface Errors, Source Details**, or **Virtual Circuit** to display additional information on the WAN interface. For ISDN interfaces, you can select only **Source Details** for additional information because there are no errors specific to ISDN and no virtual circuits for ISDN. For T1/E1 interfaces, you can select only **Interface Errors** for additional information.

You can press **Leave Stats** to exit the WideAreaWizard test.

The individual statistics displayed depends on the MIB used. Refer to Table 10-1 for a listing of the individual statistics that are displayed for each MIB.

For a detailed listing of wide area network errors, refer to Table 10-2.

Table 10-1. Statistics Displayed per Source MIB

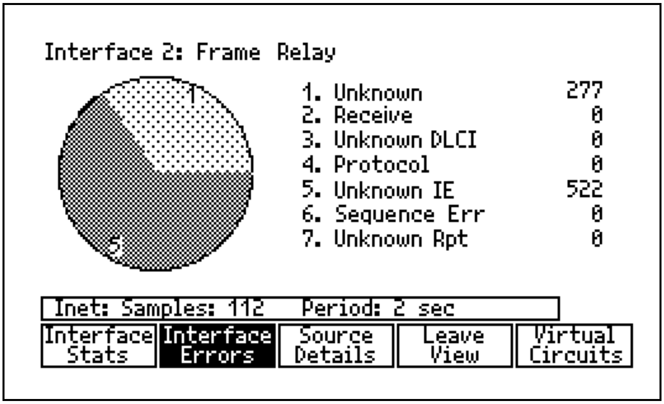
	Source MIBs		
Statistic	**MIB-II**	**ISDN**	**FR DTE**
Util In %	X		
Util Out %	X		
Errs %	X		
Errs In %	X		
Errs Out %	X		
Calls In %		X	
Calls Out %		X	
DLCI Util %			X

For the ISDN MIB, the Calls In % is the percentage of incoming calls accepted out of all incoming calls and the Calls Out % is the percentage of outgoing calls completed out of all outgoing calls.

Table 10-2. Wide Area Network Errors

MIB	Errors
MIB-II	None
FR DTE (RFC 1315)	Unknown Receive (Rcv Short plus Rcv Long) Illegal DLCI Unknown DLCI Protocol Error Unknown IE Sequence Error Unknown Report
ISDN (RFC 2127)	None
FR SVC (RFC 1604)	None
DS1 (RFC 1406)	Errored Seconds Severely Errored Seconds Severely Errored Framing Seconds Unavailable Seconds Controlled Slip Seconds Path Code Violations Line Errored Seconds Burst Errored Seconds Line Code Violations

Figure 10-6 shows sample Interface Errors results for Frame Relay. The T1/E1 has a similar Interface Table result screens.



Interface 2: Frame Relay

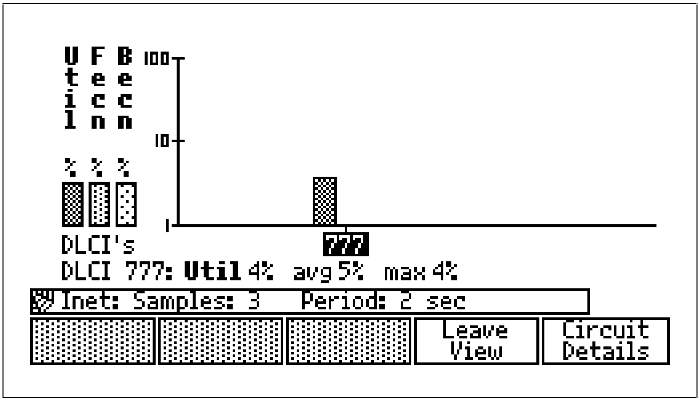
1. Unknown	277
2. Receive	0
3. Unknown DLCI	0
4. Protocol	0
5. Unknown IE	522
6. Sequence Err	0
7. Unknown Rpt	0

Inet: Samples: 112   Period: 2 sec

Figure 10-6. Frame Relay Interface Errors Sample Results

Virtual Circuits

Figure 10-7 shows sample Virtual Circuit results for Frame Relay.



DLCI 777: **Util** 4% avg 5% max 4%

Inet: Samples: 3   Period: 2 sec

Figure 10-7. Frame Relay Virtual Circuits Sample Results

In this sample Virtual Circuit display, the virtual circuits are identified by their Data Link Connection Identifier (DLCI). You can use TAB or the arrow keys to select the desired DLCI circuit. The bargraph shows the maximum and current percentage values for Utilization, Errors, Forward Error Congestion (FECN), and Backward Error Congestion (BECN), and the Interface Detail line (above the status line) displays their current percentage values.

The DLCIs shown will have Utilization, FECN, and BECN statistics updated every polling period (the default is 2 seconds). The DLCIs discovered but not displayed will have maximum and average Utilization, FECN, and BECN values updated automatically about every 60 seconds.

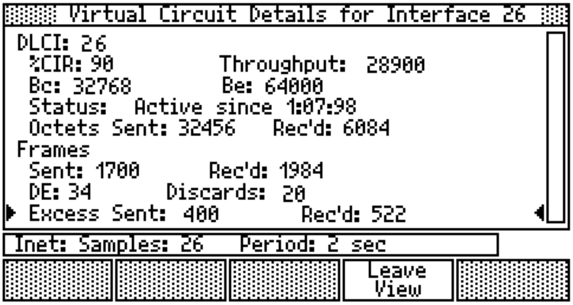
The Virtual Circuit screen can display up to four DLCIs simultaneously. Additional DLCIs can be displayed by using the navigation keys. You can navigate through the Virtual Circuit display by using the keys listed in Table 10-3. Access to the Virtual Circuit display can also be available through a hyperlink from the Source Details screen.

Table 10-3. Virtual Circuit Key Navigation

Key	Function
△	Selects the interface to the far-left on the display. Pressing a second time scrolls the display to the left by one full screen (if available).
▽	Selects the interface to the far-right on the display. Pressing a second time scrolls the display to the right by one full screen (if available).
◁	Selects the next interface to the left (same as SHIFT, then TAB).
▷	Selects the next interface to the right (same as TAB).
SHIFT, then ◁	Selects the first interface of the list.
SHIFT, then ▷	Selects the last interface of the list.

Circuit Detail

You can view information specific to the selected virtual circuit by pressing **Circuit Details**, from the Virtual Circuits screen. Figure 10-8 shows Circuit Detail sample results for Frame Relay.



```
Virtual Circuit Details for Interface 26
DLCI: 26
 %CIR: 90          Throughput:  28900
 Bc: 32768         Be: 64000
 Status:  Active since 1:07:98
 Octets Sent: 32456   Rec'd: 6084
Frames
 Sent: 1700       Rec'd: 1984
 DE: 34      Discards:  20
 Excess Sent: 400        Rec'd: 522
Inet: Samples: 26   Period: 2 sec
```

Figure 10-8. Frame Relay Circuit Detail Sample Results

Source Details

You can press **Source Detail**, from the Interface Statistics screen, to display Source Detail information for each of the following interface types:

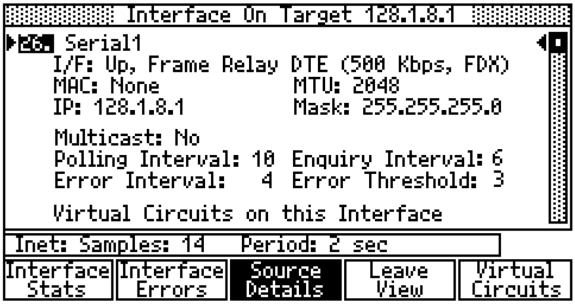
- ❒ Frame Relay
- ❒ ISDN
- ❒ T1/E1

Frame Relay

The following Frame Relay information is displayed for each DLCI:

1. Number of the DLCI or a list of DLCIs.
2. Percentage of circuit used (%CIR)
3. Throughput
4. Committed burst rate (Bc)
5. Excess burst rate (Be)
6. Status of the link and time this link has been up
7. Number of octets sent and received
8. Number of frames sent and received
9. Number of discard eligibility (DE) bits and discards
10. Number of excess frames sent and received

Figure 10-9 shows sample Source Detail results for Frame Relay. If this information is not available, the Source Detail screen reports all zero values.



```
Interface On Target 128.1.8.1
26. Serial1
    I/F: Up, Frame Relay DTE (500 Kbps, FDX)
    MAC: None                MTU: 2048
    IP: 128.1.8.1            Mask: 255.255.255.0

    Multicast: No
    Polling Interval: 10  Enquiry Interval: 6
    Error Interval:    4  Error Threshold: 3

    Virtual Circuits on this Interface
Inet: Samples: 14   Period: 2 sec
```

Figure 10-9. Frame Relay Source Detail Sample Results

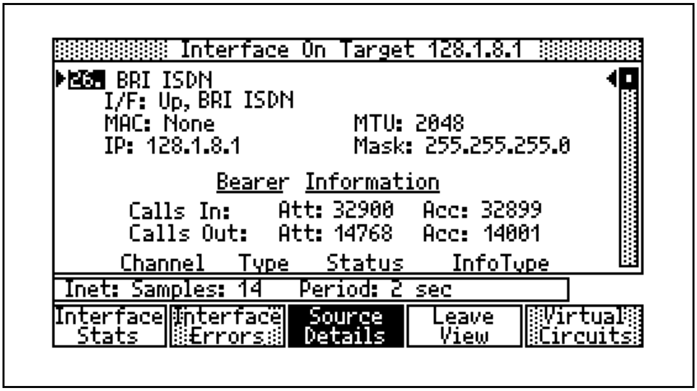
ISDN

The following ISDN information is displayed for each interface:

1. Basic Rate Interface (BRI) or Primary Rate Interface (PRI). For BRI two channels are shown and for PRI, you can scroll through up to 24 or 30 channels.
2. Bearer Information
3. MIB-II interface information
4. Incoming calls attempted and accepted
5. Outgoing calls attempted and accepted
6. Channel number
7. Channel type
8. Bearer status
9. Information Type (audio, speech, etc.)

Figure 10-10 shows sample Source Detail results for ISDN. If this information is not available, the Source Detail screen reports all zero values.

There are no Interface Errors or Virtual Circuits for ISDN interfaces, therefore those softkeys are grayed out.



```
Interface On Target 128.1.8.1
26. BRI ISDN
    I/F: Up, BRI ISDN
    MAC: None            MTU: 2048
    IP: 128.1.8.1        Mask: 255.255.255.0

            Bearer Information
      Calls In:    Att: 32900   Acc: 32899
      Calls Out:   Att: 14768   Acc: 14001
     Channel   Type   Status    InfoType
Inet: Samples: 14   Period: 2 sec
```

Figure 10-10. ISDN Source Detail Sample Results

T1/E1

The following T1/E1 information is displayed for each interface:

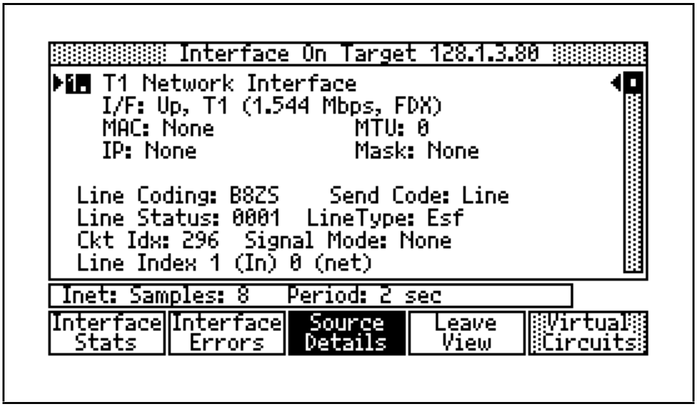
For T1/E1, you access the Source Detail screen by selecting the Interface Table. The following T1/E1 information is displayed for each interface:

1. Line Coding indicates the type of Zero Code suppression used on the link.
2. Send Code indicates the type of code being sent across the DS1 interface.
3. Line Status provides alarm information. Refer to Table 10-4 for information on decoding the Line Status.
4. Line Type indicates the type of DS1 or E1 line implementing the circuit.
5. Circuit Index indicates the vendor-assigned ID number.
6. Signal Mode indicates in-band signaling or error channel signaling.
7. Line Index In indicates the MIB ID of the side of the DSU/CSU going into the user's LAN.
8. Line Index Out indicates the MIB ID of the user's DSU/CSU on the WAN side of the DSU/CSU.

Table 10-4. Decoding the Line Status Field

Value	Meaning
1	No Alarm Present
2	Far End Loss of Frame (LOF) [a.k.a. the “Yellow Alarm”]
4	Near End Sending LOF Indication
8	Far End Sending Alarm Indication Signal (AIS)
16	Near End Sending AIS
32	Near End LOF [a.k.a. the “Red Alarm”]
64	Near End Loss Of Signal
128	Near End is Looped Back
256	E1 TS16 AIS
512	Far End Sending TS16 Loss Of MultiFrame (LOMF)
1024	Near End Sending TS16 LOMF
2048	Near End detects a test code
4096	any line status not otherwise defined

Figure 10-11 shows sample Source Detail results for T1/E1. If this information is not available, the Source Detail screen reports all zero values.



```
Interface On Target 128.1.3.80
1. T1 Network Interface
   I/F: Up, T1 (1.544 Mbps, FDX)
   MAC: None              MTU: 0
   IP: None               Mask: None

 Line Coding: B8ZS    Send Code: Line
 Line Status: 0001  LineType: Esf
 Ckt Idx: 296  Signal Mode: None
 Line Index 1 (In) 0 (net)
Inet: Samples: 8   Period: 2 sec
```

Figure 10-11. T1/E1 Source Detail Sample Results

Chapter 11
Web Agent / WebRemote Control

Introduction

Web Agent is a feature supported in the Fluke Enterprise LANMeter (68x Series) instrument software version 8.00 and later, that gives your instrument Web server capability. Web Agent allows you to access LANMeter instrument information using your Web browser. Web Agent supports Netscape Navigator 4.0 and later, and Microsoft Internet Explorer 4.0 and later. Refer to your Web browser documentation for information on how to use your browser.

WebRemote Control is an optional feature supported in the Fluke Enterprise LANMeter (68x Series) instrument software version 9.00 and later that adds the ability to control your LANMeter instrument remotely using Web Agent. WebRemote Control preserves the functionality of Web Agent and gives you the capability to start and stop measurements and tests from a location physically separate from the instrument. Remote operation is password protected.

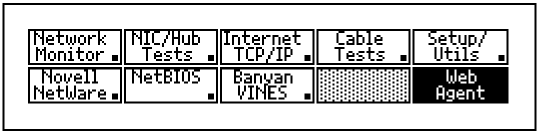


Figure 11-1. Web Agent Softkey Location

This chapter contains the following sections:

❒ Your Instrument as a Web Server
❒ Viewing Instrument Information with a Web Browser
❒ WebRemote Control Option

Your Instrument as a Web Server

To use your LANMeter Instrument as a Web Server you must first configure your LANMeter instrument’s IP parameters and then configure and run Web Agent.

Use the IP Auto Config test to configure your LANMeter instrument’s IP parameters. Refer to “IP Auto Config” in Chapter 6 for information on using IP Auto Config.

Configuration Parameters

The following are the configuration parameters for Web Agent:

- ❒ **LMServer** address as dotted decimal decimal (press the **Station List** softkey to select from the IP station list). LANMeter Server is a software application that permits management and tracking of your LANMeter as it is moved about your intranet. A UDP frame is sent to the device at this address whenever Web Agent is started. Configure LMServer with the IP address of the station running your web browser to enable the web browser to find the LANMeter instrument quicker on your network.

❒ **Web Auto Start** (software Version 9.50 and later) used to automatically enable Web Agent after IP Auto Config and some other measurements are run. If Auto Start is enabled then Web Agent will automatically start when a test that uses the EPI stack is run (e.g. most Internet TCP/IP tests, NetBIOS Discovery, etc.).

❒ **Passwd** used for WebRemote Control access. It can be up to fifteen ASCII characters. Use the softkeys for special characters and other editing functions. The **Caps Lock** softkey (LANMeter) or the **Caps Lock** key (PC) must be used to enter capital letters (not the **Shift** key on your PC or LANMeter instrument keyboard). The default password is *guest*.

Configuring and Running Web Agent

Use the following procedure to configure and run Web Agent. While Web Agent is active, the LANMeter instrument runs a full TCP/IP protocol stack with Web Server capabilities in the background. Your LANMeter instrument responds to ICMP Pings, SNMP queries, and HTTP requests. This processing takes a portion of your LANMeter instrument’s available capacity and may decrease the instrument’s performance in some measurements, such as Top MAC or Protocol Mix.

Note

Web Agent automatically shuts off when you run certain measurements such as Station List, IP Auto Config, Cable Tests or File Manager. A warning message will be displayed allowing you to cancel the selected measurement and leave Web Agent enabled. If Web Auto Start is enabled, then Web will automatically restart after a test that uses the EPI stack is run (e.g. most Internet TCP/IP tests, NetBIOS Discovery, etc.).

The Print All function will also cause Web Agent to shut off. In software version 9.50 and later, Web Agent will automatically restart after the Print All has completed.

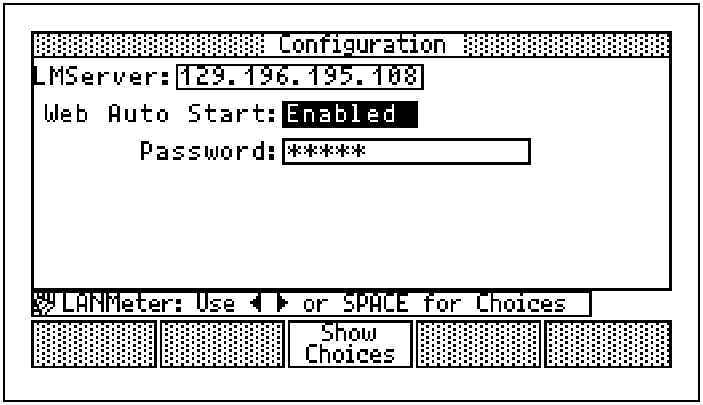
1. Use IP Auto Config to configure your LANMeter instrument’s IP parameters. Refer to “IP Auto Config” in Chapter 6 for information on using IP Auto Config.

2. From the LANMeter instrument top-level display, select the MORE key and then press the **Web Agent** softkey.

3. Press MENU. This also selects the **Configure** option.

4. Press ENTER RUN. Configure the desired parameters. See Figure 11-2. Refer to the “Configuration Parameters” section earlier in this chapter for information on each field.

   To undo any configuration changes you make, press MENU, select **Cancel Changes** in the Configuration Menu, and then press ENTER RUN.



Configuration

LMServer: 129.196.195.108

Web Auto Start: Enabled

Password: *****

▨ LANMeter: Use ◀ ▶ or SPACE for Choices

Figure 11-2. Sample Configuration Menu

Press ENTER RUN or EXIT STOP to save the configuration to non-volatile memory and exit the configuration screen.

5. Press the **Web Agent** softkey to start Web Agent.

6. The Web Agent status displayed on the screen changes from `Starting...` to `Listening...`. The Web Agent icon (▨) is also displayed on the Status Line to indicate that the Web Agent is running.

7. Press EXIT STOP to close the Web Agent screen while continuing to run Web Agent or press the **Stop Agent** softkey to stop Web Agent.

The Web Agent icon (▨) is displayed on the Status Line as long as the Web Agent is running. Web Agent is halted whenever the LANMeter instrument accesses a test or function that may disconnect it from the network (e.g. IP Auto Config, Station List, Cable Tests, File Manager or Print All). If Web Agent Auto Start is enabled then it will automatically restart after IP Auto

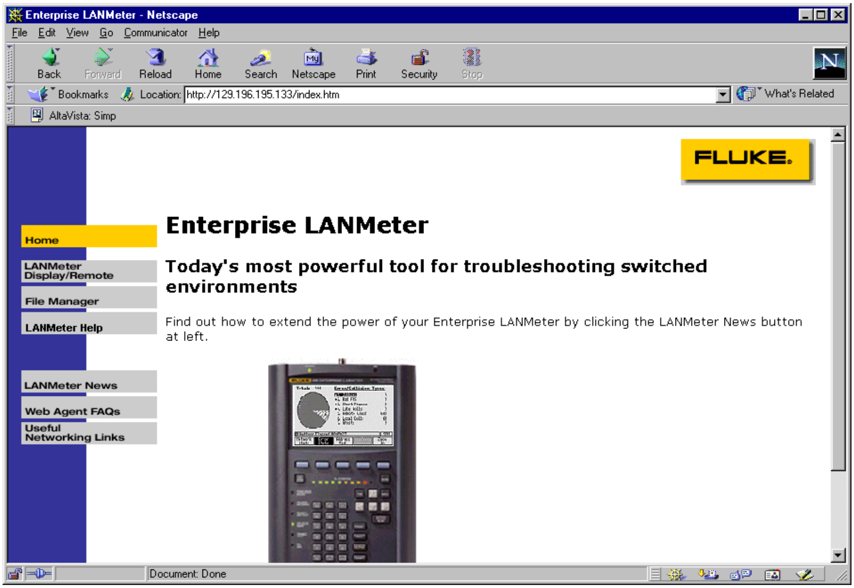
Config or Print All has been run. Web Agent will also automatically start (Auto Start enabled) whenever any measurement that uses the EPI stack is run (e.g. Segment Discovery, Trace Route, NetBIOS Discovery, Scan Host, etc.).

Viewing Instrument Information with a Web Browser

Use the following procedure to view LANMeter instrument information with your Web browser:

1. Configure the LANMeter instrument's Web Agent function as described in the previous section.
2. Start up your Web browser.
3. Enter the LANMeter instrument's IP address into your Web browser.

The LANMeter instrument displays its home page on your browser as shown in Figure 11-3.



Location: http://129.196.195.133/index.htm

Enterprise LANMeter

Today's most powerful tool for troubleshooting switched environments

Find out how to extend the power of your Enterprise LANMeter by clicking the LANMeter News button at left.

Figure 11-3. LANMeter Instrument's Home Page

The Home Page displays the following hyperlink selections for obtaining LANMeter instrument information:

❒ Home
❒ LANMeter Display/Remote
❒ File Manager
❒ LANMeter Help
❒ LANMeter News
❒ Web Agent Frequently Asked Questions
❒ Useful Networking Links

Home

Selecting **Home** will return you to LANMeter's Home Page (see Figure 11-3).

LANMeter Display/Remote

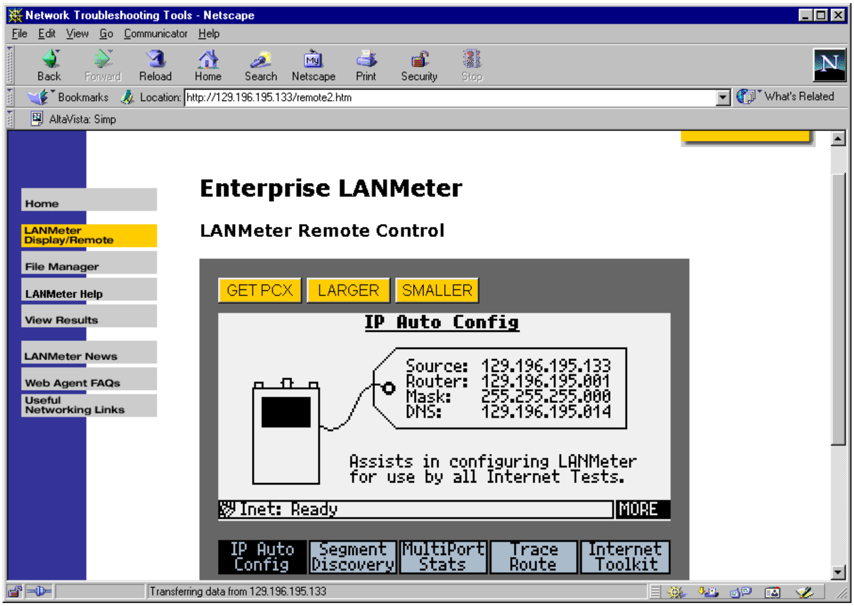
You can view the LANMeter instrument's current display by selecting **LANMeter Display/Remote** from the instrument's Home Page. The Web Browser then displays the instrument's current display as shown in Figure 11-4. The Web Browser continuously updates the current display and reflects changes in the state of the LANMeter instrument display.

View Results

A **View Results** button will appear (see Figure 11-4) when you select **LANMeter Display/Remote**. Select **View Results** to display the results of the last measurement run. This is the save as running **View All** from your LANMeter instrument. You can save the results to a file on your PC by selecting **File**, **Save As**... from your web browser.

WebRemote Control

You can also access the optional WebRemote Control features through this button. Refer to the "WebRemote Control Option" section later in this chapter.



Location: http://129.196.195.133/remote2.htm

Enterprise LANMeter

LANMeter Remote Control

IP Auto Config

```
Source:  129.196.195.133
Router:  129.196.195.001
Mask:    255.255.255.000
DNS:     129.196.195.014
```

Assists in configuring LANMeter for use by all Internet Tests.

Inet: Ready

Transferring data from 129.196.195.133

Figure 11-4. Sample Current LANMeter Display

The following buttons are available from the Current LANMeter display:

GET PCX Allows you to download the current LANMeter instrument display to your PC as a PCX formatted file. After selecting the **Get PCX** button, you are prompted to enter a filename, path, and directory location where you would like to put the file on your PC.

LARGER Displays the current LANMeter instrument screen at an enlarged size.

SMALLER Displays the current LANMeter instrument screen at a reduced size.

