User’s Guide

HP Internet Advisor LAN

Notice

The information contained in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

A copy of the specific warranty terms applicable to your product can be obtained from your local Sales and Service office.

Trademarks

HP is a registered trademark of Hewlett-Packard Company

Microsoft, MS, MS-DOS, Windows, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Product Support

If you have questions, concerns or need more information, call or contact us -
U.S.A. Technical Response Center - 1-800-698-0061,
on the Web - http://www.hp.com/go/internetadvisor,
by FAX - 303-754-4802,
or internationally by calling your local Sales and Service office.

Hewlett-Packard Company
Communications Measurements Division - Colorado
5070 Centennial Boulevard
Colorado Springs, Colorado 80919-2497

Contents

Introduction

Getting Started

Running Statistical Measurements

Running Decode Measurements

Running Application Measurements

Using The Expert Analyzer

Using the Event Log

Using the Capture Filters window

Using the Node/Station List Window

Using the Advisor's Utilities

Using Utilities in DOS

Using the FDDI Ring Manager

Glossary

Safety Information

Before you use this instrument, be sure to pay special attention to the "Safety" and "Warning" sections in this Manual. Failure to comply with the precautions or with specific warnings in this book violates safety standards of design, manufacture, and intended use of this instrument. Hewlett-Packard Company assumes no liability for the customer's failure to comply with these requirements.

Electric Shock Hazard. Do not remove the system covers. To avoid electric shock, use only the supplied power cords and connect only to properly grounded (3-pin) wall outlets.

Explosion Hazard. Do not operate in the presence of flammable gases.

Fire Hazard. For continued protection against fire hazard replace only with fuse of same type and rating.

Hazardous Material. Should the LCD be damaged the liquid crystal material can leak. Avoid all contact with this material, especially swallowing. Use soap and water to thoroughly wash all skin and clothing contaminated with the liquid crystal material.

Cleaning. To clean the instrument, use a damp cloth moistened with a mild solution of soap and water. *Do not* use harsh chemicals. *Do not* let water get into the instrument.

Product Damage. Do not use this product when:

- the product shows visible damage,
- fails to perform,
- has been stored in unfavorable conditions,
- or has been subject to severe transport stresses.

Make the product inoperative and secure it against any unintended operation. Contact your nearest Hewlett-Packard Sales office for assistance.

Warning Symbols Used in This Book:

Instruction book symbol: the product will be marked with this symbol when it is necessary for the user to refer to the instruction book in order to protect against damage.

A product marked with this symbol indicates it is a laser product. When necessary, this symbol will be included in the instruction book for the user to refer to in order to protect against personal injury and/or correct product handling.

Indicates potential for electrical shock.

WARNING An operating procedure, practice, etc. that, if not correctly followed could result in personal injury or loss of life.

CAUTION An operating procedure, practice, etc., which, if not strictly observed, could result in damage to, or destruction of, equipment or software.

Product Information

This is an Installation Category II product.

This is a Pollution degree 2 product.

This product is intended only for indoor use.

Conventions Used in this Book

NOTE An operating procedure, practice, or information of importance, separated form normal text.

Operating Restrictions

The following warnings and operating information are shown in French with the English translation.

MISE ENGARDE

Cet appareil répond aux normes de la «Classe de sécurité I» et est muni d'un fil de mise à la terre pour votre protection.

MISE ENGARDE

Pour prévenir les risques de choc électrique, la broche de mise à la terre du cordon d'alimentation ne doit pas être désactivée.

Restrictions d'utilisation

L'utilisateur se doit d'observer les mesures de précaution énumérées ci-dessous pour toutes les phases d'utilisation, de service et de réparation de cet appareil. Le fait de ne pas s'y conformer équivaut à ne pas respecter les mises en gardes spécifiques contenues dans ce manuel et constitue une violation des normes de sécurité relatives à la conception, la fabrication et l'utilisation prévue de cet appareil. La société Hewlett-Packard n'assume aucune responsabilité envers un client qui manquerait de se conformer à ces exigences.

Mise à la terre

Afin de minimiser les risques de choc électrique, le chÀssis et le cabinet de l'appareil doivent être mis à la terre. L'appareil est équipé d'un cordon d'alimentation muni d'une fiche homoloquée à trois lames, compatible c.a. La prise murale et la prise femelle de la rallonge électrique doivent respecter les normes de sécurité de la «Commision électrotechnique internationale» (IEC).

WARNING

This product is a Safety Class I instrument with a protective earth terminal.

WARNING

For protection from electric shock hazard, power cord ground must not be defeated.

Operating Restrictions

The following general safety precatuions must be observed during all phases of operation, service, and repair of this instrument. Failure to comply with these precautions with specific warnings in this manual violate safety standards of design, manufacture, and intended use of this instrument.

Grounding

To minimize shock hazard, the instrument chassis and cabinet must be connected to an electrical ground. The instrument is equipped with a three-conductor AC power cable compatible with an approved three-contact electrical outlet. The power jack and mating plug of the power cord must meet International Electrotechnical Commission (IEC) safety standards.

Environnement
Ne faites pas fonctionner cet appareil en présence de gaz inflammables ou de vapeurs dangereuses. L'utilisation de n'importe quel appareil électrique dans ces conditions constitue un risque élevé pour votre sécurité.

Service et ajustement
Des «tensions dangereuses» résident dans cet appareil. Par conséquent, le service et l'ajustement doivent être effectués uniquement par une personne qualifiée.

Ne remplacez pas de composantes lorsque le cordon d'alimentation est sous tension. Il pourrait y avoir présence de «tensions dangereuses» même lorsque l'appareil est déconnecté.

Ne faites pas de service interne ou d'ajustement sauf en présence d'une autre personne, capable de prodiguer les premiers soins et de pratiquer la réanimation.

Matiere dangereuse
Si l'affichage LCD est endommagé, la matière constituant les cristaux liquides peut se répandre. Eviter tout contact avec cette matière, et en particulier ne pas l'avaler. Utiliser de l'eau et du savon pour nettoyer soigneusement la peau et les vêtements qui auraient été contaminés par la matière constituant les cristaux liquides.

