



# OneTouch Series II

Network Assistant

## Users Manual

September 1999 Rev. 3 03/02

© 1999 - 2002 Fluke Corporation. All rights reserved. Printed in USA  
All product names are trademarks of their respective companies.

## LIMITED WARRANTY & LIMITATION OF LIABILITY

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

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

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

To obtain warranty service, contact your nearest Fluke Networks authorized service center to obtain return authorization informa-

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

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

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

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

6/01/01

# Table of Contents

Chapter	Title	Page
<b>1</b>	<b>Introduction.....</b>	<b>1-1</b>
	Introducing the OneTouch Series II Network Assistant.....	1-1
	Software Version.....	1-2
	Supplied Equipment.....	1-2
	Optional Equipment.....	1-2
	Getting Assistance.....	1-3
<b>2</b>	<b>Autotest and Central Setup.....</b>	<b>2-1</b>
	Introduction.....	2-1
	Device Discovery Process.....	2-2
	Identifying Routers.....	2-2
	Device Icons.....	2-3
	Station Detail Display.....	2-8
	Viewing Multiple Protocols on Station Detail Displays.....	2-9
	NetWare Devices List.....	2-9
	NetWare Print Server List.....	2-11
	TCP/IP Devices Display.....	2-11
	Sorting.....	2-15
	Address Entry Keypad.....	2-16

	Central Setup .....	2-16
	IP Config .....	2-17
	Using DHCP to Get an IP Source Address .....	2-19
	SNMP .....	2-20
<b>3</b>	<b>Network Health .....</b>	<b>3-1</b>
	Introduction .....	3-1
	Interpreting Error Results .....	3-7
	Collisions .....	3-7
	Late Collisions .....	3-7
	Short Frames .....	3-7
	Jabbers .....	3-7
	Bad Frame Check Sequence (FCS) .....	3-7
	Tracking Addresses .....	3-8
	Local vs. Remote Stations .....	3-8
<b>4</b>	<b>Cable Tests .....</b>	<b>4-1</b>
	Introduction .....	4-1
	Cable Autotest .....	4-2
	Split Pairs .....	4-2
	Cable Length Results .....	4-2
	Wiremap Cable .....	4-2
	Identifying Cables .....	4-4
	Toner .....	4-4
	Define Cable .....	4-4
	Basic Cable Concepts .....	4-4
	Twisted Pair Cables .....	4-5
	Reversed Pair .....	4-6

	Crossed Pair .....	4-6
	Split Pair .....	4-6
	Cable Length .....	4-7
	Cable Termination .....	4-8
	Test Fiber Optic Cable .....	4-10
	Ensuring Accurate Measurements .....	4-10
	Setting a Reference .....	4-10
	Measuring Optical Loss .....	4-11
	Measuring Output Power .....	4-11
<b>5</b>	<b>NIC/Hub Tests .....</b>	<b>5-1</b>
	Introduction .....	5-1
	NIC Autotest .....	5-2
	Hub Autotest .....	5-3
	Viewing Hub Capabilities .....	5-3
	NIC Detector .....	5-4
	Flash Hub Port .....	5-4
<b>6</b>	<b>Connectivity Tests .....</b>	<b>6-1</b>
	Introduction .....	6-1
	IP Trace Route .....	6-2
	IP & NetWare Ping .....	6-2
	Entering IPX Addresses .....	6-3
	Conducting a Ping Station Test .....	6-4
	Key Device Ping .....	6-6
	Interpreting Ping Test Results .....	6-8
	ConfigMaster .....	6-8
	Station Locator .....	6-10

	Find MAC.....	6-10
	Find IP .....	6-11
	Mode of Operation .....	6-11
	Results.....	6-11
<b>7</b>	<b>ITO – Internetwork Throughput Option .....</b>	<b>7-1</b>
	Introduction .....	7-1
	ITO/xDSL Throughput Test .....	7-2
	ITO/xDSL Theory of Operation .....	7-2
	Basic Operation .....	7-4
	Conducting a Throughput Test .....	7-4
	Connecting and configuring the Remote Unit .....	7-7
	Connecting and configuring the Local Unit .....	7-7
	Results Displayed During the Throughput Test .....	7-13
	Final Test Results .....	7-13
	ITO/xDSL Traffic Generator.....	7-15
	MAC Mode.....	7-17
	IP Mode .....	7-17
	MAC and IP Mode Results.....	7-18
	Ping Mode .....	7-19
	Ping Mode Results.....	7-20
	<b>Appendices</b>	
	A Specifications .....	A-1
	B Basic Maintenance .....	B-1
	C Web Remote Control.....	C-2
	D Glossary .....	D-1
	E SNMP Discovery .....	E-1
	<b>Index</b>	

## **List of Tables**

<b>Table</b>	<b>Title</b>	<b>Page</b>
2-1.	Device Icons .....	2-4
2-2.	TCP/IP Device Icons.....	2-13
3-1.	Network Health Meters .....	3-4
4-1.	Fiber Test Terminology .....	4-11
7-1.	ITO and xDSL Terminology .....	7-1





# List of Figures

Figure	Title	Page
1-1.	OneTouch-10/100 Series II Network Assistant .....	1-2
2-1.	Autotest Display .....	2-2
2-2.	Station Filter .....	2-6
2-3.	Station List Information .....	2-6
2-4.	NetBIOS Information .....	2-6
2-5.	NetWare Server Information .....	2-7
2-7.	Ping SNMP Results .....	2-9
2-8.	Station Running Multiple Protocols .....	2-9
2-9.	NetWare File Server List .....	2-10
2-10.	Netware File Server Information .....	2-11
2-11.	TCP/IP Devices Display .....	2-12
2-12.	Local Station List .....	2-15
2-13.	Sort Options .....	2-16
2-14.	Address Entry Keypad .....	2-16
2-15.	Central Setup .....	2-17
2-16.	IP Address Configuration .....	2-17
2-17.	Address Entry Keypad .....	2-18
2-18.	DHCP Display .....	2-19
2-19.	Security Setup .....	2-20

2-20. SNMP .....	2-21
2-21. Password Setup .....	2-22
2-22. Community String Editor.....	2-22
3-1. Network Health.....	3-1
3-2. Top Senders Display .....	3-2
3-3. Station Detail .....	3-3
3-4. Network Health Test Meter Icon .....	3-3
3-5. Station Addresses .....	3-8
4-1. Cable Tests .....	4-1
4-2. Wiremap Results .....	4-3
4-3. Reversed Pair.....	4-6
4-4. Crossed Pair.....	4-6
4-5. Split Pair.....	4-7
4-6. Cable Termination .....	4-9
4-7. Fiber Test Results .....	4-12
4-8. Connections for Setting a Reference Level .....	4-13
4-9. Connections for Measuring Optical Loss .....	4-14
4-10. Connections for Measuring Output Power .....	4-15
5-1. NIC/Hub Test.....	5-1
5-2. NIC Autotest .....	5-2
5-3. Hub Autotest Display.....	5-3
5-4. NIC Detector.....	5-4
5-5. Flash Hub Port Display.....	5-6
6-1. Connectivity Tests Display .....	6-1
6-2. IP Trace Route .....	6-2
6-3. IP & NetWare Ping Display.....	6-2
6-4. NetWare Ping .....	6-3
6-5. IP Ping.....	6-3

6-6. IP and NetWare Ping .....	6-5
6-7. IP Ping Results .....	6-5
6-8. NetWare Ping Results.....	6-5
6-9. Ping Key Devices.....	6-6
6-10. Add Key Devices.....	6-7
6-11. Edit Key Devices.....	6-7
6-12. ConfigMaster .....	6-9
6-13. Station Locator.....	6-10
6-14. Station Locator Information.....	6-12
7-1. Local and Remote Units.....	7-3
7-2. ITO Local Unit and Possible Remote Unit Locations .....	7-5
7-3. xDSL Test Connections .....	7-6
7-4. Local Unit Configuration Display for Throughput Test.....	7-8
7-5. xDSL Central Office (Remote) Connections .....	7-9
7-6. xDSL Subscriber-end Connections.....	7-10
7-7. ITO Results Shown During the Test.....	7-13
7-8. Final ITO Throughput Test Results.....	7-14
7-9. Traffic Generator Setup Display.....	7-16
7-10. MAC or IP Mode Sample Results .....	7-19
7-11. Ping Mode Sample Results.....	7-22
C-1. Web Agent .....	C-2
E-1. Central Setup.....	E-3
E-2. Security Setup .....	E-3



# Chapter 1

## Introduction

### **Introducing the OneTouch Series II Network Assistant**

The Fluke OneTouch™ Series II Network Assistant (hereafter referred to as the "Network Assistant") provides quick solutions to the most common problems found when installing and troubleshooting Ethernet networks. The Network Assistant is a portable, handheld instrument that is operated using a touchscreen user interface.

#### **Caution**

**Take care not to damage the touchscreen with any sharp, pointed, or hard objects. For additional information, see "Essentials" in the Getting Started Manual.**

The OneTouch Series II is available in these models:

- ❑ OneTouch Series II 10/100
- ❑ OneTouch Series II 10/100 Pro

OneTouch Series II Pro features include:

- ❑ Station Locator
- ❑ Key Device Ping
- ❑ ConfigMaster™
- ❑ Web Remote Control


These features are discussed throughout this manual in the pertinent sections. Read the *OneTouch Series II Network Assistant Getting Started Manual* (P/N 1595893) that came with your purchase to become familiar with and quickly begin using your OneTouch Series II Network Assistant. You can also access <http://www.flukenetworks.com> and navigate to the OneTouch Series II area to access software and documents. Adobe Acrobat Reader is required to view the

## OneTouch Series II

### Users Manual

documents. It is included on the CD-ROM that came with your purchase or downloadable from [www.adobe.com](http://www.adobe.com).

### Software Version

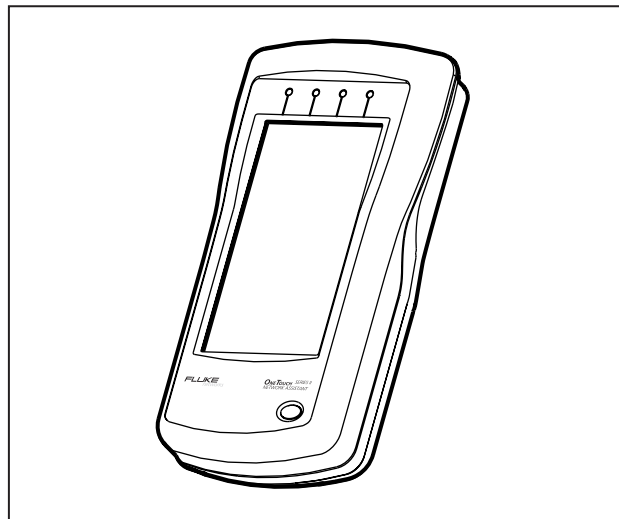
To determine the version of the software in the OneTouch Series II Network Assistant, press the green button to turn the Network Assistant on then press .

The software version number is displayed on the Help screen. To update the software version for your Network Assistant, read the *OneTouch Series II Getting Started Manual* and the OneTouch Link program online help.

### Supplied Equipment

The following is supplied with the Network Assistant:

- NiMH Rechargeable Battery Pack
- Universal AC Power Adapter
- Cable Identifier 1
- Instrument Softcase
- Power Cord
- Network Assistant Strap and Holster
- CD-ROM Disk
  - OneTouch Series II Users Manual*
  - OneTouch Link Program
  - OneTouch Reporter (Trial Version)



ace010f.eps

**Figure 1-1. OneTouch-10/100 Series II Network Assistant**

### Optional Equipment

The following optional items and can be purchased through Fluke or your local distributor:

- NiMH Rechargeable Battery Pack (P/N N6600/NBP)
- Cable Identifier Set -- numbers 2 through 6 (P/N N6600/RA)

- ❑ UTP Accessory Kit (P/N N6703)
- ❑ Extra *OneTouch Series II Network Assistant Getting Started Manual*

### **Getting Assistance**

For operating assistance in the USA, call 1-800-283-5853.  
For a complete list of contact numbers, check Appendix B  
or visit the Fluke Networks web site at  
[www.flukenetworks.com](http://www.flukenetworks.com).








## Chapter 2


# Autotest and Central Setup


### Introduction

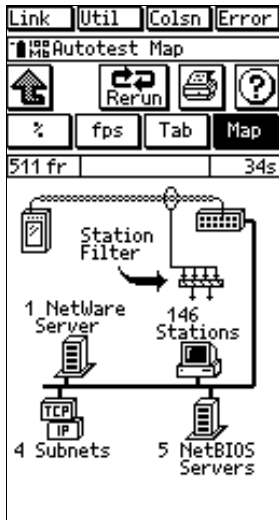
AutoTest and Central Setup are two critical elements of using your Network Assistant. To run AutoTest, press  (**AutoTest**) on the top-level display. The Network Assistant will take one of several courses of action.

- ❑ If a link pulse is detected, it searches for devices on the network. The devices on your segment are shown by protocol on the AutoTest display. The map view shows a summary of device types, including the Network Assistant  itself and the hub , which shows hub capability (Figure 2-1).
  - ❑ If it detects a wire mapper (office locator), it will map the cable.
  - ❑ If it detects the Fiber Optic Module (FOM), it will report the results.
- ❑ If it detects an open cable, it will perform Time Domain Reflectometry (TDR) on the cable to determine cable length, characteristic impedance, and other parameters.
  - ❑ If no link pulse is detected but it detects termination, no data will be found and you will see the message, `waiting for Link Pulse`. This could happen if it is plugged into a hub or NIC that is not turned on.

If link is detected, you can get the same information via AutoTest or Network Health from the main menu. You can then use the tabs to navigate between the different views. The difference between AutoTest and Network Health is that AutoTest restarts the discovery process from the beginning, including DHCP addresses (if enabled). Network Health allows you to view the information without a discovery restart. Pressing AutoTest is the same as unplugging the network cable and then


plugging it back in. This is also the same as pressing the  (**Rerun**) button.

Press a displayed device, cable, or filter icon to see a popup screen showing more information about that item. Close the resulting popup screen by pressing  (**Up One Level**).




**Figure 2-1. AutoTest Display**

ace201s.bmp

AutoTest continues to discover devices and to count frames and errors even after you exit the screen by pressing  (up one level). The Network Health test runs in the background (read Chapter 3).

### **Device Discovery Process**

When you attach the Network Assistant to a network, it immediately begins searching for servers, routers, printers, and switches. This search occurs whenever the Network Assistant gains link pulse regardless of the current menu.

During the discovery process ( $\pm 8$  seconds, depending on network), the Network Assistant processes only the discovery response frames and broadcast frames. The magnifying glass  signifies discovery is in progress. When the discovery process has finished, the magnifying glass goes away and the Network Assistant goes into promiscuous mode. In this mode, it processes all frames and reports all stations that talk on the network.

### **Identifying Routers**

The Network Assistant also transmits RIP requests and ICMP router requests as part of its router discovery process. These discovery packets request router information, allowing the Network Assistant to locate

routers that have little traffic and are not sending routing updates.



The Network Assistant will identify as a router any device advertising one of the following router protocols: RIP, IGRP, EIGRP, IRDP, OSPF, and ICMP TTL expiring or redirects.

Therefore, if a router is statically configured (i.e., is not sending out routing updates), it may not show up as a router.








The Network Assistant will identify any IP device that is transmitting periodic router updates as a router. Therefore, the Network Assistant identifies a workstation that is inadvertently configured as a router.

### *Device Icons*




Pressing a device icon displays further information about that device type.

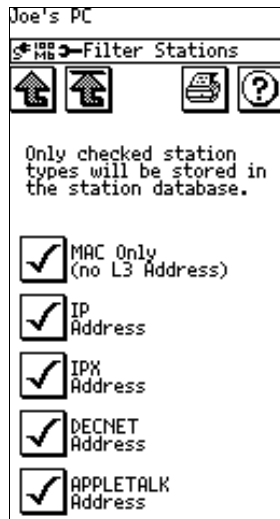
Return by pressing  or . The device icons are described in Table 2-1.

**Table 2-1. Device Icons**

Icon	Meaning	Information
	Network Assistant	Press to display the MAC and IP address and software/hardware versions for your instrument.
	Station Filter	Press to filter out station types of low or no interest to you (Figure 2-2). You can unselect the following: MAC Only (no L3 Address), IP Address, IPX, DECNET, and APPLETTALK addresses.
	Stations	Press to display a list of stations on the network (Figure 2-3). Stations are listed by name by default. You can also sort other ways (Frame Count, Protocol, Device Type, and MAC address) by pressing  ( <b>Station List Sort</b> ). For more details, see "Tracking Addresses" and "Local versus Remote Stations" in Chapter 3. The Network Assistant can list up to 500 stations. Press an entry in the station list to see a Station Detail display (Figure 2-6). For more information, read "Station Detail Display."
	NetWare	Press to display a list of NetWare servers (Figure 2-5). Read "NetWare Devices List" for more information. Press the finger  ( <b>View Server</b> ) to see a list of file and printer servers. To ping and see details on a given server, press the finger icon by that server. If there are more devices than will fit on the display, you can scroll through the list.
	NetBIOS	Press to display a scrollable list of all NetBIOS servers with their network addresses and protocols detected on the segment (Figure 2-4).

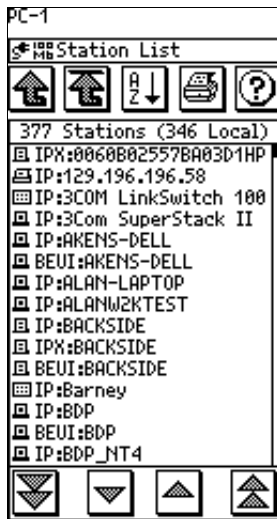
**Table 2-1. Device Icons (Cont.)**

Icon	Meaning	Information
	TCP/IP Devices	Press to display IP routers, servers, stations and other devices detected on the network that are running TCP/IP (Figure 2-11). Pressing an icon on the TCP/IP Devices display generates a list of devices of that type. For more information, read "TCP/IP Devices."
	Hub	Press to display general information about the status of the Hub. This information includes whether the link is active and its activity level. The following fields within the Hub popup window indicate the Hub's status.  <b>Capability</b> Speed Duplex Mode <b>Link Pulse Status</b> Speed Duplex Polarity RX Level (receive pair) <i>Normal:</i> Hub signal level is within specification. <i>Marginal:</i> Hub signal level is not within specification. (The problem is either excessive attenuation in the cable or a defective hub port.)
	Cable	Press to display cable length and fault information (when the Network Assistant is not connected to an active device). The Network Assistant displays the length to the first fault it detects. For more details, see "Cable Autotest" in Chapter 4.