File Manager

The **File Manager** button gives you the following options:

❒ Reports and Graphics
❒ Data Logs
❒ Station Lists

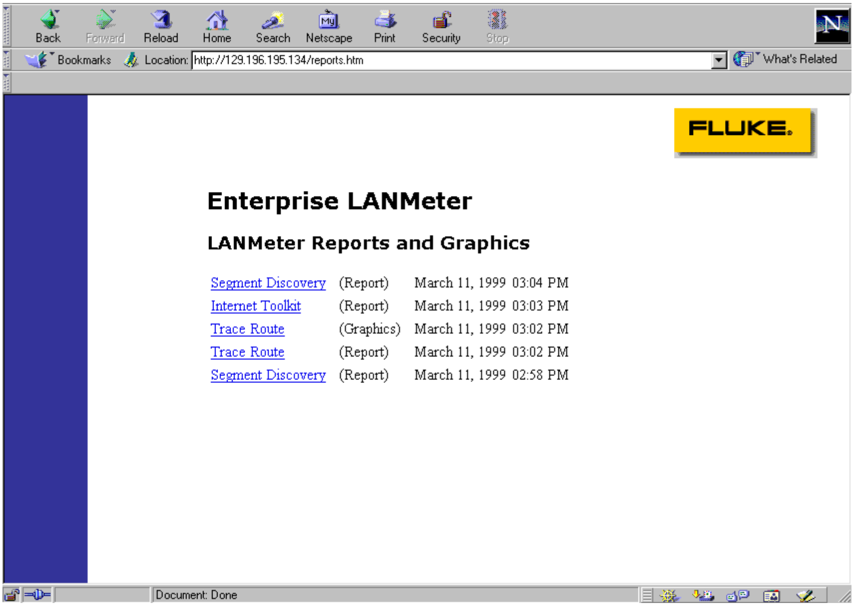
Reports and Graphics

After selecting the **Reports and Graphics** button, the Web Browser displays a list of available reports and graphics files as shown in Figure 11-5. This list is the same as the list displayed by accessing the LANMeter instrument’s File Manager, Report/Graphics screen. Refer to chapter 12 “File Manager” for more information on reports and graphics.

Select the hyperlink name of the file to view a report or a graphic. You can utilize report information by using cut and paste functions to transfer the information to another Windows application. You may need to scroll down to view the entire report. You can also use the browser’s **File, Save As...** function to save a report to a file on your PC.

Web Agent uses a Java applet to display LANMeter instrument graphics. Your browser must support Java to view these images. If the browser does not support Java, you will be offered the option of accessing the image as a PCX file.

You can use the **Get PCX** button on the Java applet to save the graphics file. Refer to the “LANMeter Display/Remote” section in this chapter for more information.



Enterprise LANMeter

LANMeter Reports and Graphics

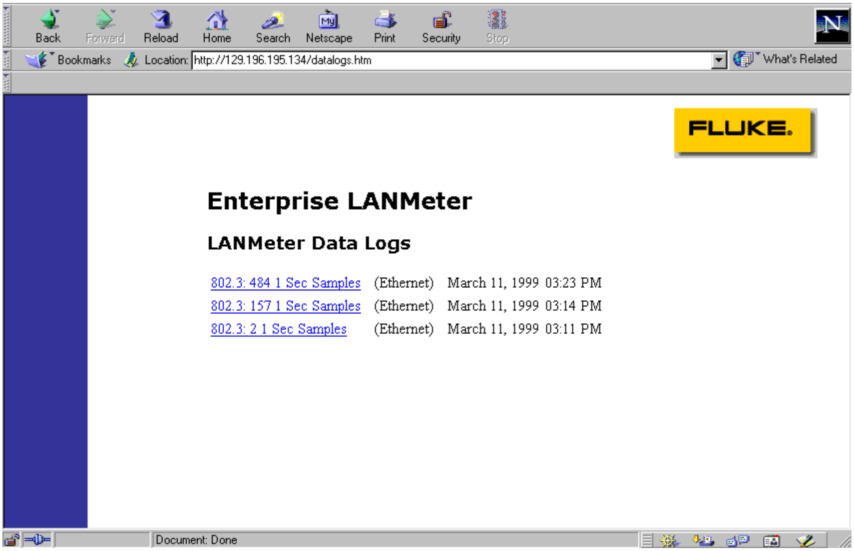
Segment Discovery	(Report)	March 11, 1999 03:04 PM
Internet Toolkit	(Report)	March 11, 1999 03:03 PM
Trace Route	(Graphics)	March 11, 1999 03:02 PM
Trace Route	(Report)	March 11, 1999 03:02 PM
Segment Discovery	(Report)	March 11, 1999 02:58 PM

Figure 11-5. Sample Reports and Graphics Display

Data Logs

After selecting the **Data Logs** button, the Web Browser displays a list of the LANMeter instrument’s current data log files as shown in Figure 11-6. This list is the same as the list displayed by accessing the LANMeter instrument’s File Manager Data Logs screen.

Select the hyperlink name of the file to view a data log. You may need to scroll down to view the entire data log. Data logs files are in CSV (Comma Separated Variable) format. You can use HealthScan, Network Inspector LANMeter Edition, or a spreadsheet program to view data log results. For information on HealthScan refer to Appendix D “Utilities.” In North America you can call 1-800-44-FLUKE to order Network Inspector LANMeter Edition or you can access the FLUKE Networks home page (refer to the section “Useful Networking Links” later in this chapter). You can also use the browser’s **File, Save As...** function to save a data log to a file on your PC.



Enterprise LANMeter

LANMeter Data Logs

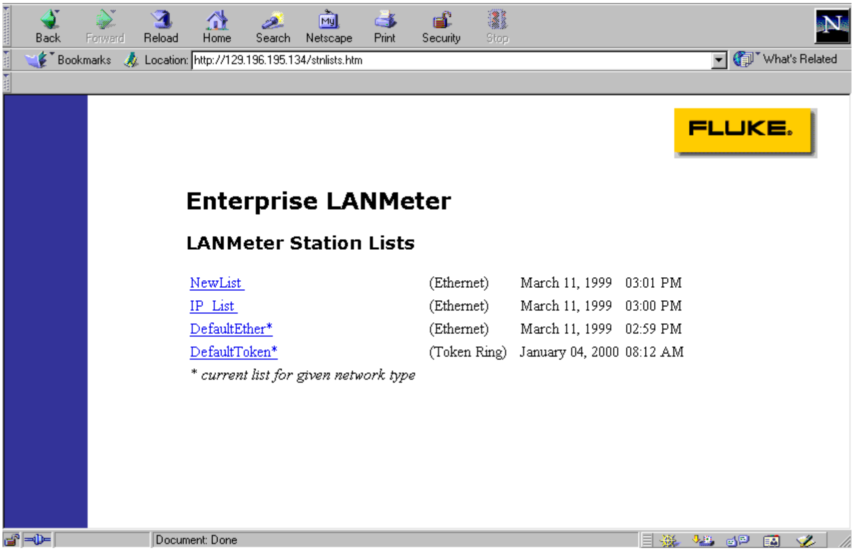
802.3: 484 1 Sec Samples	(Ethernet)	March 11, 1999 03:23 PM
802.3: 157 1 Sec Samples	(Ethernet)	March 11, 1999 03:14 PM
802.3: 2 1 Sec Samples	(Ethernet)	March 11, 1999 03:11 PM

Figure 11-6. Sample Data Logs Display

Station Lists

After selecting the **Station Lists** button, the Web Browser displays a list of the LANMeter instrument’s current station list files as shown in Figure 11-7. This list is the same as the list displayed by accessing the LANMeter instrument’s File Manager Station Lists.

Select the hyperlink name of the file to view a station list. You can utilize station list information by using cut and paste functions to transfer the information to another Windows application. You may need to scroll down to view the entire station list. You can also use the browser’s **File, Save As...** function to save a station list to a file on your PC.



Location: http://129.196.195.134/stnlists.htm

Enterprise LANMeter

LANMeter Station Lists

NewList	(Ethernet)	March 11, 1999	03:01 PM
IP_List	(Ethernet)	March 11, 1999	03:00 PM
DefaultEther*	(Ethernet)	March 11, 1999	02:59 PM
DefaultToken*	(Token Ring)	January 04, 2000	08:12 AM

* *current list for given network type*

Figure 11-7. Sample Station Lists Display

LANMeter Help

Available in software version 9.50 and later. This is the same as pressing the HELP key on your LANMeter instrument, except that you can view Help while a measurement is running.

LANMeter News

The **LANMeter News** button will take you to Fluke's LANMeter web page where you can obtain current LANMeter instrument news and software upgrade information.

Web Agent Frequently Asked Questions

Select **Web Agent Frequently Asked Questions** to get additional information on using Web Agent.

Useful Networking Links

Select **Useful Networking Links** for hyperlinks to Fluke Networks home page, useful network industry web pages and other pertinent links.

WebRemote Control Option

WebRemote Control can be accessed by configuring and running Web Agent. Web Agent must be running for the WebRemote Control option to work.

The WebRemote Control option comes configured in a trial usage mode. You can use WebRemote Control for a predefined number of days before your Enterprise LANMeter reverts back to an instrument without the WebRemote Control option. A trial day is used when you run WebRemote Control any number of times in one day. You can run **Manage Options**, from **Setup/Utils**, to view the number of trial days remaining.

Enabling WebRemote Control

If you have purchased the WebRemote Control option, you can permanently enable it by performing the following steps:

1. Complete the supplied FAX-back form including your Enterprise LANMeter's Ethernet or Token Ring MAC address and serial number and FAX it to Fluke to receive your enabling key.

   The Ethernet or Token Ring MAC address and serial number are available on the back of your Enterprise LANMeter. The MAC address is also available from the **Enable Option** softkey screen (Figure 11-8).

2. Press the top-level **Setup/Utils** softkey.

3. Press **Manage Options**, and ENTER RUN to view a list of your LANMeter instrument's available options. Each option can be enabled or disabled. This procedure assumes that your WebRemote Control option is disabled.

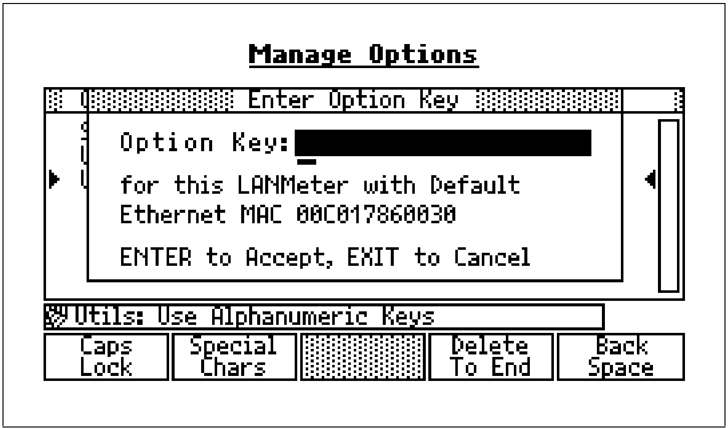
   If you are using the WebRemote Control option in the trial usage mode, the number of remaining trial days is shown here.

4. Select the WebRemote Control option and press **Enable Option** to display the Enter Option Key screen, shown in Figure 11-8.

5. Enter your enabling key and then press ENTER RUN to enable the WebRemote Control option.

6. After the option is enabled, place the WebRemote Control label onto the back of your Enterprise LANMeter. The WebRemote Control label is included in the option 68X-RW and 68X-RWK kits. This label will help identify units that have the option enabled.

7. The option information is stored in non-volatile memory in your LANMeter instrument and is not affected by software upgrades of the operating system.



Manage Options

Enter Option Key

Option Key:

for this LANMeter with Default
Ethernet MAC 00C017860030

ENTER to Accept, EXIT to Cancel

Utils: Use Alphanumeric Keys

Figure 11-8. Enabling the WebRemote Control Option

Configuring WebRemote Control

WebRemote Control requires no further configuration (other than changing the password) beyond configuring your LANMeter instrument to run Web Agent.

1. Refer to the section “Configuring and Running Web Agent” to configure your LANMeter instrument to run WebRemote Control.
2. WebRemote Control is password protected. The password can be changed via the Web Agent configuration menu.

Note

Web Agent and therefore WebRemote Control automatically shuts off when you run certain tests (e.g. Cable Tests, Station List or File Manager) or the Print All command. A reminder popup will be displayed prior to Web Agent shutting down. If Web Agent is disabled then it can only be restarted from the LANMeter keyboard except after a Print All command is executed. Web Agent will automomatically restart after the Print All command is finished.

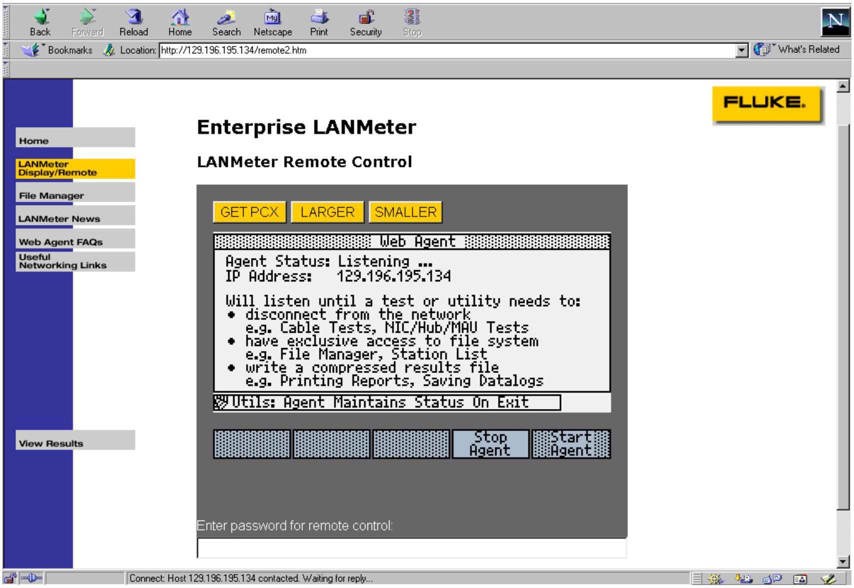
Running WebRemote Control

If the WebRemote Control option is enabled on your LANMeter instrument then selecting **LANMeter Display/Remote** from the instrument's Home Page brings up the display as shown in Figure 11-9.

1. Select the line below "Enter password for remote control:".
2. Type in the password. The default password is `guest` and it is case sensitive. Press Enter.

Note

You can verify or change the password via the Web Agent configuration menu. Refer to the section on "Configuring and Running Web Agent" for more information.



Enterprise LANMeter

LANMeter Remote Control

```
Web Agent
Agent Status: Listening ...
IP Address:   129.196.195.134

Will listen until a test or utility needs to:
• disconnect from the network
  e.g. Cable Tests, NIC/Hub/MAU Tests
• have exclusive access to file system
  e.g. File Manager, Station List
• write a compressed results file
  e.g. Printing Reports, Saving Datalogs
Utils: Agent Maintains Status On Exit
```

Enter password for remote control:

Connect: Host 129.196.195.134 contacted. Waiting for reply...

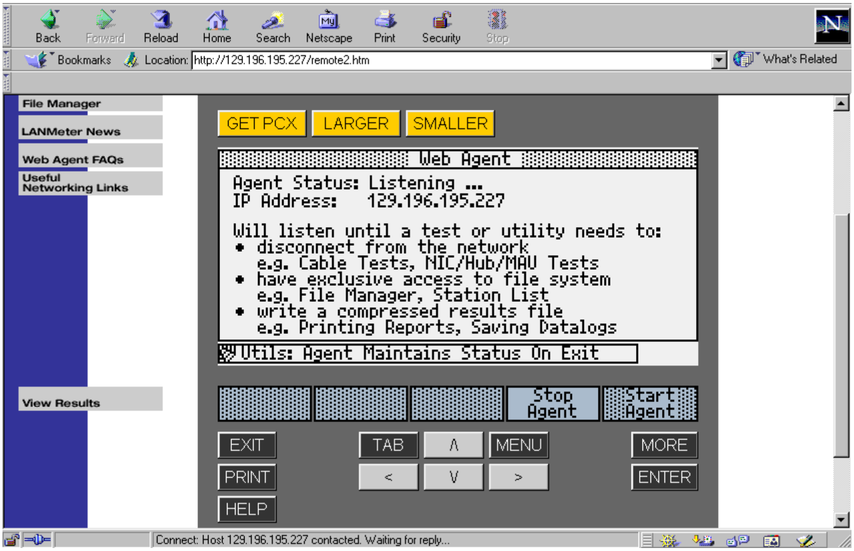
Figure 11-9. WebRemote Control Password Entry

Once the correct password has been supplied, your browser then shows a line of softkeys below the display and function keys below that. Refer to Figure 11-10.

You now have remote control capability of your LANMeter instrument. You can now use your mouse or PC keyboard to select the softkeys or the function keys to operate your LANMeter instrument. You can use WebRemote Control to start and stop tests, collect data and manipulate your LANMeter instrument as if it were physically present. Refer to the relevant chapter in this manual for information on running a specific test.

You can use the **View Results** button to see the results of a measurement. You will see a report displayed that is the same as the report that is generated when you execute the **Print All** function, however **View Results** won’t cause Web Agent to shut down. **View Results** can only be run after a measurement has been stopped. Refer to Figure 11-11 for a sample **View Results** display.

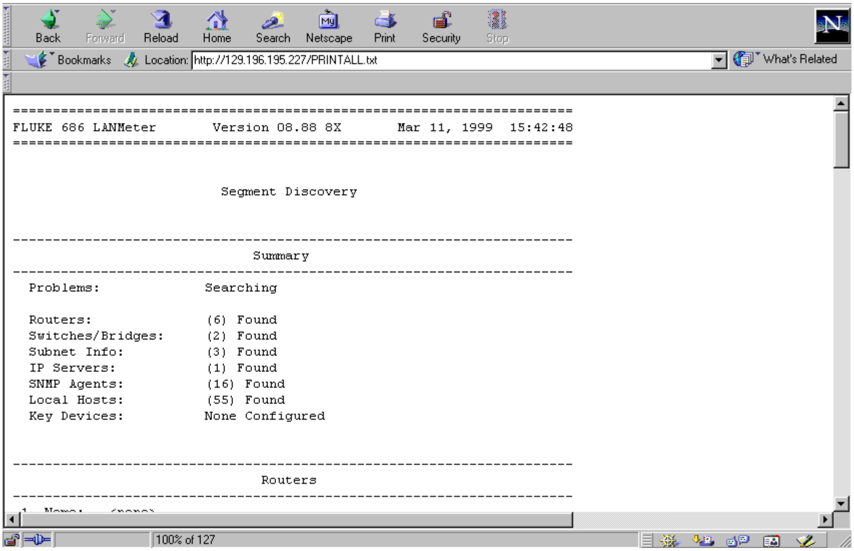
You use the browser’s **File, Save As...** function to save a report to a file on your PC.



```
Web Agent
Agent Status: Listening ...
IP Address:   129.196.195.227

Will listen until a test or utility needs to:
• disconnect from the network
  e.g. Cable Tests, NIC/Hub/MAU Tests
• have exclusive access to file system
  e.g. File Manager, Station List
• write a compressed results file
  e.g. Printing Reports, Saving Datalogs
Utils: Agent Maintains Status On Exit
```

Connect: Host 129.196.195.227 contacted. Waiting for reply...

Figure 11-10. WebRemote Control



```
======================================================================
FLUKE 686 LANMeter       Version 08.88 8X       Mar 11, 1999  15:42:48
======================================================================


                          Segment Discovery


----------------------------------------------------------------------
                              Summary
----------------------------------------------------------------------
  Problems:              Searching

  Routers:               (6) Found
  Switches/Bridges:      (2) Found
  Subnet Info:           (3) Found
  IP Servers:            (1) Found
  SNMP Agents:           (16) Found
  Local Hosts:           (55) Found
  Key Devices:           None Configured


----------------------------------------------------------------------
                               Routers
----------------------------------------------------------------------
```

Figure 11-11. Sample View Results Display

Chapter 12
File Manager

Introduction

File Manager is a set of features supported in the Fluke Enterprise LANMeter™ (68x Series) Instrument Software Version 8.00 and later, that provides the capability to print, email, import, export, rename, or delete selected files.

For file management capabilities using an IBM-compatible, personal computer (PC), refer to Appendix D “Utilities.”

The following sections are included in this chapter:

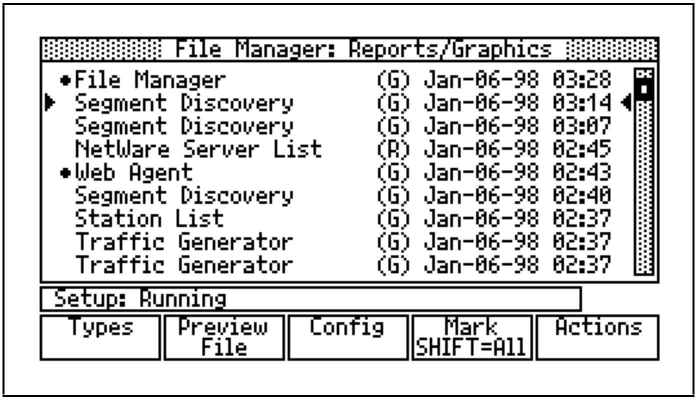
❒ File Types
❒ Preview Files
❒ Configure File Manager
❒ Mark Files
❒ File Manager Actions

You can access File Manager by first pressing the top-level **Setup/Utils** softkey and then pressing the **File Manager** softkey twice. Figure 12-1 shows the File Manager screen. File Manager first displays a scrollable list of any saved Reports and Graphics files. The Data Logs and Station Lists screens are similar to the Reports and Graphics screen.

File Manager allows you to use the files that you have created by printing the results of a measurement or a screen shot to a file, creating a data log file with Network Statistics, or saving a station list.

A screen shot (Graphics) of the LANMeter instrument’s display can be printed to a file at any time by pressing PRINT, and then selecting **To File**. Tests must be stopped before ASCII formatted results (Reports) can be printed using the MENU, **Print All** selection. To bypass the popup window asking which operation to take when PRINT or **Print All** is selected, configure the **Setup/Utils, File Manager, Config, Printer/Port, Print To** selection to **To File** instead of the default selection of **Ask User**.

Screen shots (Graphics) and ASCII formatted results (Reports) can be saved to a virtual disk for later screen previewing or printing. Data Log files cannot be printed. All printable files are stored in a printer-independent format. Data Log files are stored in Comma Separated Variable (CSV) format. When you print one or more saved print files, the instrument formats the file according to the configured printer type.



```
           File Manager: Reports/Graphics
 •File Manager          (G) Jan-06-98 03:28
▶ Segment Discovery     (G) Jan-06-98 03:14 ◀
  Segment Discovery     (G) Jan-06-98 03:07
  NetWare Server List   (R) Jan-06-98 02:45
 •Web Agent             (G) Jan-06-98 02:43
  Segment Discovery     (G) Jan-06-98 02:40
  Station List          (G) Jan-06-98 02:37
  Traffic Generator     (G) Jan-06-98 02:37
  Traffic Generator     (G) Jan-06-98 02:37
Setup: Running
```

Figure 12-1. File Manager Screen

As each file is saved, File Manager automatically names the file with the test name, date and time stamp, and assigns a file type. In front of each date and time stamp, the instrument displays either **(R)** for Reports or **(G)** for Graphics. The **(R)** indicates an ASCII formatted report file and the **(G)** indicates a graphic image file.

Saving files has the following advantages over printing directly to a printer:

- ❒ You can save a print file at any time; a printer is not required.
- ❒ You can preview report and graphic files.
- ❒ All printed results are immediately available through the network connection from a Web Browser (see Chapter 11, "Web Agent/WebRemote Control").
- ❒ Printed results may be immediately emailed to any SMTP mail account through the attached network connection. Email can be sent through firewall connections that would otherwise block Web Browser access. See the "File Manager Actions" section later in this chapter for more information on Email.

The following procedure generally shows how to use File Manager. For specific information on how to perform each of the following File Manager tasks, refer to the various sections of this chapter:

1. Specify the file type.
2. Preview the selected file or files (for Reports and Graphics files only).
3. Configure the instrument for File Manager actions.
4. Mark one or more files.
5. Execute a File Manager action on the selected file or files.