Service non autorisé
L'installation de pièces étrangères, ou toute modification apportée à l'appareil sans le consentement de Hewlett-Packard est formellement interdit. Le fait de procéder à de tels modifications sans autorisation pourrait entraîner l'annulation de la garantie de l'appareil ou de tout contrat de service.

Pour un service et des réparations autorisées, retournez l'appareil à un point de vente et service Hewlett-Packard.

Environment
Do not operate the instrument in the presence of flammable gases or fumes. Operation of any electrical instrument in such an environment constitutes a definite safety hazard.

Service and Adjustment
Dangerous voltages exist within this instrument. Service and adjustment of this instrument is to be performed only by trained service personnel.

Do not replace components with the power cable connected. Dangerous voltages may be present even when the power cable is disconnected.

Do not perform internal servicing or adjustment unless another person, capable of rendering first aid and resuscitation is present.

Hazardous Material
Should the LCD be damaged the liquid crystal material can leak. Avoid all contact with this material, especially swallowing. Use soap and water to thoroughly wash all skin and clothing contaminated with the liquid crystal material.

Unauthorized Service
The installation of substitute parts or the installation of any instrument modification not authorized by Hewlett-Packard is specifically forbidden. The performance of such unauthorized service can negate the instrument warranty or any maintenance agreements.

Return the instrument to a Hewlett-Packard Sales and Service Office for authorized service and repair.

Printing History

New editions are complete revisions of this book. Update packages may contain new or additional material and be released between editions. See the date of the current edition on the back cover of this book.

First Edition	Dec 1995	5964-0562
Second Edition	July 1996	5965-0124
Third Edition	Oct 1996	5965-0166
Fourth Edition	June 1997	5966-5373
Fifth Edition	Oct 1997	5967-1424
Sixth Edition	Nov 1998	5967-9414

1

Introduction

What's in this Chapter

The HP Internet Advisor LAN family of products includes Ethernet, Fast Ethernet, Token-Ring, and FDDI Advisors. The hardware for the different Advisors can be any of the following:

- a streamlined portable Internet Advisor - built in Ethernet or Token-Ring with an optional Fast Ethernet or FDDI undercradle
- an Internet Advisor - WAN with a LAN undercradle
- a ruggedized transportable Network Advisor (and attachable modules)
- Advisor PC cards for Ethernet or Token-Ring

Whatever form the hardware takes, all the Internet Advisors consist of measurements and applications to help you monitor, analyze, and troubleshoot your network.

There are many different applications that run on the Internet Advisor LAN. This manual discusses the basic operation of typical measurements involved in monitoring, troubleshooting, and analyzing your networks. Most measurements and techniques are similar across all network types. Where the procedure or measurements differ, an example is given for each.

This User's Guide covers the basic operating information for the Internet Advisor LAN. There is online help built into the Internet Advisor LAN. You can find specific information for the tests you are running in the area of the Internet Advisor LAN you are in. There is also a Glossary of terms.

NOTE

This User's Guide explains general procedures for operating the Internet Advisor LAN. Detailed instructions and field definitions for each measurement are found in that measurement's online help window

This chapter introduces you to the Internet Advisor LAN:

- The six top level windows
- Description of the different measurements

The Six Top Level Windows

The Internet Advisor LAN has six main or top level windows from which you can run measurements, generate node lists, set up filters, monitor events, and diagnose network problems. The top level windows are:

- Measurements
- Setup
- Node List
- Filters
- Utilities
- Event Log

When you start the Internet Advisor LAN, you can choose which top level window is open and ready for you to run a measurement. The other top level windows are iconized (shrunk into small graphical symbols and displayed in a reserved area at the bottom of the screen). You can explode these icons (de-iconize by double clicking the mouse) and use them whenever you want.

Starting the Internet Advisor LAN is described in detail in chapter 2, “Getting Started.”

The Internet Advisor LAN Quick Reference Card shows keyboard short cuts and a map of the top level windows to help you find the different functions at a glance.

The Measurements Window

The main purpose of the Measurements window is to let you select and run various measurements. These Measurements report information about your network, help you troubleshoot network problems, or show you the contents of packets on the network.

The Measurements window organizes measurements using a hierarchy of categories and subcategories similar to the way that DOS uses directories and subdirectories to organize files.

Refer to the section titled “Measurement Descriptions” later in this chapter for a list and description of the Internet Advisor LAN's measurements.

These are the general categories of measurements:

- Expert Analyzer
- Statistics
- Decodes
- Commentators
- Stimulus/Response Tests
- Network Discovery
- Screen Snapshots
- Troubleshooters
- Demo Tools