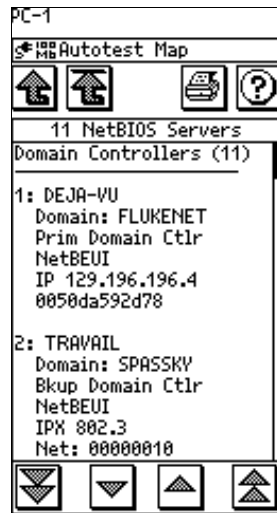
ace216s.bmp

Figure 2-2. Station Filter



ace202s.bmp

Figure 2-3. Station List Information

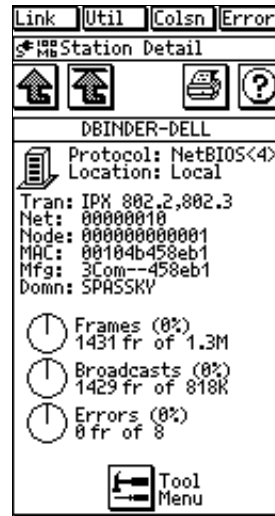


ace205s.bmp

Figure 2-4. NetBIOS Information



ace206s.bmp

**Figure 2-5. NetWare Server Information**

ace207s.bmp


**Figure 2-6. Station Detail**

### Station Detail Display

Pressing an entry in a station or server list brings up a Station Detail display (Figure 2-6). This display shows information pertaining to the resource. The information may include the frame type used, the network, node, and MAC addresses, the equipment manufacturer, and the types of router protocols or algorithms available.


From the Station Detail Display menu, press  (**Tool Menu**) to access the following:

- IP Trace Route
- Ping + SNMP
- Ping
- Key Device Ping
- Add to/Remove from Key Devices
- Find Node

Press  (**Ping + SNMP**) to ping the station or resource and get any SNMP information available. For an IP ping, the Network Assistant uses the source and router IP addresses currently entered in the IP configuration screen under Connectivity Tests. These addresses must be valid to get a ping response. For an IPX ping, the Network Assistant automatically determines a source address.

To access the SNMP agent, the Network Assistant uses the "public" community string (password). If the agent has

a different community string, access the **SNMP Config** menu from the Measurement Setup screen (read "SNMP" section).


After you press  (**Ping+SNMP**), the station's ping results, SNMP name, description, and uptime (in days, hours, minutes, and seconds) are displayed (Figure 2-7). Note that the SNMP name is cut off at 22 characters to fit on the display.






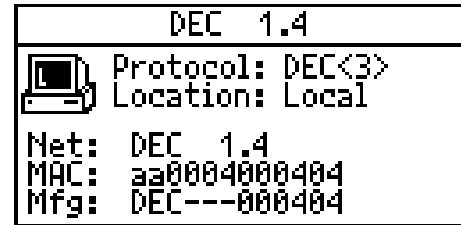
ace208s.bmp

Figure 2-7. Ping SNMP Results

From the Tool menu press  (**Find Node**) to activate the Station Locator feature, which details switch information. Read “Station Locator” in Chapter 6 for more information.

### Viewing Multiple Protocols on Station Detail Displays


The Station Detail display tells you if the station is running multiple protocols. If multiple protocols are discovered, the protocol name on the Station Detail display is followed by a number. For example, Figure 2-8 shows PC Station Detail information for a station running three protocols. Press the device icon (example shows  **Station** icon) to cycle through the protocols.



ace209s.bmp

Figure 2-8. Station Running Multiple Protocols

### NetWare Devices List

To see a NetWare file server list, run AutoTest then press  (**NetWare Servers**) on the AutoTest Map display.

The NetWare File Server display (Figure 2-9) shows the nearest server for each of the four Ethernet frame types

(IEEE 802.2 and 802.3, Ethernet II, and SNAP). If more than one server responds for a given file type, the Network Assistant reports the first server that responded.

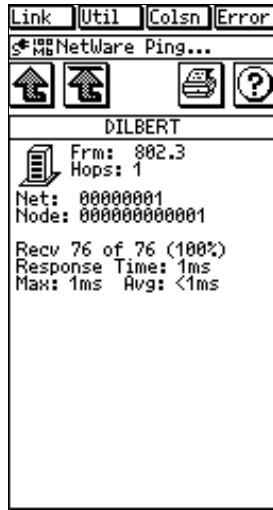
The File Server List shows the nearest 50 file servers, based on hop count. This list is derived from SAP responses from the first server in the Nearest Server list.

If the list takes up more than one screen, use the arrow keys to scroll through the list. Press on a server name to see its frame type, hop count, network address, ping results, SNMP information, and uptime (Figure 2-10).



ace210s.bmp


**Figure 2-9. NetWare File Server List**



ace211s.bmp

**Figure 2-10. NetWare File Server Information**

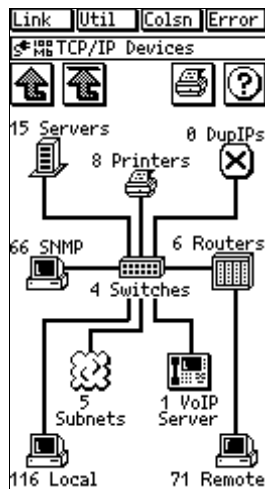
### **NetWare Print Server List**

From the NetWare File Server display (Figure 2-9), press  (**View Print Servers**) to see a list of the nearest 50 print servers based on hop count. Pressing a print server name sends an SNMP query to the server and displays the results (Figure 2-10). The SNMP query uses the "public" community string in addition to the SNMP strings

configured in the SNMP Config menu (see "Central Setup").

### **TCP/IP Devices Display**






Pressing the TCP/IP icon from the Autotest Map display brings up the TCP/IP Devices display (Figure 2-11). This display may include such items as servers, printers, SNMP devices, VoIP devices, switches, routers, stations (local and remote), or subnets that are running TCP/IP. The device icons are described in Table 2-2.









ace204s.bmp

**Figure 2-11. TCP/IP Devices Display**

**Table 2-2. TCP/IP Device Icons**

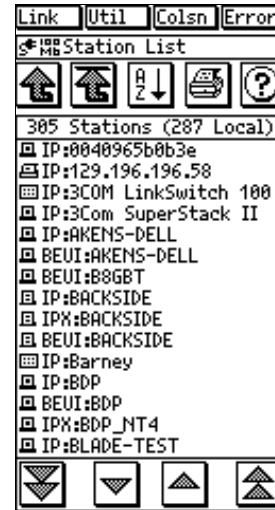
Icon	Meaning	Information
	Servers	TCP/IP Servers OneTouch has discovered. The Network Assistant will discover DNS, WINS, POP2, POP3, SMTP, HTTP, DHCP, and BOOTP servers.
	Duplicate IPs	IP addresses that are in use by more than one device on the network. The Network Assistant actively discovers devices using the same IP address and lists them in the TCP/IP menu in Autotest. From that point, you can see all known information for each device using duplicate IP addresses.
	Printers	Discovers printers running TCP/IP.
	SNMP	TCP/IP stations running SNMP.
	Switches	Automatically queries a switch and displays basic information (port summary and some SNMP information).

**Table 2-2. Device Icons (Cont.)**

<b>Icon</b>	<b>Meaning</b>	<b>Information</b>
	Routers	Local Routers and routing protocols on each router. The following routing protocols are identified: RIP, RIP2, OSPF, IGRP, EIRGP, IRDP.
	Servers	TCP/IP Servers the Network Assistant has discovered. It will discover DNS, WINS, POP2, POP3, SMTP, HTTP, DHCP, and BOOTP servers.
	Subnets	Subnets discovered on the local segment. The valid range of IP addresses that are legal for the subnet, the broadcast address, and the mask are listed for each subnet.
	VoIP	Voice over IP (VoIP) devices. There is a tab for each level: Endpoint (VoIP devices), Servers (local VoIP server), and Gateways (routers configured for VoIP traffic).
	Remote	Stations not physically located on the local segment but which have transmitted packets onto the network.
	Local	Stations physically located on the local segment. The Network Assistant can list up to 500 stations.

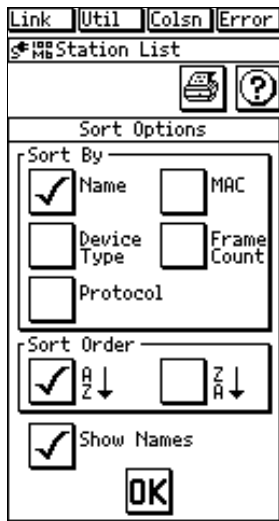
**Sorting**

Figure 2-12 shows a sample TCP/IP device list. Sorting for devices running TCP/IP functions the same way as Station Detail Display discussed in Table 2-1. Pressing **⇅** (**Station List Sort**) enables you to list devices based on Name, Protocol, Device Type, Frame Count (Local Stations), or MAC Address on the Sort Options screen (Figure 2-13). You can also choose ascending or descending sort order. Sorting does not apply for Subnets and Routers.



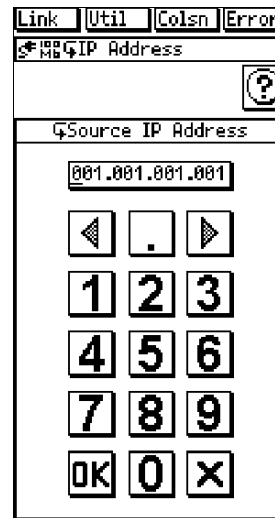
ace212s.bmp

**Figure 2-12. Local Station List**



ace214s.bmp

Figure 2-13. Sort Options





ace213s.bmp

Figure 2-14. Address Entry Keypad

### Address Entry Keypad


The Address Entry Keypad (Figure 2-14) is a decimal keypad for entering addresses. Press the Left-Arrow and Right-Arrow keys to select digits to change (or touch the entry box directly at the desired position), the period (.) to move between IP address octets, the **OK** button to save changes then exit, and **X** to exit without saving changes.

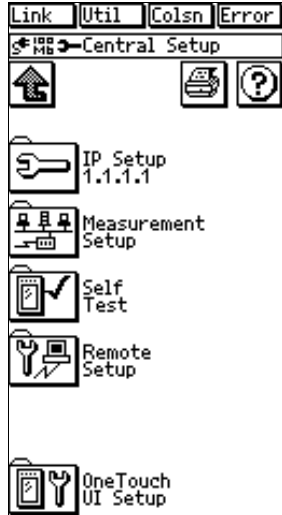
### Central Setup

This section covers the elements of the Central Setup screen (Figure 2-15) that are not covered in the *Getting Started Manual*:  (IP Config) and  (SNMP Config).



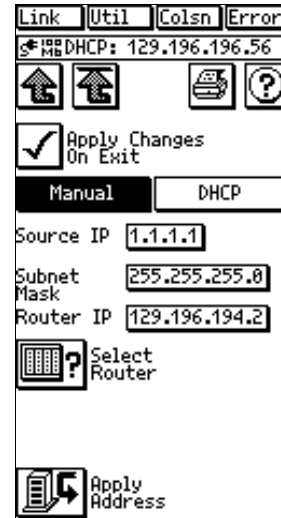
*IP Config*

From the Central Setup screen (Figure 2-15), press  (IP Setup) to access the IP Address screen (Figure 2-16).



**Figure 2-15. Central Setup**

ace219s.bmp



ace217s.bmp



**Figure 2-16. IP Address Configuration**


You can enter the Source IP manually or by using DHCP. The Source IP Address is the address you assign to the Network Assistant. The Network Assistant responds to pings received from a network station. To return a response, the Network Assistant must have a valid IP source address.

The address must be:

- ❑ Correct for the particular subnet to which the Network Assistant is attached (to determine what range of addresses is valid for a particular subnet you must know the subnet mask).
- ❑ Unique (there must not be a duplicate address on the network).

The Network Assistant checks for duplicate IP addresses before using a source address. Therefore, you can choose just about any address. It is still best, however, to check with your local IP address administrator to find out the Source IP Address to use for the Network Assistant. If the source IP address is not valid for the local subnet, you probably will not get any ping responses.

Enter a known router address or press  (**Find Router**) to automatically fill in the Router's IP Address. Pressing  (**Find Router**) again cycles through a list of the detected routers. This lets you see more routers than just the first one detected. If the Network Assistant has discovered more than one router, it assumes you want to ping the busiest router, and so uses that router's address.

Press  (**Apply Address**) to see if the Source IP address is duplicated on the local subnet. If a duplicate is found, its MAC address is displayed. Select **Apply**

**Changes on Exit** and this process will occur when you exit the screen.

### Manually Entering Addresses

To display the Address Entry Keypad (Figure 2-17) for manual entry, press a boxed IP address. Use the keypad to input digits for the desired IP address.

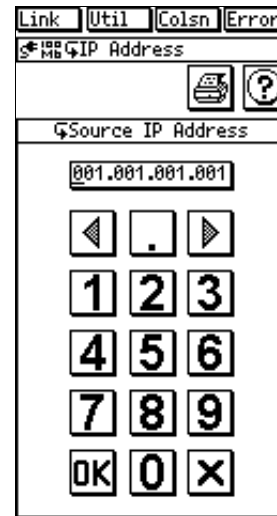


Figure 2-17. Address Entry Keypad

ace218s.bmp



To move the cursor, use the arrow keys or press the desired octet within the IP address box.


To quickly move between address octets, press the "." key, then press the octet you want to modify.

After entering the address, press **OK**.

### Using DHCP to Get an IP Source Address

The DHCP feature lets you use Dynamic Host Configuration Protocol to automatically get an IP source address for your Network Assistant.

To activate DHCP, press  (**IP Setup**) from the Central Setup screen; then select the **DHCP** tab. When you press  (**Get Address**), the Network Assistant requests to lease an IP address from a DHCP server (Figure 2-18). The DHCP address request also occurs automatically if DHCP is already selected when the Network Assistant detects a link pulse.

If a DHCP server is found, the display shows the accepted source IP address, DHCP server information, and lease time. Pressing  (**Get DHCP Address**) again restarts the DHCP process.



ace220s.bmp

Figure 2-18. DHCP Display

The Network Assistant determines if an assigned address is already used by another device, and requests another address if necessary. This cycle can occur up to five times before the DHCP process fails.


Network Assistant will renew its lease according the RFC2131, which is the RFC that defines DHCP, or by

using the renew and rebind values received from the server.

The time at which Network Assistant will renew its lease depends on whether the DHCP server issued a renew time period. If the DHCP server issued a renew time period, OneTouch will attempt to renew its lease at the specified time. Otherwise, Network Assistant will attempt to renew the lease at 50% of the lease period. If OneTouch is unable to contact the DHCP server, it will try again to renew the lease at 87.5% of the lease period or the time specified by the server. This is called the rebind time.

If Network Assistant is still unable to contact the DHCP server to renew the lease, it continues to use the IP address it was given, but it continues to try to renew the lease at the renew and rebind times.

If at any time, the DHCP server explicitly notifies Network Assistant that its lease is no longer valid, Network Assistant will discontinue its use of the IP address it was given.

Pressing  (**View Log**) shows the details of the DHCP process, including the DHCP offers, any addresses declined because they were in use, and the address of the server providing the accepted IP address.

If no DHCP server is found, the message **No Server Found** displays. In this case, you can enter the IP source address manually as described earlier.

### SNMP




From the Central Setup screen, press  (**Measurement Setup**) then  (**SNMP Setup**) to access the Security Setup screen (Figure 2-19).



Figure 2-19. Security Setup

ace223s.bmp


Press  **SNMP Communities** on the Security Setup screen to access the SNMP Community String List (Figure 2-20). The Network Assistant uses the “public” community string (password) as the first default and also provides the capability to enter four additional community strings different than “public” for any given device or set of devices.

You can also password-protect strings so they are not visible on the Network Assistant screen.



ace221s.bmp

**Figure 2-20. SNMP**

Press  (**Password Protection**) on the Security Setup display to password-protect the community strings, an entry box displays (Figure 2-21), enabling you to enter and enable the password. Thereafter, you will be prompted to enter that password in order to see and access the Community String screen.



ace224s.bmp

**Figure 2-21. Password Setup**



ace222s.bmp

**Figure 2-22. Community String Editor**

Press one of the address boxes to display a special keypad to enter community strings (Figure 2-22). Refer to the Help on the Network Assistant for an explanation of the keypad.

# Chapter 3

## Network Health

### Introduction

Network Health displays utilization (**Util**), errors (**Error**), collisions (**Colsn**), broadcasts (**Bcast**), protocols, and stations (**Stations**), as shown in Figure 3-1. To enter the Network Health menu, press **[F5]** (**Network Health**) on the top-level display. The Network Health menu displays six meter icons that indicate the overall health of the network.

Press a meter icon to get more information about the network indicator shown on that meter.

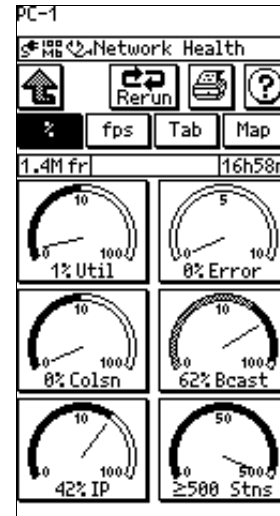



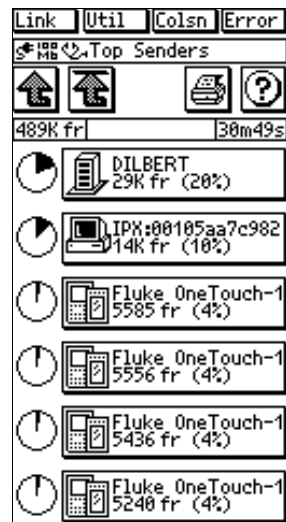
Figure 3-1. Network Health

ace301s.bmp

For example, pressing **Util** displays the Top Senders display (Figure 3-2).