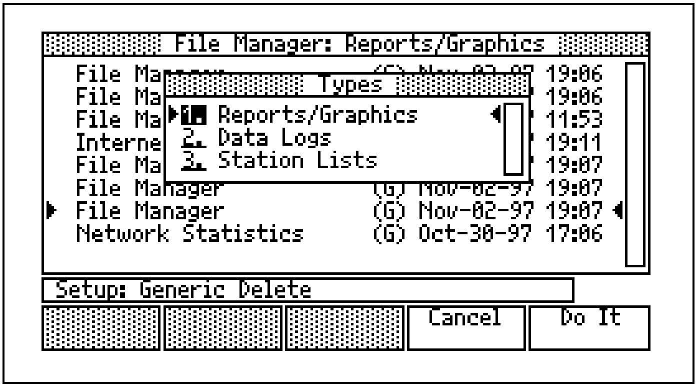
File Types

You can select the following file types:

- ❒ Reports and Graphics
- ❒ Data Logs
- ❒ Station Lists

Use the following procedure to select the file type:

1. Press the **Types** softkey.
2. Select the desired file type as **Reports/Graphics**, **Data Logs**, or **Station Lists** by pressing the number of the type or by using TAB or the arrow keys. Refer to Figure 12-2.
3. Press ENTER/RUN to select the file type.



```
File Manager: Reports/Graphics
  File Ma                               19:06
  File Ma                               19:06
  File Ma                               11:53
  Interne                               19:11
  File Ma                               19:07
  File Manager                  (G) Nov-02-97 19:07
▶ File Manager                  (G) Nov-02-97 19:07 ◀
  Network Statistics            (G) Oct-30-97 17:06

Types
▶1. Reports/Graphics ◀
 2. Data Logs
 3. Station Lists

Setup: Generic Delete
```

Figure 12-2. File Type Pop-up Menu

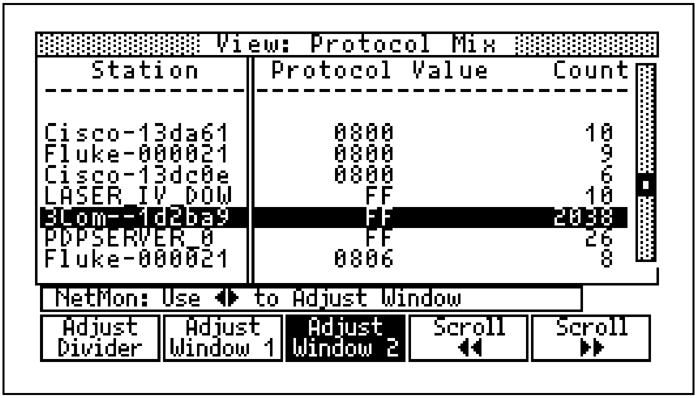
Preview Files

You can preview a selected Report or Graphics file by pressing **Preview File**. For a Graphics file, press **Preview File** again (or any key) to return to the File Manager screen. Refer to the following "Preview ASCII Report Files" for details on how to preview a Report file. Station lists can only be viewed from the **Station List** test. Data Logs cannot be previewed.

Preview ASCII Report Files

Previewing an ASCII Report file takes up more space than can be displayed on a single screen. Pressing **Preview File**, after selecting a Report file, displays a report of up to a maximum of 512 items or nodes. This capability is supported in any function or test that supports the Print All capability; such as Protocol Mix, Top IP, Active Monitor History, and Station List.

Figure 12-3 shows an example Report Preview File screen.



```
View: Protocol Mix
    Station       Protocol Value    Count
-------------    ----------------------

Cisco-13da61        0800               10
Fluke-000021        0800                9
Cisco-13dc0e        0800                6
LASER_IV_DOW          FF               10
3Com--1d2ba9          FF             2038
PDPSERVER_0           FF               26
Fluke-000021        0806                8
NetMon: Use ◀▶ to Adjust Window
```

Figure 12-3. Preview File Example ASCII Report Screen

When previewing an ASCII Report file, the display is split into two windows that stay synchronized keeping related data on the same horizontal lines. You can view the rest of the available results in Figure 12-3 by changing the location of the divider and scrolling left and right in either of the two windows.

You can change the information shown by selecting the **Adjust Divider**, **Adjust Window 1**, or **Adjust Window 2** softkeys. Selecting **Adjust Divider** allows you to change the relative size of the two windows. Selecting **Adjust Window 1** or **Adjust Window 2** allows you to scroll left or right throughout the report. Pressing the **Adjust Divider**, **Adjust Window 1**, or **Adjust Window 2** softkey a second time displays, and allows for the use of, the **Prev Page** and **Next Page** softkeys. The default setting is for the entire display to show Window 1.

Using the example of Figure 12-3, from a **Print All** report from the Protocol Mix test, you can display MAC Address and Protocols by first selecting **Adjust Window 2**, scrolling to the left until the `MAC Address` and `Protocols` columns are displayed. Selecting **Adjust Window 2** again displays, and allows for the use of, the **Prev Page** and **Next Page** softkeys.

Table 12-1 shows a portion of a Report (ASCII) file when printed.

Table 12-1. Printed Report File Example

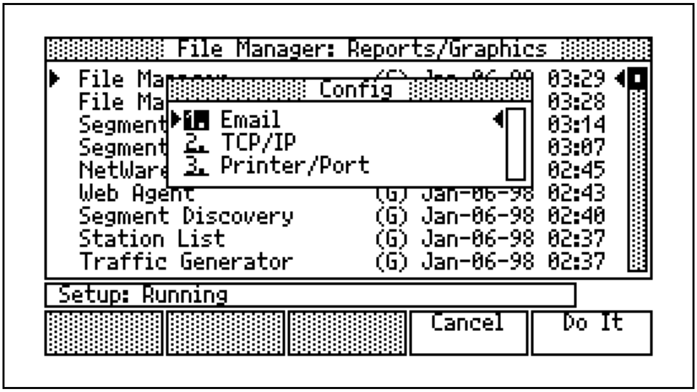
```
------------------------------------------------------------
  Station    MAC Address    Protocol   Protocol Value  Count
------------------------------------------------------------
Cisco-13da61 00000c13da61           IP      0800          10
Fluke-000021 00c017000021           IP      0800           9
Cisco-13dc0e 00000c13dc0e           IP      0800           6
LASER_IV_DOW 08000994aa86 NetWare802.3        FF          10
3Com--1d2ba9 0020af1d2ba9 NetWare802.3        FF        2038
PDPSERVER_0  00403200d5c6 NetWare802.3        FF          26
Fluke-000021 00c017000021          ARP      0806           8
Cisco-13da61 00000c13da61          ARP      0806           8
LAW          0020af67ffa1 NetWare802.3        FF          22
TLH          0000f4a02c47 NetWare802.3        FF         501
DEB          0020af68009b NetWare802.3        FF        1465
Cisco-13da61 00000c13da61     Loopback      9000           2
Cisco-13dc0e 00000c13dc0e     Loopback      9000           2
             001b21000000     VINES IP      0BAD           2
Cisco-13da61 00000c13da61     VINES IP      0BAD           1
JK           0020af68010a NetWare802.3        FF           3
Cisco-13dc0e 00000c13dc0e     VINES IP      0BAD           1
```

Configure File Manager

You can configure the following parameters for File Manager operations:

- ❐ Email
- ❐ TCP/IP
- ❐ Printer/Port

Figure 12-4 shows the Configuration pop-up menu.



```
File Manager: Reports/Graphics
▶ File Ma                              03:29
  File Ma     Config                   03:28
  Segment ▶ 1. Email                   03:14
  Segment   2. TCP/IP                  03:07
  NetWare   3. Printer/Port            02:45
  Web Agent                            02:43
  Segment Discovery     (G) Jan-06-98 02:40
  Station List          (G) Jan-06-98 02:37
  Traffic Generator     (G) Jan-06-98 02:37
Setup: Running
                                 Cancel   Do It
```

Figure 12-4. Configuration Pop-up Menu

Use the following procedure to configure File Manager operations:

1. Press the **Config** softkey.
2. Select the desired operation to configure as **Email**, **TCP/IP**, or **Printer/Port** by pressing the number of the configuration item or by using TAB or the arrow keys and then pressing ENTER/RUN.
3. Configure the desired parameters. Refer to the following sections for specific configuration parameters for each function:

   - ❐ Email Configuration Parameters
   - ❐ TCP/IP Configuration Parameters
   - ❐ Printer/Port Configuration Parameters

   To undo any configuration changes you made, press MENU, select **Cancel Changes** in the Configuration Menu, and then press ENTER/RUN.

4. Press EXIT STOP to save your configuration to non-volatile memory and exit the Configuration screen.

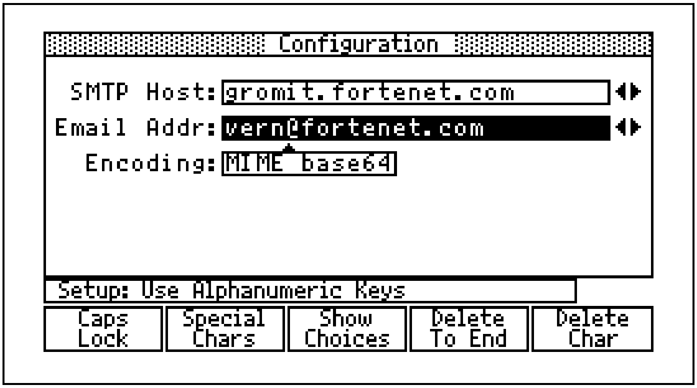
Email Configuration Parameters

You can configure the following parameters for the Email function. The defaults are underlined (when appropriate). The **Show Choices** softkey either displays a list of available choices or displays a list of the most recent entries used.

- ❐ SMTP Host as a DNS name or an IP address.
- ❐ Email Address is the destination email address.
- ❐ Encoding type as MIME base64 or UU Encoding.

The SMTP Host is the machine that will handle the delivery of your email. The Email Address is the final destination for your email and the SMTP Host must support delivery to this address. The encoding type is used to determine how your message is encoded. Email is sent as multipart MIME messages.

Figure 12-5 shows a sample Email Configuration screen. Use the **Special Chars** softkey for special ASCII characters needed for name entry.



Configuration

SMTP Host: gromit.fortenet.com

Email Addr: vern@fortenet.com

Encoding: MIME base64

Setup: Use Alphanumeric Keys

Figure 12-5. Email Configuration Screen

TCP/IP Configuration Parameters

You can configure the following parameters for TCP/IP communications. These parameters are shared with the Enterprise LANMeter’s IP configuration parameters.

❒ Source IP address as dotted decimal (press the **Station List** softkey to select from the IP station list). The symbolic name associated with the station will be displayed if there is a corresponding entry in the IP station list.

❒ Default Router address as dotted decimal (press the **Station List** softkey to select from the IP station list).

❒ Default Mask as dotted decimal (press the **Show Choices** softkey to select from list of legal masks).

❒ DNS address as dotted decimal (press the **Station List** softkey to select from the IP station list).

Printer/Port Configuration Parameters

You can configure the following parameters for the Printer/Port operations. The default parameters are underlined. The **Show Choices** softkey either displays a list of available choices.

❒ Print To as Ask User, Printer, or File.

❒ Printer as HP LaserJet Series, HP ThinkJet, or Epson Series.

❒ Handshake as DTR/DSR, XON/XOFF, or None. Verify that your printer is also set to a matching flow control and for 8 bits with no parity.

❒ Print Baud as 1200, 2400, 4800, 9600, or 19,200. Verify that your printer is set to the matching Baud rate.

❒ Import and Export Baud as 1200, 2400, 4800, 9600, or 19,200.

Mark Files

After you set the file type for File Manager, you can mark one or more files to print, email, export, or delete. You can mark a single file by first selecting it with the ▽ or △ keys, and then pressing the **Mark** softkey. Marked files are indicated by the Mark icon (●). If you press the **Mark** softkey again, it unmarks the selected file. You can mark multiple files using this same method.

To mark all of the files, press and release SHIFT and then press **Mark**. Repeating this sequence unmarks all files.

If there are files available and none of them are marked, the LANMeter instrument will consider the currently selected file as marked.

File Manager Actions

After you have marked one or more files, you can execute an action by pressing **Actions**, selecting one of the following actions, and then pressing ENTER/RUN.

Preview
Reports/Graphics

The **Preview** action allows you to view reports or graphics files on the LANMeter display. Use this function to verify the contents of a file prior to printing, emailing, exporting or deleting a selected file.

Print
Reports/Graphics

The **Print** action allows you to print the marked files to a printer that is connected to the LANMeter instrument's RS-232 port. Refer to the following "Attaching Printer Cables" section for information on wiring the printer cable and on connecting a printer to the LANMeter instrument.

Email
Reports/Graphics
Data Logs
Station Lists

The **Email** action allows you to send marked files as attachments to a generic LANMeter instrument email.

The Email function supports Eudora 2.0 and later, Netscape Navigator 3.0 and later, and Microsoft Internet Explorer 3.0 and later. Refer to the following "Email Error Handling" section for information on email errors.

Export
Reports/Graphics
Data Logs
Station Lists

The **Export** action allows you to export the marked files from the LANMeter instrument to a PC.

See Appendix D “Utilities” for information on running LANMeter Utilities on your PC. LANMeter Utilities gives you the capability to set up your PC to receive the exported files.

Import
Station Lists

The **Import** action allows you to import a station list file from a PC to the LANMeter instrument.

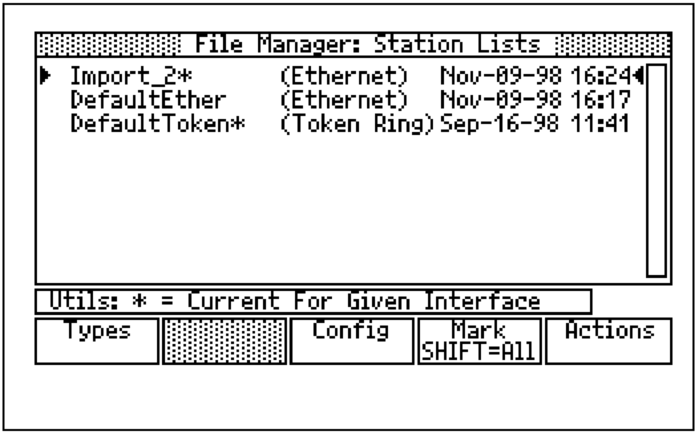
See Appendix D “Utilities” for information on running LANMeter Utilities on your PC. LANMeter Utilities gives you the capability to set up your PC to send a Station List file to the LANMeter instrument.

Rename
Station Lists

The **Rename** action allows you to rename the selected station list file. This can be very useful because imported files are named **`Import_x`**, where **`x`** is an integer value 0 through 7, in the LANMeter instrument.

Delete
Reports/Graphics
Data Logs
Station Lists

The **Delete** action allows you to delete the marked files from the LANMeter instrument. The current Station List will be indicated by an **`*`** and it can not be deleted. Figure 12-6 shows a sample File Manager: Station Lists screen.



File Manager: Station Lists

```
▶ Import_2*       (Ethernet)   Nov-09-98 16:24◀
  DefaultEther    (Ethernet)   Nov-09-98 16:17
  DefaultToken*   (Token Ring) Sep-16-98 11:41
```

Utils: * = Current For Given Interface

Figure 12-6. File Manager: Station Lists Screen

Email Error Handling

If the LANMeter instrument encounters an error sending email, it displays an error message with error information. If an error occurs, you need to acknowledge the error and confirm that the email was not sent and then resolve the error condition.

The following are common errors:

- ❒ Using the wrong address (including misspellings) for the SMTP host or email destination.
- ❒ The SMTP host is down.
- ❒ The DNS is wrong or down (this causes DNS lookup failures).

Attaching Printer Cables

Use an IBM AT computer style printer cable with DB-9 female and DB-25 male connectors. The Fluke RS-232 cable is an example of the correct printer cable. Connect the LANMeter instrument to your serial printer as shown in Figure 12-7.

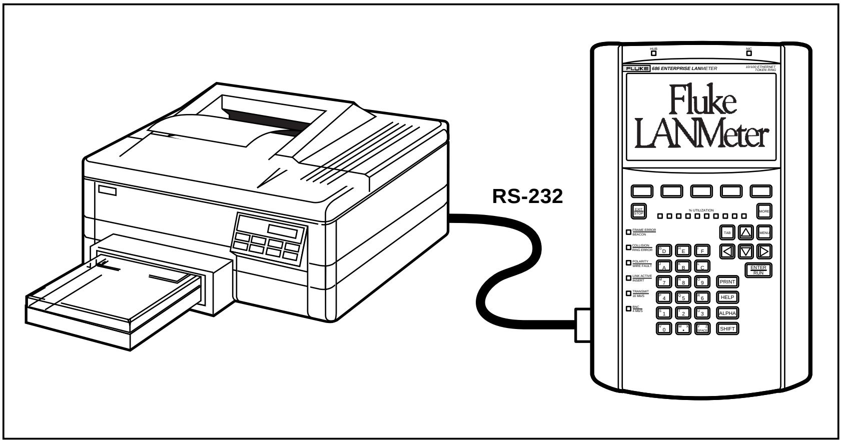
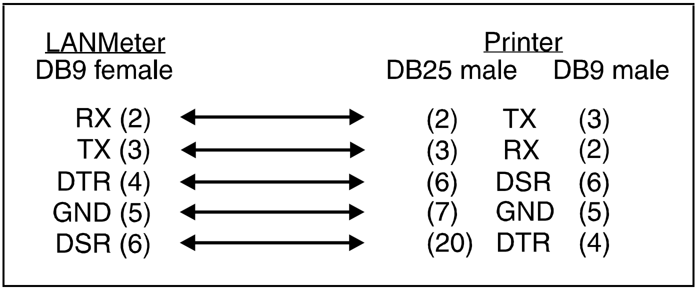


Figure 12-7. Printer Connection

Your printer cable must be wired as shown in Figure 12-8.



LANMeter		Printer		
DB9 female		DB25 male		DB9 male
RX (2)	↔	(2)	TX	(3)
TX (3)	↔	(3)	RX	(2)
DTR (4)	↔	(6)	DSR	(6)
GND (5)	↔	(7)	GND	(5)
DSR (6)	↔	(20)	DTR	(4)

Figure 12-8. Printer Cable Connections

Chapter 13
Terminal Emulator Option

Introduction

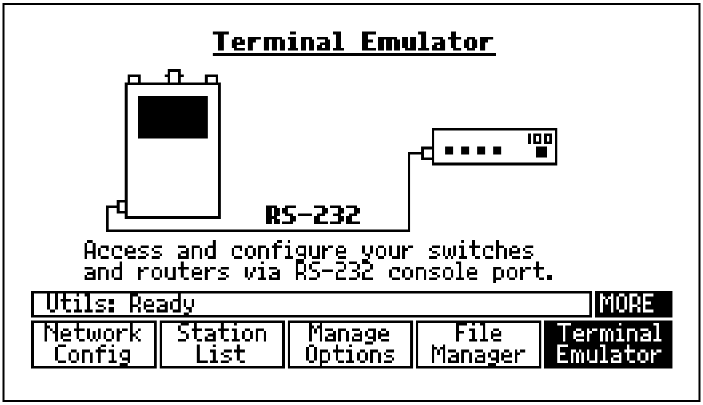
Terminal Emulator is an optional feature supported in the Fluke Enterprise LANMeter (68x Series) instrument software version 9.50 and later. Terminal Emulator is automatically enabled whenever the SwitchWizard or WideAreaWizard options are enabled.

Terminal Emulator is a character based utility that supports a command line interface to your network device (e.g. a switch or router). Terminal Emulator gives you the ability to use your LANMeter instrument’s serial port to establish a direct connection to your configurable network device. You may then use Terminal Emulator to inspect or change the setup of the device.

This chapter contains the following sections:

❒ Configuring the Terminal Emulator Option
❒ Running the Terminal Emulator

You can access Terminal Emulator by pressing the **Setup/Utils** softkey from your LANMeter instrument’s top level display. Pressing the **Terminal Emulator** softkey will give you the display as shown in Figure 13-1.



Terminal Emulator

Access and configure your switches
and routers via RS-232 console port.

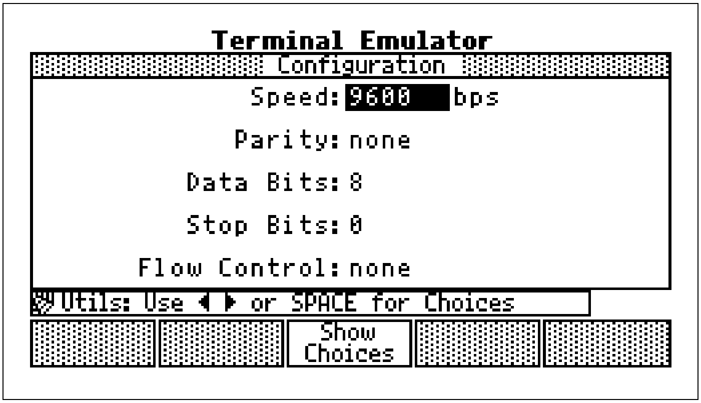
Utils: Ready

Figure 13-1. Terminal Emulator Screen

Configuring the Terminal Emulator Option

The default configuration settings for Terminal Emulator are 9600 baud, no parity, 0 data Bits, 0 Stop bits and no Flow Control. Only the speed is configurable. Use the following procedure to change the Terminal Emulator configuration.

1. Press **Setup/Utils** from the top-level softkey menu.
2. Press the **Terminal Emulator** softkey, then MENU, **Configure**. See Figure 13-2.



Terminal Emulator

Configuration

Speed: 9600 bps

Parity: none

Data Bits: 8

Stop Bits: 0

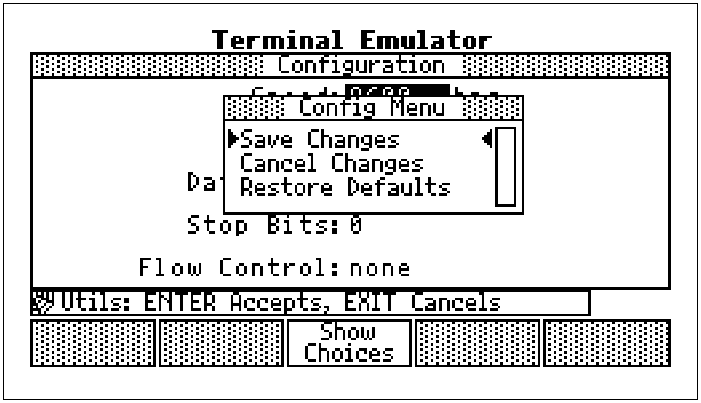
Flow Control: none

Utils: Use ◀ ▶ or SPACE for Choices

Figure 13-2. Terminal Emulator Configuration Menu

3. Select the **Show Choices** softkey or use the ◁ or ▷ keys to select a new speed.

4. Press EXIT STOP to save your changes and close the configuration window. You may also press MENU again and get a Config Menu popup as shown in Figure 13-3. You may elect to **Save Changes**, **Cancel Changes** or **Restore Defaults** from the Config Menu.



Terminal Emulator

Configuration

Config Menu

- ▶Save Changes
- Cancel Changes
- Restore Defaults

Da

Stop Bits: 0

Flow Control: none

Utils: ENTER Accepts, EXIT Cancels

Show Choices

Figure 13-3. Terminal Emulator Config Menu

Running Terminal Emulator

Use the following procedure to run Terminal Emulator.

1. Connect a serial cable between the network device and your LANMeter's instrument serial port. Refer to Figure 13-4 for the location of the serial port on your LANMeter instrument. Refer to Table 13-1 for the pinout description of the serial port. Refer to your network device's documentation for information on its requirements.

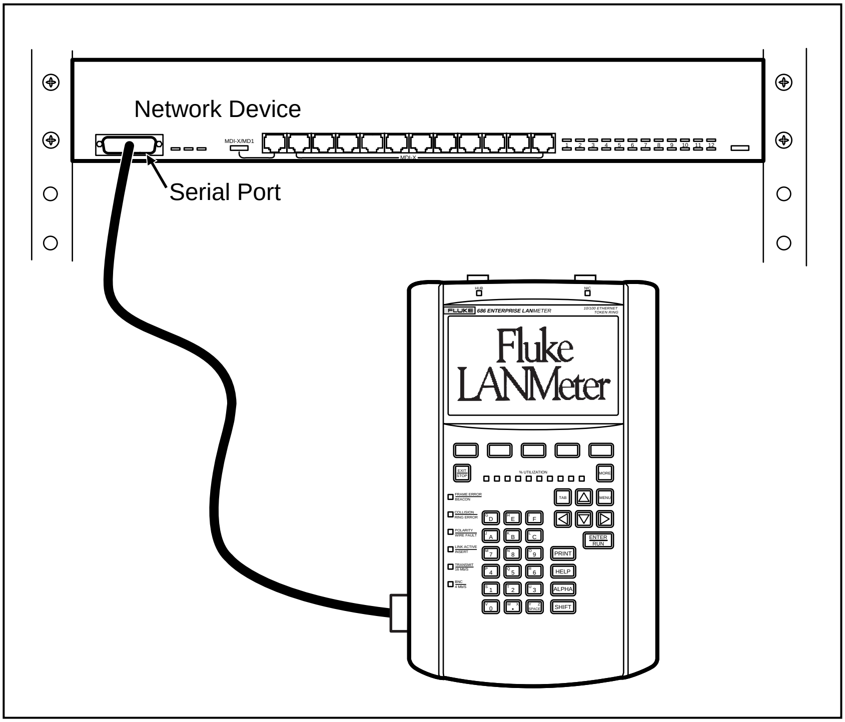


Figure 13-4. Serial Connection

Table 13-1. LANMeter Serial Port Pinout

DB9	
Pin No.	Signal
1	-
2	RX
3	TX
4	DTR
5	GND
6	DSR
7	RTS
8	-
9	-

2. Once you have connected the appropriate serial cable, press **Setup/Utils** from the top-level softkey menu. Then press the **Terminal Emulator** softkey followed by ENTER RUN.

3. Press ENTER RUN to get a response from the network device. You are now ready to inspect or change the configuration of your network device. There are two rows of keyword softkeys (refer to Figure 13-5) provided to facilitate entering configuration commands.

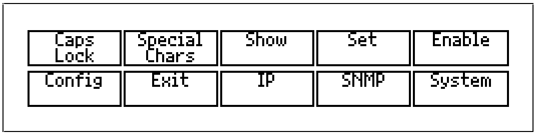


Figure 13-5. Terminal Emulator Softkeys

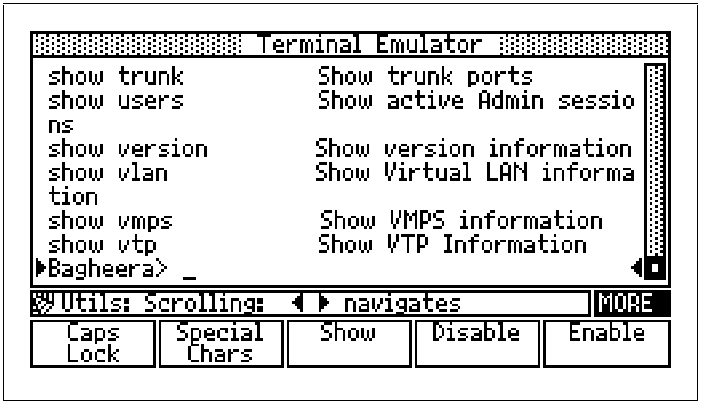
The second row of softkeys depicted in Figure 13-5 is available by pressing the MORE softkey.