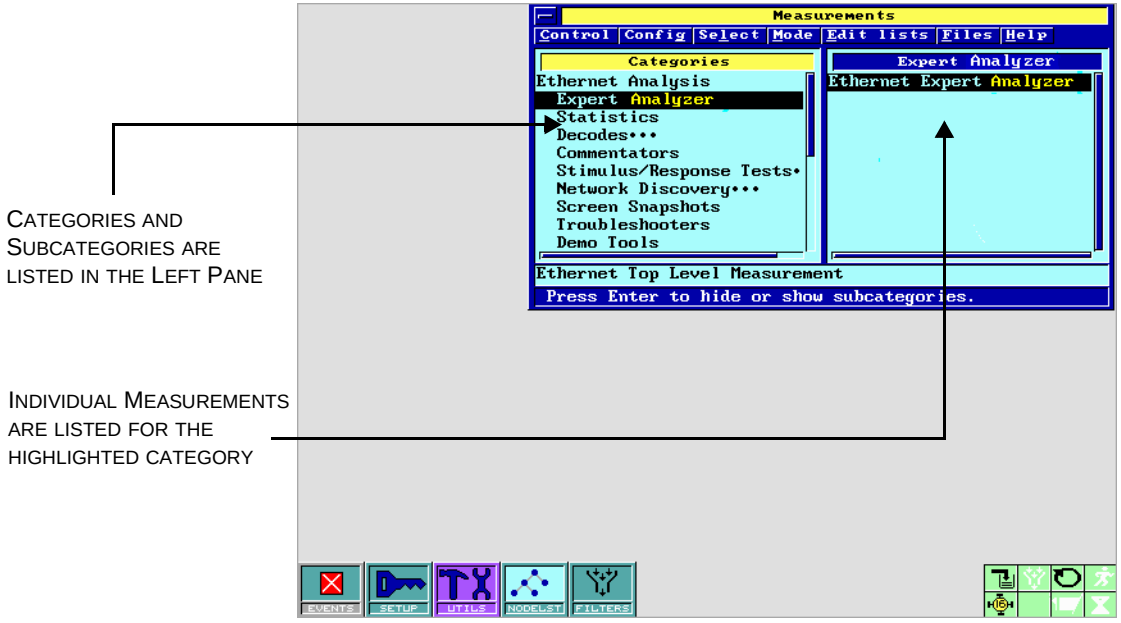


Figure 1-1: Measurements window

Expert Analyzer

The Expert Analyzer window is a measurement that gives you an overview of an Ethernet, Fast Ethernet, Token-Ring, or FDDI network's health. The Expert Analyzer automatically opens and runs specialized versions of other Internet Advisor LAN measurements, and then uses the results from these tests to present the data in graphical and numerical form.

In addition to the data displayed in the Expert Analyzer window, you can "drill down" to see more detailed information in additional windows. See the online help in the Expert Analyzer measurement for more information about the Expert Analyzer measurement.

Refer to chapter 6, "Using Expert Analyzer," for more information on using Expert Analyzer.

Statistics

The Internet Advisor LAN statistical measurements show you important information about a Ethernet, Fast Ethernet, FDDI, or Token-Ring network's overall performance or about particular nodes or stations.

For example, the Ethernet, Fast Ethernet, FDDI, and Token-Ring Summary Stats measurements use graphs, gauges, and pie charts to show information about the network's overall performance. Some of the information they show are the percentage of the network's capacity being used, the number and type of errors occurring, the mix of protocols on the network, and the number of stations or nodes on the network. You can choose four of the items from the Summary Stats window to plot together in the Trends Graphical display, or you can list four of the items in the Trends Tabular display. This lets you detect correlations between the items.

In addition to the data presented in the Statistics window, you can get more detailed information by "drilling down" to additional statistical windows.

There are several graphical and tabular node statistics measurements that identify critical users on the network, such as the nodes that are generating the most traffic (top talkers) or the nodes that are generating the most errors (top error sources).

The Vital Signs measurements provide a tabular list of significant events that may be preludes to network performance degradation or network failure. There are Vital Signs measurements for Ethernet, Fast Ethernet, Token-Ring, FDDI, Appletalk, DECNet, Novell, OSI, TCP/IP, and Vines protocols.

The Ethernet, Fast Ethernet, FDDI, and Token-Ring Top Talkers measurements list up to 50 nodes generating the most frames and how many bytes and frames they each are sending and receiving.

The Fast Ethernet, Ethernet Top Error Sources, FDDI Top Error Sources, and Token-Ring Top Error Reporters measurements list up to 50 nodes generating the most errored frames and how many and what type of errors they are generating.

The Node Stats (for Fast Ethernet and Ethernet) and the Station Stats (for Token-Ring or FDDI) graphically show you, in either bar or pie chart form, a variety of statistical information about 20 nodes or stations.

For Example. . . You can configure the Token-Ring Station Stats measurement to show the 20 stations sending source routed broadcasts, all stations broadcasts, functional address frames, and source routed frames.

. . . . . .

The Protocol Statistics measurement graphically shows statistical information for up to 20 protocols running on your network. You can look at data link layer protocols, the IP stack, Appletalk stack, Banyan Vines stack, DECNet stack, OSI stack, or Novell stack protocols. The measurement shows you number of frames, number of bytes, number of errors, and average frame length for each discovered protocol.

Refer to chapter 3, “Running Statistical Measurements,” for more information on statistical measurements.

Decodes

The Internet Advisor LAN provides a set of decodes for many Ethernet, Fast Ethernet, FDDI, and Token-Ring protocols such as 802.2, Apollo Domain, AppleTalk, Banyan Vines, DECNet, Novell, XNS, 3COM, SNA, TCP/IP, and IBM PC.

Decode measurements interpret the data in frames according to a protocol so you can examine the contents of the frames. There are three decode formats:

- The summary format shows a one line overview of each decoded frame.
- The detailed format shows the decode for each field of each frame.
- The data format shows the raw hexadecimal data.

When the Decodes category is selected, you can choose a stack decode measurement which shows all the protocols working in the selected networking environment.

For Example. . . In the Novell Stack Decode, fields in the IPX, SPX, and NCP protocols are all decoded and displayed.

You can also select an individual layer protocol decode that decodes only the selected protocol.

When you start a decode measurement, a window opens showing the data in the detailed format. From the detailed display, you can open windows that show the same data in the summary format and the data format.

Refer to chapter 4, “Running Decode Measurements,” for more information on decode measurements.

Commentators

These measurements identify high level significant network events. These are events which are possible signs of to network performance degradation or network failure.

You can get more detailed information about a particular event by double clicking the mouse on the event. Doing this opens another window which describes the event and offers advice on how to resolve the problem.

Commentators let you identify network problems without sifting through pages of decodes. Commentators can be configured to comment on events in the following protocols: AppleTalk, Banyan Vines, OSI, TCP/IP, ICMP, Novell, DECNet, IBM LAN Manager. See the online help in the Commentator windows for more information.

Stimulus/Response

These are measurements such as traffic generators and server lists that perform a specific test by transmitting onto the network and listening for responses.

For Example. . . A Nearest Server measurement can query the network to find the nearest server of a type you specify. See the online help in each of the measurement windows for more information.

Network Discovery

These measurements search for physical and network addresses. Node Discovery, Automatic Baseline, and Server lists are examples of Network Discovery measurements. See the online help in each of the measurement windows for more information.

Screen Snapshots

Screen Snapshots (Fast Ethernet, Ethernet and Token-Ring Internet Advisor LANs) are a convenient way to position and start several measurements at once. After you open the snapshot, you configure the measurements you want to run, size the windows and position them. Then, when you run the snapshot, those same measurements open, size, position, and run. See the online help in the snapshot window for step-by-step instructions.