To get more detail about a particular station, press the boxed address of that station. Details about that station will be displayed as shown Figure 3-3. Press  ( **Tool Menu**) to access the following (as applicable):

- IP Trace Route
- Ping + SNMP
- Ping
- Key Device Ping
- Add to/Remove from Key Devices
- Find Node



**Figure 3-2. Top Senders Display**

ace303s.bmp





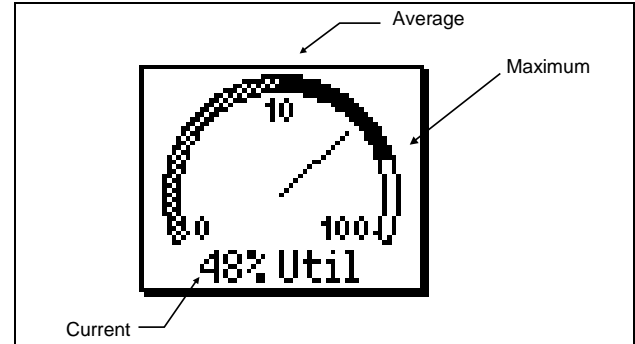
**Figure 3-3. Station Detail**

ace304s.bmp

The Network Health test display has six meter icons, each of which indicates the current, average, and maximum values. A representative meter icon is shown in Figure 3-4.

Each meter icon (except where indicated) has a logarithmic scale with 0 at the minimum, 1K at the mid-point, and 10K at the maximum. The meter's scale switches to high range when the frame rate exceeds 10,000/second.

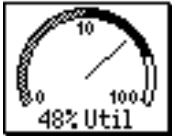

Tic marks identify the average and maximum data points.





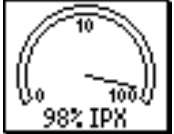
**Figure 3-4. Network Health Test Meter Icon**

Table 3-1 summarizes tests performed from the Network Health test display.

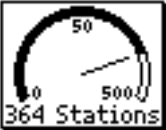


**Table 3-1. Network Health Meters**

Icon	Description
 The icon shows a semi-circular gauge with a needle pointing to approximately 48%. The scale has markings at 0, 10, and 100. Below the gauge, the text "48% Util" is displayed.	<p>Press to display network utilization.</p> <p><b>Percent Display</b> – Displays the utilization percentage for the last one-second sample period.</p> <p><b>Count Display</b> – Displays the frame count, for the last one-second sample period.</p> <p>The meter's scale switches to high range when the frame rate exceeds 10,000/second.</p>
 The icon shows a semi-circular gauge with a needle pointing to approximately 8%. The scale has markings at 0, 5, and 10. Below the gauge, the text "8% Error" is displayed.	<p>Press to display the types of errors received.</p> <p><b>Percent Display</b> – Displays the number of errors as a percentage of the number of frames received for the last one-second sample period.</p> <p>Errors counted are: bad FCS, short frames, late collisions, and jabbers.</p> <p><b>Count Display</b> – Displays the error count for the last one-second sample period.</p> <p>The meter has a logarithmic scale.</p>

**Table 3-1. Network Health Test Icons (Cont.)**

Icon	Operation
	<p>Press to display collision details (% collisions and collisions/second).</p> <p><b>Percent Display</b> – Displays the number of collisions as a percentage of the number of frames received for the last one-second sample period.</p> <p>The Network Assistant identifies preamble collisions.</p> <p><b>Count Display</b> – Displays the collision count for the last one-second sample period.</p> <p>The meter's scale switches to high range when the collision rate exceeds 1,000/ second.</p>
	<p>Press to display stations sourcing the most broadcasts.</p> <p><b>Percent Display</b> – Displays the number of MAC broadcasts presented as a percentage of the number of frames received for the last one-second sample period.</p> <p><b>Count Display</b> – Displays the MAC broadcast count for the last one-second sample period.</p>
	<p>Displays the percent of frames on the network that are the top protocol since the beginning of the test .</p> <p>Press to display top protocols detected on the attached segment.</p>

**Table 3-1. Network Health Test Icons (Cont.)**

Icon	Operation
 A circular gauge with a needle pointing to the right. The scale is logarithmic, with markings at 0, 50, and 500. Below the gauge, the text "364 Stations" is displayed.	<p>Displays the number of unique source addresses monitored since the beginning of this test. Some of the source addresses may be off-segment, which are sourced from stations on the other side of a router.</p> <p>The meter has a logarithmic scale with 0 at the minimum, 50 at the mid-point and 500 at the maximum.</p> <p>Press to display the Station List. This information is the same for the Percent Display and Count Display.</p>
 A square icon containing a circular arrow and the word "Rerun" below it.	<p><b>Rerun</b> - Press to clear all of the Network Health test information and reset the elapsed time. The Erase Health function does not change the display mode.</p>
 Four rectangular tabs labeled "%", "fps", "Tab", and "Map". The "Tab" tab is highlighted with a dark background.	<p>Press these tabs to view network statistics in terms of percent, frames per second, or a tabular view. You can also display the Autotest Map by pressing (<b>Map</b>).</p>

## **Interpreting Error Results**

### **Collisions**

A collision is the result of two or more nodes transmitting at the same time on the segment. Collisions are not necessarily bad. They are a normal part of Ethernet's operation. In general you need not worry about collisions unless the AVERAGE collision rate is greater than 20%.

Excessive collisions are more often associated with too much network traffic and less often a physical problem with the network. Usually the best way to fix a "collision problem" is to understand why there is excessive traffic.

You may find that the Network Assistant collision count does not agree with that of some protocol analyzers that under report collisions. Just like a Hub, the Network Assistant identifies collisions that occur in the frame's preamble. These are the most common types of collisions in a 10BASE-T network.

### **Late Collisions**

A late collision is one that occurs after the first 64 bytes in a frame. Consider late collisions a serious network error to be resolved quickly. Late collisions may manifest themselves as frames with a bad Frame Check Sequence (FCS). Late collisions are caused by either a faulty NIC or a network that is too long (i.e., end-to-end signal

propagation time is greater than the minimum legal frame size of ~57.6 microseconds for 10BASE-T).

### **Short Frames**

A short frame is a frame that is 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 most likely cause of a short frame is a faulty card or an improperly configured or corrupt NIC driver file.

### **Jabbers**

A jabber is a frame greater than the maximum legal size (greater than 1518 bytes) with a good or bad frame sequence.

Consider jabbers a serious network error to be resolved quickly. The most likely causes of Jabbers are a faulty NIC or driver or perhaps a cabling problem.

### **Bad Frame Check Sequence (FCS)**

A legal sized frame with a bad frame check sequence (FCS) has been corrupted in some way. Bad FCSs can be caused by late collisions, a faulty NIC/driver, cabling, hub or induced noise.

If the percentage of frames with a bad FCS is greater than 1%, then it should be considered a serious problem that is affecting network throughput.

A given rate of bad FCS frames has a much more serious effect on network throughput than a similar collision rate. This is because the retransmission time is so much longer. When a collision occurs, the frame is retransmitted within a few milliseconds because the sending station knows that there was a problem acquiring the media for transmission. Conversely, when a frame is corrupted (resulting in a bad FCS) the receiving station ignores the frame. The sending station does not know the frame was corrupted and therefore it is up to the upper protocol layer timeouts to cause a retransmission to occur. This process can take several seconds to retransmit a single frame.

### Tracking Addresses

The Network Assistant tracks addresses by their layer-3 address when possible. It displays layer-3 addresses for IPX, IP, NetBIOS, AppleTalk, and DECnet.

A station can appear in the station list more than once if it is configured to run more than one protocol or has more than one layer-3 address. (Figure 3-5.)



Figure 3-5. Station Addresses

ace306s.bmp

### Local vs. Remote Stations

The Network Assistant initially classifies the location of all stations as *Unknown* until it observes traffic that proves that the station is either remote or local.

A local station is one that is connected to the same Ethernet segment as the Network Assistant. In a switched

environment, a local station is one that is in the same broadcast domain as the Network Assistant.

A remote station is one that is not on the same Ethernet segment or broadcast domain as the Network Assistant.





# Chapter 4

## Cable Tests

### Introduction

The Network Assistant quickly identifies the most common cable and wiring faults on twisted pair cabling systems and automatically tests all four pairs. It also detects fiber optic cable and enables you to begin fiber tests if a fiber optic module is detected.

You can perform the following tests and operations from the Cable Tests display (Figure 4-1).

- Run Cable Autotest
- Verify pin-to-pin continuity (wiremap)
- Transmit toner
- Fiber tests
- Set units (feet or meters) and define category of cable under test

Read the “Basic Cable Concepts” section of this chapter for more information.

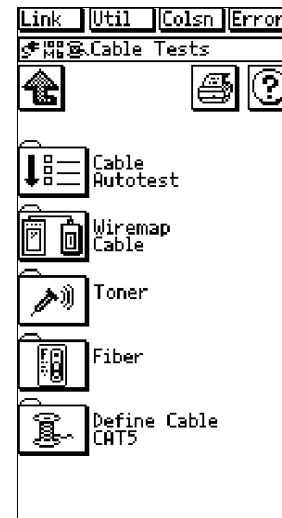




Figure 4-1. Cable Tests

ace401s.bmp

### Cable Autotest

Press  (**Cable Autotest**) to measure cable length, detect split pairs, and/or perform a wiremap test. The Network Assistant does not measure cable length when it detects a link pulse (i.e., when connected to an active device such as a Hub).

The Network Assistant also starts the fiber tests automatically if a DSP-FOM is connected and turned on when you press  (**Autotest**). Read “Test Fiber Optic Cable” later in this chapter.

### Split Pairs

The Network Assistant automatically checks for split pairs whenever Autotest or Cable Autotest is run. It will not check for split pairs if the end of the cable is attached to a Hub, a cable identifier, or the internal Wiremap connection. Disconnect it to obtain a complete test.

#### Note

*The cable under test must be longer than 20 feet.*

The Network Assistant can identify split pairs that occur either at the connector or at an intermediate point, such as a punchdown block.

### Cable Length Results

When displaying cable length, the Network Assistant always reports the length to the first fault (e.g., opens, shorts, or split pairs). It shows the distance to the fault and to the end of the cable on the same pair as illustrated in the following example test results table.

<u>Pair</u>	<u>Length</u>	<u>Status</u>
1,2	135 ft	Open
3,6	91 ft	Split Pair
4,5	135 ft	Open
7,8	91 ft	Split Pair


In the case of pairs 3,6 and 7,8 there is a split pair at 91 feet and it is most likely that both pairs continue for the entire cable length of 135 feet.

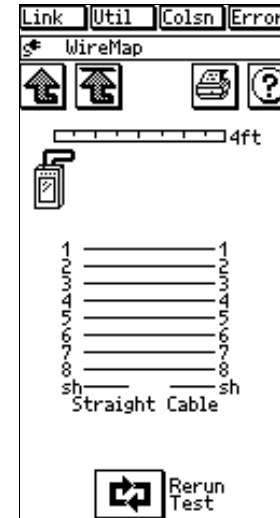
A split pair at the connector is represented as **Split/Open?** with a length of less than 5 feet (1.5 m). A **Split/Open?** indication could also be an open at the indicated distance.

### Wiremap Cable

The Wiremap Cable test verifies pin-to-pin continuity from the near to the far end of the cable, making it easy to identify miswires (the most common installation problem) and other wiring errors.

The Wiremap Cable test can be run as a standalone test or automatically when you run Cable Autotest or AutoTest. The standalone test and Cable Autotest are run under Cable Tests.

To run a standalone test Wiremap Cable test, attach the cable to the Network Assistant and a remote unit to the far end of the cable under test, then press  (**Wiremap Cable**). Figure 4-2 shows an example of the Wiremap Cable test results.



ace402s.bmp

**Figure 4-2. Wiremap Results**

If the Wiremap Cable test is conducted as part of the Cable Autotest or AutoTest, and if the Wiremap Cable test cannot run completely due to poor cable termination or quality, the Network Assistant displays a message recommending that you run the standalone version of the test to obtain additional error information.



If you explicitly run the Wiremap Cable test while the far end of the cable is attached to a Hub, you may see unexpected results like wires shorted together. This is a normal side effect of forcing a wiremap to be done on a remote device other than a Cable Identifier.

### Identifying Cables


Use the Cable Identifiers in mapping a cable. (Cable Identifier #1 is standard equipment and comes with the Network Assistant; Cable Identifiers #2 through #6 are optional. See "Optional Equipment" in Chapter 1.)

In mapping cables to individual offices from the wiring closet, the Network Assistant identifies unique Cable Identifiers and displays the wiremap and adapter number.


To map a cable, connect a Cable Identifier to the far end of the cable that you wish to identify (in the wiring closet, for example) and connect the near-end of the cable to the Network Assistant's RJ-45 network connector.

You can also connect the optional RJ-45-to-Punchdown block adapter to the RJ-45 network connector (with an RJ-to-RJ cable) and quickly map cables to individual offices by running either the  (**Wiremap Cable**) or  (**Cable AutoTest**).

### Toner

Press  (**Toner**) to transmit a low (185 Hz to 200 Hz) or high (350 Hz to 375 Hz) tone on the cable for use with a user supplied receiver, such as the Fluke 140 Tone Probe. Using the tone is a way to trace a cable on the network.

### Define Cable

Press  (**Define Cable**) to select units (meters or feet) and the cable category for the cable you are ready to test.

This Define Cable operation is the same as the one that can be accessed through the Measurement Setup screen.

### Basic Cable Concepts

This section provides some general information about cabling.

### *Twisted Pair Cables*

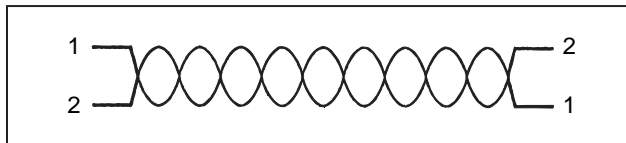
Twisted pair cable is currently the most popular cable in LAN systems. The 10BASE-T standard for twisted pair cabling systems is much more popular than coaxial based Ethernet networks because it is easier to work with and is inherently more reliable. The 10BASE-T standard is valid for Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (ScTP).

UTP cable typically consists of four pairs of 24 AWG (American Wire Gauge) solid or stranded wire surrounded by an insulating jacket. ScTP cable adds a foil shield around the four pairs to improve its noise immunity. The wires in each pair are twisted around each other, and the four pairs, in turn, are twisted together inside the cable sheath. Most UTP and ScTP cables have characteristic impedance of 100Ω. However, in some countries UTP is also available in 120Ω. The Cable Tests described in this chapter are designed to work with 100Ω cabling systems.

### Reversed Pair

A cable pair is reversed when two individual wires of a pair are reversed from end-to-end, as shown in Figure 4-3.

A reversed pair is not necessarily a catastrophic failure. Some 10BASE-T adapter cards and Hubs can sense the reversed polarity and continue to operate. It is always a good idea, however, to fix this problem when found.



ace404f.eps

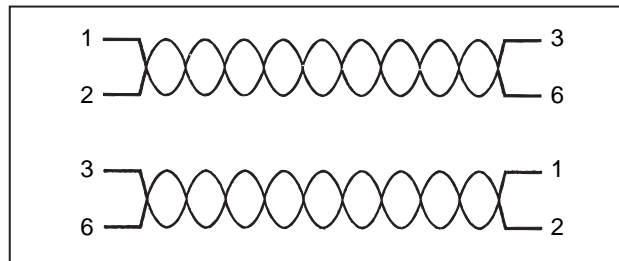
**Figure 4-3. Reversed Pair**

### Crossed Pair

A pair is crossed when a wire pair is mapped to a different set of connector pins on the other end of the cable. Figure 4-4 shows an example of a crossed pair.

Sometimes pairs are crossed intentionally. A cable with a 1-2 to 3-6 cross is commonly known as a crossover cable, which is used for cascading Hubs together that do not have uplink ports.

Special crossed-pair patch cords are useful when working with non-standard cabling systems.



ace405f.eps

**Figure 4-4. Crossed Pair**

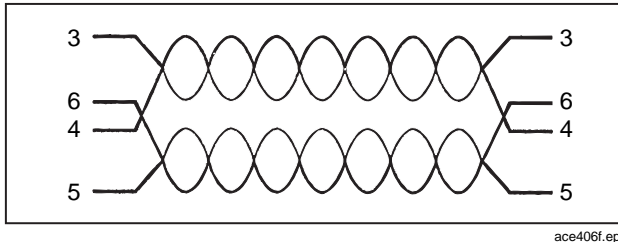
### Split Pair

A split pair is different from a crossed pair in that the pin-to-pin wiring is correct but the wire pairing is incorrect. That is, a “connector” pair is made up of two wires from a “cable” pair. Figure 4-5 shows an example of a split pair.

A split pair is much more susceptible to noise because the two wires in the “pair” are not twisted around each other. Split pairs can be especially difficult to find because the symptoms depend upon the particular wires involved, the cable length, and ambient noise.

The symptoms of a split pair range from non-existent to a complete lack of communication. In some cases a split

pair cable may work just fine for 10BASE-T but not at all for 100BASE-TX.



ace406f.eps

**Figure 4-5. Split Pair**

A split pair cannot be identified with a conventional wiremap test because it is the wire pairing that is incorrect rather than the physical connection. Another technique must be used.

The most common method of identifying a split pair is by measuring the Near End Crosstalk (NEXT). This is a very reliable method but, unfortunately, it requires the use of a remote unit at the far end. The Network Assistant uses another equally reliable method that does not require a remote unit at the far end (except in the case of short cable lengths). The Network Assistant identifies split pairs by measuring the characteristic impedance of each wire pair. A split pair's characteristic impedance is much greater than the impedance of correctly paired wires.

### **Cable Length**

The 10BASE-T and 100BASE-TX cabling specifications limit the maximum device-to-device cable length to 100 meters. There are many ways to measure a cable length; the Network Assistant uses a very accurate method called Time Domain Reflectometry (TDR).

The TDR method works much like a radar system that emits a pulse of electrical energy and then interprets the reflected electrical energy. To measure the length of a cable using the TDR method, a pulse of electrical energy is sent down a wire pair, the reflected electrical energy is interpreted to get the time delay between the transmitted and reflected pulse, and the length of the cable is computed using the cable's Nominal Velocity of Propagation (NVP).

The NVP is a value for how fast a pulse travels down a given cable. Cable manufacturers specify how fast electricity travels down a cable as a percentage of the speed of light (186,000 miles/second or 300,000,000 meters/second). A cable with an NVP of 72, for example, means that electricity travels at 72% of the speed of light along the cable.

The Network Assistant is preprogrammed with typical NVP values for CAT 3, 4, and 5 UTP cable. In addition, there

are two user-definable Cable Types for you to enter your own NVP values.

### ***Cable Termination***

In addition to determining cable length, the TDR technique provides information on the kind of termination at the far end of the cable and the cable's characteristic impedance.