4. Figure 13-6 shows a sample Terminal Emulator display. You can use the ◁, ▷, ▽, and △ keys to help navigate your LANMeter's display. Use the ◁ and ▷ keys to move the cursor to the top and bottom of the screen. Use the △ and ▽ keys to move the cursor up and down the screen one line at a time.

   When you are entering a command, the ◁ key changes its function. Pressing ◁ will cause the cursor to backspace one character and delete the previously entered character. Pressing SHIFT ◁ will clear the whole line.

   Note

   Refer to the specific network device reference manual for information on the appropriate commands to use to configure or query the device.



```
show trunk              Show trunk ports
show users              Show active Admin sessio
ns
show version            Show version information
show vlan               Show Virtual LAN informa
tion
show vmps               Show VMPS information
show vtp                Show VTP Information
▶Bagheera> _
```

Figure 13-6. Sample Terminal Emulator Display

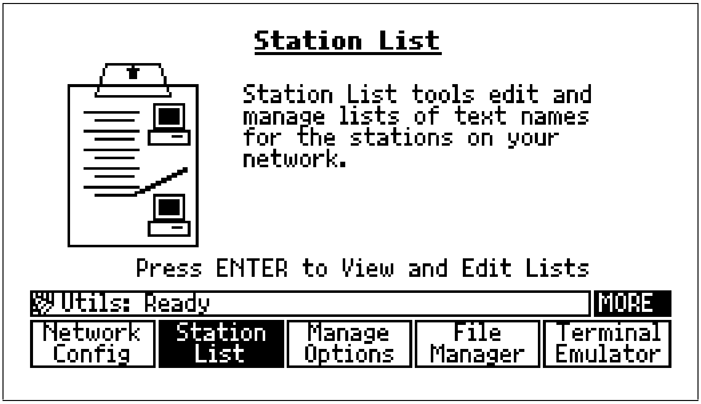
5. Press EXIT STOP to stop the utility. After you have stopped Terminal Emulator, pressing the MENU key will bring up the Test Menu popup. Select **Last Result** to view the screen display when Terminal Emulator was stopped. Select **Print All** to save the results to an ASCII file in File Manager, or to print the results to a printer. Select **View All** to review the results on your LANMeter instrument.

Chapter 14
Station List

Introduction

A Station List is a list of network addresses and their associated symbolic station names. The use of symbolic names rather than station addresses (such as selecting a target address to run NetWare Ping) make many tests in LANMeter easier to configure and test results easier to read.   You can access the Station List utility by pressing the **Setup/Utils** softkey from your LANMeter instrument's top-level display.

Pressing the **Setup/Utils, Station List** softkeys will give you the display shown in Figure 14-1.



Station List

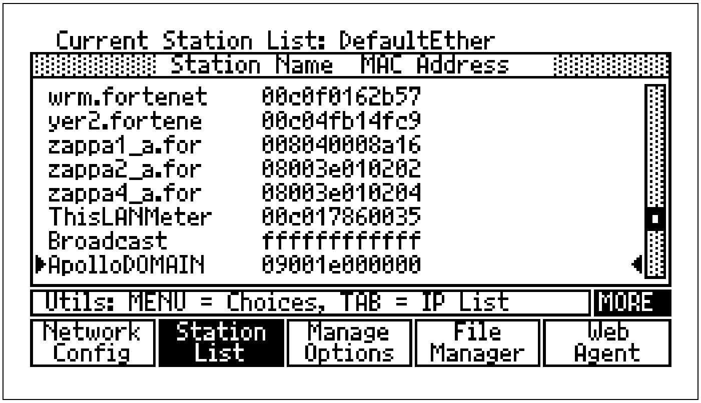
Station List tools edit and manage lists of text names for the stations on your network.

Press ENTER to View and Edit Lists

Utils: Ready

Figure 14-1. Station List Softkey Location

Press the Station List softkey again to run station list. Figure 14-2 shows a sample station list.



```
 Current Station List: DefaultEther
      Station Name  MAC Address
 wrm.fortenet     00c0f0162b57
 yer2.fortene     00c04fb14fc9
 zappa1_a.for     008040008a16
 zappa2_a.for     08003e010202
 zappa4_a.for     08003e010204
 ThisLANMeter     00c017860035
 Broadcast        ffffffffffff
▶ApolloDOMAIN     09001e000000   ◀
Utils: MENU = Choices, TAB = IP List
```

Figure 14-2. Sample Station List

Description

The station list consists of two columns. The selected station is shown with arrowheads on either side of the selection. The left column contains the symbolic names (if any) and the right column contains the address information

You may store up to 8 separate station lists.   On Fluke Model 686 and 685 LANMeters, the total of 8 lists includes both Ethernet and Token Ring station lists (they are stored separately). There is always one default Ethernet and Token Ring station list. The default name of the Ethernet station list is DefaultEther and the default name of the Token Ring station list is DefaultToken. See the section "*Editing the Station List*" in this chapter for details on saving multiple station lists.

Each station list has four sublists: MAC, IP, IPX, and VIP. You can view each sublist by pressing TAB. The right column heading shows the current address type (such as, MAC Address (Hex), IP Address, IPX Address, VIP Address). Only stations with addresses of the type selected are displayed. For example, if a station does not have an entry in the MAC sublist then the station name will not be displayed when this address type is selected.

Duplicate symbolic names are permitted, but duplicate addresses are not.

Features

Station List has the following features:

❐ Maximum Station List size of 512 entries (Up to 12 characters each.)

❐ Multiple address types per Station List (MAC, IP, IPX, and VIP)

❐ Multiple Station Lists. (Up to 8 lists maximum with a maximum of 4,096 combined entries from all lists.)

❐ Merge new stations to a Station List from qualified tests (i.e. Top MAC or Top IP).

User-Defined Stations

You can edit each station list to add, delete, assign symbolic names, sort or print. Refer to the “Editing the Station List” section in this chapter for information on editing the station list.

Predefined Stations

The station list has predefined entries that are stored in the MAC address sublist. Table 14-1 shows a Token Ring example of predefined stations. The instrument displays these predefined symbolic names at the end of the list in mixed upper and lower case. These entries cannot be modified or deleted and are included as part of the maximum 512 entries per list.

Table 14-1. Token Ring Predefined Stations Sample List

Name	Address
ThisLANMeter	Predefined (ROM) address[1]
Broadcast	`ffffffffffff`
Func Bdcst	`c000ffffffff`
Novell Bdcst	`c00000800000`
NetBIOSbdcst	`c00000000080`
Active Mon	`c00000000001`
Ring Err Mon	`c00000000008`
Ring Prm Srv	`c00000000002`
Report Srv	`c00000000010`
Bridge	`c00000000100`
LAN Manager	`c00000002000`
Bandwith Mgr	`c00000000020`
Directry Srv	`c00000000040`
IMPL Server	`c00000000200`
Rng Auth Srv	`c00000000400`
LAN Gateway	`c00000000800`
Wirng Concnt	`c00000001000`
Note 1. If you change the instrument MAC address, the station list does not reflect the change.	

Adding Stations

You can add stations to the Station List using any of the following methods:

❒ Use the Add Station function. See the following section, “Editing the Station List.”

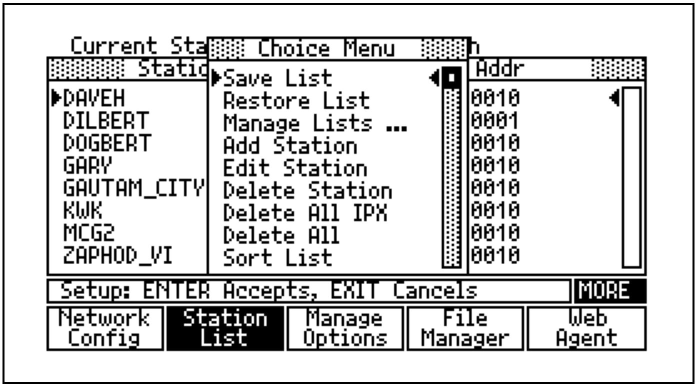
❒ Merge discovered stations into Station List from tests that provide this option.

❒ Use the Import function. See Chapter 12, “*File Manager*” for more information on importing station lists.

Editing the Station List

Use the following procedure to Edit a station list:

1. Press the top-level **Setup/Utils** softkey, select the **Station List** softkey and select it again to run Station List.
2. If you want to edit or delete a single entry, use △ and ▽ to select a station. Alternately, you can press ENTER/RUN and then edit the desired parameters in the pop-up window.
3. Press MENU. Figure 14-3 shows the Station List pop-up menu.



Static	Addr
DAVEH	0010
DILBERT	0001
DOGBERT	0010
GARY	0010
GAUTAM_CITY	0010
KWK	0010
MCG2	0010
ZAPHOD_VI	0010

Setup: ENTER Accepts, EXIT Cancels

Figure 14-3. Station Editing Pop-up Window

The Station List pop-up menu provides the following selections for managing your Station Lists and is accessed by pressing MENU from the Station List Setup window. Press △, ▷, ◁, or ▽ to scroll through the list.

❐ Save List
❐ Restore List
❐ Manage Lists...
❐ Add Station
❐ Edit Station
❐ Delete Station
❐ Delete All (MAC, IP, IPX, or VIP)
❐ Delete All
❐ Sort List
❐ Print All

Save List

The **Save List** selection saves the current list into non-volatile memory.

Restore List

The **Restore List** selection restores the list from non-volatile memory. You must use this selection prior to exiting Station List, because the current list is automatically saved to non-volatile memory when you exit Station List. Executing the **Restore List** function will cause any changes that you have made to the Station List since the last time you saved it to be lost.

Manage Lists

The **Manage Lists** selection shows a list of the available Station Lists. If there are more entries than can be seen on the screen, then use △ or ▽ to view the entire list.

Pressing MENU from this window causes the following choices to be available:

Save As.. allows the current Station List to be saved by another name.

Load allows you to load a previously stored list into the current Station List.

Delete allows you to delete the selected Station List. The current Station List cannot be deleted.

Rename allows you to rename the current Station List.

Merge allows you to merge the selected Station List with the current Station List. If there are any duplicate address entries, you are given the choice to keep all of the current entries or to replace them all.

Add Station

The **Add Station** selection creates a new station list entry by prompting you to enter a symbolic name and an address. You can switch between the fields by pressing either △ or ▽.

Enter the symbolic name by using a combination of the base alphanumeric keys, the ALPHA key, and the SHIFT key. The following softkeys are also provided to make editing easier:

> **Caps Lock** provides capital alpha characters from the keyboard when enabled.

Special Chars brings up a pop-up menu of special ASCII characters for name entry.

Delete To End deletes all characters from the cursor position to the end of the field.

Backspace deletes the character behind the cursor position.

Enter the MAC address using the numbers 0 through 9 and the letters A through F. Press ENTER RUN to add this station to the list.

The selected address type affects the address display format (Hex versus dotted decimal, for example). In the case of the address type IPX, you need to configure a network number.

Edit Station

The **Edit Station** selection is used to modify the fields of a selected Station List entry. The **Edit Station** selection performs the same function as pressing ENTER RUN after selecting an entry in the Station List. The following softkeys are provided to make editing easier:

Caps Lock provides capital alpha characters from the keyboard when enabled.

Special Chars brings up a pop-up menu of special ASCII characters for name entry.

Delete To End deletes all characters from the cursor position to the end of the field.

Backspace deletes the character at the cursor position.

The following are the available parameters:

❐ Symbolic name (optional)
❐ Address for the selected entry
❐ Network Number (depends on Address Type)

When you edit an IP Address, press W • X to move between the dotted decimal fields. No leading zeros are required in the address (for example, enter `5` not `005`).

Delete Station

Pressing ENTER RUN when **Delete Station** is selected deletes the selected station from the list without requesting your confirmation. The factory-predefined entries cannot be deleted.

Delete All (MAC, IP, IPX, or VIP) — The **Delete All (MAC, IP, IPX, or VIP)** selection deletes all MAC, IP, IPX, or VIP address types for the current Station List.

Delete All — The **Delete All** selection deletes the current station list after prompting you for confirmation. The predefined stations are not deleted.

Sort List — The **Sort List** selection sorts the current symbolic names alphabetically or by address.

Print All — The **Print All** selection prints the current station list using the current printer configuration parameters.

Importing Novell and IP Host Tables

Refer to Appendix D “Utilities,” for information on importing and exporting station lists to and from the LANMeter instrument.

Appendices

Appendix A
Troubleshooting Scenarios

Introduction

This appendix describes how to use the Enterprise LANMeter with the most common troubleshooting scenarios. The following sections are covered in this appendix:

❒ Troubleshooting with SwitchWizard
❒ Troubleshooting in a TCP/IP Environment
❒ General Troubleshooting Scenarios
❒ Ethernet Troubleshooting Scenarios
❒ Token Ring Troubleshooting Scenarios
❒ TCP/IP Troubleshooting Scenarios

Troubleshooting with SwitchWizard

The following troubleshooting scenarios are covered in this section:

❒ Source of Excessive Broadcasts using SwitchWizard
❒ Source of Errors on a Switched Network
❒ SwitchWizard Port versus Interface Reporting

Generally, the problems found in a switched environment are identical to those experienced in a shared media environment. The following issues should be considered:

1. How busy is each segment (port)?
2. How do you identify and track the source of errors?
3. What stations are attached to specific segments?

Typically, it is not the switch that causes the problem, but the inability to “see” inside the switch. SwitchWizard’s ability to see inside switches is what provides its great value. Refer to Chapter 7 “SwitchWizard Option” for additional information on SwitchWizard.

Source of Excessive Broadcasts using SwitchWizard

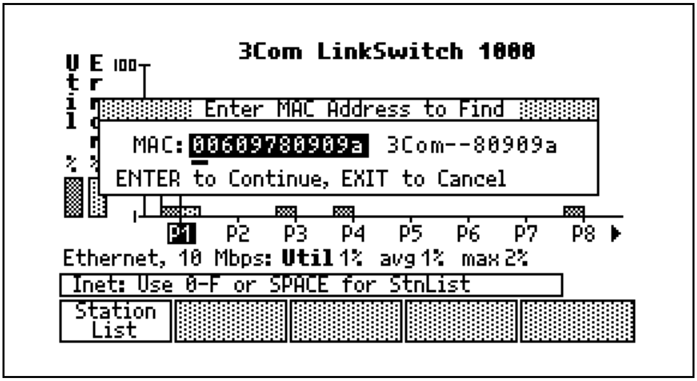
You notice an excessive percent of broadcasts from the Network Statistics test. You exit Network Statistics, press MORE, select **Top MAC** and then the **Top Brdcasts** test. By setting the Display Mode to Broadcast Sources, you see that the MAC address **`3com-80909a`** is generating 80% of the broadcasts. You would like to investigate further; however, you are not sure where in your switched network this station is located.

You press EXIT STOP to stop the Top Broadcasts test and then you press MENU and merge the discovered station addresses into the station list. This saves the broadcasting MAC addresses for you to use later from SwitchWizard.

To run SwitchWizard, you select the Internet TCP/IP test suite, configure an IP address for the LANMeter instrument, and run the Segment Discovery test. You zoom in on the discovered Switches/Bridges and use TAB to select the switch of interest. Then you enter into the SwitchWizard functionality by pressing **Use Toolkit** and then run the MultiPort Statistics tool. The Enterprise LANMeter takes a few seconds to query the switch and build a graphical representation of the activity on your switch ports.

You then select **Find Port**, press **Station List**, and then repeatedly press TAB until you select the MAC address that was broadcasting so many frames: **`3com-80909a`**.

Within seconds after pressing ENTER RUN, the LANMeter instrument identifies the port for that MAC address (refer to Figure A-1). By selecting that port and looking at Source Details, you can display the MAC address of the station along with its Symbolic Name and IP address (refer to Figure A-2).



3Com LinkSwitch 1000

Enter MAC Address to Find

MAC: 00609780909a 3Com--80909a

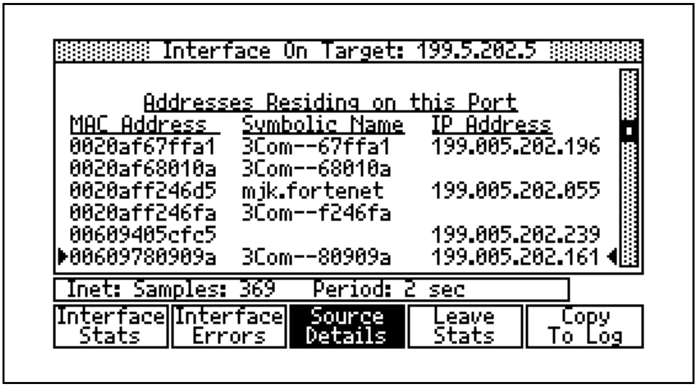
ENTER to Continue, EXIT to Cancel

Ethernet, 10 Mbps: Util 1% avg 1% max 2%

Inet: Use 0-F or SPACE for StnList

Station List

Figure A-1. MultiPort Statistics Find Port



```
Interface On Target: 199.5.202.5

      Addresses Residing on this Port
 MAC Address    Symbolic Name    IP Address
 0020af67ffa1   3Com--67ffa1     199.005.202.196
 0020af68010a   3Com--68010a
 0020aff246d5   mjk.fortenet     199.005.202.055
 0020aff246fa   3Com--f246fa
 00609405cfc5                    199.005.202.239
▶00609780909a   3Com--80909a     199.005.202.161 ◀
 Inet: Samples: 369   Period: 2 sec
```

Figure A-2. MultiPort Statistics Source Details

Source of Errors on a Switched Network

Assume that you are using a cut-through switch. A cut-through switch makes the packet forwarding decision after the destination MAC address has been read into the buffer. Because a cut-through switch starts forwarding before the complete frame is received, the packet can be forwarded with errors.

You plug the LANMeter instrument into one of your switched segments to perform a routine network health check.

Examining the Network Errors test within the LANMeter instrument’s Network Monitor function, you notice that your error rate is 5%, which is abnormally high for this segment. Drilling down into the Errors, you see that the errors are being caused by Jabbers. You then drill down into the Jabbers and you do not recognize the error source address as being on this switched segment.

You can use SwitchWizard to find the source of the errors. To run SwitchWizard, you select the Internet TCP/IP test suite, configure an IP address for the LANMeter instrument and run the Segment Discovery test.

You then zoom in on your switch. Enter into the SwitchWizard functionality by pressing the **Use Toolkit** softkey and then running the MultiPort Statistics tool. LANMeter will take a few seconds to query the switch and build a graphical representation of the activity on the switch ports.

You can then select **Sort Options** and select Sort by Errors. Within a few seconds after pressing ENTER RUN, the LANMeter instrument rebuilds the switch graphic showing the ports with the highest errors first. You can select the port that you want to display using TAB. You probably want to look at the first port which shows the highest errors. Pressing **Interface Errors** should show a high amount of Oversize frames being generated on this port.

SwitchWizard Port versus Interface Reporting

When the SwitchWizard and the MultiPort Statistics graphic reports an interface using an **I** rather than a **P**, it means that MultiPort Statistics cannot determine the port number for that interface. The number after the **I** is the number reported in the Interface Table index. When port numbers are available from the Bridge MIB, SwitchWizard reports a **P** followed by the port number. Because non-bridge ports may be reported in the Interface Table, the first bridge port found (**P1**) may not be the first entry in the Interface Table.

Troubleshooting in a TCP/IP Environment

The following troubleshooting scenarios are covered in this section:

❐ Correct IP Address for the Network
❐ Duplicate IP Addresses
❐ Incorrect Subnet Mask
❐ Incorrect Default Router
❐ Incorrect DNS Server

There are several steps that can be taken to prevent or reduce the likelihood of problems in a TCP/IP environment. The most important step is to have thorough documentation of the network itself. While it may seem that such careful documentation is not needed in a small network, hours of down-time and network troubleshooting can be avoided by attention to these issues. The most common problems in a TCP/IP environment relate to IP addresses and related configuration parameters. So, a little proactive work in the beginning goes a long way toward avoiding problems later, as well as solving the problems that that do occur more quickly.

Correct IP Address for the Network

If a host is using an invalid address for the subnet to which it is connected, it will be able to send packets out, but the reply does not come back (it may have gone somewhere else or have been discarded by the router.)

Check the configuration described in your documentation to ensure that the configured address falls within the range allowed by the local subnet, check the configuration of a nearby station in the same subnet to ensure that your documented subnet is accurate, or run the LANMeter instrument's TCP/IP Top IP (Top Senders or Top Receivers) test to see if most of the listed addresses match the subnet range you are expecting and if the assigned address is within that range.

The Internet TCP/IP Segment Discovery test rapidly assembles a list of all active IP hosts on the local segment—regardless of whether they have the correct address for this subnet. The test will disregard any traffic from off the local segment, so that you get a list of only the local hosts. A quick glance through the sorted list will reveal whether there is a host with an IP address that does not match the subnet.

Duplicate IP Addresses

A duplicate IP address is probably the most well-known problem in TCP/IP networks. Two stations with the same IP address will cause either intermittent connection problems for both stations or several problems with one station until one of the stations is turned off. Later, when both stations are active again at the same time, the problems reappear.

One method to discover stations with duplicate IP addresses is to send ARP packets to the common IP address. All duplicated stations respond to the ARP along with their MAC addresses. The Internet TCP/IP Segment Discovery test will quickly identify any duplicate IP addresses on the local IP segment. Once detected, the duplicated address is shown together with each MAC address that is using the problem IP address. Further testing may be performed on any of the listed address pairs by using the Toolkit of SNMP queries.

Incorrect Subnet Mask

The subnet mask tells a host station how much of the 32-bit IP address is used for the network address, and how much is used for the host address. The most common subnet mask problem is created when "non-standard" subnets are used or when an address range is further subnetted to allow for additional segments. If a host is using the wrong subnet mask, it may decide that it does not really exist on the same logical network segment as certain other local hosts and the first host will not talk directly with them. In some cases, enabling proxy ARP on a local router will permit these incorrect configurations to operate normally.

The Internet TCP/IP Segment Discovery test quickly identifies hosts on the local IP segment with subnet masks that do not match other hosts. Further testing may be performed on any of the listed hosts by using the Toolkit of SNMP queries.

Incorrect Default Router

If a host does not have a default router configured (sometimes shown as a default gateway), all off-net communications will fail. More often, problems occur when the configured router is not actually a router or is a sub-optimal router. If a non-router is sent packets to forward, it may return the ICMP message, “Destination unreachable: Network unreachable.” Other host implementations may actually forward those packets to their own default router, consuming valuable CPU and memory resources. Some UNIX workstations and other IP hosts permit routing protocols to be enabled, and will look like routers to the local subnet.

The Internet TCP/IP Segment Discovery test identifies all local hosts that are sending routing protocols—whether or not they are actually routers. Usually, the associated MAC address will supply enough information to determine whether the host is really a router or not. If a particular host is suspect, run the Internet TCP/IP Scan Host test to quickly determine how the host is configured using a variety of SNMP queries and Ping tests.

Incorrect DNS Server

If possible, hosts should have more than one DNS server configured. DNS allows secondary servers to keep current from primary servers. If a host is configured for at least two DNS servers that can be connected over different paths, the probability of applications failing due to no access to DNS is lower.

A number of tests can be run to help identify this problem. First the LANMeter instrument’s ICMP Ping can be used to verify that the configured DNS server is reachable. If it cannot be reached, the Trace Route test can be used to locate where the communications failure is occurring. Also, the Internet TCP/IP Toolkit can be used to query the configured DNS server—thus verifying valid configurations. The Internet TCP/IP Segment Discovery can be used to identify other DNS servers available from this segment.

General Troubleshooting Scenarios

The following troubleshooting scenarios are for both Ethernet and Token Ring interface modes:

❒ Tuning Your NetWare Network
❒ Finding an IP Station’s MAC Address
❒ Testing Bridge and Router Throughput

Tuning Your NetWare Network

In a multi-segment, or multi-ring, NetWare network it is useful to know how each segment, or ring, is used. Performance related problems can sometimes be tracked to an overloaded router, segment, or ring due to traffic taking non-optimal routes. To identify this type of problem, it is necessary to look beyond the MAC addresses to the network layer (IPX). The Novell Routing Analysis test classifies the nature of network layer source and destination traffic into three categories: Local to Local, Remote to Local, and Remote to Remote. Using this information you can tune your network by adjusting the network configuration and strategically placing servers and routers in you network.

Before running the Routing Analysis test, you should know the location of the segment (or ring) in question on the network and be able to answer these questions:

1. What kind of traffic should be on this network?
2. What off-network resources are used?
3. Should there be any remote-to-remote traffic?

You can first run the Server List test and merge the discovered names into Station List. This allows you to see the server names when you run the Routing Analysis test. To save these discovered names in non-volatile memory, press MENU from Station List and select the **Save List** option.

Then run the Routing Analysis test and look for anything out of the ordinary. Highlight the remote-to-remote or remote-to-local traffic categories and press the **Zoom In** softkey to look at the traffic counts. Press TAB to view the IPX network number. If there are a lot of remote server accesses, consider moving the server or using a dedicated router. Make sure there are no surprises in the remote-to-remote category. If performance is sluggish, consider making topology and/or configuration changes to resolve the problem. Rerun the Routing Analysis test on a regular basis to check for significant changes.