Troubleshooters

This category contains many different troubleshooting measurements. These measurements are custom designed snapshots that have been configured to start several useful measurements. The online help for the custom snapshots explains how to add filters and use these troubleshooters as a basis for your own customized snapshots.

Demo Tools

These measurements let you run demonstrations that show the features of the statistics measurements. Also, you can use a demo to generate traffic on the network to demonstrate other measurements.

Refer to chapter 5, “Running Application Measurements,” for more information on application measurements.

Setup Window

The Setup window let you set global parameters that affect the way measurements run.

Data Source

The Data Source field in the Setup window can be set to Network Under Test, Capture Buffer, or Advisor Data File. The choice you make determines whether measurements will capture data from the network or analyze data already in the capture buffer or data from a file.

Network Interface

The Network Interface field determines what type of network you can test and what measurements you can run.

For Example. . . If you choose Ethernet, you can run only Ethernet measurements.

Capture Buffer Control

The Capture Buffer Control parameters let you control the Internet Advisor LAN's capture buffer.

You can select the buffer mode you want. In Continuous mode, data fills the buffer until you stop the measurement, which means that once the buffer is full, newer data overwrites the oldest data. In Stop When Full mode, the measurement stops as soon as the buffer is full.

You can also select the buffer size you want.

Finally, you can select whether or not to use partial packet store (packet slicing). Enabling partial packet store causes the Internet Advisor LAN to capture only the first portion of each packet. This lets you store more packets for a given buffer size. If you enable partial packet store, you can select the partial packet size.

NOTE If you choose to use partial packet store (packet slicing) remember that it can affect other measurements and their outcome.

Ethernet, Fast Ethernet, FDDI, or Token-Ring Parameters

Depending on the selection you make for the Network Interface field (Ethernet, Fast Ethernet, FDDI, or Token-Ring), you can enter parameters to configure the Internet Advisor LAN for that interface.

The Fast Ethernet and Ethernet Media Connection parameter tells the Internet Advisor LAN which one of the Internet Advisor LAN's Ethernet connectors (MII, TX, FX, AUI, or THINLAN/10base2) is connected to the network.

Depending on the Media Connection you select for Fast Ethernet, you can select between 10 or 100 MBits/sec for Line Speed. The Line Mode parameter lets you choose whether the Internet Advisor is connected as a Node on the network or is connected in a Monitor mode. With Fast Ethernet, the Line Mode parameter also lets you select between Half Duplex (HDX) and Full Duplex (FDX).

The FDDI parameters are Connection Type and Connection Mode. They configure the ports for attaching the Internet Advisor LAN to an FDDI network. You can also specify a Target Token Rotation Time, and choose whether to monitor Link Confidence Test frames.

The Token-Ring parameters select whether to participate in the ring or not. If you choose not to participate in the ring, the Internet Advisor LAN passively monitors the network and inserts into the ring, but you cannot perform measurements that transmit such as Traffic Generator or Request Station ID.

You can also select the appropriate line speed (4 or 16 Mbits per second) depending on the type of Token-Ring to which you are connected.

Finally, you can select whether or not to have early token release. Early token release causes the Internet Advisor LAN to release the token immediately after it transmits the last bit of a frame. You can select early token release only with 16 Mbits per second line speed.

Advisor Physical Address

The Advisor Physical Addr. field in the Setup window contains the Internet Advisor LAN's unique physical-layer address. This address can be modified. See the section titled, "Setup for an Ethernet Network" in chapter 2 of this manual for instructions on how to change the Internet Advisor LAN's physical address.

Transmit Password

All measurements which transmit on the network require a password when the Transmit Password field is set to Required. After the password is entered correctly, the value of this field changes to Entered, and all transmitting measurements run without prompting for the password until this field is changed to Required again.

The password is ***Advisor***. See the online help for information on how to change the password.

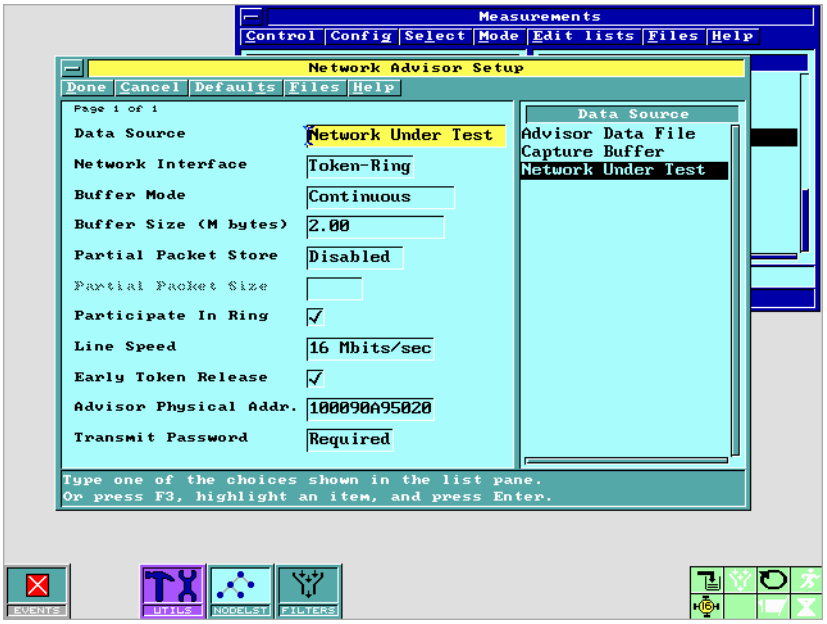
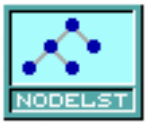


Figure 1-2: Internet Advisor LAN Setup window



Node/Station List Window

In the Node/Station List window, you can create a node list (symbolic name table) so you can use meaningful names rather than hexadecimal addresses to identify the nodes or stations on your network.

NOTE

The Node Discovery Measurement for Ethernet, the Station Discovery Measurement for Token-Ring, and the Station Discovery Measurement for FDDI can automatically create a node list for you. See the online help with each one of these measurements for more information about creating node lists.

The node list is a global database that can be used by the Internet Advisor LAN's measurements to provide name/address mapping. For each node, you can identify the general type of node, add comments about the node, and identify address information about the node. You can add new nodes to the list, modify information about an existing node in the list, and delete nodes from the list.