The Network Assistant examines the polarity of the reflected pulse to determine if the cable end is an open or short, as shown in Figure 4-6. If the wire pair is perfectly terminated there is no reflection.



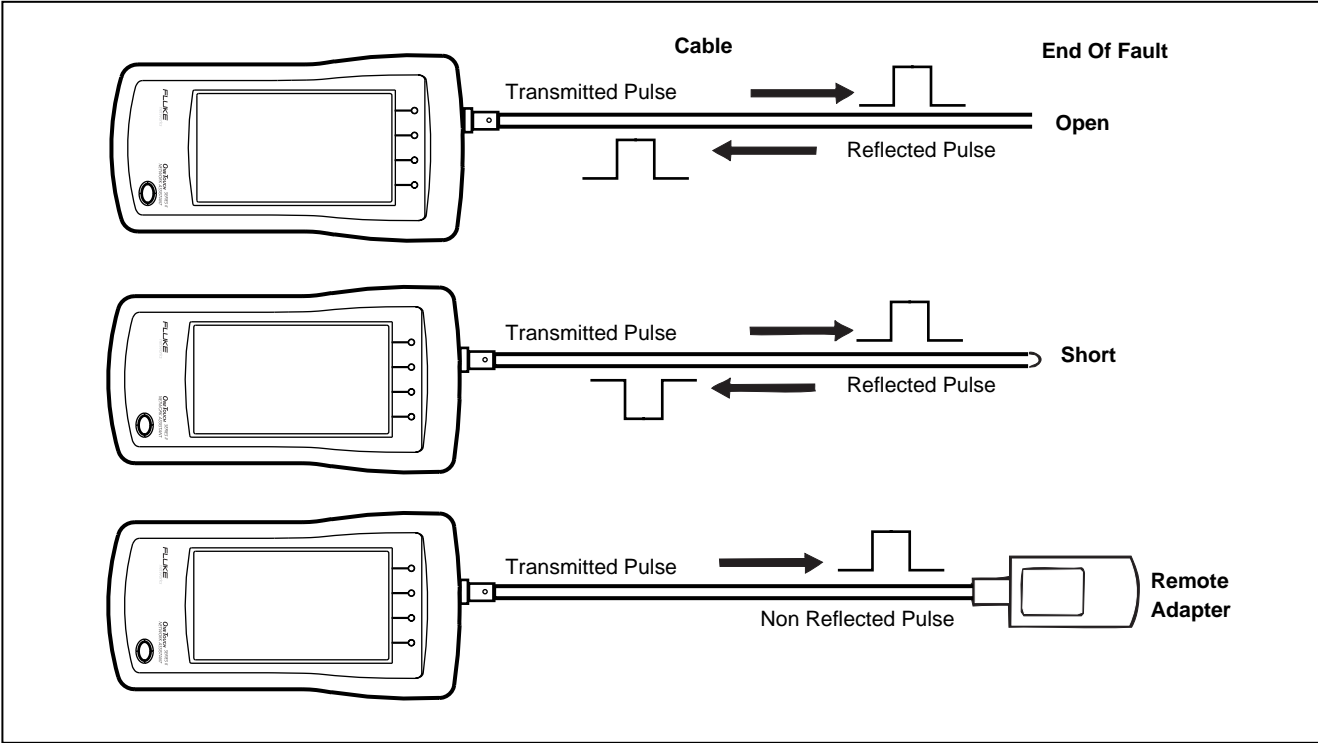


Figure 4-6. Cable Termination

ace407f.eps

## **Test Fiber Optic Cable**

This section describes how to use the Network Assistant with a Fluke Fiber Optic Meter (FOM) to test fiber optic cable. You can measure optical loss and output power on multimode or singlemode cable.

The fiber tests require the following:

- A Fluke DSP-FOM (Fiber Optic Meter; See "Placing Orders and Getting Assistance" in Chapter 1 for ordering information.)
- A multimode fiber optic source, such as is included with the Fluke DSP-FTK (Fiber Test Kit)
- Two fiber optic patch cables (provided with the DSP-FOM and DSP-FTK)
- Latest Network Assistant software (Read "Updating Software" in the *Getting Started Manual* for information on software updates.)

### **⚠ 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 and damage your eyes.**

See the instruction sheet provided with the DSP-FOM/FTK for specifications and maintenance information for the fiber optic meter and source.


## **Ensuring Accurate Measurements**


To help ensure accurate fiber measurements, do the following:

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


## **Setting a Reference**

Before measuring a cable's optical loss, set a reference level by measuring the loss in the fiber patch cables and connectors, as follows:


1. Make the connections shown in Figure 4-8. Use the same type of cable as the cable to be tested.
2. From the Network Assistant's top level display, press  (**AutoTest**). The Network Assistant detects the active fiber optic meter and the meter's wavelength setting and displays the fiber test results (Figure 4-7).

Press  (**Set Ref**) from the Network Assistant's fiber test display.

### **Measuring Optical Loss**

After setting the reference, do not disturb the source connection as you make connections to measure optical loss (Figure 4-9). If the fiber test is not already running, press  (**AutoTest**) from the top level display to start the test.

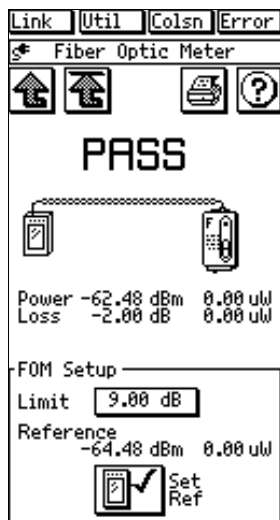
### **Measuring Output Power**

Make the connections shown in Figure 4-10. If the fiber test is not already running, press  (**Autotest**) from the top-level display to start the test.

Output power, optical power loss, and the current reference level are shown in microwatts ( $\mu W$ ) and decibels (dBm or dB) (Figure 4-7). The power and loss measurements are updated continuously. Table 4-1 defines the terms used during the Fiber Test.

**Table 4-1. Fiber Test Terminology**

<b>Term</b>	<b>Definition</b>
<b>Reference</b>	Power measured on a known reference cable.
<b>Power</b>	Measured power in milliwatts and dBm. dBm is the ratio of the measured power to one miliWatt. The formula the Network Assistant uses for calculating dBm is: Power (dBm) = $10 \times \log \times$ Power (mW)
<b>Loss</b>	The amount of power loss on the measured cable. Loss = Reference - Measured Power
<b>Loss Limit</b>	Acceptable power loss. If the Loss is greater than this value, the test reports FAIL. Otherwise, it reports PASS.



ace403s.bmp

Figure 4-7. Fiber Test Results

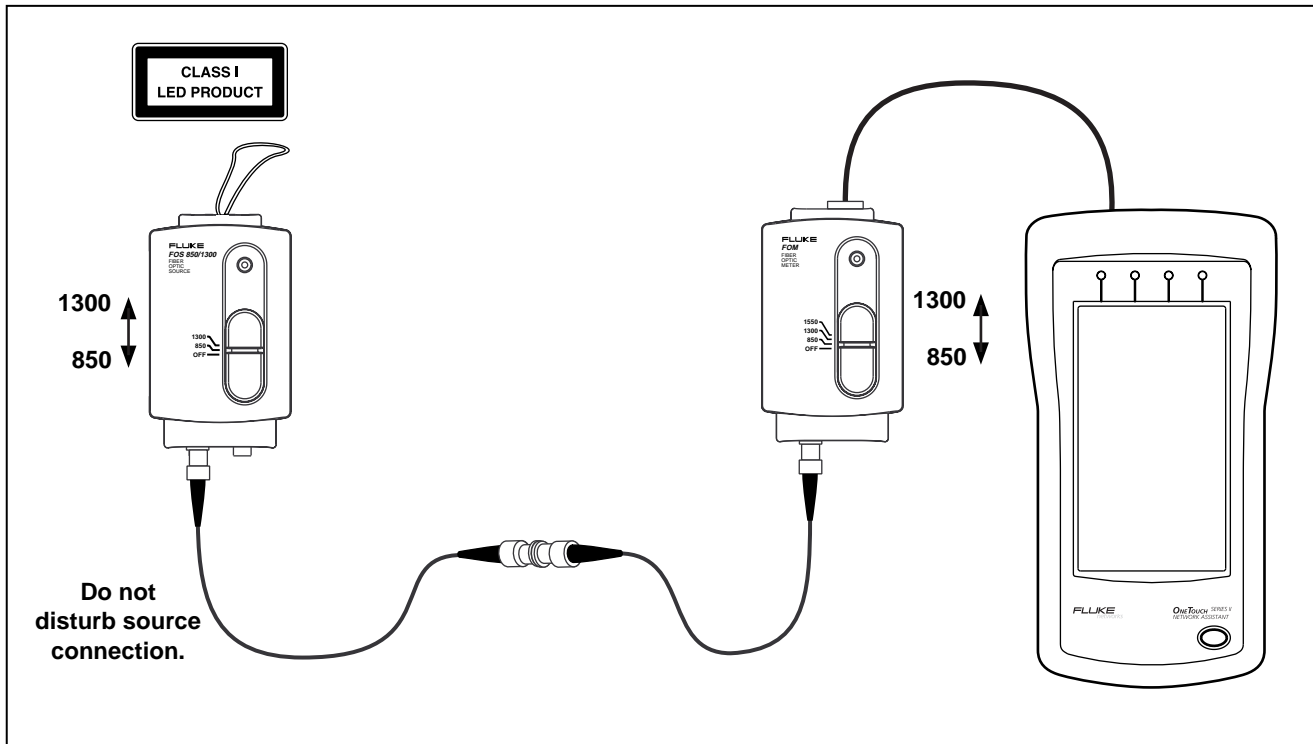


Figure 4-8. Connections for Setting a Reference Level

ace408f.eps

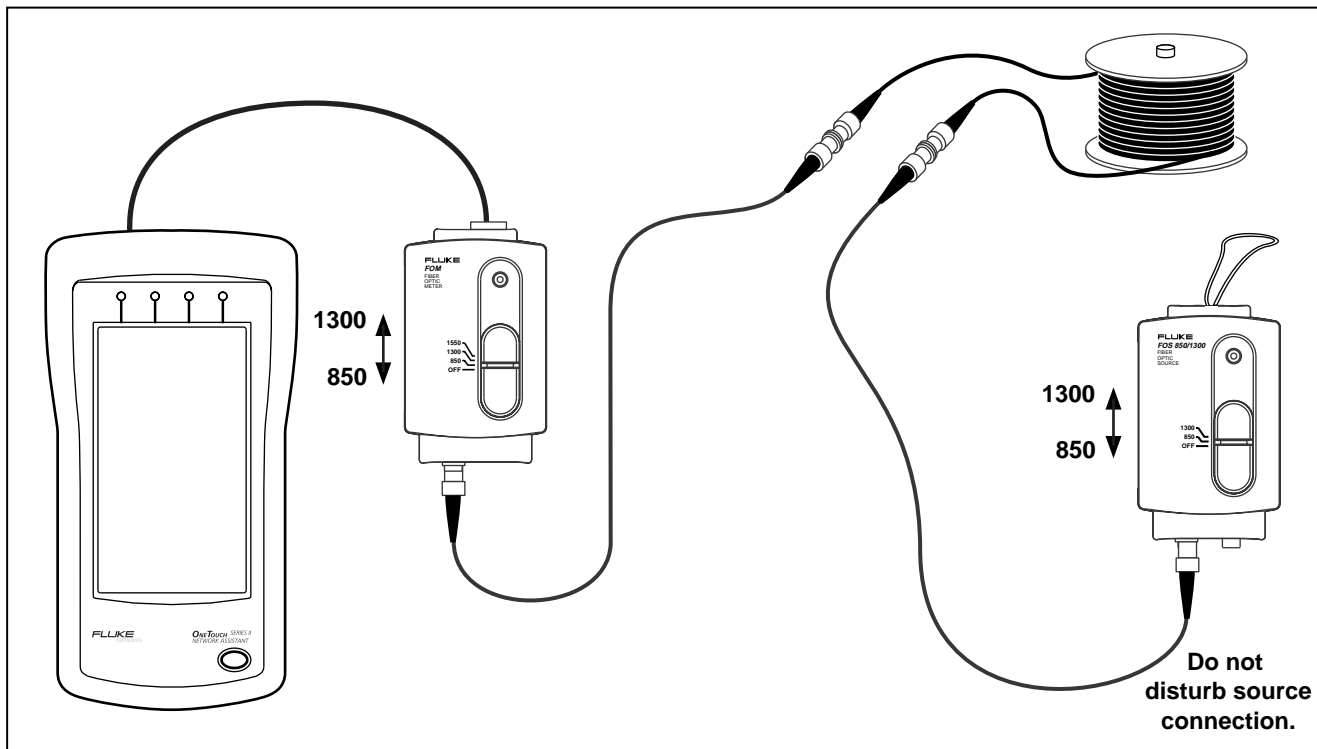


Figure 4-9. Connections for Measuring Optical Loss

ace409f.eps

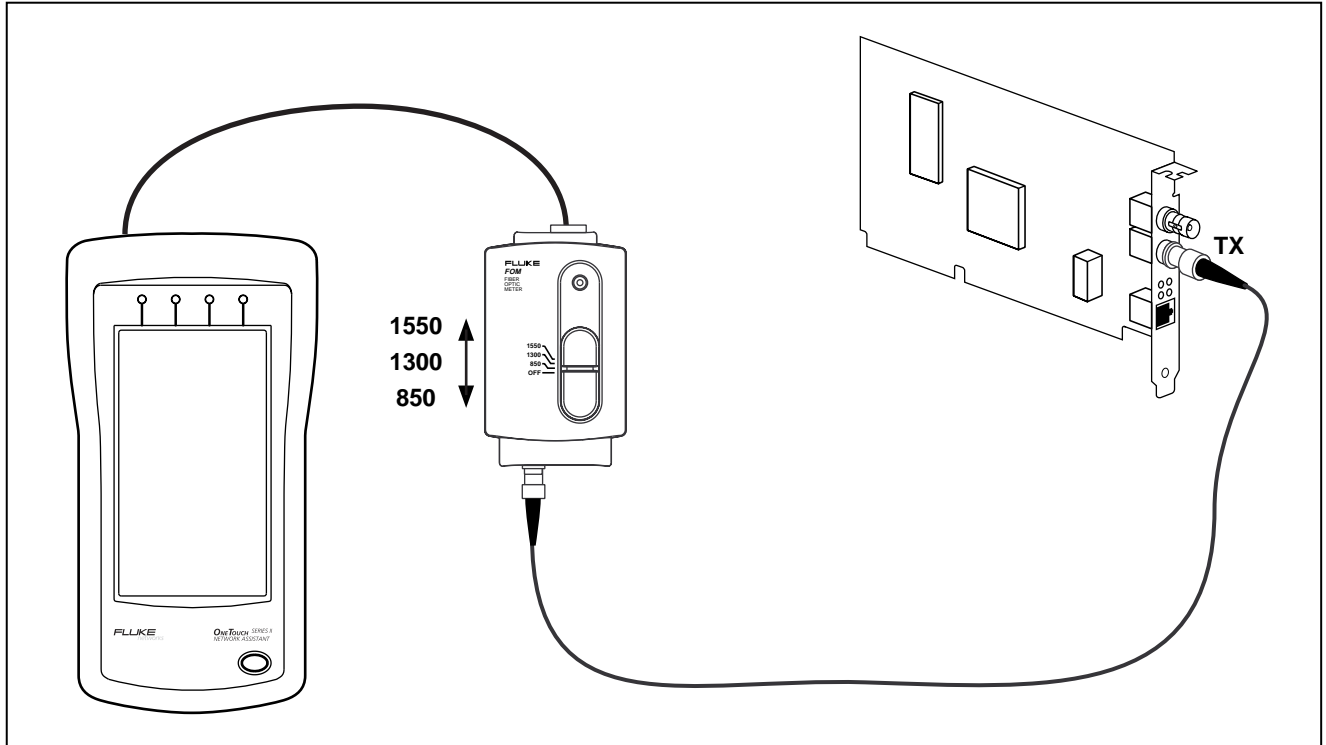


Figure 4-10. Connections for Measuring Output Power

ace410f.eps






# Chapter 5


## NIC/Hub Tests

### Introduction

The  (**NIC/Hub Tests**) display provides access to the following tests:

- NIC Autotest
- Hub Autotest
- NIC Detector
- Flash Hub Port

If the Network Assistant has a valid network connection, it continues to monitor the network until one of these tests is executed.

From the Network Assistant top level display, press  (**NIC/Hub Tests**) to access the NIC/Hub Tests display (Figure 5-1).

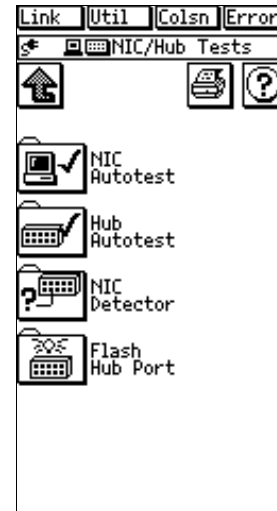



Figure 5-1. NIC/Hub Test

ace501s.bmp

**NIC Autotest**

In order for the NIC Autotest to complete, the NIC needs to be set up (power on, drivers running, etc.).

Press  (**NIC Autotest**) to verify the correct operation of an Ethernet (10 or 100 Mbps) adapter card.

The NIC Autotest determines as much as possible about the physical connection to the network adapter card by:

- Verifying the cabling from the desktop to the NIC.
- Checking for a 100 Mbps or 10 Mbps link pulse and configuring the Network Assistant accordingly.
- Confirming network connectivity by pinging the NIC.

The NIC Autotest displays the network address used by the device. It will also display packet errors if any are detected. For example, it will tell you if a packet with a bad CRC is transmitted by the NIC.

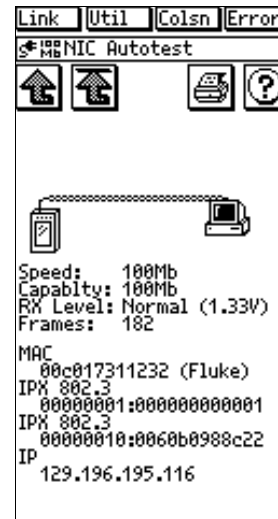
The NIC Autotest display is shown in Figure 5-2.

The following fields on the NIC Autotest screen indicate the results of the NIC test:

**RX Level (Normal/Marginal)**

*Normal:* The NIC signal level is within specification.