Finding an IP Station’s MAC Address

You can easily identify the MAC address of an IP node by using the ICMP Ping test (a TCP/IP test). ICMP Ping reports the MAC address that the instrument uses to send an ICMP Echo Request packet. If that IP address is on the other side of a router, the router’s MAC address is displayed; otherwise the MAC address of the IP station is displayed.

Testing Bridge and Router Throughput

Bridge and router throughput can be a network bottleneck, especially in WAN (Wide Area Network) connected networks. You can use the Traffic Generator to help quantify the network’s end-to-end throughput.

Bridges

Set the MAC destination address to an address known to be on the other side of a bridge. The bridge ignores the protocol specific fields and automatically forwards the packet.

Routers

Set the Type field to a routed protocol (Netware or TCP/IP). Set the MAC DST address to that of the router. Set the network address to a subnet on the other side of the router. This is the IPX Network parameter for Novell networks or the IP Address parameter for IP networks.

If you have a second LANMeter instrument (or other monitoring device), you can install it on the target segment. Try to quantify the network throughput by running Traffic Generator and using the arrow keys (while the test is running) to vary frame size and frame rate. You should also attempt to pass traffic in both directions simultaneously.

You can get a better feeling for the application-to-application performance and account for network latency by using a network loading program like PERFORM3 (on Novell networks), or FTP (on TCP/IP networks). Run the network loading program with different background traffic levels and record the throughput results reported by the network loading program for various background frame sizes and rates.

Ethernet Troubleshooting Scenarios

The following Ethernet troubleshooting scenario sections are discussed:

❒ Testing Connectivity for Auto-Speed Ports
❒ Sources of Excessive Collisions
❒ Misconfigured Novell Frame Types

Testing Connectivity for Auto-Speed Ports

You can test an auto-speed port's connectivity at 10 Mbps by configuring the LANMeter instrument to 10 Mbps Ethernet Speed, connecting it to an auto-speed port, and then running a test. Similarly, the same connectivity test can be performed on an auto-speed port at 100 Mbps. Also, you can test 10 Mbps ports for connectivity by configuring the LANMeter instrument to 10 Mbps Ethernet Speed, connecting it to a 10 Mbps port, and then running a test. In any of these cases, the instrument will display an error message if there is a connectivity problem.

Caution

Always configure the Fluke 686 and 683 LANMeter instrument's Ethernet Speed parameter to Auto Detect when you are unsure whether you are attaching to a 10 Mbps or to a 100 Mbps Ethernet network.

Do not configure the LANMeter instrument for 100 Mbps and then attach it to a 10 Mbps network. The presence of the 100 Mbps link pulse on a 10 Mbps network effectively brings down the network by preventing all stations from transmitting.

Configuring the LANMeter instrument to 10 Mbps and then attaching it to a 100 Mbps network causes erroneous results (such as excessive collisions) to be reported.

Sources of Excessive Collisions

One of the most common problems on Ethernet networks is excessive collisions. The symptoms of excessive collisions are anything from a network slowdown to a completely unusable network. Many times it seems a completely unusable network is preferable to a network slowdown because you have more testing freedom than if you have to work around user's schedules. Most of the time, excessive collisions can be traced to a media or cabling related problem. 10BASE2 or ThinLAN networks are especially trouble-prone to excessive collisions.

Run the Network Statistics test (a Network Monitor test) to obtain network information to evaluate. If the average collision rate is greater than 5% (or you are seeing very high collision bursts), further testing is warranted. If possible, try to isolate the problem domain by breaking the network into functional pieces and by using the LANMeter instrument to look for symptoms. This network isolation technique can quickly identify problems.

It is necessary to have traffic on the network to resolve collision problems. You can use the background Traffic Generator function to add a moderate amount of traffic (100 frames/second) to the network and then observe the results of the Network Statistics test. Some media related problems are traffic level dependent. Try varying the traffic level by using the arrow keys from the Traffic Generator screen while watching the ERROR and COLLISION LEDs. Be careful when adding traffic because you can easily saturate the network.

Collision related problems can be difficult to resolve because measurements are largely dependent upon the observation point. Results can vary between two observation points on the same cable even when separated by only a few feet. It may help to make several measurements from different points on the network and to observe changes seen in the collision problem.

Once the problem is isolated to a single segment or part of the network, you can test the cable (with Cable Scan), test hubs and adapter cards (with Expert-T Autotest), and perform a physical inspection of the network.

10BASE2 and ThinLAN coaxial networks are trouble-prone because they are easily expanded beyond specifications with a cable and a T connector by uninformed users.

Watch out for the following in 10BASE2 and ThinLAN networks:

❒ Excessive cable lengths. (Each segment should be 185 meters or less.)

❒ Loose or bad barrel and T connectors.

❒ Additions of 75 ohm or 93 ohm cable.

❒ Excessive taps. (10BASE2 or ThinLAN segments should have 30 taps or less.)

❒ T connector to adapter card stubs.

❒ Excessive terminators. (Many repeaters terminate the cable and they must be at the end of a segment.)

❒ Improper grounding. (Each coaxial segment should be grounded at one and only one point.) Watch out for inadvertent rotating back-of-the-PC T connectors causing ground loops. The easiest way to isolate this problem is with a current probe.

10BASE-T networks are generally more robust than 10BASE2 or ThinLAN networks. Watch out for the following in 10BASE-T networks:

❒ Excessive cable lengths (100 meters or less).
❒ Split pairs (verify the wire pairing using the Cable Scan test).
❒ Bad hub ports and adapter cards.
❒ Poor punchdown block connections.

Misconfigured Novell Frame Types

In Novell Ethernet networks there are four possible frame types: 802.3 (raw), 802.2, Ethernet II, and SNAP. The 802.3 method has been common but it caused interoperability problems in some multi-protocol networks. The other frame types are based upon agreed upon standards. Starting with NetWare 4.0, the default frame type is 802.2.

For a client and server to communicate they both must be configured for the same frame type. A mismatch in frame type can be a source of interoperability problems. You can configure a client for a single frame type, while a server can optionally be configured to recognize some or all frame types.

The LANMeter instrument offers several tools to solve frame type related problems. These include Server List, NetWare Ping, Protocol Mix, and NIC Autotest. Use the following approaches to help resolve frame type related problems:

1. To determine the frame types used, run the Protocol Mix test (a Network Monitor test) to break out the different NetWare frame types. (The Ethernet II and SNAP types are mapped to the same description.)
2. If you suspect a misconfigured client, run the NIC Autotest (a NIC/Hub test) to report the frame type used.
3. To determine what frame types are enabled, run the Server List test (a Novell NetWare test) configured for Auto frame type.

Token Ring Troubleshooting Scenarios

The following Token Ring troubleshooting scenario sections are discussed:

- Beaconing Ring
- Sources of a Network Slowdown
- Station Cannot Log into Server
- Bad Cable
- Determining which Stations Use a Network Resource Most
- Identifying the Physical Location of a Station
- Tracking Sources of Phase Jitter

Beaconing Ring

A ring is beaconing if the network has a hard error that prevents the network from working. You will probably first learn of a beaconing ring when several network users complain of being dropped from their servers or not being able to log into the network.

In most cases the Token Ring protocol will automatically recover a beaconing network. If the beaconing ring does not recover automatically, you must manually correct the problem to resume network activity. To correct the problem you must determine the fault domain, isolate the problem, and fix the network defect.

The fault domain limits the problem to two stations, their connecting cables, and any equipment (a MAU, for example) between the two stations. The two fault domain stations are the station reporting the error and its Nearest Active Upstream Neighbor (NAUN).

To determine the fault domain, you must use the LANMeter instrument to enter the ring. Use the following procedure to enter a beaconing ring.

1. Press the **Network Monitor** softkey.
2. Connect the instrument as shown in Figure A-3.
3. Press the **Network Stats** softkey or ENTER RUN to run the test.

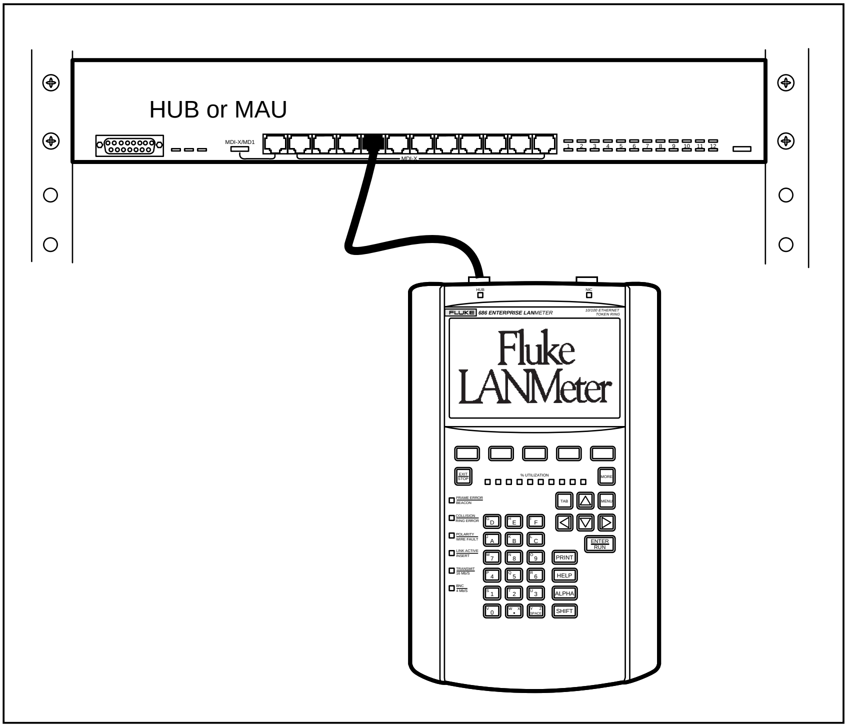


Figure A-3. TO MAU Connection

The instrument attempts to enter the ring normally, lights the BEACON LED, and displays a Beacon Alert pop-up window to inform you that beacon frames are on the ring. The Beacon Alert pop-up window shows the fault domain. Use the fault domain information to isolate the problem.

If you have good network documentation, you can remove lobe cables within the fault domain until the ring recovers.

Otherwise, you can remove the entire MAU to isolate the problem and allow the rest of the ring to operate.

You can remove the entire MAU by disconnecting the Ring In (RI) and Ring Out (RO) cables. For Type 1 MAUs, this activates the secondary (or backup) ring, which allows the network to function while you fix the problem.

Finding the problem is now a process of elimination. Use the instrument to test the fault domain NICs [using NIC Autotest (a NIC/MAU test)], lobe cables (using Cable Tests), and MAU [using MAU Autotest (a NIC/MAU test)]. Replace or fix the defective part and reconnect to the ring.

Sources of a Network Slowdown

The following questions and their related actions should help you locate the sources of a network slowdown:

1. Has anything changed recently? If so, first suspect that change as the source of the network slowdown.
2. Is a single station affected? If so, suspect the workstation (or server), a misconfiguration, or an application problem as the source of the network slowdown.
3. Does the problem seem to be related to a particular application being run? If so, suspect that application as the source of the network slowdown.
4. If only a particular traffic pattern is affected by the network slowdown, does this traffic go through routers, bridges, or both? If so, a throughput problem may exist with the routers, bridges, or both.

If the problem seems to be affecting all users and is application independent, try using the following process to isolate the problem to the physical media, an offending station affecting the entire network, or a server, bridge, or router bottleneck:

1. Use the following procedure to verify the integrity of the physical media.
    a. Run the Network Statistics test (a Network Monitor test) and look for ring purges, claim tokens and soft errors. Do not change the ring topology during this test. (Do not insert or remove stations from the ring.)
    b. If you see ring purges and soft errors, use the Error Statistics test (a Network Monitor test) to find the fault domain. If the errors seem to be distributed throughout the network, use the following procedure:
        1. Run the Phase Jitter test (a Network Monitor test). Refer to the “Tracking Down Sources of Phase Jitter” section in this chapter or refer to Chapter 4 “Testing Network Components,” for information on running the Phase Jitter test.
        2. You could have a problem with certain stations becoming the active monitor. Use the Active Monitor History display from the

Ring Stations test (a Network Monitor test) to see the list of active monitors. Verify that the stations that have tried to become the active monitor have the most recent network drivers, or replace their network interface card.

c. If you see beacons on the network, the beacon pop-up window will give you the fault domain.

2. Check the network utilization percentage by using the Network Statistics test. As long as the peak utilization is less than about 70% it is fairly safe to assume the bandwidth of the media itself is not a problem.
3. Use the Top Senders, Top Receivers, and Top Broadcasts tests (all Network Monitor tests under the **Top MAC** softkey) to help isolate the problem to nodes that are sending and receiving the most traffic. Check for stations sending a lot of broadcasts, especially all-routes broadcasts.
4. If you suspect a device (server or router) may be overloaded, you can configure the Top Senders test to only display the traffic sent to that device. Do this by selecting the Top Senders configuration screen and entering the MAC address of the suspected overloaded device in the **Senders to a Single stn** field. The Top Senders test shows a pie chart of the stations asking the most of the overloaded device.

Station cannot Log into Server

Use the Expert-T Autotest to identify why a station cannot log into a server or insert onto the network. Use the following procedure to run Expert-T Autotest:

1. Press the top-level **NIC/MAU Tests** softkey. This also highlights the **Expert-T Autotest** softkey.
2. Connect the instrument as shown in Figure A-4.
3. Configure the test. Refer to the Configuration section in Chapter 4 “Testing Network Components,” under the “Expert-T Autotest” section.
4. Press the **Expert-T Autotest** softkey or [ENTER RUN] to run the test.
5. Observe the test results.
6. Press [EXIT STOP].

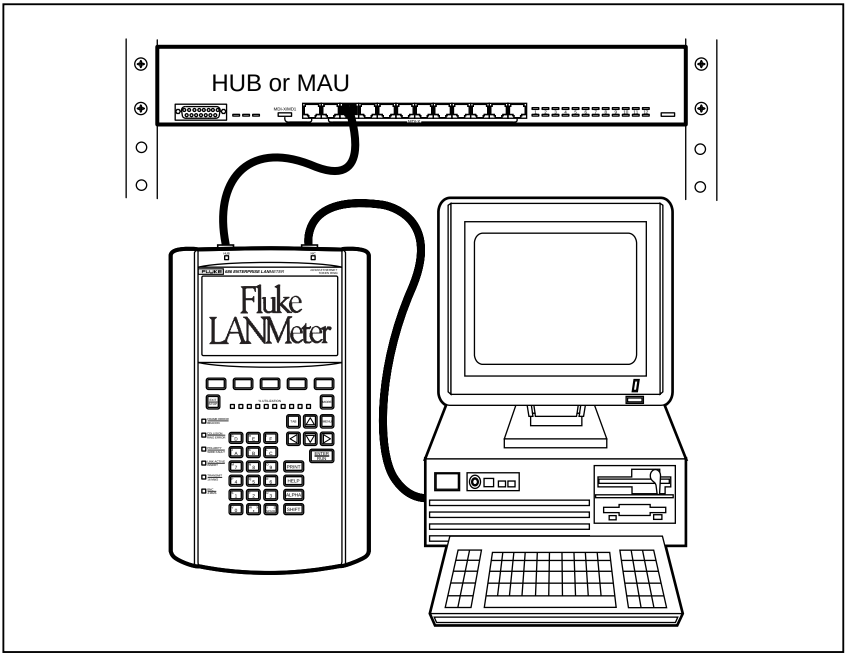


Figure A-4. Expert-T Autotest Connections

Expert-T Autotest identifies the following problems:

1. Ring and station speed mismatch
2. Duplicate station address
3. Network interface card applying insufficient voltage to the MAU
4. Bad cables or connectors

Bad Cable

You can locate a bad cable by first determining the soft error fault domain and then testing the fault domain cables.

The instrument determines the soft error fault domain with the Error Statistics test. You can access Error Statistics by selecting **Network Monitor** from the top-level softkeys.

The instrument displays Error Statistics results after calculating the statistics for the first sample period. Press the **Zoom In** softkey to display the soft error fault domain. Use Cable Tests on the cables of these listed stations to identify the faulty cable.

After you have isolated a cable problem to a specific cable, use Cable Tests to pinpoint the cable defect. Use the following procedure to pinpoint a cable defect. You could also use the Cable Autotest with the optional 100 MHz Remote to pinpoint the cable defect.

1. Press the **Cable Tests** softkey. This also highlights the **Cable Scan** softkey.
2. Connect the instrument as shown in Figure A-5.
3. Configure the instrument for the correct cable type by pressing MENU, then pressing ENTER RUN. Refer to Chapter 2 “Testing Cables and Connectors,” the Configuring Cable Test section, for detailed information on configuring Cable Tests.
4. Press ◁ or ▷ to select the correct cable type to match the cable to be tested. Refer to Chapter 2 “Testing Cables and Connectors,” for more information on configuring Cable Tests.
5. Press EXIT STOP to save your configuration to non-volatile memory and exit the Configuration screen.
6. Press the **Cable Scan** softkey or ENTER RUN to run the test.
7. Press △ or ▽ to view the test results.

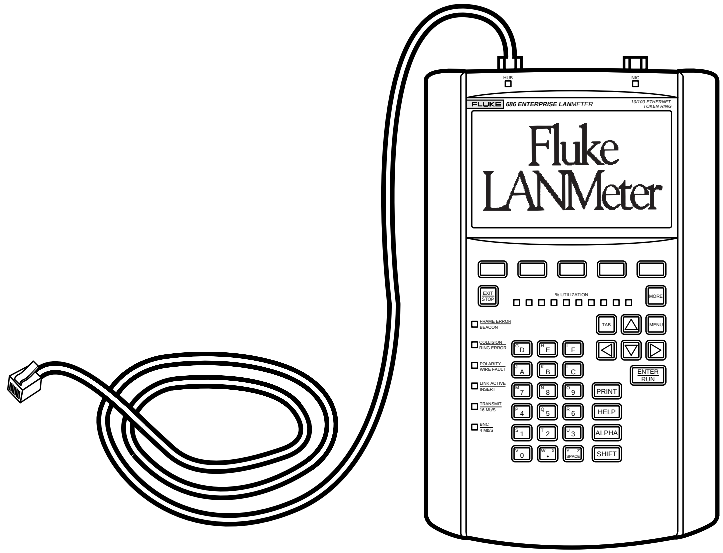


Figure A-5. Bad Cable Test Connection

Determining which Stations use a Network Resource Most

Use the following procedure to determine which stations use a network resource the most:

1. Press the top-level **Network Monitor** softkey.
2. Press MORE. This also highlights the **Top MAC** softkey.
3. Connect the instrument to a MAU as shown in Figure A-3.
4. Configure the test as follows:
    a. Press MENU. This also selects the **Configure** option.
    b. Press ENTER RUN.
    c. Set the **Senders to a Single stn** field to **On** by using ▷ or ◁.
    d. Press ▽ to highlight the **Filter Addr** field.

e. Enter the network resource’s MAC address in the **Filter Addr** field by using the alphanumeric keypad.

   To undo any configuration changes you made, press MENU, select **Cancel Changes** in the Configuration Menu, and then press ENTER RUN.

5. Press EXIT STOP to save your configuration to non-volatile memory and exit the Configuration screen.

6. Press the **Top MAC** softkey or ENTER RUN to run the test. The instrument displays a pie chart of the stations that transmit the most to the selected network resource.

Identifying the Physical Location of a Station

On a network of significant size, finding the physical location of a station by its address can be time consuming. Use the following procedure to find the physical location of a station:

1. Press the top-level **Network Monitor** softkey.
2. Press the **Ring Stations** softkey (to highlight the softkey).
3. Connect the instrument as shown in Figure A-3.
4. Press the **Ring Stations** softkey or ENTER RUN to run the test.
5. Wait for the instrument to display the results screen.
6. Press EXIT STOP.
7. Scroll through the list of stations and find the station of interest and the **This LANMeter** listings.
8. Count the number of stations (the delta) between the **This LANMeter** listing and the suspected station’s listing.

   a. If the station of interest shows up in the list before the **This LANMeter** listing, its physical position is delta active stations upstream from the instrument.

   b. If the station of interest shows up in the list after the **This LANMeter** listing, its physical position is delta active stations downstream from the instrument.

Tracking Sources of Phase Jitter

Phase jitter describes the sampling error of data as it is clocked around a network and it is expressed in terms of nanoseconds (ns.).

The instrument will measure the uncorrelated phase jitter on an operational ring and compare that to the Token Ring specification. Uncorrelated phase jitter is an indication of network noise. Since the Phase Jitter test is a quantitative measurement, you can use it to track changes in your network and anticipate problems before they become serious. It is a good idea to make phase jitter tests before and after adding new network components or expanding your network.

All network components (MAUs, network interface cards, and cables, for example) add phase jitter to a signal as it travels around your Token Ring network. If your network has an excessive amount of phase jitter you can use the instrument to isolate the most troublesome sources. There are many ways to do this; the following is one method:

Caution

Read the following procedure in its entirety prior to performing it. If your network is not in good health you can cause some data loss.

1. Use the instrument to measure the ring phase jitter by running the Phase Jitter test as described in Chapter 4, "Testing Network Components," and record the results.
2. Disconnect a MAU's **Ring In** or **Ring Out** connector to force the ring to use its backup path. (For Type 1 MAUs only.) Your ring should continue to operate normally. If the ring beacons, then check all the MAU interconnect cables and connectors.
3. Measure and record the phase jitter again. If the phase jitter increases significantly, then your Adjusted Ring Length (ARL) may be too long.
4. Remove a MAU from the ring by disconnecting the **Ring In** and **Ring Out** cables and attaching them together. This bypasses the MAU entirely and removes all stations that connected to this MAU.
5. Measure and record the phase jitter and note which MAU was removed from the network.
6. Reattach the patch cables to the MAU, connecting it to the ring.

7. Repeat steps 4, 5, and 6 until you have recorded the phase jitter with each MAU removed from the ring.
8. If there was a significant drop in phase jitter when one of the MAUs was removed, the likely cause is the MAU, one of the stations plugged into the MAU, the MAU interconnecting cables, or a combination of these.
9. Successively remove and reinstall each station from the suspect MAU, while recording the phase jitter as each station is removed. If you see a large drop in phase jitter with a particular station removed, suspect either the network interface card or the lobe cable. You can measure phase jitter after replacing each component to find the cause of the problem. If the phase jitter problem is still not resolved, suspect the MAU or its interconnecting cables.
10. Successively remove and reinstall the **Ring In** and **Ring Out** cables for the suspect MAU, while recording the phase jitter as each cable is removed, until the offending cable is found.
11. If there is still a phase jitter problem, replace the MAU.

Note

The Phase Jitter test can give erroneous results if run on networks using retiming circuits or reclocking Jitter Busters because the instrument must source the network clock to run this test.

TCP/IP Troubleshooting Scenarios

Refer to the Fluke Network Maintenance and Troubleshooting Guide for information on this topic.

Appendix B
Specifications

General Specifications

Weight	2 Kg. [4.5 lbs.] Nominal
Dimensions	29.2 x 17.8 x 6.7 cm [11.9" x 7.0" x 2.65"] Nominal
Keyboard	36-Key Elastomeric
LCD	240 x 128 pixel LCD bit-mapped Display
LED Indicators	19
Internal Battery Pack	9 Sub-C NiCad Cells 9 Sub-C NiMetal Hydride Cells
External AC Adapter/Battery Charger	AC input: 100V to 240V, 0.8A, 50-60 Hz DC output: 24V, 1.25A
Shock and Vibration	Meets requirements of MIL-T-28800E for Type II, Class 5, Style E equipment
Communication Ports	(1) RS-232C Serial Port
Network Ports	(2) MAU and/or Hub Connectors, RJ-45 and DB-9 (only on the Fluke 686, 685, and 680) (2) NIC Connectors, RJ-45 and DB-9 (the DB-9 is only on the Fluke 686, 685, and 680) (1) BNC Connector (on the Fluke 686, 685, 683, and 682)

Analog Accuracy Specifications

DC Resistance

500Ω to 500kΩ (± 10%) RJ-45

10Ω to 200Ω (± 10%) BNC

Cable Length

Note

Length specifications are relative to the calibrated NVP value using a representative reference cable. Variations, not included in the specification occur due to variations in the relative permittivity of the dielectric of the cable. The length of different pairs in a cable may vary as a result of different twist rates and should not be used to verify performance of the cable length measurement function.

	Twisted Pair Cable	**Coax, 50Ω**	**STP, 150Ω**
Range	0 to 30 m (100 ft)	0 to 30 m (100 ft)	0 to 30 m (100 ft)
Resolution	0.1 m or 1 ft	0.1 m or 1 ft	0.1 m or 1 ft
Accuracy:	± (1 m (3 ft) + 2% of reading)	±(1 m (3 ft) + 2% of reading)	±(1 m (3 ft) + 2% of reading)
Range	30 to 328 m (1000 ft)	30 to 600 m (2000 ft)	30 to 600 m (2000 ft)
Resolution	0.1 m or 1 ft	0.1 m or 1 ft	0.1 m or 1 ft
Accuracy:	± (1 m (3 ft) + 4% of reading)	± (1 m (3 ft) + 4% of reading)	± (1 m (3 ft) + 4% of reading)

❒ The length measurement range of Type 1 STP cable and 50 Ω coaxial cable exceeds 600 meters.

❒ Accuracy specification for Length excludes the error in Nominal Velocity of Propagation (NVP).