Refer to chapter 9, "Using the Node List," for more information.

Filters Window

The purpose of filters is to control which frames the Internet Advisor LAN captures or excludes when you are testing a network. Filters can also be used to stop the Internet Advisor LAN when a specified frame is encountered on the network.

The Internet Advisor LAN comes with many basic Ethernet, Fast Ethernet, FDDI, and Token-Ring filters. To create a new filter, you modify one of these provided filters or another filter you have created and save the changes to a new filter name. To use a filter, you "activate" it.

Refer to chapter 8, "Using Filters," for more information.

Utilities Window

The Utilities window contains a list of system utilities. These utilities provide functionality that is not directly related to running measurements:

- **File Manager** lets you perform common file management tasks such as copying, deleting, printing, and renaming files, and creating and deleting subdirectories.
- **PC Configuration** lets you control whether the internal LCD display or an external display is used. It also lets you control whether the PRINT SCREEN key is disabled or sends output to a printer or a file.
- **Autostart** lets you specify the Internet Advisor LAN's power-on state and whether any measurements are automatically run at power-on.
- **Version Information** shows you what version of software and hardware your Internet Advisor LAN has.
- **Install Application -** displays a list of available applications that may be installed. Select an application to display dialog boxes that guide you through the installation.
- **Proxy Port Setup -** lets you support decodes and protocol statistics for non-standard proxy ports. Network fire walls may use non-standard "proxy ports," especially for the World Wide Web. Select this item to display dialog boxes that prompt you for the proxy port information. After a proxy port is setup, the decodes display the specified protocol on the specified proxy port.
- **Exit to DOS** lets you leave the Internet Advisor LAN mode and go to either Windows 95 or to a DOS menu.

Refer to chapter 10, “Using the Internet Advisor LAN's Utilities,” for more information on using the utilities.

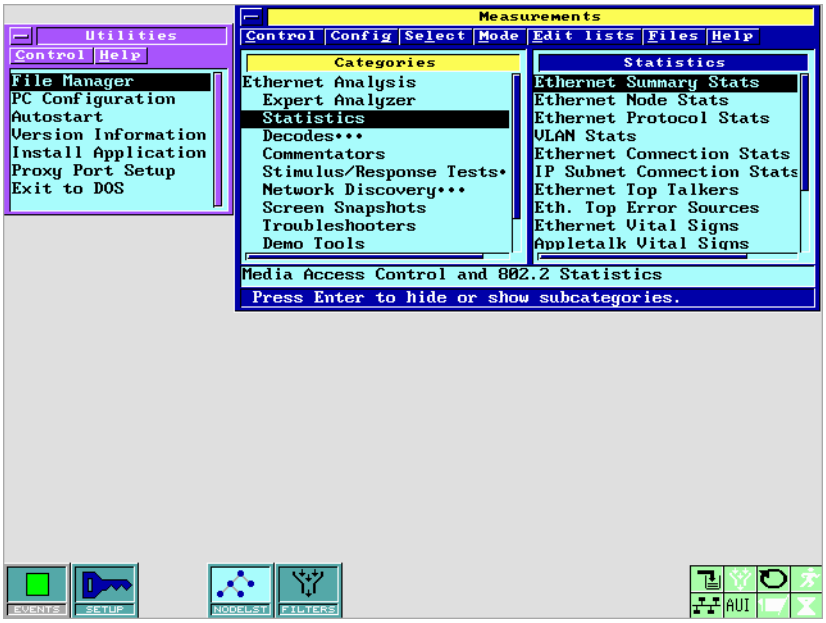


Figure 1-3: Utilities window

Event Log Window

The Event Log provides high visibility of “events” occurring on the network and in the Internet Advisor LAN. Events are occurrences that are especially significant or noteworthy.

The Event Log is a file on the Advisor’s hard disk. Events are logged until the file is full; then as a new event is logged, the oldest event is removed from the file and that space is reused. You can turn the Event Log on or off. While it is on, all events are stored on disk. While off, only instrument events are logged to the disk.

Errors, or events, that require immediate notification and user interaction open a dialog box.

There are six categories of events:

- Protocol events - are when connections are established.
- Threshold events - the number of collisions that exceeded a threshold.
- Topology events - include a ring insertion occurred or a node was unreachable.
- Fault events - include a broadcast storm occurred or there is a bad cable.
- Instrument events - include a measurement starts or stops, data capture occurred, and system errors.
- All events - This category includes all of the other categories.

Refer to chapter 7, “Using the Event Log,” for more information.

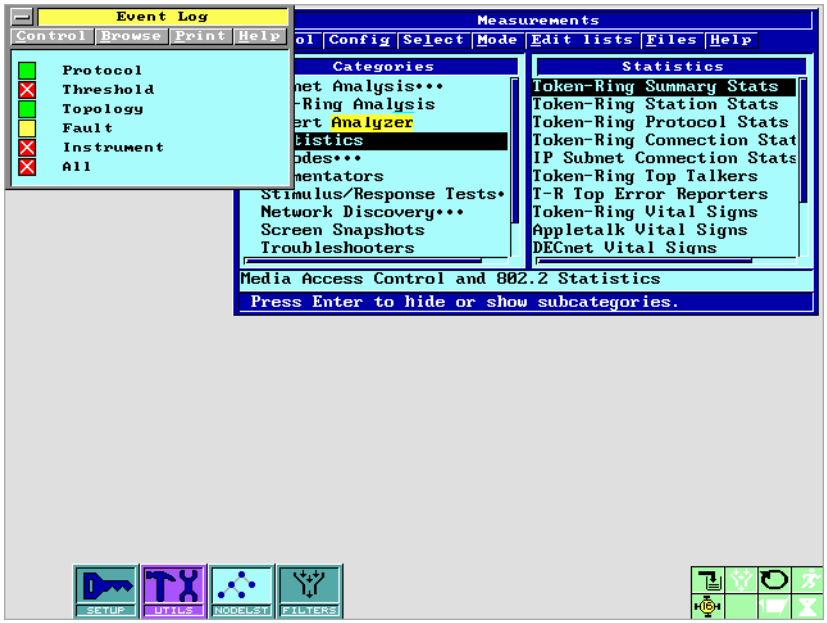


Figure 1-4: Event Log window

Printing Information from the Internet Advisor LAN Measurements

You can document network status and conditions by printing the output of the Internet Advisor LAN measurements. Summary Statistics, Node/Station Statistics, and Protocol Statistics let you log data to disk in Comma Separated Variable (CSV) format. This format is suitable for most spreadsheet applications. Other measurements have Print menu bar selections to print their results. You can either print directly to a printer attached to the Advisor, or print to a file. Use the UTILS window selection “PC Configuration” to set up the printing options you want.