*Marginal:* The NIC signal level is not within specification. The problem is either excessive attenuation in the cable or a defective NIC card.



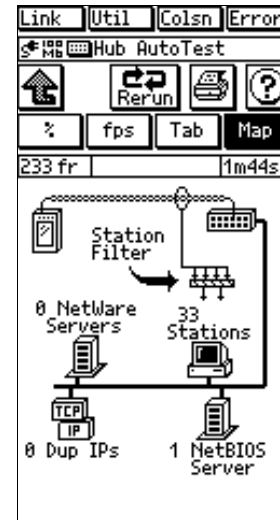
**Figure 5-2. NIC Autotest**

ace502s.bmp

### Hub Autotest

Press  (**Hub Autotest**) to verify the connectivity between the desktop and the Hub.

Hub Autotest checks the link pulse signal level and queries the NetWare and NetBIOS servers to determine the Hub's ability to send and receive frames. If successful, the Network Assistant displays the map that is identical to AutoTest (Figure 5-3).




ace505s.bmp

Figure 5-3. Hub Autotest Display

### Viewing Hub Capabilities

When the Network Assistant is connected to a hub and has an active link state, press the **Link** label at the top of the display to see the polarity of the received data. If your Network Assistant has hardware revision 2.2 or later, you

can also see the hub's transmission speed and its ability to perform half or full-duplex communication or auto-negotiation. To determine your hardware revision, press  from the top-level display.

If the polarity of the data on the cable's receive pair is reversed, the cable on the Autotest display flashes.


### **NIC Detector**

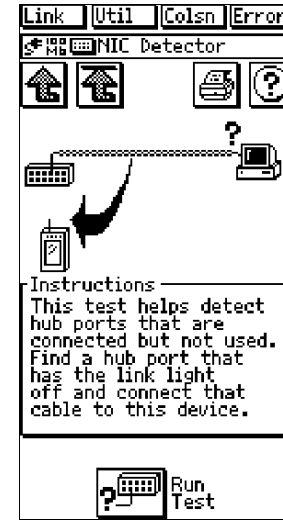
This test assists you in reclaiming unused hub ports. By looking at the LED status indicators on the hub you cannot determine whether a device is connected to the port or merely turned off. NIC Detector works by determining where there is any termination on the other end of the cable. If the Network Assistant detects an open cable, it will report that and the length of the cable.

#### *Note*

*The device at the far end does not have to be powered up.*

Locate a Hub port that you suspect is unused but that has a cable attached. Remove the cable from the Hub and connect the Network Assistant to it. Then run the NIC Detector test.



Press  (**NIC Detector**) to determine if the device is attached at the far end of the cable. The NIC Detector display is shown in Figure 5-4.



**Figure 5-4. NIC Detector**

ace504s.bmp

### **Flash Hub Port**

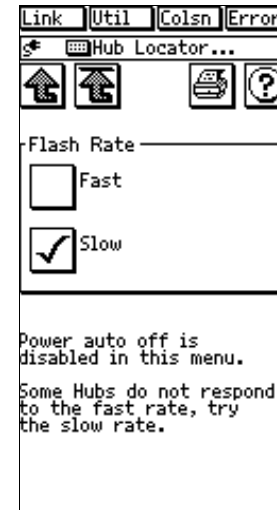
Press  (**Flash Hub Port**) to locate where a particular link connects to a hub. Connect the Network Assistant to the link you want to locate. Press , then select a flash rate (Figure 5-5). The Network Assistant sends either 1-second or 4-second link pulses

that flash the LED on the hub, indicating the port that the Assistant is connected to.

Note that some hub port link lights have a very slow response time. The Flash Hub Port feature may not work with these devices.

*Note*

*The Network Assistant will not automatically power off during Flash Hub Port.*



ace503.bmp


**Figure 5-5. Flash Hub Port Display**



# Chapter 6

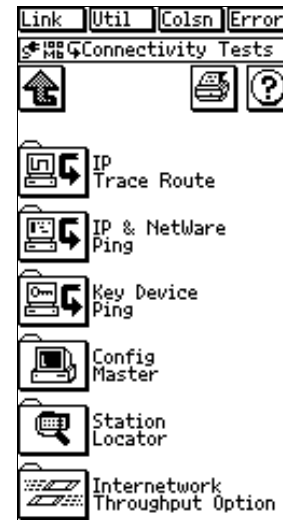
## Connectivity Tests

### Introduction

Connectivity Tests verify the IP or IPX connectivity between a specific resource or station and the Network Assistant. From the Network Assistant top-level display, press  (**Connectivity Tests**). The Connectivity Tests screen displays (Figure 6-1).

OneTouch Series II Pro features are provided on a trial basis. Read the online help in the OneTouch Link program for more information on enabling options. The following features are discussed in this chapter:



- IP Trace Route
- IP & NetWare Ping
- Key Device Ping (Pro)
- ConfigMaster™ (Pro)
- Station Locator (Pro)
- Internetwork Throughput Option (Chapter 7)

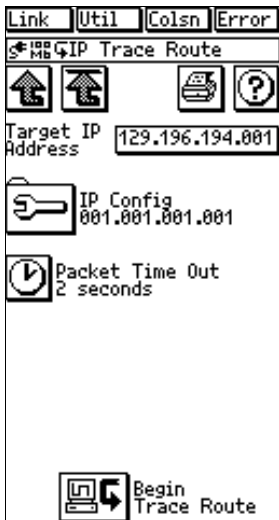


ace060s.bmp

Figure 6-1. Connectivity Tests Display

### IP Trace Route



From the Connectivity Tests display, press  (IP Trace Route) to access the Trace Route screen (Figure 6-2). Enter a target address by pressing the Target IP Address box and using the Keypad (see “Manually Entering Addresses” in Chapter 2). Press  to perform the Trace Route and view the results.



ace619s.bmp

Figure 6-2. IP Trace Route

### IP & NetWare Ping

From the Connectivity Tests display, press  (IP & NetWare Ping) to access the IP Ping Tests or NetWare Ping display (Figure 6-3). If you haven't done so already, press  (IP Config) to configure the Network Assistant addresses. You can enter addresses manually or use DHCP (read “Central Setup” in Chapter 2).




ace620s.bmp

Figure 6-3. IP & NetWare Ping Display



Press **IP Ping** or **NetWare Ping** as appropriate.

### Entering IPX Addresses

From the Connectivity Tests display, press  (**IP & NetWare Ping**), then press the (**NetWare Ping**) tab to access the NetWare Ping Configuration display (Figure 6-4).

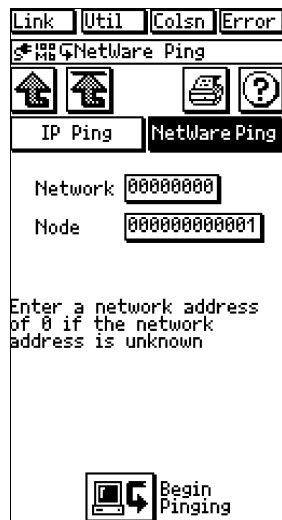


Figure 6-4. NetWare Ping

ace605s.bmp



The NetWare ping test requires only the IPX node address of the station you want to ping. If you want the Network Assistant to find the station's network address, enter 00000000 as the network address. Press an address box to access the keypad for entering IPX addresses.



Figure 6-5. IP Ping

ace604s.bmp

### **Conducting a Ping Station Test**

After you have configured the appropriate IP address, you can set the frame length from the by pressing  or  (Figure 6-6).

This sets the frame length of the ping packet between 64 and 1518 bytes. This is the total frame length.


Press  (**Begin Pinging**) from the IP Ping or NetWare Ping display (Figure 6-6) to start the test.

Figure 6-7 shows a sample IP Ping test results screen. Figure 6-8 shows an example of NetWare ping test results.



Ace620s.bmp

Figure 6-6. IP and NetWare Ping



ace606s.bmp

Figure 6-7. IP Ping Results



ace607s.bmp

Figure 6-8. NetWare Ping Results

If you have trouble making the IP Ping test work, verify that:


- The Source IP Address is correct for this subnet.
- The Target station is active.
- The Router IP Address is correct.



If you have trouble making the NetWare Ping test work, verify that:

- The station you are pinging has the Diagnostic Responder loaded.
- The node address you entered is correct.
- The network address you entered (if used) is correct.

### **Key Device Ping**

As part of your turn-on or repair procedures, you will need to verify connectivity to key network resources. Key Device Ping is a OneTouch Series II Pro option that enables you to rapidly verify the availability of important network devices. You can organize testing by business function (e.g., accounting, manufacturing, etc.), geographic locations (building 1, 2, etc.), device types (routers, servers, etc.), or other ways that fit your needs.

From the Connectivity Tests display, press  (**Key Device Ping**) to access the Key Devices display (Figure 6-9). You can also access Key Devices Station Detail


display by pressing  (**Tool Menu**). You can activate or deactivate a device quickly from the list by pressing the selection box  (left of each device).

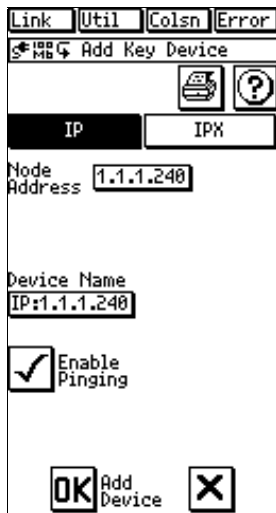
When you press an address box the Edit Key Devices screen displays (Figure 6-11) and enables you to edit address information.



**Figure 6-9. Ping Key Devices**

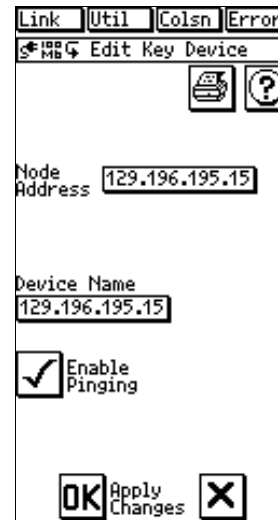
ace615s.bmp

Press  (**Add Device**) to add an IP or IPX address. The Add Key Devices screen (Figure 6-10) displays.



**Figure 6-10. Add Key Devices**

ace617s.bmp



**Figure 6-11. Edit Key Devices**

ace616s.bmp



For IP, enter the IP address of the device. For IPX, you must enter the Node and Network addresses. After you enter the address, the Device Name box displays the name assigned to the device (if available from the Station List).

To edit an existing name or address of a device, press the box that contains the item you wish to edit and make

the changes using the alphanumeric keypad (read “Central Setup” in Chapter 2). The device name you assign is for the purposes of the Key Device Ping function. You can also modify the name of a list by pressing the List Name box.

#### Note

*Renaming a device while using Key Device Ping does not modify the original name assigned to the device on the network (i.e., when the device is listed again under Station List, the original name will remain).*

To begin pinging the addresses in Key Devices List, press press  (**Begin Ping**). A set of boxes displays showing the status of the ping for each Key List. Press  (**Up One Level**) to stop.

### Interpreting Ping Test Results


In general, packets received should be at about 100%. Be aware that some devices, including routers, prioritize ICMP ping packets lower than other traffic, so some packet loss can be expected.

When evaluating the ping results it is important to consider the path taken by the packets. Sometimes the problem may be with an intermediate link.

### ConfigMaster

ConfigMaster™ is a OneTouch Series II Pro feature that provides network information you can use to properly configure a device. It lists NetBIOS, TCP/IP, and NetWare parameters (DNS, WINS, IP address range, subnet mask, default gateway, POP3 server, frame type, etc.). These parameters correspond to the **Network Properties** in Microsoft Windows and to certain e-mail settings. One or more of the following will be listed:

- |   |   |
|---|---|
| <input type="checkbox"/> IP subnet(s)                     | <input type="checkbox"/> POP3 server        |
| <input type="checkbox"/> IP address range for each subnet | <input type="checkbox"/> SMTP server        |
| <input type="checkbox"/> Subnet mask                      | <input type="checkbox"/> HTTP server        |
| <input type="checkbox"/> Default gateway                  | <input type="checkbox"/> NetBIOS domain     |
| <input type="checkbox"/> DNS server                       | <input type="checkbox"/> Frame type         |
| <input type="checkbox"/> WINS server                      | <input type="checkbox"/> IPX network number |

From the Connectivity Tests display, press  (**ConfigMaster**) to access the ConfigMaster tabular display (Figure 6-12). Press one of the tabs (**NetBIOS**, **TCP/IP**, or **NetWare**) to display the appropriate parameters as described below.

**NetBIOS** – The top two domains or workgroups, based on the number of stations, are listed along with the transport protocol used by the stations in that domain.

**TCP/IP** – Up to two devices in each category are listed. For subnets, the two most predominant are listed.

**NetWare** – The nearest file server is listed. This is a server that responded to the “Get Nearest Server” request. The network number and frame type are also listed.

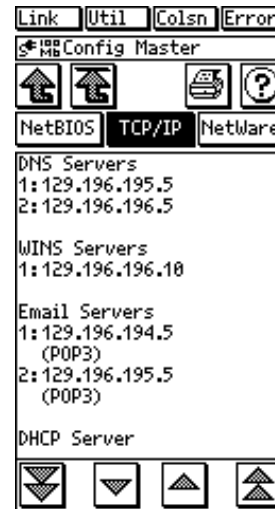




Figure 6-12. ConfigMaster

ace608s.bmp

## Station Locator

Station Locator is a OneTouch Series II Pro feature that determines the switch and switch port where a station is connected. It does this by searching for the MAC address of the station in the forwarding tables contained in the switch. Station Locator then displays pertinent switch status and configuration information with port identification and the location of a suspect station.

From the Connectivity Tests display, press  (**Station Locator**) to access the Station Locator tabular display (Figure 6-13) then the **Find MAC** or **Find IP** tab.


If you haven't done so already, press  (**IP Config**) to configure the Network Assistant addresses. You can enter addresses manually or use DHCP (read "Central Setup" in Chapter 2).



ace609s.bmp


**Figure 6-13. Station Locator**

### Find MAC

Enter the Target MAC address by pressing the address box and using the keypad. The lookup is then performed using the MAC address after you press  (**Find Node**).



### Find IP

Enter the Target IP by pressing the address box and using the keypad. Press  (**Find Node**). If you enter an IP address, the Network Assistant first tries to determine the MAC address of that station before performing the search. The actual search is performed using the MAC address. Although the IP address does not have to be on the same subnet as the Network Assistant, it does need to be on the local segment. It can determine the MAC address of the IP station only if it is on the local segment.

### Mode of Operation

Before Station Locator can search for a MAC address, it must first find all the switches on the network. Switch Discovery is performed automatically during the discovery process. When you run Station Locator, the Network Assistant searches the forwarding tables of each switch that it has discovered. It searches the Bridge MIB and some switches' private MIBs to get the port information.

In order for switch discovery to work properly, the Network Assistant needs to know the community string of the switches. You can configure the community strings in the SNMP Setup menu (read "SNMP" earlier in this chapter). If you change or add community strings, you can rerun Autotest or Network Health so the Network Assistant will use the new community strings.

### Results

The Network Assistant reports all switches that have the target MAC address in their forwarding tables. The target MAC address may appear in more than one switch. This can happen in a switch hierarchy environment. When a station on one switch communicates with a station on another switch, the MAC address of each station will appear in the forwarding tables of each switch.

The Network Assistant does not attempt to determine the switch to which the station is directly connected. To determine the switch to which the station is directly connected, you need to be familiar with switch hierarchy. If you can recognize the description or port number as an uplink port, then you can deduce that the station is not directly connected to that switch.

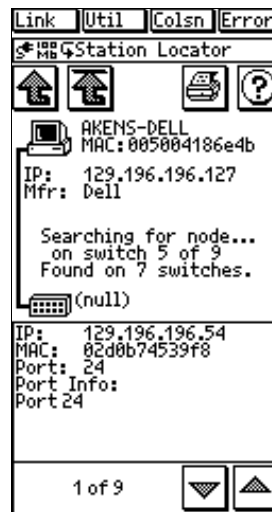
For each switch discovered, the following information is presented:

- Name** – SNMP name of the switch
- IP** – IP address of the switch
- MAC** – MAC address of the switch
- Mfr** - Manufacturer and model
- Port** – The port number on which the MAC address was found. Some switches encode the slot and port number into the port number. For example, a switch may represent slot 10/port 3 with a port value of

1003. Typically, if a switch does not have slots but looks like a hub, the port number will represent the actual port on the unit.

- **Port Info** – The interface description for the given port. Port Information is the textual description of the port on which the MAC address was found. This description is either the interface description of the port or a string constructed from the port information collected from the private MIB of the switch.

Figure 6-14 is a sample of the information provided by Station Locator.



**Figure 6-14. Station Locator Information**

ace610s.bmp

# Chapter 7

## ***ITO – Internetwork Throughput Option***

### ***Introduction***

The Internetwork Throughput Option (ITO) is a Fluke OneTouch™ Series II Network Assistant software option that is used to test enterprise-wide throughput or to evaluate line capacity. ITO's counterpart, xDSL, verifies the operation of digital subscriber lines.

ITO and xDSL throughput tests are identical in theory of operation and will be described in tandem in this chapter. The two use different terminology to reference their technology. Table 7-1 shows common terminology for ITO with its xDSL equivalent.

ITO/xDSL consists of two components:

**Throughput Test** – double ended test of network bandwidth which requires two OneTouch Series II Network Assistants.

**Traffic Generator** - tests traffic load capacity.

**Table 7-1. ITO and xDSL Terminology**

<b>ITO Term</b>	<b>xDSL Equivalent</b>
Local Unit	ATU-R Unit
	Subscriber-end Unit
Remote Unit	ATU-C Unit
	Central Office Unit

### **ITO/xDSL Throughput Test**

The following functions are covered in the Throughput section

- Theory of Operation
- Configuring the Remote Unit
- Local Unit Connections
- Configuring the Local Unit
- Results Displayed During the Test
- Final Test Results

### **ITO/xDSL Theory of Operation**

The ITO Throughput test refers to these two units as the local and remote units and the xDSL Throughput test refers to these two units as the subscriber-end unit (ATU-R) and the central office unit (ATU-C), respectively. Both options are double-ended tests of bandwidth which require two Fluke OneTouch Series II units to execute the test. Figure 7-1 shows the relationship between the local unit (ATU-R unit, for xDSL) and the remote unit (ATU-C unit, for xDSL).

For the ITO Throughput test both units must have current software versions loaded. Only the local unit must have the ITO option enabled.