❒ The LANMeter instrument allows you to enter the value for NVP or to “calibrate” the NVP of a cable type. Minimum cable length for calibration is 15 m (50 ft).

Propagation Delay

	Twisted Pair Cable	**Coax, 50Ω**	**STP, 150Ω**
Range	0 to 150 ns	0 to 150 ns	0 to 150 ns
Resolution	1 ns	1 ns	1 ns
Accuracy:	± (5 ns + 2% of reading)	± (5 ns + 2% of reading)	± (5 ns + 2% of reading)
Range	150 to 1500 ns	150 to 2500 ns	150 to 1500 ns
Resolution	1 ns	1 ns	1 ns
Accuracy:	± (5 ns + 4% of reading)	± (5 ns + 4% of reading)	± (5 ns + 4% of reading)

The propagation delay range to Type 1 STP cable and 50Ω coaxial cable exceeds 3000 ns.

Propagation Delay Skew

Propagation Delay Skew measurement accuracy is twice the accuracy of the propagation delay function, at the propagation delay that is measured. It is the difference between the propagation delay in the wire pairs and is particularly important for 100BASE-T4 and 100BASEVG standard requirements.

Fiber Test Option

DSP-FOM Optical Power Meter

Calibrated wavelengths:	850 nm, 1300 nm, and 1550 nm
Dynamic range:	+3 to -50 dBm
Measurement accuracy:	±0.25 dB at -10.0 dBm and 25° C
Display resolution:	0.01 dB (0.001 μW)
Detector type:	Germanium
Optical adapter:	ST
Operating temperature:	0° C to +40° C
Storage temperature:	-20° C to +70° C
Dimensions:	4.5 x 2.5 x 1.5 in (11.4 x 6.4 x 3.8 cm)
Weight:	5.0 oz (142g)
Battery type:	9V alkaline
Battery life:	90 hours typical

FOS-850/1300 Optical Source

Transmit wavelengths:	850 nm and 1300 nm
Power output:	-20 dBm
Source type:	LED
Optical Adapter:	ST
Operating temperature:	0° C to +40° C
Storage temperature:	-20° C to +70° C
Dimensions:	4.5 x 2.5 x 1.5 in (11.4 x 6.4 x 3.8 cm)
Weight:	5.0 oz (142g)
Battery type:	9V alkaline
Battery life:	24 hours typical

LS-1310/1550 Laser Source

Output wavelengths:	1310 nm or 1550 nm, switch selectable
Power Output:	-10 dBm, adjustable
Source Type:	Laser (Class l)
Optical adapter:	Single Mode ST
Operating Temperature:	0° C to +40° C
Storage Temperature:	-10° C to +60° C
Dimensions:	6.8 x 3 x 1.5 in (17.4 x 7.6 x 3.8 cm)
Weight:	9.4 oz (266 g)
Battery type:	9V alkaline
Battery life:	16 hours typical

Cable Test Specifications

Cable Types

Unshielded Twisted Pair LAN cables (100Ω UTP category 3, 4, and 5)

Foil-screened Twisted Pair cables (100Ω ScTP 3, 4, and 5)

Shielded Twisted Pair cables (150Ω, IBM Type 6 and 9)

Coaxial cables: RG-8 ThickLAN (10BASE5), RG-58 ThinLAN (10BASE2), RG-58 Foam

Test Standards

TIA Link Committee standards for both Channel and Basic Link, Category 3, 4, and 5

ISO/IEC IS-11801 Class C and D

IEEE 10BASE5, 10BASE2, and 10BASE-T

IEEE Token Ring 4 Mbps or 16 Mbps

IEEE 100BASE-TX

IEEE 100BASE-T4

IEEE 802.12 (100VG-AnyLAN) 4-UTP

Autotest

The Enterprise LANMeter automatically executes a series of measurements and compares the results against the selected Network Specification resulting in PASS/FAIL test results. Typical Autotest test time is < 90 seconds. The applicable tests are described below.

Cable Length

Refer to the specifications of the stand alone Cable Length test.

Characteristic Impedance

Twisted Pair Range:	50Ω to 200Ω
Coax Range:	25Ω to 100Ω
Accuracy:	+/-(5Ω + 5% of reading)

Wire Map

Tested on up to four pairs. PASS/FAIL on pairs called out in selected network specification.

DC Resistance

500Ω to 500kΩ (+/- 10%) RJ-45
10Ω to 200Ω (+/- 10%) BNC

Test Storage

Up to 128 Autotest Summary Results

100 MHz Remote (Optional)

The 100 MHz Remote meets the TIA Level I Accuracy Requirements and supports 100 ohm Twisted Pair Cable **only**.

Functions

Attenuation

Frequency Range:	1 MHz to 100 MHz in 1 MHz step sizes
Accuracy:	Typically better than +/- 1.3 dB at TIA Cat 5 Limits

Near End Crosstalk (NEXT)

100 MHz Remote measures NEXT at the far end. Measured for all cable pair combinations as called out by network specification.

Accuracy: Typically better than +/- 3.8 dB (Basic Link), +/- 3.4 dB (Channel) at TIA Cat 5 Limits

Frequency Range: 1 MHz to 100 MHz

In High Resolution Mode NEXT Test Sampling Step Size:
1-31.25 MHz (≤ 150 KHz),
31.25-100 MHz (≤ 250 KHz)

In Low Resolution Mode NEXT test Sampling Size:
1-100 MHz (≤ 500 KHz)

Residual NEXT Loss

(With Category 5 compliant connector) better than 70 dB at 1 MHz and better than 40 dB at 100 MHz.

Random Noise Floor

Typically better than 75 dB, measured as specified in the TIA Link standard.

Attenuation to Crosstalk Ratio (ACR)

Calculated from NEXT and attenuation measurements.

Physical

Case

Dimensions:	8.5” X 12.5” X 2.5” (21.6 cm X 31.8 cm X 6.4 cm) Nominal
Weight:	9.25 oz (260g) Nominal

Test Connector

RJ-45

LEDs

Three LED indicators are used for communicating AUTOTEST results; green (Pass), red (Fail), and yellow (Test in Progress).

Power

Remote Unit:	Replaceable 9 Volt Alkaline cell.

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 AC Adapter for the instrument has UL, CSA, and CE approvals or other approvals valid in the USA, Canada, and Europe.
Electromagnetic Interference	Tested to EN 50082-1. Exempt for USA and Canadian emissions regulations if it does not interfere with licensed communications.
Connection to public telephone network	The Fluke 68x Series should not be connected to the public telephone network at any time.

Appendix C
Maintenance

General Maintenance

Periodically wipe the Enterprise LANMeter's case with a damp cloth and detergent. Do not use abrasives or solvents. Clean and dry as required. There are no adjustments inside the instrument.

The LANMeter instrument performs a power-up self test designed to verify operational performance of main components including ROM, RAM, clock, display, and processor. It is recommended that the full instrument self-test be performed on a weekly basis and that the instrument be returned to an Authorized Fluke Service Center on an annual basis for full performance verification tests.

Maximizing Battery Life

The life of NiCad or NiMH batteries is strongly influenced by the care that they receive. If properly maintained, the battery pack is capable of more than 500 charge/discharge cycles before dropping to 80% of capacity.

The greatest enemy of your battery pack is heat. Try to avoid charging your batteries when they are hot. Leaving the LANMeter instrument in a hot place, such as a car on a warm day, and then charging the batteries immediately upon return to your office will shorten battery life if done often.

Over-charging your batteries also causes heat. When a NiCad or NiMH battery reaches full charge, it begins to heat up. Charging a fully charged or nearly fully charged battery causes unnecessary heat build up. It's better to allow the batteries to discharge before recharging. It is okay to leave the AC adapter plugged in for long periods of time as long as the AC power is not turned on and off. Once the battery pack is fully charged, the charger switches to a trickle charge mode which can be maintained for a long time. This state is indicated by the rapid blinking of the battery status LED.

Battery Installation

Power for any of the Fluke Enterprise LANMeter (68x Series) instruments is supplied by a rechargeable battery pack. The instrument continuously monitors the battery and displays a low battery indicator in the status line when the battery voltage is low. The Wire Map and Cable Identifier Remote Units do not require battery power.

Use the following procedure to replace the battery pack:

1. Turn off the instrument.
2. Place the instrument face down.
3. Flip up the standup leg.
4. Unscrew the two screws in the battery compartment door using a Phillips screw driver. Remove the battery pack cover as shown in Figure C-1.
5. Unplug and remove the old battery pack.

Ni-Cd
Ni-MH

Note

> *This instrument contains a Nickel-Cadmium or a Nickel-Metal Hydride battery. Do not dispose of this battery with other solid waste. Used batteries should be disposed of by a qualified recycler or hazardous materials handler. Contact your Fluke Service Center for recycling information.*

6. Install and plug-in the new battery pack. Use accessory N6701 (NiCd) or N6702 (NiMH) when ordering from your Fluke Sales Office, or Fluke Part Number 932645 or 655085 when ordering from a Fluke Service Center.
7. Reassemble the battery pack cover and install the two screws.

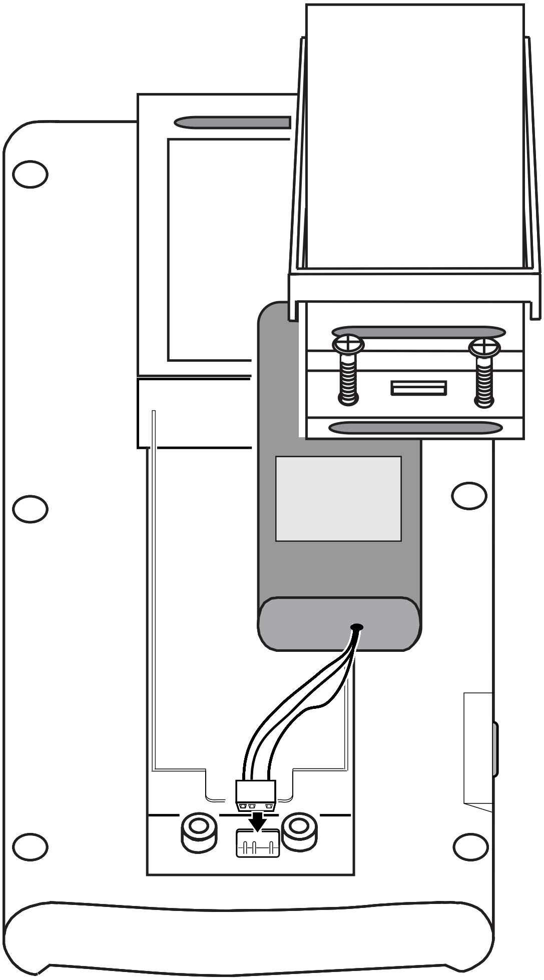


Figure C-1. Battery Replacement Exploded View

Service Center Repair

Repairs and servicing are not covered in this manual and should be performed only at an authorized Fluke Service Center. If it appears that the instrument is failing, perform the following steps before returning the instrument:

1. Check the charge condition of the battery pack. Refer to the rear panel decal for instructions, or to the “Battery Charger Status” section in the *Getting Started* manual, on how to interpret the Battery-Charge Status LED. If necessary, charge the battery pack and verify that the failure persists.
2. Perform the appropriate self-test, depending on the suspected mode of failure. You can run the Auto Test to test the internal workings, the Serial Test to test the serial port, and the Keyboard Test to test the keyboard. Verify that all tests pass, as reported on the display. Refer to the “Self Test” section in the *Getting Started* manual for more information on performing self-tests.
3. Run the Wire Map test (a Cable Test) with the Wire Map Adapter directly attached to the instrument **TO HUB/MAU** RJ-45 connector.

If the problem is not resolved by the preceding steps, **write a description of the failure**, and include it with the LANMeter instrument when shipping. Pack the instrument in the original shipping container. Call the appropriate number listed below for shipping instructions. Fluke assumes NO responsibility for damage in transit.

An Enterprise LANMeter covered by the limited warranty will be promptly repaired or replaced (at Fluke’s option) and returned to you at no charge. If the warranty has lapsed, the instrument will be repaired and returned for a fixed fee. Contact Fluke using the appropriate number listed below for more information and prices.

1-888-99-FLUKE (1-888-993-5853) in U.S.A.

1-800-36-FLUKE (1-800-363-5853) in Canada

+31 402-678-200 in Europe

+1-425-446-5500 in other countries

Japan +81-3-3434-0181

Singapore +65-738-5655

Accessories

The following are Enterprise LANMeter accessory configurations for the Fluke 686, 685, 683, 682, and 680.

Model Number	Description
C6700	Large Soft Carrying Case, Storage for LANMeter and Accessories
N6701	Spare Battery Pack, Ni-Cd
N6702	Spare Battery Pack, Ni-MH
N6703	**UTP Accessory Kit:** 66 Punch Down to RJ45 Adapter 110 Punch Down to RJ45 Adapter RJ45 to RJ45 Female Coupler RJ45 to 8-Clip Lead Adapter RJ45 UTP Cable, 2m (6 ft)
N6704	**Expert-T Accessory Kit:** DB9 Male-to-Male STP Cable, 2m (6 ft) RJ45 UTP Cable, 2m (6 ft) IBM Data Connector-to-DB9 Male Adapter
N6705	**Coaxial Accessory Kit:** BNC T Adapter 50Ω BNC Terminator BNC to Type N Adapter RG-58 Cable, 2m (6 ft) BNC Male-to-Male Coupler BNC Female-to-female Coupler
N6708	**Cable Identifier Kit 1:** One set of Cable Identifier Units number 1 through 6
N6709	**Cable Identifier Kit 2:** One set of Cable Identifier Units number 7 through 12
N6707	IBM Type 1 Data Connector to RJ-45
N6800/T	HealthScan PC Software for Token Ring
N6800/E	HealthScan PC Software for Ethernet
N6800/ET	HealthScan PC Software for Ethernet and Token Ring
68X-002	100 MHz Cable Test Option
68X-SW	SwitchWizard Option
68X-WW	WideAreaWizard Option

Replacement Parts List

Part Number	Description	Comments
943261	680 Main PCB Assembly	680 with Serial Number < 6311800
106994	680 Main PCB Assembly	680 with Serial Number >6311800
943212	682 Main PCB Assembly	682 with Serial Number <6291600
107000	682 Main PCB Assembly	682 with Serial Number > 6291600
662434	683 Main PCB Assembly	Applies to all Serial Numbers
943233	685 Main PCB Assembly	685 with Serial Number < 6281700
107018	685 Main PCB Assembly	685 with Serial Number > 6281700.
662442	686 Main PCB Assembly	Applies to all Serial Numbers
943266	68x PCB Assembly, Power Supply	Applies to all models
946954	68x Assembly, LCD-BL Display	Applies to all models
928333	68x PCB Assembly, Keypad	Applies to all models
928341	68x Elastomeric Keypad	Applies to all models
928465	Wire Map Unit (Cable Identifier #0)	Applies to all models
928408	Cable Identifier #1	Applies to all models
928411	Cable Identifier #2	Applies to all models
928416	Cable Identifier #3	Applies to all models
928424	Cable Identifier #4	Applies to all models
928429	Cable Identifier #5	Applies to all models
928432	Cable Identifier #6	Applies to all models

Part Number	Description	Comments
928437	Cable Identifier #7	Applies to all models
928440	Cable Identifier #8	Applies to all models
928445	Cable Identifier #9	Applies to all models
928452	Cable Identifier #10	Applies to all models
928457	Cable Identifier #11	Applies to all models
928460	Cable Identifier #12	Applies to all models
628567	68x Cable, Battery Harness	Applies to all models
628559	68x Power Supply Cable	Applies to all models
628534	AC Power Adapter 100-240V	Applies to all models
928353	Instrument Soft Case	Applies to all models
689197	68x User Manual	Applies to all models
655115	Utilities Diskette (V8)	
107034	680 Top Shell Assembly	
107042	682 Top Shell Assembly	
107078	685 Top Shell Assembly	
666195	683 Top Shell Assembly	
666198	686 Top Shell Assembly	
666187	68x Bottom Shell Assembly	Applies to all models.
662726	680 Assembly, Battery cover	
662731	682 Assembly, Battery cover	
662749	683 Assembly, Battery cover	
666179	685 Assembly, Battery cover	
666180	686 Assembly, Battery cover	
621547	Bale	Applies to all models
928374	Adapter, 66 Punch to RJ45	
928379	Adapter, 110 Punch to RJ45	
928473	Coupler, Female, RJ45-RJ45	
928478	Adapter, RJ45 to 8-clip lead	

Part Number	Description	Comments
928481	Cable, RJ45 Category 5, UTP, 2m (6 ft)	
928494	Cable, DB9 male to male STP, 2m (6 ft)	
928499	Connector, IBM Data to DB9 male	
623113	LANMeter Battery Pack, Ni-Cd	Applies to all models
938451	68x-002, CTO Battery Cover	
943399	BNC T-adapter	
943279	Cable, RG-58, 2m (6 ft)	
943238	Adapter, BNC to Alligator Clip Lead	
943241	Adapter, BNC to Type N	
943246	Coupler, BNC female-to-female	
943253	Coupler, BNC male-to-male	
943183	Terminator, BNC 50Ω	
110780	Cable, 100 MHz CTO, .3m (1 ft.)	

Appendix D
Utilities

Introduction

The CD ROM supplied with your Enterprise LANMeter contains utility functions for use on an IBM-compatible, personal computer (PC) running Windows 95, NT, or 3.1. This appendix has been updated for Enterprise LANMeter software version 9.50 and greater.

After you install and run the Fluke LANMeter Utilities on your PC, you can select the desired button to run one of the following utilities:

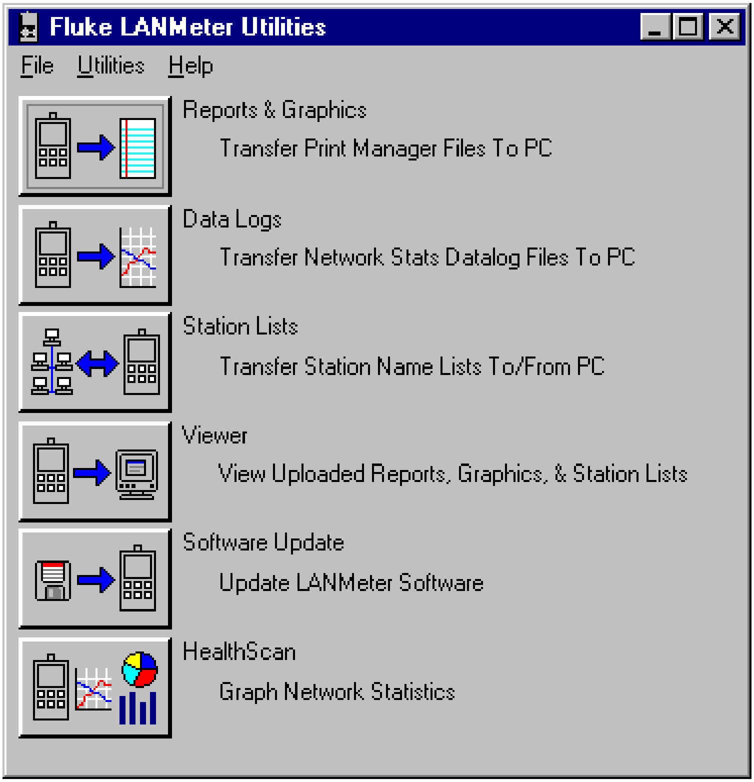
- Reports & Graphics – Transfer Print Manager Files to a PC
- Data Logs – Transfer Network Stats Datalog Files to a PC
- Station Lists – Transfer Station Name Lists to or from a PC
- Viewer – View Uploaded Reports, Graphics, & Station Lists
- Software Update – Update LANMeter Instrument Software
- HealthScan – Graph Network Statistics

Figure D-1 shows the Fluke LANMeter Utilities selection window.

PC System Requirements

The following are the minimum PC system requirements:

Computer:	286, or greater, IBM-compatible PC, with one open COM port
RAM:	4 MB
Hard Disk Space:	2.5 MB
Floppy Disk Drive:	1.44 MB, 3 1/2"
Windows version:	95, NT Workstation or Server Version 3.51 or 3.1 (or a later version of these)



Reports & Graphics

Transfer Print Manager Files To PC

Data Logs

Transfer Network Stats Datalog Files To PC

Station Lists

Transfer Station Name Lists To/From PC

Viewer

View Uploaded Reports, Graphics, & Station Lists

Software Update

Update LANMeter Software

HealthScan

Graph Network Statistics

Figure D-1. Fluke LANMeter Utilities Selection Window

Installing Instrument Utilities

Use the following procedure to install the Fluke LANMeter Utilities:

1. Select your PC's operating system from the following and perform the appropriate steps:

   a. **From Windows 95 or NT Desktop:**

      1. Select the **Start** button on the Taskbar and then select **Run**.
      2. Type **a:\setup** and select **OK**.

   b. **From Windows 3.1 Program Manager:**

      1. Select **File** from the Menu Bar and then select **Run**.
      2. Type **a:\setup** and select **OK**.

2. Select or enter the drive and directory for installing the Fluke LANMeter Utilities. You can select **Install** to accept the default drive and directory, or you can enter changes and then select **Install**. To enter changes, use the **Browse...** button to locate the desired drive and directory.

Your PC displays the Fluke LANMeter Utilities window after the installation has completed.

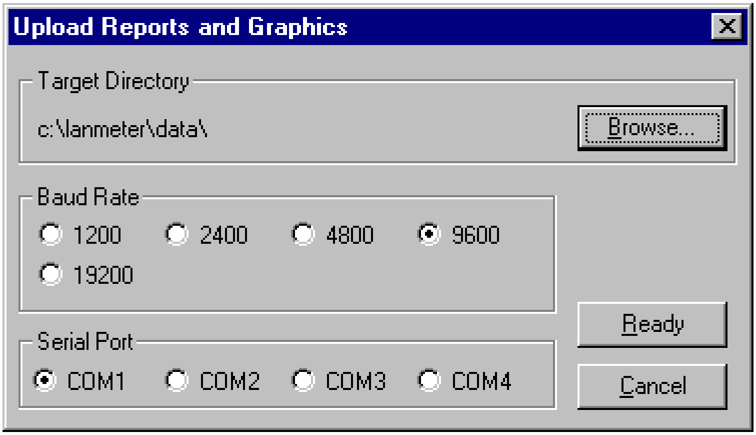
Utilities Setup

The Reports & Graphics, Data Logs, Station Lists, and Software Update utilities require a serial null modem cable between the PC and the instrument. Refer to Figures D-10 and D-11 for wiring and connection information.

All of the utilities, except Viewer and HealthScan, automatically open a setup window like the one shown in Figure D-2 prior to running the utility. You can use this window to configure the required parameters or you can configure default parameters for all of the utilities by selecting **File, Set Up** (in the Fluke LANMeter Utilities window), selecting the desired setup item, and then configuring the required parameters.

The following setup items are available from the **File**, **Set Up** menu:

- Use **Communications...** to set the default baud rate and serial port.
- Use **Target Directory...** to set the default destination for files uploaded from the LANMeter instrument to your PC.
- Use **Software Upgrade Directory...** to set the drive and directory where the LANMeter instrument’s upgrade software is located.
- Use **HealthScan...** to select the directory and executable file to run the optional HealthScan utility.
- Use the **Preferences...** item to select which Warning popups to display.



Upload Reports and Graphics

Target Directory
c:\lanmeter\data\

Baud Rate
○ 1200 ○ 2400 ○ 4800 ● 9600
○ 19200

Serial Port
● COM1 ○ COM2 ○ COM3 ○ COM4

Figure D-2. Upload Reports and Graphics Setup Window

If another application is using the PC’s COM port, the utility program will not be able to communicate with your LANMeter instrument.

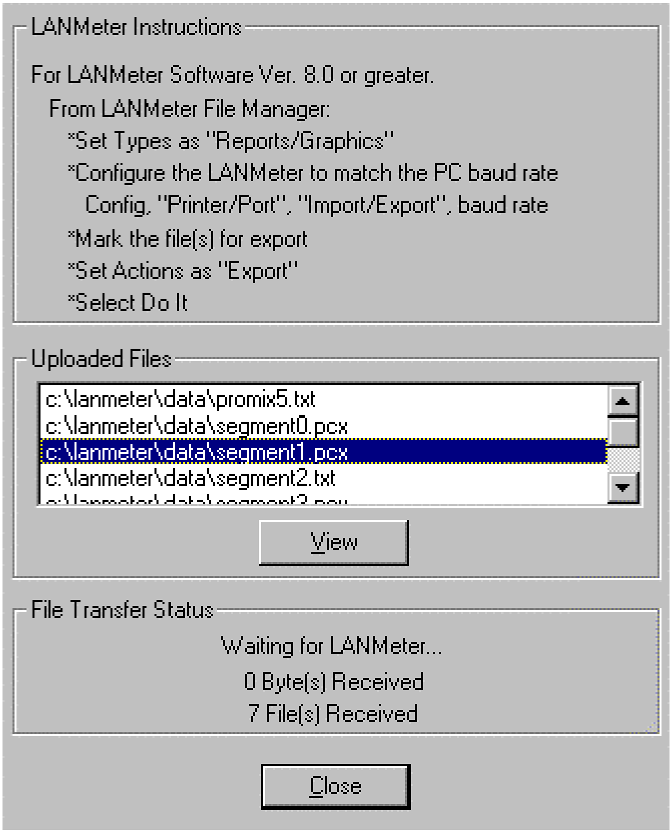
Reports & Graphics

You can use the Reports & Graphics utility to transfer Print Manager files from the LANMeter instrument to your PC. Use the following procedure to upload Print Manager files to your PC:

1. Select the **Reports & Graphics** utility button.
2. Configure the Target Directory and the PC's Baud Rate and Serial Port. The Target Directory is where you want the files to be put on your PC. Refer to Figure D-2.
3. Select the **Ready** button and follow the LANMeter Instructions shown in the Upload Reports and Graphics window to start the file transfer. Refer to Figure D-3.