You can print an online help topic for any window using the Print menu bar selection in the Help window. For Help windows with the Related menu bar item active, use Print/Related to print all related topics.

Measurement Descriptions

This section lists the measurements provided in the Internet Advisor LAN.

Not all of the measurements listed here are discussed in this manual. For specific information on each measurement, detailed online help is provided in every window and for each configuration window if the measurement has one.

Online help is easily accessed by pressing **ESC + H** in any window. Select the measurement “Topics” menu item for a detailed list of the help topics for the current window. System help topics discuss topics which are not specific to any one window, such as help for the status icons.

The left pane of the Measurements window, labeled Categories, contains a hierarchy of categories and subcategories to organize related measurements.

There are three top level categories: Fast Ethernet, Ethernet Analysis; FDDI Analysis; and Token-Ring Analysis. These categories correspond to the three network interfaces you can use with the Internet Advisor LAN.

Categories that have subcategories are marked by a trailing ellipsis (...). When such a category is highlighted, pressing **Enter** or clicking on it expands the subcategory structure.

The right pane of the Measurements window displays measurements. The Select menu bar item controls the format of the measurement display.

Ethernet Measurements

The following table lists the categories, subcategories, and measurements, and describe the function of each Ethernet measurement.

Table 1-1: Ethernet Analysis

Fast Ethernet, Ethernet Analysis		
Expert Analyzer		
	Ethernet Expert Analyzer	Ethernet top level measurements including protocols, network health, and network utilization
Statistics		
	Ethernet Summary Stats	Graphical and tabular displays show statistics mostly for the entire network (rather than for any particular nodes)
	Ethernet Node Stats	Graphical displays show various statistics for 20 nodes
	Ethernet Protocol Stats	Graphical displays show various statistics for 20 protocols
	Ethernet Connection Stats	Graphical displays show MAC connection statistics
	IP Subnet Connection Stats	Graphical displays show IP Subnet connection statistics
	Ethernet Top Talkers	Tabular display lists 50 nodes sending the most frames
	Eth. Top Error Sources	Tabular display lists 50 nodes generating the most error frames
	Ethernet Network Counts	Tabular display shows the network capacity being used, and the number of frames, collisions, bad FCS, runts, jabbers, and misaligns
	Ethernet Vital Signs	Tabular display shows local, remote, late, and remote late collisions. Shows runts, jabbers, jabbers with bad FCS, dribbles, broadcast, and multicast frames
	AppleTalk Vital Signs	Tabular display shows network utilizations and stats for DDP, ATP, ADSP, NBP, AARP, RTMP, and ZIP protocols
	DECNet Vital Signs	Tabular display includes DRP, NSP, LAT, MOP, and CLNP statistics
	Novell Vital Signs	Tabular display includes RIP, SAP, Read, Write, Busy Server statistics
	OSI Vital Signs	Tabular display includes CLNP, TP, ESIS, and ISIS stats
	TCP/IP Vital Signs	Tabular display includes ICMP, Low TTL, SNMP, DNS, and ARP stats
	Vines Vital Signs	Tabular display includes VIP, VIPC, VSPP, and VARP stats

Fast Ethernet, Ethernet Analysis		
Decodes		
	Network Stack Decode	Shows what protocols are running on the network, decodes all fields for each protocol, and displays the entire frame in hex
	Apollo Stack Decode	Shows the Ethernet and Apollo Domain protocols running on the network
	AppleTalk Stack Decode	Shows what AppleTalk protocols are running on the network and decodes all fields for each protocol
	ARPA Stack Decode	Shows what ARPA protocols are running on the network and decodes all fields for each protocol
	DECNet IV Stack Decode	Shows what DECNet IV protocols are running on the network and decodes all fields for each protocol
	DECNet IV& V Stack Decode	Shows what DECNet IV and V protocols are running on the network and decodes all fields for each protocol
	Ethernet/LAT Stack Decode	Shows what Ethernet/LAT protocols are running on the network and decodes all fields for each protocol
	ISO Stack Decode	Shows what ISO protocols are running on the network and decodes all fields for each protocol
	Novell/Eth. Stack Decode	Shows what Novell protocols are running on the network and decodes all fields for each protocol
	SUN Stack Decode	Shows what SUN protocols are running on the network and decodes all fields for each protocol
	VINES Stack Decode	Shows what Banyan protocols are running on the network and decodes all fields for each protocol
	XNS Stack Decode	Shows what XNS protocols are running on the network and decodes all fields for each protocol
	Brief Network Stack Decode	Shows what protocols are running on the network, decodes a subset of fields for each protocol, displays the entire frame in hex
Ethernet/ LLC	802.3/Ethernet Decode	Decodes the 802.3/Ethernet protocol
	802.2 Decode	Decodes the 802.2 protocol
	SNAP Decode	Decodes the Sub-Network Access Protocol
	ELAP Decode	Decodes the EtherTalk Link Access Protocol
Fast Ethernet	ISL Decode	Decodes the Inter Switch Link protocol
Apollo Domain	Apollo Stack Decode	Shows the Ethernet and Apollo Domain protocols running on the network