Read the *OneTouch Series II Network Assistant Getting Started Manual* (P/N 1595893) and the OneTouch Link

program online help for more information on enabling options.

#### *Note*

*For the best operation, it is recommended that you update all of your Network Assistants' xDSL software version 4.50, or later.*

For the ITO Throughput test, a second, unattended Network Assistant (the remote unit) is used as a remote traffic source. For the xDSL Throughput test, a second, unattended Network Assistant (the ATU-C unit) is used as a remote traffic source. The subscriber-end unit (ATU-R for xDSL) is used to configure the test, execute the test, and display the test results.

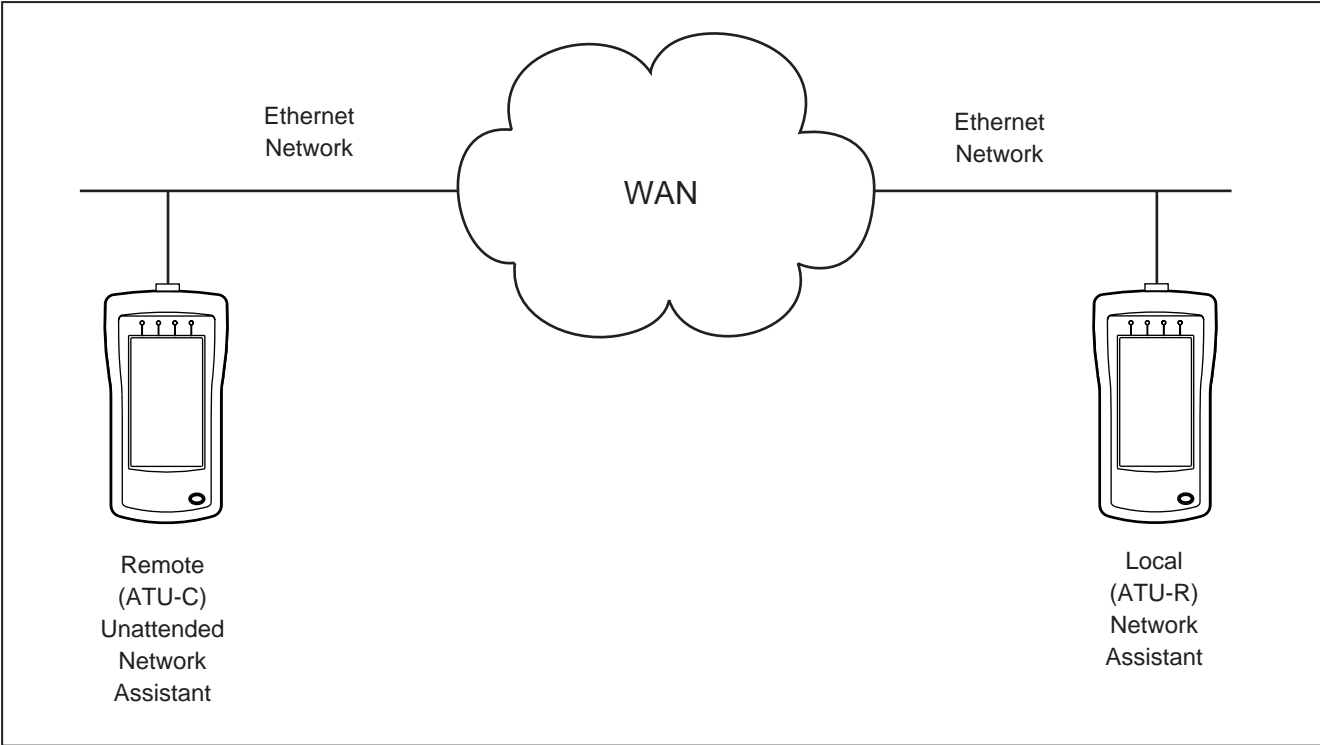


Figure 7-1. Local and Remote Units

ace702f.eps

### Basic Operation

For the ITO and xDSL Throughput Tests, starting the test causes the following actions:

1. The local unit (ATU-R for xDSL) sends an ARP request to the remote unit (ATU-C for xDSL) specified in its **Remote IP Address (Target ATU-C IP)** in xDSL) and waits for a response to that request.
2. After the ARP response is received, the local unit (ATU-R for xDSL) requests the remote unit (ATU-C for xDSL) to generate traffic using the local unit's (ATU-R for xDSL) user-configured duration, data pattern, rate, and frame length. The local unit (ATU-R for xDSL) waits for the remote unit (ATU-C for xDSL) to acknowledge the receipt of the traffic generation request.

The number of frames per second for the upstream and downstream bit rates is also calculated and displayed. The Ethernet preamble and inter-frame gap are used in this calculation and the number of frames per second is rounded up.

3. After the remote unit (ATU-C for xDSL) acknowledges the receipt of the traffic generation request, both units zero their counters and setup for

tracking the number of packets received from the other unit. Then, both units generate the user-configured traffic for the specified duration. The traffic generated is IP level data-grams, which allows routing. Both units transmit traffic simultaneously.

4. After the user-configured duration, the local unit (ATU-R for xDSL) requests the remote unit (ATU-C for xDSL) to send the number of packets counted from the local unit (ATU-R for xDSL). Knowing the number of packets sent and received from the remote (ATU-C for xDSL) and itself, the local unit (ATU-R for xDSL) calculates and displays the results.

### Conducting a Throughput Test

The Throughput Test is part of the Internetwork Throughput Option (ITO) or xDSL. The Throughput Test is a double-ended test of line or network bandwidth that requires two Network Assistants. After configuring each unit, you connect the remote and local units to your network in locations that allow you to test between the two units. Figure 7-2 shows the relationship between the local unit (ATU-R unit, for xDSL) and remote (A, B, C, or D) units (ATU-C unit, for xDSL). Figure 7-3 shows the equivalent connections for xDSL.

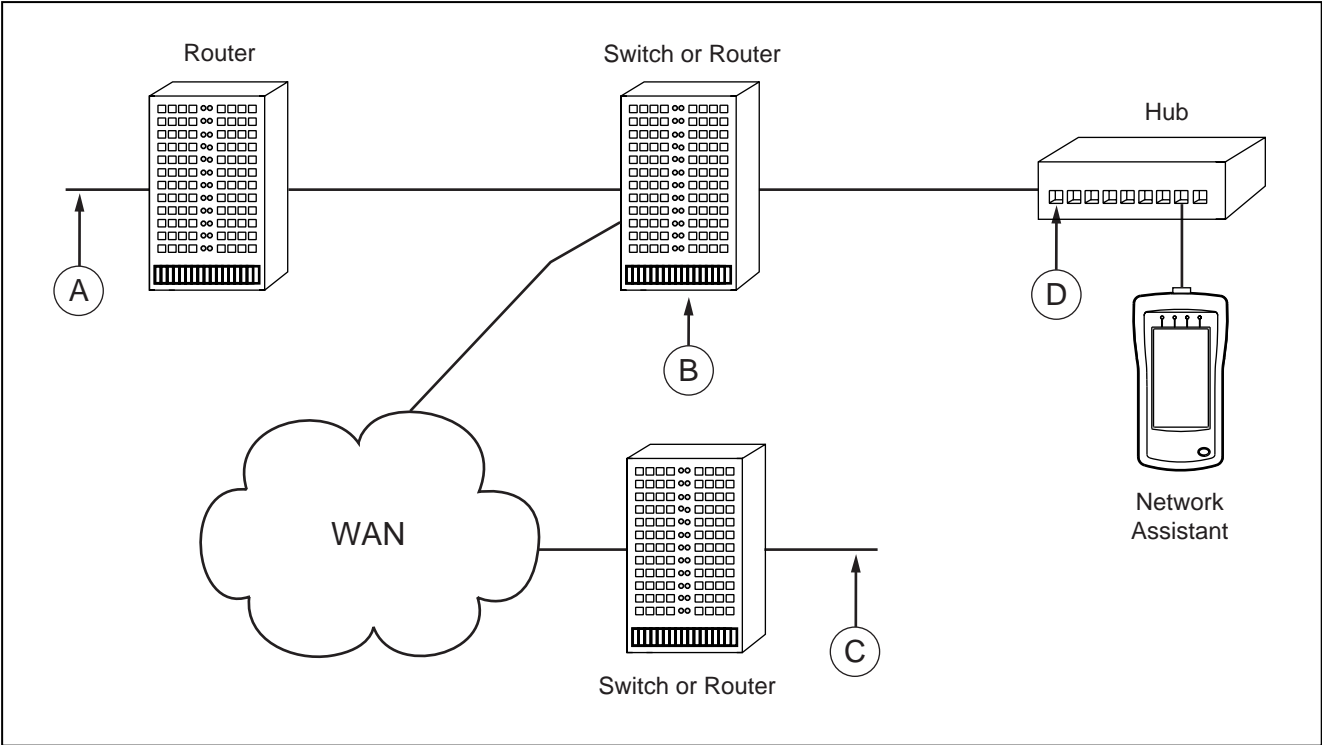
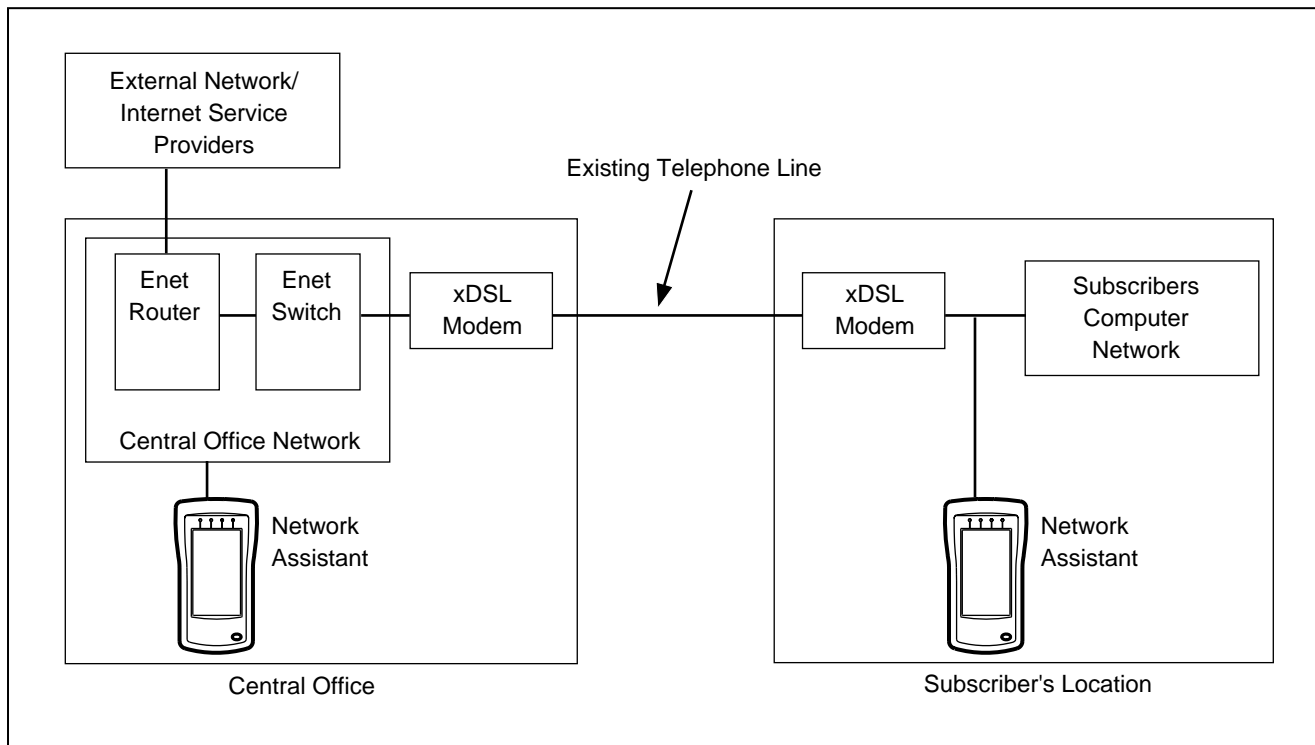


Figure 7-2. ITO Local Unit and Possible Remote Unit Locations (A, B, C, or D)

ace703f.eps



**Figure 7-3. xDSL Test Connections**

ace710f.eps



The test allows Ethernet to Ethernet testing of any link. A link can be wireless, routed, transparent LAN service, or asymmetric service (such as xDSL or cable modems).

The ITO Throughput test requires both units to have updated software. Only the local unit must have the ITO option enabled. Read “Updating Software” in the *OneTouch Series II Getting Started Manual* for more information.

The following are some of the possible ways to use the Throughput Test:

- ❑ Test end-to-end WAN/LAN throughput
- ❑ Test pattern, frame size, or rate sensitivity for network devices such as modems, FRADS, hubs, switches, or routers.
- ❑ Compare your current WAN capacity to a Service Level Agreement (SLA).
- ❑ Test or evaluate equipment on the bench



### *Connecting and configuring the Remote Unit*

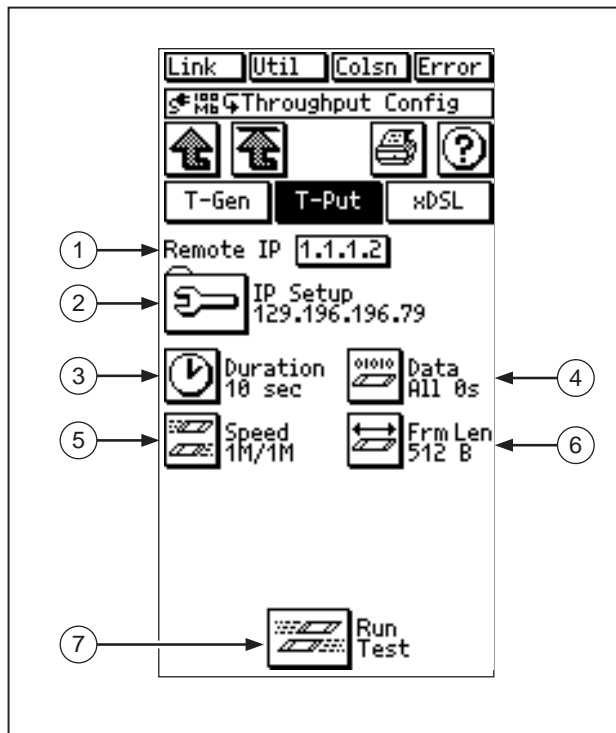
All you have to do with the remote (ATU-C Central Office unit for xDSL) Network Assistant is to connect its AC adapter, connect it to the network, and enter and set its IP address as described in Chapter 6. Figure 7-5 shows the connections for xDSL.

Once a valid IP address is set, manually or through DHCP, the remote unit is designed to remain unattended and to respond to any local unit’s request to participate in the testing. The **Remote IP Address** parameter on the local unit must be configured with the remote unit’s source IP address.

### *Connecting and configuring the Local Unit*

At the local (subscriber-end for xDSL) end, connect a Network Assistant to the desired segment. Figure 7-6 shows a sample connection. For xDSL, connect the Network Assistant to the Ethernet port on the xDSL modem.

To configure Network Assistant at the local end, press  (**Connectivity Tests**) from the top-level display then press  (**Internetwork Throughput Option**). Select either the **T-Put** or **xDSL** tab to access the corresponding menu.



ace704f.eps

Figure 7-4. Local Unit Configuration Display for Throughput Test

Note

For xDSL, the central office unit only requires you to enter an IP address. If the Network Assistant's Source IP Address is not set correctly for the network segment that it will be attached to, you must set it prior to performing any tests.