The status of the upload is shown in the File Transfer Status box. After the transfer has completed, you can view the uploaded file by highlighting it with the left mouse button and then selecting the **View** button.

Reports have a **`.txt`** file extension and can be viewed with a text editor. Graphics have a **`.pcx`** extension and can be viewed with a graphics program. Refer to the description of the Viewer utility, later in this appendix, for additional information.



LANMeter Instructions

For LANMeter Software Ver. 8.0 or greater.
From LANMeter File Manager:
*Set Types as "Reports/Graphics"
*Configure the LANMeter to match the PC baud rate
Config, "Printer/Port", "Import/Export", baud rate
*Mark the file(s) for export
*Set Actions as "Export"
*Select Do It

Uploaded Files

c:\lanmeter\data\promix5.txt
c:\lanmeter\data\segment0.pcx
c:\lanmeter\data\segment1.pcx
c:\lanmeter\data\segment2.txt

File Transfer Status

Waiting for LANMeter...
0 Byte(s) Received
7 File(s) Received

Figure D-3. Upload Reports and Graphics Window

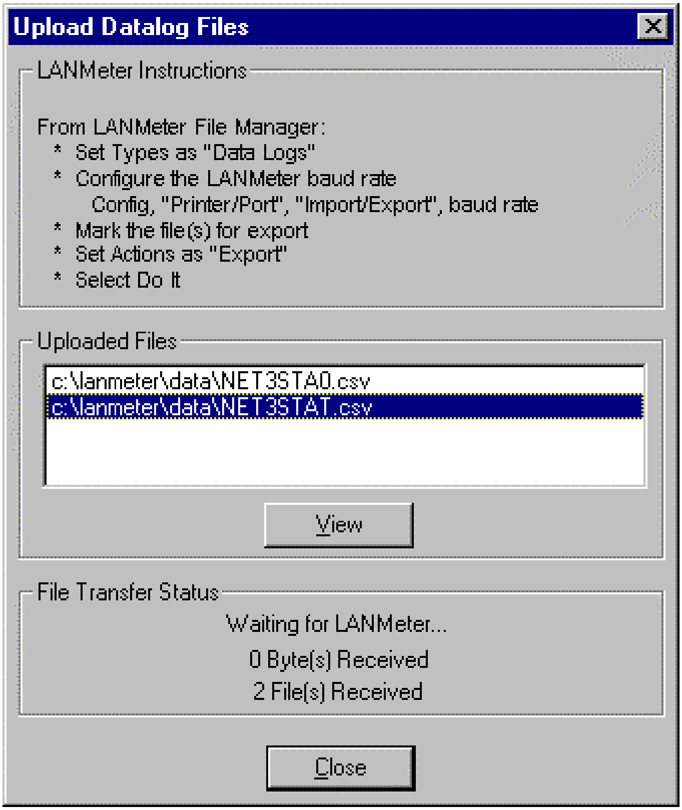
Data Logs

You can use the Data Logs utility to transfer Network Statistics Datalog files from the LANMeter instrument to your PC (upload). Use the following procedure to upload Network Statistics Datalog files to your PC:

1. Select the **Data Logs** utility button.
2. Configure the Target Directory and the PC's Baud Rate and Serial Port. The Target Directory is where you want the files to be put on your PC. Refer to Figure D-2.
3. Select the **Ready** button and follow the LANMeter Instructions shown in the Upload Datalog Files window to start the file upload from the LANMeter instrument to your PC. Refer to Figure D-4.

The status of the upload is shown in the File Transfer Status box. After the transfer has completed, you can view the uploaded file by highlighting it with the left mouse button and then selecting the **View** button.

Datalog files are in comma separated variable (CSV) format and can be viewed by a spreadsheet program or HealthScan. (For more information on HealthScan, refer to the "HealthScan" section later in this appendix.) If you have a problem viewing a Datalog file, refer to the Note in the Viewer utility section.


Upload Datalog Files

LANMeter Instructions

From LANMeter File Manager:
- * Set Types as "Data Logs"
- * Configure the LANMeter baud rate
  Config, "Printer/Port", "Import/Export", baud rate
- * Mark the file(s) for export
- * Set Actions as "Export"
- * Select Do It

Uploaded Files

c:\lanmeter\data\NET3STA0.csv
c:\lanmeter\data\NET3STAT.csv

File Transfer Status

Waiting for LANMeter...

0 Byte(s) Received

2 File(s) Received

Figure D-4. Upload Datalog Files Window

Station Lists

You can use the Station Lists utility to transfer Station Name Lists to or from your PC. You will be able to create and maintain station list files on your PC. This allows you to view names on LANMeter instrument displays, which makes troubleshooting easier.

You can preserve station lists during a LANMeter instrument software update, for example, by uploading them to your PC prior to performing the software update. To do this, simply follow the procedure for uploading a LANMeter Station List file in the following “Upload: LANMeter --> PC” section.

You can modify or generate station lists on your PC using one of two methods. First, you can upload an existing LANMeter Station List file to your PC, modify it, and then download it back to the LANMeter instrument. The second method is to generate the station list file from scratch or obtain a station list file from another source and then download it to the LANMeter instrument. For these methods, you can use one or both of the procedures in the following “Upload: LANMeter --> PC” and “Download: PC --> LANMeter” sections.

You can refer to one of the following sections for specific information on how to use the Station List Utility:

❒ Collecting NetWare User Names and Addresses
❒ Collecting IP Host Names and Addresses

Collecting NetWare User Names and Addresses

You can create a NetWare User List file to use for updating the LANMeter instrument’s IPX and/or MAC station lists. To do this, you first create the NetWare User List file on your PC and then you download it from your PC to the LANMeter instrument.

You create a NetWare User List file by running a NetWare utility on your NetWare server. The NetWare utilities are provided with your NetWare operating system and are not part of the Fluke LANMeter Utilities.

The output file from the NetWare utility contains station MAC or IPX addresses with logon user names that are used to update the LANMeter instrument’s IPX and/or MAC station lists using the user logon names.

The NetWare utility that you will use for NetWare 2.x and 3.x servers is **USERLIST** and for NetWare 4.x servers is **NLIST**. The following are examples of how to use each NetWare utility:

```
F:>NLIST USER /A > USERLIST.TXT
or
F:>USERLIST /A > USERLIST.TXT
```

After you have created the NetWare User List file, you then download it from your PC to the LANMeter instrument using the Station Lists utility, as described later in the "Download: PC **-->** LANMeter" section.

Collecting IP Host Names and Addresses

The Fluke LANMeter Utilities can read IP Host files in standard format (see below). So you can create a new IP Host file from scratch or use an existing IP Host file, edit the file (using the following example as a guide), and then download the file to the LANMeter instrument.

```
#
#Comments begin with a "#".
#The first column is the dotted decimal address, followed by
#  the name.
#Additional columns after the name (aliases or comments) are
#  ignored.
#Columns are separated by a tab or a space.
#
#IP Address      Name
#
199.5.202.1      router3
199.5.202.2      dilbert
199.5.202.3      server1
199.5.202.5      Mary
199.5.202.20     Jim
```

Download: PC --> LANMeter

Caution

The LANMeter instrument's current station list (CSL) will be lost when a new Station List is downloaded from the PC. Refer to the Station List section in this Users Manual or to the LANMeter Help System for information on how to save the CSL prior to downloading a New Station List.

1. Select the **Station Lists** utility button.
2. Select the **PC --> LANMeter** button, as shown in Figure D-5, to download Station Name Lists to your LANMeter instrument.
3. Read the Caution popup and select **OK** to proceed or **Cancel** to abort.
4. Use the **Browse...** button in the Station List: PC --> LANMeter window to select the LANMeter Station List and the Station List File Name to update, with the appropriate source file type configured as one of the following. Also refer to Figure D-6.

   ❒ IP station list using an IP Host File. It uses a standard IP Host file.

   ❒ IPX and MAC station lists using a NetWare User List File.

   ❒ MAC station list using a NetWare User List File. This selection will not update the IPX station list. It will only update the MAC list.

   ❒ ALL station lists can be updated with a LANMeter Station List File. The fastest way to create your own file is to upload a station list from the LANMeter instrument and modify its contents. You can enhance this station list file by first using your LANMeter instrument to merge addresses discovered on the network prior to uploading the file. The different address types are MAC, IP, IPX, and VIP (VINES).

Note

For the LANMeter instrument to download a station list, its filename on your PC must be **`stnlst.imp`**. *LANMeter Utilities converts your selected file to* **`stnlst.imp`** *prior to downloading the file.*

1. Set the Baud Rate and Serial Port for the PC from the Station List: PC **-->** LANMeter window. Refer to Figure D-2.
2. Select the **Ready** button and follow the LANMeter Instructions shown in the Station List: PC **-->** LANMeter window to start the file transfer.

   The **Ready** button is not activated until a valid filename and matching file type are selected earlier in this procedure.

The status of the download is shown in the File Transfer Status box. The downloaded station lists will be named **`import_X`**, where **`X`** is an integer 0 to 7, in the LANMeter instrument. For information on how to rename the downloaded station list files, refer to the "File Manager Actions" section of Chapter 12 "File Manager."

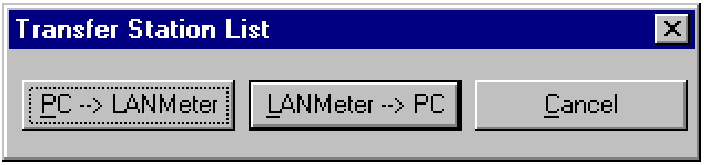
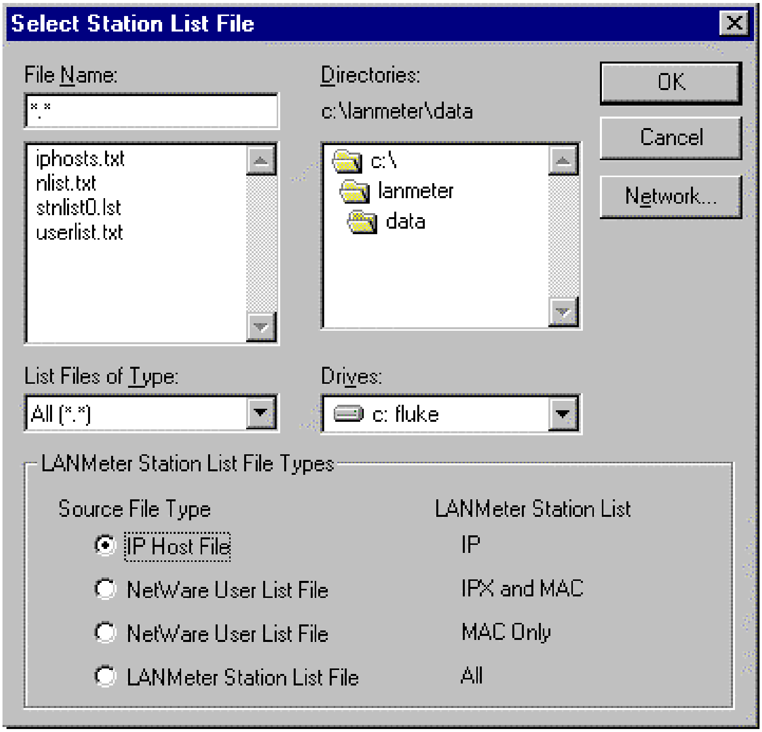


Figure D-5. Transfer Station List



Select Station List File

File Name: *.*

iphosts.txt
nlist.txt
stnlist0.lst
userlist.txt

Directories: c:\lanmeter\data

c:\
lanmeter
data

List Files of Type: All (*.*)

Drives: c: fluke

LANMeter Station List File Types

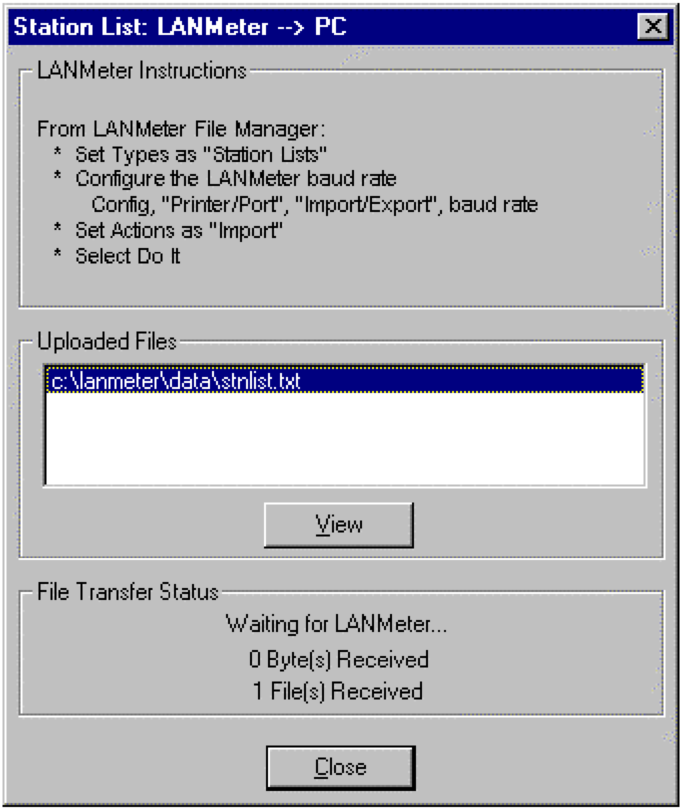
Source File Type	LANMeter Station List
● IP Host File	IP
○ NetWare User List File	IPX and MAC
○ NetWare User List File	MAC Only
○ LANMeter Station List File	All

Figure D-6. Select Station List File Window Upload: LANMeter --> PC

Upload: LANMeter --> PC

1. Select the **Station Lists** utility button.
2. Select the **LANMeter --> PC** button, as shown in Figure D-5, to upload Station Name Lists to your PC.
3. Use the **Browse...** button in the Station List: LANMeter **-->** PC window to select the Target Directory. The Target Directory is where you want the files to be put on your PC.
4. Set the Baud Rate and Serial Port from the Station List: LANMeter **-->** PC window. Refer to Figure D-2.
5. Select the **Ready** button and follow the LANMeter Instructions shown in the Station List: LANMeter **-->** PC window to start the file transfer. Refer to Figure D-7.

The status of the upload is shown in the File Transfer Status box. After the transfer has completed, you can view the uploaded file by highlighting it with the left mouse button and then selecting the **View** button. The uploaded station list will be named **`stnlistX.txt`**, where **X** is an integer.



From LANMeter File Manager:
- * Set Types as "Station Lists"
- * Configure the LANMeter baud rate
  Config, "Printer/Port", "Import/Export", baud rate
- * Set Actions as "Import"
- * Select Do It

c:\lanmeter\data\stnlist.txt

Waiting for LANMeter...

0 Byte(s) Received

1 File(s) Received

Figure D-7. Station List: LANMeter --> PC (Upload) Window

Viewer

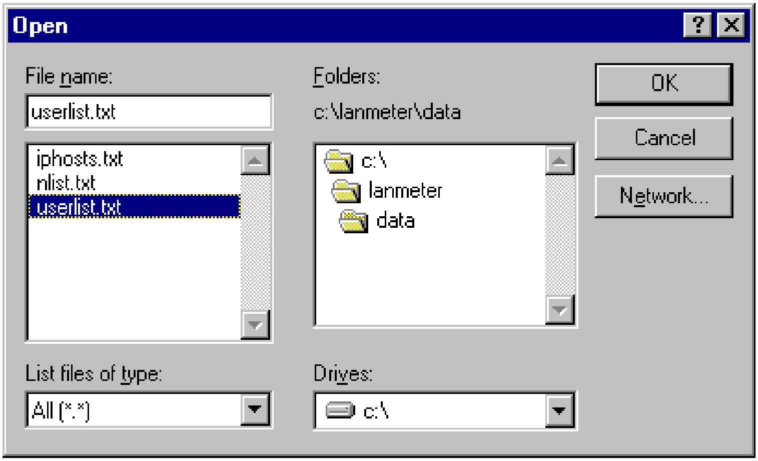
You can use the Viewer utility to view uploaded LANMeter instrument reports, graphics, and station lists on your PC. The Viewer utility opens and displays the selected file using the Windows program that is associated with the file type.

Note

> *If your operating system does not have a registered file type for the* **`.csv`**, **`.txt`**, *and* **`.pcx`** *extensions, you can try one of the following steps to view the file. If you still have problems viewing the file, refer to your Windows 95, NT, or 3.1 documentation.*
>
> *For Windows 95 or NT: Select a spreadsheet program (e.g. Microsoft Excel) to view a* **`.csv`** *file, a text editor (e.g. Microsoft Notepad) to view a* **`.txt`** *file, or a graphics program (e.g. Microsoft Paint) to view a* **`.pcx`** *file when prompted to select a program.*
>
> *For Windows 3.1: Select* **File** *and then* **Associate...**, *from File Manager, and then select a spreadsheet program (e.g. Microsoft Excel Worksheet) to view a* **`.csv`** *file, a text editor (e.g. Microsoft Notepad) to view a* **`.txt`** *file, or a graphics program (e.g. Microsoft Paintbrush) to view a* **`.pcx`** *file when prompted to select a program.*

Use the following procedure to use Viewer:

1. Select the **Viewer** utility button.
2. Highlight the file to be viewed with the left mouse button and select **OK**. Refer to Figure D-8.



File name: userlist.txt

iphosts.txt
nlist.txt
userlist.txt

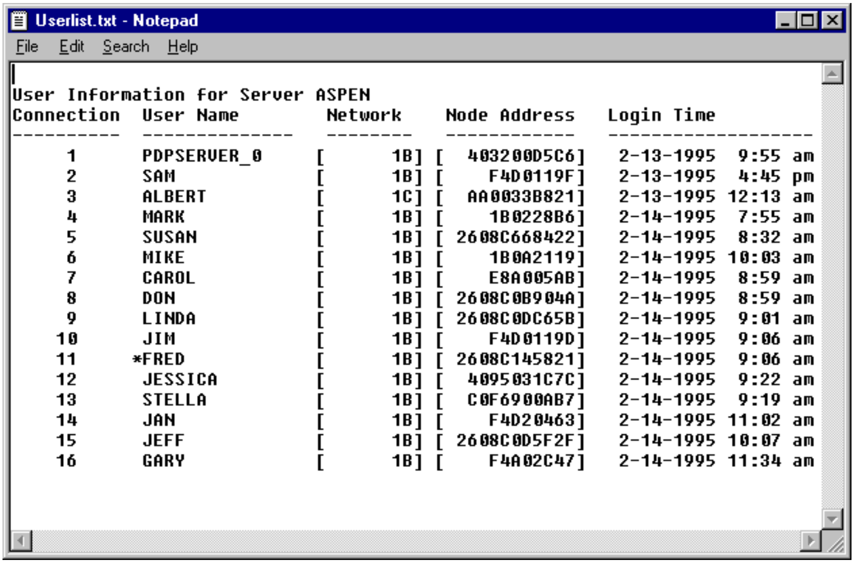
Folders: c:\lanmeter\data

c:\
lanmeter
data

List files of type: All (*.*)

Drives: c:\

Figure D-8. Open Viewer File



```
User Information for Server ASPEN
Connection  User Name        Network    Node Address   Login Time
----------  --------------   --------   ------------   -------------------
     1      PDPSERVER_0     [      1B] [  403200D5C6]   2-13-1995  9:55 am
     2      SAM             [      1B] [    F4D0119F]   2-13-1995  4:45 pm
     3      ALBERT          [      1C] [  AA0033B821]   2-13-1995 12:13 am
     4      MARK            [      1B] [    1B0228B6]   2-14-1995  7:55 am
     5      SUSAN           [      1B] [ 2608C668422]   2-14-1995  8:32 am
     6      MIKE            [      1B] [    1B0A2119]   2-14-1995 10:03 am
     7      CAROL           [      1B] [    E8A005AB]   2-14-1995  8:59 am
     8      DON             [      1B] [ 2608C0B904A]   2-14-1995  8:59 am
     9      LINDA           [      1B] [ 2608C0DC65B]   2-14-1995  9:01 am
    10      JIM             [      1B] [    F4D0119D]   2-14-1995  9:06 am
    11     *FRED            [      1B] [ 2608C145821]   2-14-1995  9:06 am
    12      JESSICA         [      1B] [  4095031C7C]   2-14-1995  9:22 am
    13      STELLA          [      1B] [  C0F6900AB7]   2-14-1995  9:19 am
    14      JAN             [      1B] [    F4D20463]   2-14-1995 11:02 am
    15      JEFF            [      1B] [ 2608C0D5F2F]   2-14-1995 10:07 am
    16      GARY            [      1B] [    F4A02C47]   2-14-1995 11:34 am
```

Figure D-9. Example Text Viewer File

Software Update

As new software becomes available, the LANMeter instrument can be updated by using an IBM-compatible, personal computer (PC) and a Fluke supplied software update disk.

Use the following procedures to update the LANMeter instrument software:

❒ Installing the Upgrade Software onto Your PC
❒ Loading Software into the LANMeter Instrument

Caution

All stored files in your LANMeter instrument will be lost during the software upgrade process. Upload any important files to your PC prior to starting the Software Update procedure.

Installing the Upgrade Software onto Your PC

Use the following procedure to load the new LANMeter instrument software onto your PC:

1. Locate the floppy disk containing the new LANMeter instrument software and insert it into your PC’s floppy drive.
2. Use the following procedure from DOS or a DOS Window to display the **`readme.txt`** file. This file contains any additional information that was not available when this manual was published.
   a. Type **a:** (or the drive letter of your floppy disk, if different) and press **Enter**.
   b. Type **readme** and press **Enter** to display the **`readme.txt`** file.
   c. Use the spacebar or arrow keys to page through the file.
3. Use the following procedure from DOS or a DOS Window to start the installation of LANMeter update software onto your PC:
   a. Type **a:** (or the drive letter of your floppy disk, if different) and press **Enter**.
   b. Type **Install** and press **Enter**.
   c. Enter **Y** to accept the default installation directory or enter **N** to change the directory. After the directory is selected the software upgrade files are transferred to your PC.

Loading Software into the LANMeter Instrument

Use the following procedure to load the new Enterprise LANMeter software into your LANMeter instrument:

Caution

Once the LANMeter instrument has erased its main ROM, it displays "DO NOT TURN OFF LANMeter." If communications become disrupted, do not turn off the LANMeter instrument. It will recover when communications resume.

It is highly recommended that you use the LANMeter instrument's AC Adapter during software updates.

1. Attach the AC Adapter to a power outlet and to the LANMeter instrument.
2. Attach a serial null modem cable between the PC's serial port and the LANMeter instrument, as shown in Figure D-10. Figure D-11 shows an example of how to wire a 9 or 25-pin D connector, if required.
3. Run the Fluke LANMeter Utilities application on your PC.
4. Turn on your LANMeter instrument.
5. Select the **Software Update** utility button from the Fluke LANMeter Utilities. Read the Caution popup and select **OK** to proceed or **Cancel** to abort.
6. Select the directory for the Software Update File(s) Location from the LANMeter Software Update window, by using the **Browse...** button. Refer to Figure D-12. By default, your LANMeter software update files are loaded into the **`c:\lanmeter\swupdate`** directory. Refer to Figure D-14.
7. Select the PC's Baud Rate and Serial Port from the LANMeter Software Update window (Figure D-12).
8. Select the **Ready** button and follow the LANMeter Instructions shown in the LANMeter Software Update window to set up the LANMeter instrument for the software update. Refer to Figure D-14.

   The **Ready** button is not activated until a directory that has valid software update files is selected earlier in this procedure.
9. Follow the instructions on the LANMeter instrument's display to begin the update process.

The progress of loading the software is shown in the File Transfer Status box.

If you have any problems:

❒ Check the cabling. Make sure the cable is connected to the correct serial port and is correctly wired.

❒ Verify that the baud rates match for the PC and LANMeter instrument.