Fast Ethernet, Ethernet Analysis		
AppleTalk	AppleTalk Stack Decode	Shows what AppleTalk protocols are running on the network and decodes all fields for each protocol
	ELAP Decode	Decodes the EtherTalk Link Access Protocol
	AARP Decode	Decodes the AppleTalk Address Resolution Protocol
	DDP Decode	Decodes the Datagram Delivery Protocol
	ATP Decode	Decodes the AppleTalk Transaction Protocol
	RTMP Decode	Decodes the Routing Table Maintenance Protocol
	AEP Decode	Decodes the AppleTalk ECHO Protocol
	ANBP Decode	Decodes the Appletalk Name Binding Protocol
	SNMP Decode	Decodes the Simple Network Management Protocol
	ADSP Decode	Decodes the AppleTalk Data Stream Protocol
	ZIP Decode	Decodes the Zone Information Protocol which coordinates zone names in AppleTalk networks
Banyan	VINES Stack Decode	Shows what Banyan protocols are running on the network and decodes all fields for each protocol
	VIP Decode	Decodes the Vines Internet Protocol
	VARP Decode	Decodes the Vines Address Resolution Protocol
	VRTP Decode	Decodes the Vines Routing Update Protocol
	VSPP Decode	Decodes the Vines Sequenced Packet Protocol
	VIPC Decode	Decodes the Vines Internet Control Protocol
	VICP Decode	Decodes the Vines Interprocess Communication Protocol
DECNet	DECNet IV Stack Decode	Shows what DECNet IV protocols are running on the network and decodes all fields for each
	DECNet IV & V Stack Decode	Shows what DECNet IV & V protocols are running on the network and decodes all fields for each
	LAT Stack Decode	Shows LAT protocols running on the network and decodes all fields for each
	DRP Decode	Decodes the DECNet Routing Protocol
	NSP Decode	Decodes the Network Services Protocol
	SCP Decode	Decodes the Session Control Protocol
	DAP Decode	Decodes the Data Access Protocol
	LAT Decode	Decodes the Local Area Transport Protocol
	CLNP Decode	Decodes the Connectionless-Mode Network Protocol
	TP Decode	Decodes the Connection Oriented Transport Protocol
ISO	ISO Stack Decode	Shows what ISO protocols are running on the network and decodes all fields for each protocol

Fast Ethernet, Ethernet Analysis		
	ES-IS Decode	Decodes the End System Intermediate System Protocol
	CLNP Decode	Decodes the Connectionless Network Protocol
	TP Decode	Decodes the Transport Protocol classes 0 thru 4
	IS-IS Decode	Decodes the Intermediate System to Intermediate System Protocol
Microsoft/ IBM LAN Mngr.	NETBIOS Decode	Decodes the NETBIOS protocol
	SMB Decode	Decodes the IBM PC Server Message Block protocol
	NetBIOS over TCP/UDP	Decodes the NetBIOS over TCP/UDP protocol
Novell	Novell Stack Decode	Shows what Novell protocols are running on the network and decodes all fields for each protocol
	IPX Decode	Decodes the Internet Packet eXchange Protocol
	Novell NetBios Decode	Decodes the NetBios Protocol
	SPX Decode	Decodes the Sequenced Packet eXchange Protocol
	NCP Decode	Decodes the Netware Code Protocol
	Novell RIP Decode	Decodes the Routing Information Protocol
	Novell SAP Decode	Decodes the Service Advertising Protocol
	SNMP Decode	Decodes the Simple Network Management Protocol
	SMB Decode	Decodes the Server Message Block Protocol
	Oracle TNS Decode	Decodes the Oracle Transparent Network Substrate Protocol
SNA	IBM Stack Decode	Shows what SNA protocols are running on the network and decodes all fields for each protocol
	SNA Decode	Decodes the SNA, TH, RH, and RU protocols
SUN	SUN Stack Decode	Shows what SUN protocols are running on the network and decodes all fields for each protocol
	RPC Decode	Decodes the SUN Remote Procedure Protocol
	NFS Decode	Decodes the Network File System Protocol
	NIS Decode	Decodes the SUN Network Information System protocol
	PMAP Decode	Decodes the SUN Port Mapper Protocol
	Mount Decode	Decodes the SUN Mount Protocol
TCP/IP	ARPA Stack Decode	Shows what ARPA protocols are running on the network and decodes all fields for each protocol
	HTTP (WWW) Decode	Decodes the HyperText Transport Protocol
	Oracle TNS Decode	Decodes the Oracle database protocol

Fast Ethernet, Ethernet Analysis		
	Sybase TDS Decode	Decodes the Sybase Tabular Data Stream Protocol
	IGMP Decode	Decodes the Internet Group Management Protocol
	IP Decode	Decodes the Internet Protocol
	ARP/RARP Decode	Decodes the Address Resolution Protocol
	ICMP Decode	Decodes the Internet Control Protocol
	TCP Decode	Decodes the Transport Control Protocol
	UDP Decode	Decodes the User Datagram Protocol
	BOOTP Decode	Decode for remote booting stations
	Telnet Decode	Decodes the Telnet Protocol
	SNMP Decode	Decodes the SNMP Protocol
	FTP Decode	Decodes the File Transfer Protocol
	TCP/IP Routing Protocols Decode	Decodes the RIP, IGRP, and OSPF Protocols
XNS	XNS Stack Decode	Shows what XNS protocols are running on the network and decodes all fields for each protocol
	IDP Decode	Decodes the Internetwork Datagram Protocol
	SPP Decode	Decodes the Sequence Packet Protocol
	SMB Decode	Decodes the Server Message Block Protocol
3Com	3Com NBP Decode	Decodes the 3Com-optimized implementation of the NETBIOS Protocol
	SMB Decode	Decodes the Server Message Block Protocol
Commentators		
	Network Commentator/ Eth.	Provides a high-level report of significant Ethernet, DECNet, TCP/IP ICMP, AppleTalk, Banyan Vines, OSI, and Novell protocol events
	AppleTalk Commentator/ Eth.	Provides a high-level report of significant AppleTalk protocol events
	DECNet Commentator/ Eth.	Provides a high-level report of significant DECNet protocol events
	Novell Commentator/Eth.	Provides a high-level report of significant Novell protocol events
	OSI Commentator/Eth.	Provides a high-level report of significant OSI protocol events
	TCP/IP Commentator/Eth.	Provides a high-level report of significant TCP/IP protocol events
	Vines Commentator/Eth.	Provides a high-level report of significant Vines protocol events