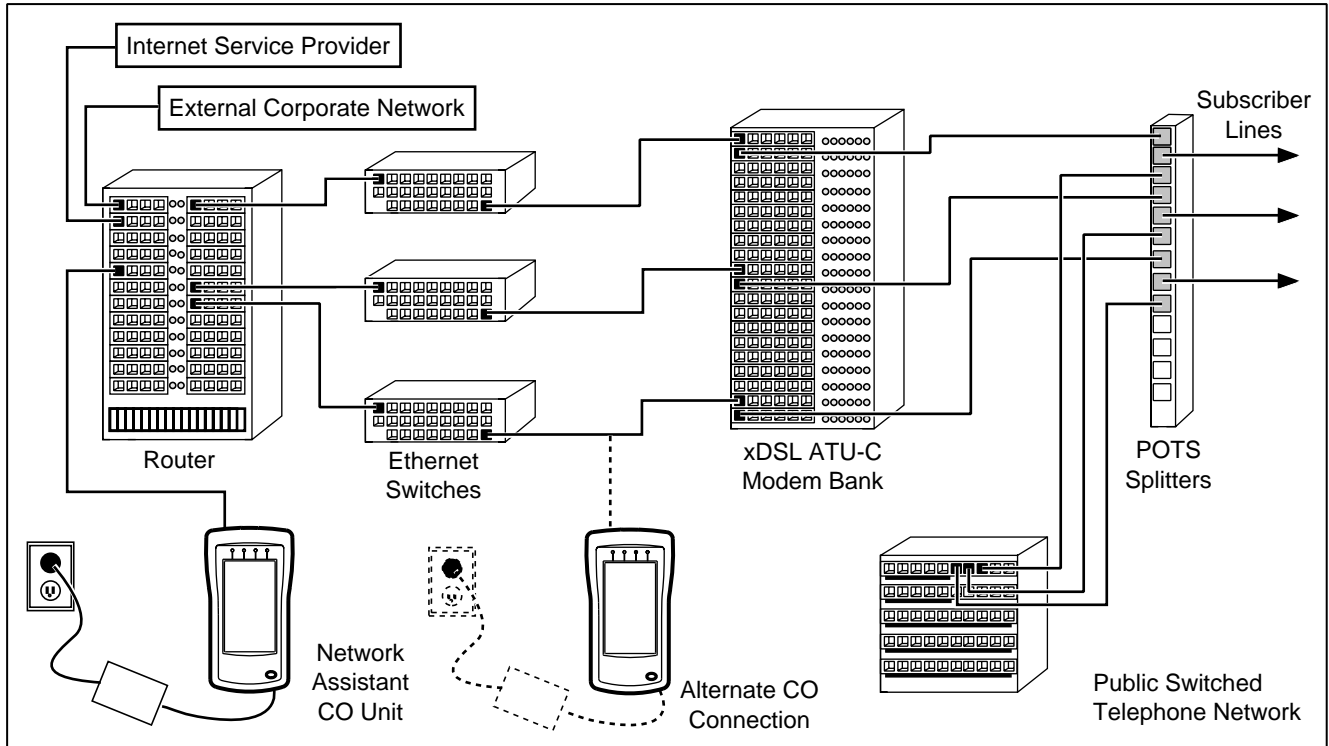
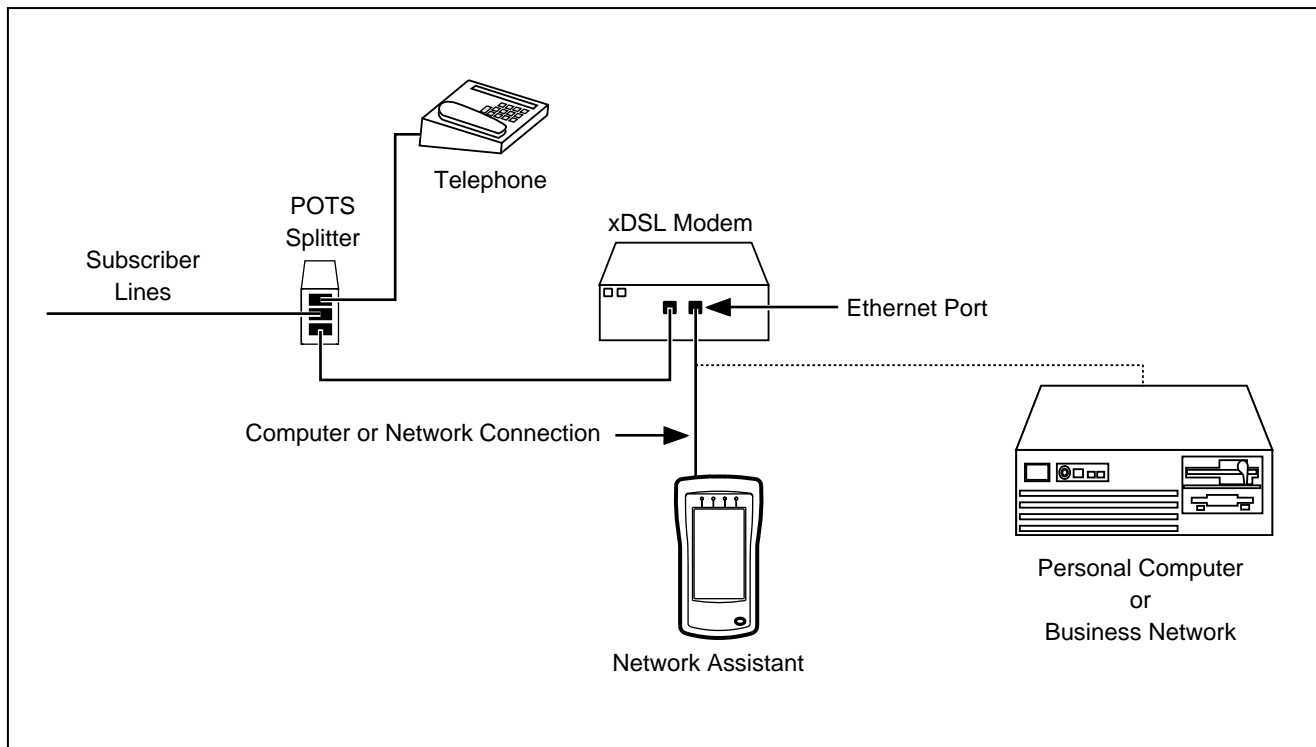





Figure 7-5. xDSL Central Office (Remote) Connections


ace712f.eps



**Figure 7-6. xDSL Subscriber-end Connections**

ace711f.eps

1. **Remote IP Address** Enter the source IP address of the Network Assistant at the remote end by pressing the **Remote IP** box. For xDSL, enter the **Target ATU-C IP Address**. Enter the address with the keypad then press **OK**.
2.  **IP Config** Enables you to enter the IP address for the local (this) unit. Select the method for configuring the IP Address (**Manual** or **DHCP**). See Chapters 2 and 6 for more information.
3.  **Duration** Select 2, 10, 30, 60, 120 or 300 seconds, 1 hr, 12 hrs, or 18hrs as the duration of the test.
4.  **Data PRBS** Select to send all zeros (All 0s), all ones (All 1s), alternating ones and zeros (Alt 1/0), or a Pseudo-Random Bit Sequence (PRBS). The PRBS pattern simulates normal data traffic.

5.  **Speed**

Select from the following upstream (to remote unit or central office for xDSL) and downstream (from remote unit) speeds to be tested:

#### ITO Speed Parameters

- ISDN 128 Kbps, T1 1.544 Mbps, E1 2.048 Mbps, and 1 Mbps/1 Mbps

#### XDSL Speed Parameters

- ANSI Asymmetrical Rates: 64 Kbps/1.5 Mbps, 160 Kbps/3 Mbps, 384 Kbps/4.6 Mbps, 640 Kbps/6 Mbps, 1 Mbps/1 Mbps.
- Auto:** Tests a range of speeds to determine the operating speed of RADSL modems. The following additional icons are displayed:

-  **Start at**

Select the lowest speed for the range of downstream rates to be tested.



**Stop at**

Select the highest speed for the range of downstream rates to be tested.



**Upstream**

Select the speed of the upstream traffic generated during the test.



**Incr by**

Select the increment size of the downstream speeds within the range you defined with the **Start at** and **Stop at** selections. The test increments the downstream speed and continues testing only if the channel passes 95% of the transmitted data at the current speed.

- User 1 through User 4:** Allows you to define your own upstream and downstream rates.



The total upstream and downstream rates must not exceed the values listed below:

**10 Mb**

<u>Frame Size</u>	<u>Max Bps</u>
64	37Mbps
128	64Mbps
256	78Mbps
512	87Mbps
768	87Mbps
1024	91Mbps
1280	93Mbps
1518	85Mbps

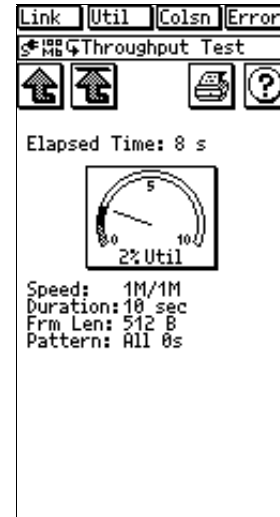
**100 Mb**

Frame Size	Max Bps
64	32.8Mbps
128	65.5Mbps
256	75.8Mbps
512	86.0Mbps
768	86.0Mbps
1024	90.1Mbps
1280	92.2Mbps
1518	85.0Mbps

6.  Select from the following RFC 1242 frame sizes: 64, 128, 256, 512, 768, 1024, 1280, and 1518 bytes.  
**Frm Len**
7.  After entering the above parameters, press **Run Test** to start the test.  
**Run Test**

**Results Displayed During the Throughput Test**

While the Throughput Test is running, the display (Figure 7-7) shows the elapsed test time, current network utilization (the meter), and the test parameters that were selected on the Throughput Test configuration display. The needle indicator on the Utilization meter shows total network utilization, which includes both the generated traffic and any other traffic present on the network.



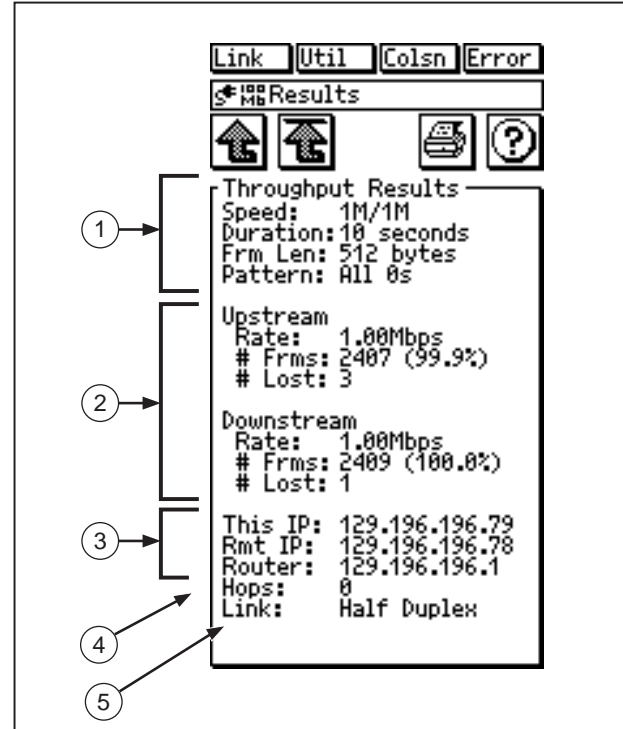
ace705s.bmp

**Figure 7-7. ITO Results Shown During the Test**

**Final Test Results**

When Throughput Test is complete, the Network Assistant displays the final results. Figure 7-8 shows an example of final Throughput Test results screen, which includes the following information:

1. The first four items show the upstream and downstream test speeds (**Speed**), the duration of the test (**Duration**), the frame length (**Frm Len**), and the data pattern (**Pattern**) as selected on the Throughput Test configuration display.
2. The **Upstream** and **Downstream** rates show the actual data upstream and downstream transmission rates used during this Throughput Test excluding the Ethernet overhead of preamble and inter-frame gap. The number of frames (**# Frms**) shows the number of frames successfully transmitted and the percentage of successful transmissions. The number of frames lost (**# Lost**) shows the number of frames lost during transmission.
3. The bottom of the display shows the addresses used for the local unit (**This IP** or **ATU-R IP** for xDSL), the unit at the remote end (**Rmt IP** or **ATU-C IP** for xDSL), and the router (**Routr IP --** if any).
4. **Hops** are the number of routers (hops) between the remote unit and the local unit.
5. **Link** displays duplex level: Half or Full.



ace706f.eps

**Figure 7-8. Final ITO Throughput Test Results**



### ITO/xDSL Traffic Generator

Traffic Generator lets you generate network traffic to see how your network responds to varying traffic loads. Traffic Generator is available in trial mode. Read the *OneTouch Network Assistant Getting Started Manual* (P/N 1595893) and the OneTouch Link program online help for more information on enabling options.

The following Traffic Generator modes are available and are covered in this section:

- MAC Mode
- IP Mode
- Ping Mode

The following are some of the possible ways to use Traffic Generator in MAC or IP mode:

- Test for errors on a segment by loading it to a predetermined level of traffic
- Test network error reporting by generating bad frames (such as short or jabber frames)
- Test single ended throughput by monitoring with a remote device
- Verify router/switch/probe RMON and SNMP interface statistics
- Simulate additional users on a LAN

The following are some of the possible ways to use Traffic Generator in Ping mode:

- Verify that a drop-to-network connection can pass a high rate of traffic without having to do a cable test
- Identify bottlenecks by successively pinging devices along the suspect path
- Stress a targeted PC with network activity
- Test WAN/LAN's two way throughput using a single Network Assistant
- Test symmetrical throughput of WAN links

#### Caution

**Traffic Generator can generate enough traffic to saturate a 10 MB or 100 Mb Ethernet network. Take care when using Traffic Generator.**

Figure 7-9 shows the Traffic Generator setup display.

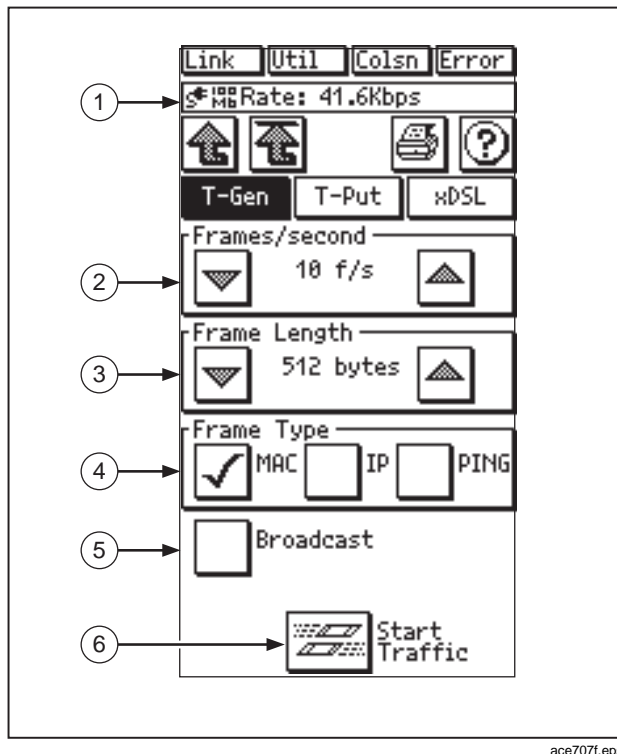


Figure 7-9. Traffic Generator Setup Display

1. **Rate** indicates the current Traffic Generator bit rate excluding the Ethernet overhead of preamble and inter-frame gap.
2. Use the arrow icons to set the number of frames transmitted per second.
3. Use the arrow icons to set the frame length.
4. Select the **Frame Type** as **MAC** (Media Access Control), **IP**, or **PING**. Refer to the following sections on Traffic Generator modes for more information.
5. Select **Broadcast** (only available for a Frame Type of MAC) to transmit traffic as broadcast or do not select it to transmit traffic as unicast.

If you selected a Frame Type of IP or PING, the **Broadcast** selection changes to **Target IP Address** allowing you to specify an IP address by pressing the box and then entering the address from the displayed keypad.








6. Press  (**Start Traffic**) to start generating traffic.

Press  (**Stop Traffic**) to stop the Traffic Generator.

## MAC Mode

Traffic Generator's MAC mode allows you to transmit traffic on the local segment. You can transmit unicast or broadcast packets.

To run Traffic Generator in the MAC mode, do the following:







1. Connect the Network Assistant to your network.
2. Press  ( **Connectivity Tests**) from the top-level display. Press  **Internetwork Throughput Option**.
3. Select the **T-Gen** tab.
4. Press  or  to configure **Frames/second**.
5. Press  or  to configure **Frame Length** as 60, 64, 128, 256, 512, 768, 1024, 1280, 1518, or 1520 bytes.
6. Select **MAC** as the frame type.
7. Select **Broadcast** if you want Traffic Generator to transmit broadcast traffic. Otherwise the transmitted traffic is unicast to 00c017310000 (Fluke - 310000), which is an unused MAC address.
8. Press  (**Start Traffic**) to start generating traffic.

Press  (**Stop Traffic**) to stop the Traffic Generator.

## IP Mode



Traffic Generator's IP mode allows you to transmit traffic to a specific device or network. The target device can be on the other side of a router.

To run Traffic Generator in the IP mode, do the following:

1. Connect the Network Assistant to your network.
2. Press  (**Connectivity Tests**) from the top-level display.
3. Press  (**Internetwork Throughput Option**).
4. Select the **T-Gen** tab. The Traffic Generator screen displays.
5. Press  or  to configure **Frames/second**.
6. Press  or  to configure **Frame Length** as 60, 64, 128, 256, 512, 768, 1024, 1280, 1518, or 1520 bytes.

### Note

*The illegal sized frames of 60 and 1520 bytes will not pass through a router and may not pass through a switch.*

7. Select **IP** as the frame type.
8. Configure the **Target IP** box by pressing the box and entering the address from the displayed keypad.
9. Press  (**Start Traffic**) to run Traffic Generator.  
Press  (**Stop Traffic**) to stop the Traffic Generator.

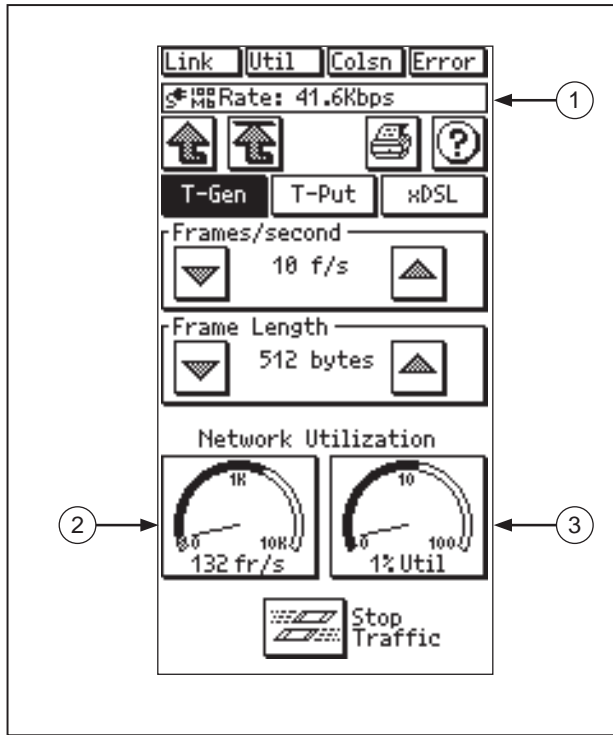
The generated traffic for IP Mode consists of an IP frame containing all zeros in the data field.

Traffic is transmitted to the specified Target IP Address. If the Target IP Address specifies a station on the local segment, the station must respond to an ARP request sent by the Network Assistant before traffic generation is started. If the Target IP address specifies a non-local station, the default router must respond to an ARP request sent by the Network Assistant before traffic generation is started.

### *MAC and IP Mode Results*

Traffic Generator displays MAC and IP mode results as it is running. You can adjust **Frames/second** and **Frame Length** while Traffic Generator is running to see the effect of traffic loading on your network (MAC mode) or a station (IP mode).

Two meters show the overall network utilization. One meter shows the current measured frame rate (in frames per second) and the other meter shows the utilization percentage. Figure 7-10 shows MAC or IP mode sample results.



ace708f.eps

Figure 7-10. MAC or IP Mode Sample Results

1. **Rate** is the raw data rate, excluding the Ethernet framing overhead (preamble and inter-frame gap).
2. This gauge shows the Network Assistant's Traffic Generator transmission rate.
3. This gauge shows the Ethernet Utilization for all traffic in the current collision domain. It does not include the minimum inter-frame gap.







### Ping Mode

Traffic Generator's Ping mode allows you to rapidly transmit ICMP Echo Request packet traffic to a specific device or network. The target device can be on the other side of one or more routers. The Network Assistant does not wait for a response before transmitting the next ICMP Echo Request. The ICMP Echo Request sets the don't fragment bit in the IP header.

### Caution

**Using Traffic Generator in Ping mode can generate enough traffic to stress or saturate a 10 MB or 100 Mb Ethernet station. Take care when using Traffic Generator in Ping mode.**



To run Traffic Generator in Ping mode, do the following:

1. Connect the Network Assistant to your network.
2. Press  (**Connectivity Tests**) from the top-level display.
3. Press  (**Internetwork Throughput Option**).
4. Press the **T-Gen** tab.
5. Press  or  to configure **Frames/second** to the desired amount.
6. Press  or  to configure **Frame Length** as 60, 64, 128, 256, 512, 768, 1024, 1280, 1518, or 1520 bytes.