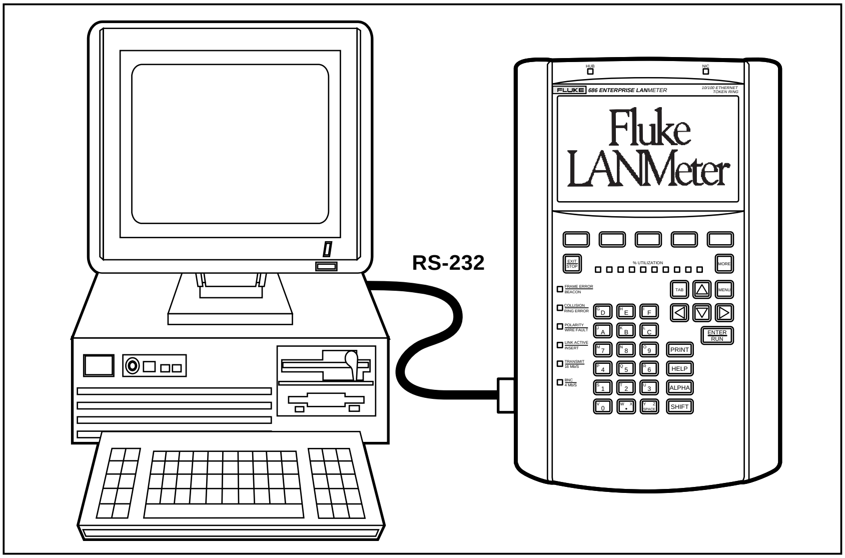


Figure D-10. Software Update and File Transfer Connection

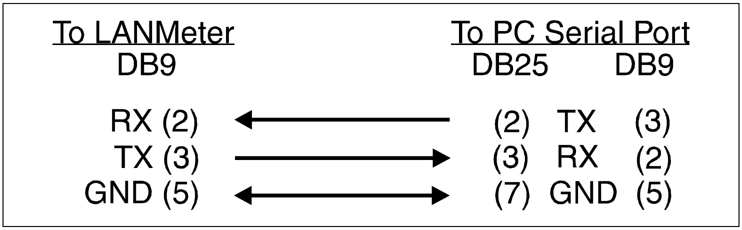
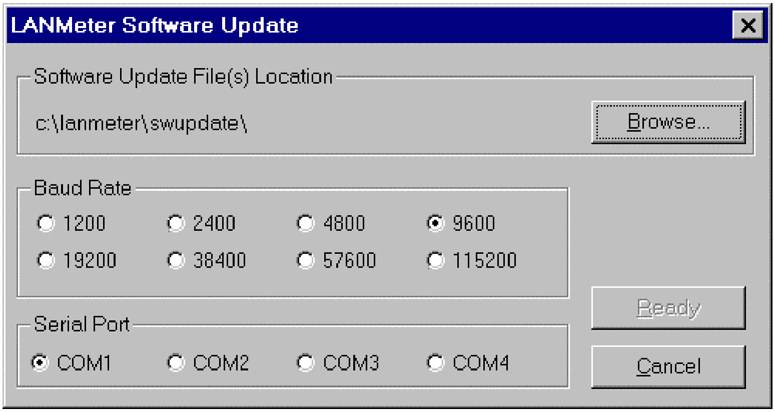


Figure D-11. Software Update and File Transfer Cable


LANMeter Software Update

Software Update File(s) Location

c:\lanmeter\swupdate\

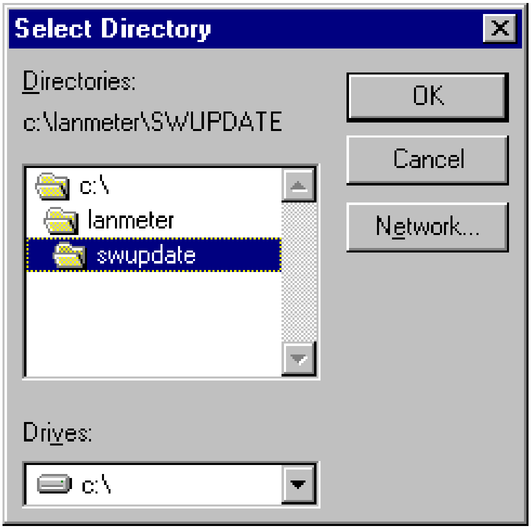
Baud Rate

○ 1200 ○ 2400 ○ 4800 ● 9600
○ 19200 ○ 38400 ○ 57600 ○ 115200

Serial Port

● COM1 ○ COM2 ○ COM3 ○ COM4

Figure D-12. LANMeter Software Update Setup Window

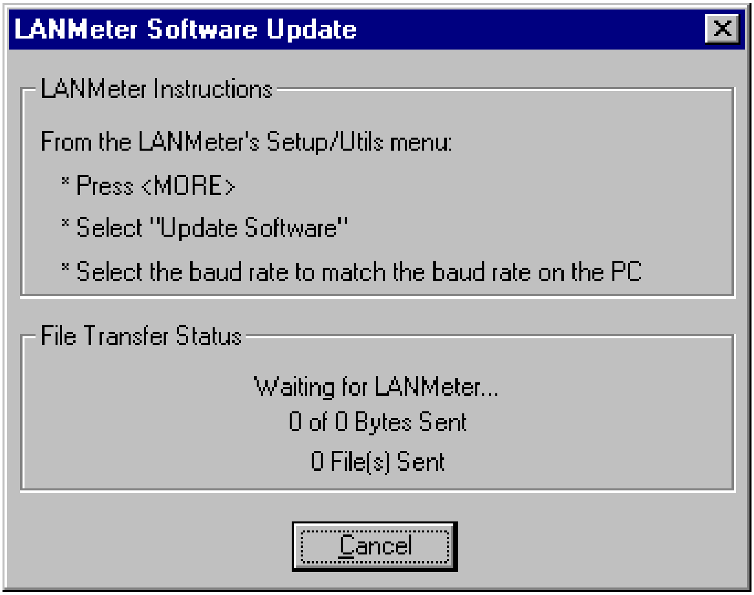


Select Directory

Directories:

c:\lanmeter\SWUPDATE

Figure D-13. LANMeter Software Update Select Directory



From the LANMeter's Setup/Utils menu:

* Press <MORE>

* Select "Update Software"

* Select the baud rate to match the baud rate on the PC

Waiting for LANMeter...
0 of 0 Bytes Sent
0 File(s) Sent

Figure D-14. LANMeter Software Update Window

HealthScan

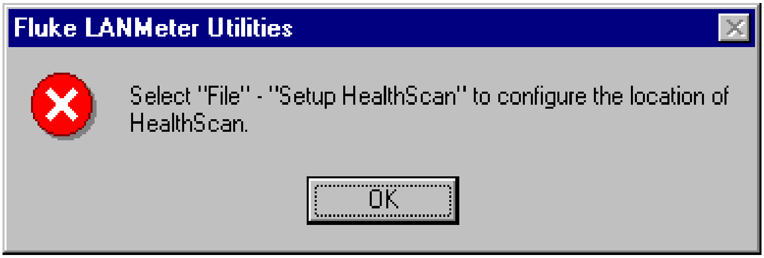
You can use the optional HealthScan utility to generate reports from LANMeter instrument measurement data. These reports can be used to proactively characterize the baseline performance of your network and to identify network fault domains. In North America, you can call 1-800-44-FLUKE to order the HealthScan utility.

If you have purchased the optional HealthScan utility, use the following procedure to start the utility:

1. Configure the directory and the executable file for the HealthScan software (if you have not already done so) by selecting **File**, **Set Up**, **HealthScan...** and then selecting the appropriate directory and file (**hscan.exe**).

   If you did not successfully complete the above step #1, the message shown in Figure D-15 is displayed. Try the above procedure again to resolve this situation.

2. Select the **HealthScan** utility button and then select **Help** or refer to the *HealthScan Users Manual* for information on using HealthScan..



Select "File" - "Setup HealthScan" to configure the location of HealthScan.

Figure D-15. Configure HealthScan Location Message

Appendix E
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-T4

Fast Ethernet; 100 Megabit version of Ethernet that can operate on category 3 cable using all 4 pairs.

100BASE-TX

Fast Ethernet; 100 Megabit version of Ethernet that operates on two pair of a 4 pair category 5 cable.

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.

802.5

See Token Ring Protocol.

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 Collision Sense Multiple Access/Collision Detection (Ethernet) and token passing (Token Ring and ARCNET).

Active Monitor

A single station on the ring that initiates the transmission of tokens and provides token error recovery actions. Any station can become the active monitor when the current active monitor fails.

Anomaly

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

AppleTalk

The set of protocols that define Apple Computer’s networking specification.

ARCNET

Attached Resource Computer NETwork. A token bus local area network standard developed by Datapoint Corporation. ARCNET runs on RG-62 coax, twisted pair, or fiber optic cable with a basic signaling rate of 2.5 Mbps.

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.

ARP Cache

The ARP cache is where each IP host maintains the most recent IP to MAC address mapping. The ARP cache is maintained so that the IP can quickly send IP packets with the correct Ethernet, Token Ring, or FDDI MAC address.

ASCIl (American Standard Code for Information Interchange)

A standard for character-to-number encoding that is widely used in the computer industry. An ASCII file is generally referred to as a text file.

Attenuation

The loss of signal strength over the length of the cable. It is caused by a loss of electrical energy due to the resistance of a cable and by leakage of energy through a cable's insulating material. Attenuation losses due to cable resistance increases as the transmission frequency increases and losses due to insulation leakage increases as temperature increases.

Autonomous System

A group of routers exchanging routing information via a common routing protocol.

Backward Error Congestion Notification (BECN)

Notification by the network that an end user is sending frame relay data onto the network that is either causing or encountering congestion within the WAN network.

Bandwidth

Bandwidth is the rate at which of 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.

Basic Rate Interface (BRI) ISDN

ISDN service consisting of two 64 Kbps B channels for data transmission and one 16 Kbps D channel for signaling information. Some providers may provide alternate configurations of BRI ISDN.

Beacon

A MAC error frame transmitted by the NIC that detects a problem with the token claiming process. A beacon frame on the network indicates a serious problem, such as a broken cable. A ring starts beaconing after normal error recovery methods, such as ring purge and the token claiming process, have failed.

Beaconing

The condition of a ring that has one or all NICs transmitting beacon frames.

BNC

A coaxial cable connector used with ThinLAN (10BASE2) Ethernet networks.

Border Gateway Protocol 4 (BGP-4)

Border Gateway Protocol 4 (RFC 1771) is used to connect different Autonomous Systems. While most routing protocols (such as OSPF, IGRP and RIP) use broadcast or multicasts (which are used by Enterprise LANMeter), BGP uses TCP which requires that you be in the two routers’ connection path to discover the use of BGP.

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

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; for Token Ring networks, the broadcast addresses are FFFFFFFFFFFF and C000FFFFFFFF.

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.

Browser

A program that provides a graphical interface to the World Wide Web.

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

Coaxial

A type of cable in which the inner conductor is surrounded by a tubular conductor, which acts as a shield. Coaxial cables typically have a wide bandwidth.

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.

Collision Frames = 1 RFC-1398

“Single Collision Frames”, a count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Collision Frames > 1 RFC-1398

“Multiple Collision Frames”, a count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Committed Burst Rate (Bc)

A contractually agreed upon, guaranteed, bandwidth rate above the Committed Information Rate that a carrier agrees to provide a frame relay PVC (under normal network conditions).

Committed Excess Burst Rate (Be)

A contractually agreed upon, guaranteed, bandwidth rate above the Committed Burst rate that a carrier agrees to try and sustain for a frame relay PVC. Excess burst rate traffic is automatically flagged as discard eligible.

Committed Information Rate (CIR)

For frame relay service, a contractually agreed upon minimum bandwidth that is available to an end user's permanent virtual circuit (PVC) at all times.

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.

DLCI (Data Link Connection Identifier)

The local frame relay permanent, virtual circuit address assigned by a frame relay provider to designate the channel between the user and the network.

DB

Abbreviation for decibel. A logarithmic unit of measure expressing the amplitude ratio between two signals.

DB-9 Connector

A modular connector used for STP wiring. The DB-9 connector has four conductors to accommodate two pairs of wires and has become the dominant connector used in Token Ring STP installations.

DECnet

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

Designated Bridge

For IEEE 802.1d or DEC spanning tree, only the designated bridge (one per LAN segment or collision domain) can forward frames and transmit spanning tree Bridge Protocol Data Units (BPDU). The designated bridge is the bridge on a given segment that has the lowest cost to the root bridge.

Destination Address

The address of the station receiving a frame.

Discard Eligible (DE) bit

Frame relay users can designate the discard eligibility of frames by configuring their routers or switches to set flags within the frame relay data frames. When the network becomes congested, the frames with the discard eligible bit set will be the first to be discarded.

DNS (Domain Name Server)

A general purpose distributed data query (or look up) service based on host names that are in the form of domain names. A domain is a unique name given to a logical collection of computers connected to one or more networks. Domain names typically end in a suffix denoting the type of site (such as, **`fluke.com`**). The **`.com`** stands for a commercial company.

Downstream

Downstream is in the direction of data flow on a Token Ring network.

E1

Digital line service that provides a transmission rate of 2.048 Mbps. Most common outside North America.

EIA568

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

EIGRP

Cisco Systems Enhanced version of their IGRP routing protocol. While still a distance-vector routing protocol, EIGRP offers fast reaction to network changes.

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.

Excess Collisions

RFC-1398 "ExcessiveCollisions," a count of frames for which transmission on a particular interface fails due to excessive collisions."

Fast Ethernet

See 100BASE-TX and 100BASE-T4.

Fault Domain

The fault domain defines the boundaries of a problem on a Token Ring network. The fault domain limits the problem to two stations, their connecting cables, and any equipment, such as a MAU, between the two stations. The two fault domain stations are the station reporting the error and its Nearest Active Upstream Neighbor (NAUN).

FCS (Frame Check Sequence)

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

FDDI (Fiber Distributed Data Interface)

A 100 Mbps fiber optics LAN standard that uses fiber-optic cable on dual-attached, counter-rotating token rings.

Fiber-Optic Cable

Communications cable that use light as the signal carrier. Fiber-optic cable is immune to electrical and magnetic interference.

Fiber-Optics

A technology that transmits light beams along optical fibers. The light beams are used as a digital information carrier. The optical fibers are formed into fiber optic cables and are a direct replacement for conventional cables and wire pairs. Fiber optic cables are immune to electrical interference and occupy much less physical space than conventional cables and wire pairs.

Forward Error Congestion Notification (FECN)

Notification by the network to an end user that frame relay data being received is either causing or encountering congestion within the WAN network.

Frame

A frame is the transmission unit on a network. In Token Ring, a frame is the token joined with node data.

Frame Errors

For FDDI, Frame Errors (RFC 1512) is the number of frames that were detected to be “in error” by this MAC and were not detected to be “in error” by another MAC.

Frame Relay

A fast form of packet switching that is accomplished with smaller packet sizes and less error checking.

Ghosts

Energy on the cable that appears to be frame, but it does not have a valid beginning of frame pattern (start delimiter: 10101011). This "frame" must be at least 72 or more bytes long, otherwise it is classified as a remote collision. Because of the nature of ghosts, it is important to note that test results are largely dependent upon the position of the LANMeter instrument in the network.

Hard Error

A serious problem on the network that requires a resolution prior to resuming reliable operation.

Hermaphroditic Connector

A loopback, or self-shorting, connector typically used with Type 1 (STP) cable.

Home Page

An introductory page of a World Wide Web site or a Web server that provides hyperlinks to other Web pages.

Hops

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

Host

A computer that is configured to allows users to communicate with other host computers on a network. Individual users can communicate with other individuals by using application programs, such as electronic mail, browser, and FTP.

HTTP (Hypertext Transfer Protocol)

The protocol used to communicate between Web clients and servers.

Hub

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.

Hyperlink

Highlighted words on a Web page that provide a jump to a different document (or page) on the World Wide Web when it is selected. The jump can be to an additional page at the current Web site or to a completely different Web site.

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.

Integrated Service Digital Network (ISDN)

The combination of voice and digital network services in a single medium. This provides voice connections and digital data services over the same phone line.

Interior Gateway Routing Protocol (IGRP)

Interior Gateway Routing Protocol is a Cisco Systems proprietary distance-vector protocol (such as RIP) that takes into account the potential bandwidth of links in its routing table determination. This makes a 10 Mb LAN have a lower cost assessment than a 9600 serial line.

Internet

The Internet is a loose collection of more than 2,000 business, education, and government networks interlinked using the TCP/IP protocol suite. These networks are located primarily in the United States, but also in other parts of the world.

Internet Protocol (IP)

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

Internetwork Packet Exchange (IPX)

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

Jabber

A frame greater than the maximum legal size (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.

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. The LANMeter instrument will generally only see late collisions on a coaxial segment. 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 (about 57.6 microseconds).

Layer

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

Link Error Rate (LER)

For FDDI, Link Error Rate (RFC 1512) is an estimate of the error rate for each physical port (PHY). Most devices will shutdown the port if the error rate is any greater than 10E-7. Error rates of 10E-12 are good, error free links.

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.

Lobe Cable

Lobe cable is the length of cable connecting the MAU to the NIC. The lobe cable can be several cable segments connected together.

Loopback Connector

A connector used at the far end of a cable for returning test signals.

Lost Frames

For FDDI, Lost Frames (RFC 1512) is the number of instances that this MAC detected a format error during frame reception which resulted in the frame being stripped off of the ring.

MAC (Media Access Control)

The MAC protocol defines the access method (i.e., token passing or CSMA/CD) for a particular network topology.

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.

MAU (Multi-station Access Unit)

A wiring concentrator for lobes on a Token Ring network that provides connectors for attaching devices to the ring. A MAU consists of a bank of electromechanical relays used to physically connect or remove stations from a ring.

Mbps

Millions of bits per second. See BPS.

MIB (Management Information Base)

The set of objects that can be used by an SNMP management station to query for information or to set parameter in the SNMP agent, such as a router. Also see RMON MIB.

MIME (Multipurpose Internet Mail Extensions)

An Internet formatting standard used for encoding files that will be attached to email messages. Also see UU Encoding.

Misaligned

RFC-1398 “AlignmentErrors”, a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.

Multicast

Packets that are directed to a group of nodes rather than to a single node or all nodes. This is contrasted to a broadcast packet, which is directed to all nodes.

NAUN (Nearest Active Upstream Neighbor)

The active station that is directly upstream from a given station.

Neighbor Notification Protocol

The Token Ring protocol that notifies every station of changes in NAUN.

NEXT

NEXT (Near-End Crosstalk) is a measure of the crosstalk coupled from one wire pair to another pair.

NIC (Network Interface Card)

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

NOS (Network Operating System)

A network operating system is the software that runs on a group a computers (clients and servers) that mediates the access to the files and resources. Examples of NOSs include Novell NetWare, and Banyan VINES.

Not Copied

For FDDI, Not Copied (RFC 1512) is a count that should as closely as possible match the number of frames that were addressed to this MAC but were not copied into its receive buffers. This might occur due to local buffer congestion.

NVP (Nominal Velocity of Propagation)

The speed of a signal through a cable expressed as a percentage of the speed of light. Typically, the speed of a signal through a cable is 60-80% of the speed of light.

Open

A break in the continuity of a circuit which prevents signal transmission.

Open Shortest-Path First (OSPF)

Open Shortest-Path First (RFC 1583) is a link-state routing protocol. It is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a list of least cost paths.

OSI (Open Systems Interconnection)

OSI is the international standard for data communication between computer systems. The OSI model provides the foundation for products from different vendors to function in the same network. The following is a list of the seven layers of the OSI model:

Layer 1: The **Physical Layer** handles the electrical and mechanical connections of network components to insure bit transmission between stations.

Layer 2: The **Data Link Layer** handles the way frames are transmitted and provides frame error controls for reliable communication between stations.

Layer 3: The **Network Layer** determines the path for communication between stations and handles routing and congestion issues on the network.

Layer 4: The **Transport Layer** handles the exchange of entire messages between stations and error recovery.

Layer 5: The **Session Layer** handles the communication session between computers.

Layer 6: The **Presentation Layer** provides transparent data communications between stations of different types.

Layer 7: The **Application Layer** provides all functions to support end-user services or applications.

Packet

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

Permanent Virtual Circuit (PVC)

A circuit that is kept up permanently like a dedicated leased line on the telephone network.

Plenum Cable

Cable which has been certified for installation in air ducts and open spaces over suspended ceilings without conduit. Plenum cable is fire-resistant and does not emit toxic fumes when burned.

Pop-Up Window

A window that the LANMeter instrument displays to communicate some information or to prompt you with a choice of actions.

Primary Rate Interface (PRI) ISDN

ISDN service based on a rate of 1.544 Mbps and including 23 B channels and one 64 Kbps D channel. The B channels provide data transmission while the D channel provides signaling information.

Propagation Delay

Propagation Delay is the time it takes for a signal to go from one end of a cable to the other end. There should be similar delay characteristics between cable pairs. Propagation Delay is very important for technologies that use parallel transmission techniques, such as 100BASE-T4 and 100BASE-VG.

Protocol

A set of rules that machines must follow to exchange information on a network.

Proxy ARP

Routers with Proxy ARP enabled will respond to ARP requests for off-net hosts. When a node relies on Proxy ARP, the node only has to ARP for the target node instead of forwarding the packet to the correct local IP router. Some vendors’ routers respond incorrectly to on-net ARP requests, which can create confusing network behavior.

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.

Remove Ring Station

The act of taking an active device from the ring.

Repeater

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

Report Soft Error Frame

A MAC frame that is transmitted when an intermittent, or soft, error causes data to be transmitted more than once. The Report Soft Error Frame contains information about the error, or errors, on the ring.

Reversed Wire

A wiring error in twisted pair cabling in which the pins on a pair are reversed between connectors on each end of the cable.

RFC-1398

Definitions of Managed Objects for the Ethernet-like Interface Types

Ring

See Token Ring Network.

Ring Ops

Ring Ops (RFC 1512) is the number of times an FDDI ring has entered the “Ring_Operational” state from the “Ring_Not_Operational” state (also known as No_OP state).

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.

RMON MIB (Remote Network Monitoring MIB)

The set of objects defined in various RFCs and private MIBs that are used to monitor various network activity. Also see MIB.

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 Token Ring and Ethernet Novell NetWare networks. 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.

Routing Information Protocol (RIP)

Routing Information Protocol (RFCs 1058, 1388, 1723) is the most widely supported IP routing protocol. RIP is a distance-vector protocol and bases its routing decisions on the number of hops. A 10 Mb LAN has the same cost assessment as a 9600 serial line.

Runts

Typically defined as a 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.

Server

A network component that is dedicated to specific functions.

Short

A near-zero resistance connection between two wires of a circuit.

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.

SMTP Host

A computer running the Simple Mail Transfer Protocol (SMTP) that handles email delivery.

SMTP (Simple Mail Transfer Protocol)

A protocol used to transfer email between hosts and ultimately to its final destination.

SNMP (Simple Network Management Protocol)

The Internet standard protocol for communicating between network managers and other network nodes. Also see MIB (Management Information Base) and RMON MIB (Remote Network Monitoring MIB).

Soft Error

An intermittent error or operation of a Token Ring network that interferes with the transmission of a frame. A soft error causes a frame to be retransmitted until it is properly received.

Source Address

The address of the station originating a frame.

Source Routing

Source routing, normally used with Token Ring, is a method by which a station discovers the route to a target station.

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.

Static Router

A device on the network that is assumed to be a router based on information monitored on the network.

STP (Shielded Twisted Pair)

Cable that is both twisted and shielded by pairs. This eliminates crosstalk to a greater degree than UTP cable and minimizes crosstalk at high transmission rates.

Symbolic Name

A symbolic name is the name given to an address to make it easier to use (MKG_SERVER versus 0003e8000008, for example).

T1

Digital line service that provides a transmission rate of 1.544 Mbps. The 1.544 Mbps bandwidth of T1 is usually divided into twenty-four 64 Kbps channels.

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.

TDR (Time Domain Reflectometer)

A TDR is a method to determine a cable's length, characteristic impedance, and other parameters by transmitting a pulse down into a cable and examining reflected energy.

Telnet

Telnet is a session-layer protocol in the TCP/IP protocol providing terminal emulation.

Terminator

A resistor connected to the end of a coax cable which is intended to match the characteristic impedance of a cable. Signals are dissipated in the terminator, eliminating reflections.

Token

A frame that gives a station permission to transmit on a Token Ring network. A token consists of a starting delimiter, a frame control field, and an ending delimiter that tells the receiving station that it is ready to be made into a frame.

Token Claiming

The process by which a new active monitor is elected.

Token Ring Network

A network arranged in ring topology and using the Token Ring protocol.

Token Ring Protocol

A network protocol based on collision avoidance. Collision avoidance is accomplished by passing permission, in the form of a token, to a station prior to allowing it to transmit onto the network. The Token Ring protocol allows signaling at 4 or 16 Mbps over UTP, STP, or fiber optic cabling.

Too Long

RFC-1398 "FrameTooLongs", a count of frames received on a particular interface that exceed the maximum permitted frame size.

Topology

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

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.

Transmit Delay

RFC-1398 “DeferredTransmissions”, a count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.

TRT Expired

For FDDI, TRT Expired (RFC 1512) is a count that should as closely as possible match the number of token rotation time (TRT) expirations since this MAC was reset or a token was received. TRT expires when the token has not been seen but a station continues to transmit frames. Stations typically negotiate a TRT from 4 to 8 ms (known as T_Neg) and TRT expires at 2 times T_Neg.

TVX Expires

For FDDI, TVX Expires (RFC 1512) is a count that should as closely as possible match the number of times that the TVX timer has expired. It monitors the amount of time that has passed without any tokens or frames arriving. TVX timer is often set to 2 ms and most often expires due to the normal processes of stations entering and leaving the FDDI ring.

Twisted Pair

A pair of wires that are 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.

Upstream

Upstream is in the opposite direction to that of the data flow on a Token Ring network. Upstream is the opposite of downstream.

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.

UU Encoding

A standard Internet format used for encoding files that will be attached to email messages. Also see MINE (Multipurpose Internet Mail Extensions).

Virtual Circuit

A network capability that lets two ports communicate as if they were directly connected without regard for the structure of the physical layer.

VLAN (Virtual LAN)

A group of ports configured into one broadcast domain (or logical LAN). VLANs can only be detected by using the private MIB associated with the device.

WAN (Wide Area Network)

A network that is usually constructed with serial lines, which covers a large geographic area. Also see LAN (Local Area Network).

Wavelength

The length of the optical wave used in fiber optic transmissions. Also used to specify the different optical sources available for fiber optic usage.

Wire Fault

A hard error caused by opened or shorted network wires.

World Wide Web (WWW)

A hyperlink-based, distributed information system that can be used to create, edit, or browse documents. It is a powerful, global, information system. The hyperlinks provide access to other information sources on the Internet. Also see Hyperlink.

Index