#### Note

*The illegal sized frames of 60 and 1520 bytes most likely will not be responded to by remote devices.*

7. Select **PING** as the frame type.
8. Configure the **Target IP Address** box by pressing the box and then entering the address from the displayed keypad.

9. Press  (**Start Traffic**) to run Traffic Generator. Traffic is transmitted to the specified Target IP Address (station or network).
10. Press  (**Stop Traffic**) to stop Traffic Generator.

Traffic is transmitted to the specified Target IP Address (station or network).

#### Ping Mode Results

Traffic Generator displays Ping mode results as it is running. You can adjust **Frames/second** and **Frame Length** while Traffic Generator is running to see the effect of traffic loading on your network or on a station.

Two meters show the Ping mode results. One meter shows the overall network traffic (in frames per second) and the other meter shows the rate of Echo Response packets received from the target device. Figure 7-11 shows Ping mode sample results.

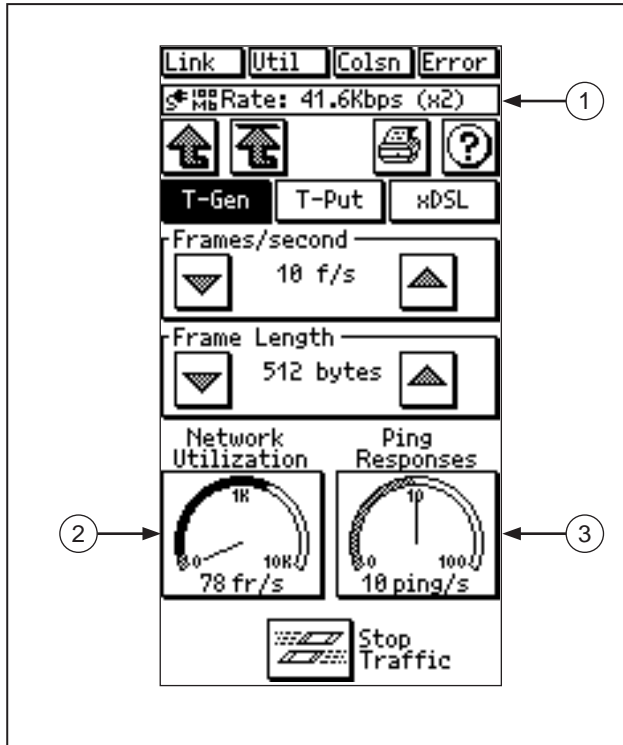


Figure 7-11. Ping Mode Sample Results

ace709f.eps

1. **Rate** is the raw data rate, excluding the Ethernet framing overhead (preamble and inter-frame gap).
2. **Network Utilization** – This gauge shows the Network Assistant's Traffic Generator transmission rate.
3. **Ping Responses** – This is the response rate (responses per second) received from the target device.





# *Appendices*

<b>Appendix</b>	<b>Title</b>	<b>Page</b>
	<b>Specifications.....</b>	<b>A-1</b>
	<b>Basic Maintenance.....</b>	<b>B-1</b>
	<b>Web Remote Control.....</b>	<b>C-1</b>
	<b>Glossary.....</b>	<b>D-1</b>
	<b>SNMP Discovery .....</b>	<b>E-1</b>



# Appendix A Specifications

## **General Specifications**

<b>Media Access</b>	10Base-T and 100Base-TX.
<b>Cable Tests</b>	Length, wiremap, and split pairs.
<b>Ports</b>	Shielded Hub/NIC connector (RJ-45). Shielded Wiremap connector (RJ-45). RS-232C PC/Printer port (DB-9).
<b>Printers Supported</b>	HP LaserJet series.
<b>Interface</b>	Icon-based touchscreen display.

<b>Battery</b>	Removable/rechargeable NiMH battery, 2-hour life.
<b>Dimensions</b>	20.3 cm x 10.7 cm x 5.3 cm (8 in x 4.2 in x 2.1 in).
<b>Weight</b>	0.7 kg (1.7 lbs).
<b>Warranty</b>	One year. (Extended warranty available).
<b>LED Indicators (5)</b>	Link, Utilization, Collision, Error, and Battery Charge.
<b>Toner Frequencies</b>	Low: between 185 Hz and 200 Hz. High: between 350 Hz and 375 Hz.

**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 Universal AC Adapter for the Network Assistant has UL, CSA, and TÜV approvals or other approvals valid in the USA, Canada, and Europe.

**Electromagnetic  
Interference**                The Fluke OneTouch Network Assistant complies with German Law Vfg. 243.1991 when it is operated at least 28 meters from the boundary of the user's facility or in a screen room. Exempt for USA and Canadian emissions regulations if it does not interfere with licensed communications.

**Certifications**                **CE**

**Connection to public  
telephone network**        The Network Assistant should never be connected to the public telephone network.

# **Appendix B**

## **Basic Maintenance**

### **Service and Repairs**

To order parts, receive operating assistance, or get the location of the nearest Fluke distributor or Service Center, call:

U.S.A.: 1-888-993-5853

Canada: 1-800-363-5853

Europe: +31-402-678-200

Japan: +81-3-3434-0181

Singapore: +65-738-5655

Anywhere in the world: +1-425-446-4519

For operating assistance in the USA, call 1-800-283-5853. Visit the Fluke Networks web site at [www.flukenetworks.com](http://www.flukenetworks.com).

### **Maximizing Battery Life**

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

The greatest enemy of your battery pack is heat. Avoid charging your batteries when they are hot.

For example, the battery life will be shortened if you frequently leave the Network Assistant in a hot place, such as a car on a warm day, and then charge the batteries immediately upon returning to your office.

### **Cleaning the Touchscreen**

Clean the touchscreen by wiping it gently with a soft cloth or tissue moistened with isopropyl alcohol.

**Precaution for Shipment**

To protect the LCD Display when shipping the OneTouch Series II unit, please ensure that it is placed in its holster and in a protective case such as the Hard Carrying Case.

**Replacement Parts List**

<b>Part</b>	<b>Part No.</b>
Top Shell Assembly	1281913
Bottom Shell Assembly	603050
Button, On/Off	603057
Digital Assembly	662509
Analog Assembly	662517
LCD/Display	688330
Softcase	603115
Universal AC Power Adapter	616216
Battery Pack	615986
Cable Identifier 1	603065
Cable Identifier 2	616232
Cable Identifier 3	616235
Cable Identifier 4	616240
Cable Identifier 5	616257
Cable Identifier 6	616265

# Appendix C

## Web Remote Control

### **Introduction**

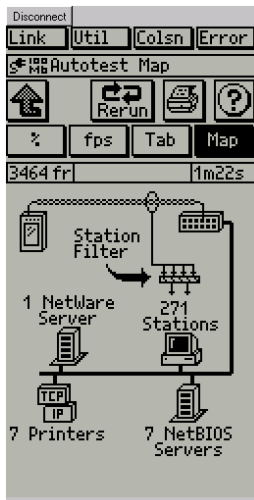
Web Remote Control is a OneTouch Series II Pro feature that enables you to view and interact with the Network Assistant attached to the network via a web browser. Your web browser software must be “Java-enabled.” If you do not have a Pro model, you will only be able to view the current screen with no interaction.

Enter the IP address of your Network Assistant in the web browser's address area. To find out the IP address, press the status line. The IP address will be listed. Enter it in the address area and press **Enter**. These options are available:

- View the Current OneTouch Screen
- Web Agent FAQ
- OneTouch News

### **View the Current Screen**

You must enter the password that you defined under Password Setup on the Network Assistant. Your web browser displays the Web Agent web page (Figure C-1) with the current screen displayed and the capability to interact with the screen via the web browser.



ace101s.bmp

**Figure C-1. Web Agent**

Enter the password `guest` (or your modified password) then press **Enter**. Press the desired buttons on the Web Agent display using the mouse and the resulting screens display on the web browser screen.

### **Web Agent FAQ**

This link addresses frequently asked questions (FAQ) about browser compatibility, configuration, and Network Assistant operation in relation to the Web Agent.

### **OneTouch News**

This link accesses the Fluke Network Solutions web page [www.flukenetworks.com](http://www.flukenetworks.com) to find out the latest about Fluke Networks products, get software downloads, etc.



## ***Appendix D Glossary***

### **10BASE2**

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

### **10BASE5**

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

### **10BASEF**

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

### **10BASE-T**

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

### **100BASE-TX**

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

### **802.2**

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

### **802.3**

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

### **Access Method**

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

### **Anomaly**

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

### **AppleTalk**

The set of protocols that define Apple Computer's networking specification.

### **ARP (Address Resolution Protocol)**

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

### **Attenuation**

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

### **Bandwidth**

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

### **BPS**

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

### **Bridge**

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 FFFFFFFF.

**Broadcast Storm**

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

**Bus Topology**

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

**Byte**

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

**Characteristic impedance**

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

**Client**

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

**Collision**

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

**Crossed Pair**

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

**Crosstalk**

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

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

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

### **dBm**

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

### **DECnet**

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

### **Destination Address**

The address of the station receiving a frame.

### **EIA568**

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

### **Encapsulation**

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

### **Ethernet**

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

### **Fast Ethernet**

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

### **FCS (Frame Check Sequence)**

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

### **Frame**

A frame is the transmission unit on a network. In Token Ring, a frame is the token joined with node data.

### **Full-Duplex**

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

**Half-Duplex**

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

**Hops**

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

**Hub**

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

**ICMP (Internet Control and Message Protocol)**

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

**IP (Internet Protocol)**

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

**IPX (Internetwork Packet Exchange)**

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

**Jabber**

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

**LAN (Local Area Network)**

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

**Late Collision**

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

**Layer**

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

### **Link Pulse**

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

### **Manufacturer Prefix**

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

### **Master Browser**

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

### **MBPS**

Millions of bits per second. See BPS.

### **Multicast**

Packets that are directed to a group of nodes rather than to a single node or all nodes. This is contrasted to a broadcast packet, which is directed to all nodes.

### **NEXT**

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

### **NIC (Network Interface Card)**

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

### **NVP (Nominal Velocity of Propagation)**

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

### **Packet**

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

### **Protocol**

A set of rules that machines must follow to exchange information on a network.

### **Primary Domain Controller**

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

### **Remote Collision**

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

### **Repeater**

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

### **RJ-45 Connector**

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

### **Router**

A router is a network-layer device that connects networks using like network-layer protocols. Routers can span different network topologies. For example, a router can interconnect 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.

### **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.

### **SAP (Service Advertising Protocol)**

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

### **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.

### **SNAP (Subnetwork Access Protocol)**

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

### **SNMP (Simple Network Management Protocol)**

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

### **Source Address**

The address of the station originating a frame.

### **Split Pair**

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

### **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 Reflectometry)**

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.

### **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.

### **Topology**

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

### **Uptime**

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

### **Transceiver**

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



### **Twisted Pair**

A pair of wires that 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.

### **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.



# ***Appendix E***

## ***SNMP Discovery***

### ***SNMP Discovery in OneTouch***

The following list details the default sequence of OneTouch IP discovery.

1. OneTouch sends a RIP1 Router Request to the IP broadcast address.
2. OneTouch sends a RIP2 Router Request to the IP broadcast address.
3. OneTouch sends an ICMP Router Solicitation to the IP broadcast address.
4. OneTouch sends an ARP Request to a proprietary IP address to detect Proxy ARP agents.
5. If the OneTouch IP was not acquired via DHCP, it sends a broadcast DHCP request.
6. For each community string configured and enabled, OneTouch sends an SNMP request for the System Table (Name and OID variables) to the IP broadcast address.
7. OneTouch sends a DNS query to the IP broadcast address.
8. OneTouch sends an SNMP request for the System Table (Name and OID variables) to the IP subnet broadcast address of each local IP subnet discovered and for each community string configured and enabled.

9. OneTouch sends an ARP request to each IP station discovered thus far.
10. OneTouch sends an SNMP request for the System Table (Name and OID variables) to each local IP host discovered that is not marked as responding to SNMP.
11. OneTouch sends an SNMP request for the Bridge MIB (NumPorts variable) to each local IP host discovered that is marked as responding to SNMP but not marked as a switch or a printer,
12. OneTouch sends an SNMP request for the Printer MIB (PrintGeneralReset variable) to each local IP host discovered that is marked as responding to SNMP but not marked as a switch or a printer,
13. Every 90 seconds, if a new local IP subnet has been detected go to step 8, otherwise go to step 9.

**NOTE**

*There are a number of network security software packages available that watch for activities such as port scanning and SNMP queries (i.e., they detect attempts to break into a network). Some of the normal IP discovery queries sent by OneTouch may trigger alarms in such software packages. For this reason, OneTouch only sends SNMP queries to devices determined to be on the LOCAL network, thus eliminating break-in alarms on remote networks discovered through promiscuous traffic monitoring.*

*You may not want to disable or modify the configuration of your security software when using OneTouch. OneTouch setup provides a configuration control that will prevent the automatic transmission of SNMP queries to any station during the IP discovery process.*

You can disable SNMP Discovery in OneTouch as follows:

1. At the OneTouch main menu press **Setup** to access the Central Setup screen (Figure E-1).
2. From the Central Setup screen press **Measurement Setup**.



Figure E-1. Central Setup

ace001s.bmp



Figure E-2. Security Setup

ace002.bmp

3. From the **Measurement Setup** screen press **SNMP Setup** to access the Security Setup screen (Figure E-2).
4. From the Security Setup screen uncheck **Enable SNMP Discovery**. When SNMP Discovery is disabled, the default IP Discovery process will not perform steps 6, 8, 10, 11, and 12.

You can still get OneTouch to send SNMP queries to hosts under your explicit direction while SNMP Discovery is disabled.

Press **Ping + SNMP** from the Tool Menu of a specific Station Detail display or press **TCP/IP** from the AutoTest display to view switches listed under the TCP/IP Devices.

# *Index*

## **—A—**

- AC adapter, universal, 1-2
- Accessory Kit (UTP)
  - Optional Equipment, 1-3
- Autotest
  - Device detection, 2-2
  - TCP/IP Devices, 2-5
- AutoTest
  - Device icons, 2-3
    - Hub, 2-5
    - Network Assistant, 2-4
    - Novell Server, 2-4
    - Popup windows, 2-3

## **—B—**

- Bad Frame Check Sequence (FCS), 3-7
- Battery
  - Battery Life
    - Maximizing, B-1
  - NiMH Rechargeable Battery Pack, 1-2

## **—C—**

- Cable Autotest, 4-2
- Cable basics, introduction to, 4-4
- Cable Identifier, 1-2
- Cable Identifier, 4-4
  - Set, 4-4
    - Optional Equipment, 1-2

- Cable Information, General
  - Cable Length, 4-7
  - Cable Termination, 4-8
  - Crossed Pair, 4-6
  - Reversed Pair, 4-6
- Cable Length
  - Cable Information, 4-7
- Cable length, test of, 4-2
- Cable Termination
  - Cable Information, 4-8
- Cable Tests
  - Cable Autotest, 4-2
  - Define Cable, 4-4
  - Toner, 4-4
  - Wiremap Cable, 4-2
    - Identifying Cables, 4-4
- Collisions, 3-7
- ConfigMaster, 6-8
- Connectivity Tests

Ping, 6-1  
Crossed Pair  
Cable Information, 4-6

## —D—

Define Cable  
Cable Tests, 4-4  
Device icons  
AutoTest, 2-3  
Hub, 2-5  
Network Assistant, 2-4  
Novell Server, 2-4  
Popup windows, 2-3  
Duplicate IPs, 2-13

## —E—

Environmental Requirements, A-2  
Equipment  
Optional, 1-2  
Supplied, 1-2

## —F—

Fiber Optic Cable, 4-10  
Find Router, 2-18  
Firmware, version, 1-2

Flash hub port, 5-4

## —G—

General Cable Information  
Cable Length, 4-7  
Cable Termination, 4-8  
Crossed Pair, 4-6  
Reversed Pair, 4-6  
Twisted Pair, 4-4

## —H—

Hub port locator, 5-4

## —I—

IP  
Duplicate, 2-13

## —J—

Jabbers, 3-7

## —M—

Maintenance, Instrument, B-1  
Manual, Users, 1-2

## —N—

NetWare  
file server list, 2-9  
ping station, 6-3  
print server list, 2-11  
Network Assistant  
Strap, 1-2  
Network Assistant  
Maintenance, B-1  
Optional Equipment, 1-2  
Softcase, 1-2  
Supplied Equipment, 1-2  
Touchscreen  
Cleaning, B-1  
Network Health, 3-1  
Meters  
Broadcasts, 3-5  
Collision, 3-5  
Error, 3-4  
Utilization, 3-4  
NIC/Hub Tests, 5-1  
NiMH Battery Pack, 1-2  
NiMH Rechargeable Battery Pack  
Optional Equipment, 1-2

## —O—

Optional Equipment, 1-2



**—P—**

Ping  
Results, 6-8  
Power cord, 1-2

**—R—**

Rechargeable Battery Pack (NiMH), 1-2  
Rechargeable Battery Pack (NiMH)  
Optional Equipment, 1-2  
Reversed Pair  
Cable Information, 4-6

**—S—**

Service and repairs, B-1  
Short frames, 3-7  
SNMP query, 2-8  
Softcase, Network Assistant, 1-2  
Software, version, 1-2  
Split Pair, 4-2  
Station detail display, 2-8  
Station Locator, 6-10  
Strap, 1-2  
Supplied Equipment, 1-2  
Switch Discovery, 6-10

**—T—**

Test Folders  
Cable Tests  
Cable Autotest, 4-2  
Define Cable, 4-4  
Toner, 4-4  
Wiremap Cable, 4-2  
Network Health, 3-1  
Meters  
Broadcasts, 3-5  
Collision, 3-5  
Error, 3-4  
Utilization, 3-4  
NIC/Hub Tests, 5-1  
Toner, 4-4  
Touchscreen  
Cleaning, B-1  
Twisted Pair, Basics, 4-4

**—U—**

Universal AC adapter, 1-2  
Users Manual, 1-2  
UTP Accessory Kit  
Optional Equipment, 1-3

**—V—**

Version number, software, 1-2

**—W—**

Wiremap Cable, 4-2  
Identifying Cables, 4-4