Fast Ethernet, Ethernet Analysis		
Stimulus/Response Tests		
	Eth. Traffic Generator	Sends 802.3/Ethernet traffic on the network
	Novell/Eth. Server List	List up to 500 Novell Servers
	Novell/Eth. Srvr Long List	List up to 2000 Novell Servers
	SNMP Trap Application	Generate an SNMP trap packet on occurrence of selected events
Ethernet	Eth. Traffic Generator	Sends 802.3/Ethernet traffic on the network
	Ethernet Transceiver Test	Tests network connectivity by sending a frame onto the network and then checks the capture buffer to see if the frame was captured correctly
Novell	Novell/Eth. Nearest Server	Find configurable server type (in time), nearest server of specified type
	Novell/Eth. Network List	Find addresses and names of remote networks
	Novell/Eth. Node Ping	Query specified node to test client reachability
	Novell/Eth. Server List	List Novell servers
	Novell/Eth. Server Long List	List up to 2000 Novell servers
	Novell/Eth. Server Ping	Ping configurable server address
	Novell/Eth. View Nodes	List all Novell clients on local segment
TCP/IP	ARP/RARP Request	Verifies connectivity to a node by sending an ARP Request packet to find the physical address for a target host
	PING (Packet InterNet Groper)	Tests whether destinations can be reached by sending an ICMP Echo Request packet and waiting for an ICMP Reply packet
	BOOTP	Bootstrap protocol which is used to boot diskless stations
Network Discovery		
	Node Discovery	Discovers Ethernet nodes on the network (MAC addresses and network addresses)
	Audit Network	Run a group of network tests. Results can be printed in a report form
	Automatic Baseline	Measurement to automatically generate baseline files for Expert Analyzer
	Automatic Vitals Baseline	Find network and physical addresses
	Novell/Eth. Server List	List Novell servers
	Novell/Eth. Server Long List	List up to 2000 Novell Servers

Fast Ethernet, Ethernet Analysis		
Novell	Novell/Eth. Nearest Server	Ping configurable server type (in time), nearest server of specified type
	Novell/Eth. Network List	Find addresses and names of remote networks
	Novell/Eth Node Ping	Ping specified node to test client reachability
	Novell/Eth. Server List	List Novell servers
	Novell/Eth. Server Long List	List up to 2000 Novell servers
	Novell/Eth. Server Ping	Ping configurable server address
	Novell/Eth. View Nodes	List all Novell clients on local segment
Screen Snapshots		
	Screen Snapshot	Create your own snapshots using the Screen Snapshot template. Use preconfigured snapshots for monitoring the network
	Monitor	Runs the Network Stack Decode in the Detailed and Summary views
Troubleshooters		
	Eth/MAC Troubleshooter	Run the Eth. Vital Signs, Eth. Top Error Sources, Eth Top Talkers, Top Broadcasting Nodes, and Top Multicast Nodes
	AppleTalk/Eth Troubleshooter	Run the AppleTalk Commentator/Eth. and Vital Signs
	AppleTalk/Eth Troubleshooter/Dec	Run the AppleTalk Commentator/Eth., Vital Signs, and Stack Decode
	DECNet/Eth. Troubleshooter	Run the DECNet Commentator and Vital Signs
	DECNet/Eth. Troubleshooter/Dec	Run the DECNet Commentator and Vital Signs and the DECNet Stack Decode
	Novell/Eth. Troubleshooter	Run the Novell Commentator and Vital Signs
	Novell/Eth. Troubleshooter/Dec	Run the Novell Commentator, Vital Signs, and the Novell Stack Decode
	OSI/Eth. Troubleshooter/Dec	Run the OSI Commentator/Eth. and Vital Signs
	OSI/Eth. Troubleshooter	Run the OSI Commentator, Vital Signs, and Stack Decodes
	TCP/Eth. Troubleshooter	Run the TCP/IP Commentator and Vital Signs
	TCP/Eth. Troubleshooter/Dec.	Run the TCP/IP Commentator and Vital Signs and the ARPA Stack Decode
	Vines/Eth Troubleshooter	Run the Vines. Commentator and Vital Signs
	Vines/Eth Troubleshooter/Dec	Run the Vines Commentator, Vital Signs, and Stack Decode

Fast Ethernet, Ethernet Analysis		
	Eth. Stats Troubleshooter	Run the Ethernet Summary Statistics and Top Errors and Node Stats
	Fault Finder	Run tests to observe, find, and inform network faults
Demo Tools		
	DEMO: Ethernet Traffic	Generates Ethernet traffic on network for demonstrating other measurements

FDDI Measurements

The following table lists the categories, subcategories, and measurements, and describe the function of each FDDI measurement.

Table 1-2: FDDI Analysis

FDDI Analysis		
Expert Analyzer		
	FDDI Expert Analyzer	FDDI top level measurements including protocols, network health, and network utilization
Ring Manager		
	FDDI Ring Manager	Graphical view of the FDDI Ring with station information and comments on important events in the network
Statistics		
	FDDI Summary Stats	Graphical and tabular displays show statistics mostly for the entire network (rather than for any particular nodes)
	FDDI Station Stats	Graphical displays show various statistics for 20 stations

FDDI Analysis		
	FDDI Protocol Stats	Graphical displays show various statistics for 20 protocols
	FDDI Connection Stats	Graphical displays show MAC connection statistics
	IP Subnet Connection Stats	Graphical displays show IP Subnet connection statistics
	FDDI Top Talkers	Tabular display lists 50 nodes sending the most frames
	FDDI Top Error Sources	Tabular display lists 50 nodes generating the most error frames
	FDDI Vital Signs	Tabular display shows local, remote, late, and remote late collisions. Shows runts, jabbers, jabbers with bad FCS, dribbles, broadcast, and multicast frames
	AppleTalk Vital Signs	Tabular display shows network utilizations and stats for DDP, ATP, ADSP, NBP, AARP, RTMP, and ZIP protocols
	OSI Vital Signs	Tabular display includes CLNP, TP, ESIS, and ISIS stats
	Vines Vital Signs	Tabular display includes VIP, VIPC, VSPP, and VARP stats
	Novell Vital Signs	Tabular display includes RIP, SAP, Read, Write, Busy Server statistics
	TCP/IP Vital Signs	Tabular display includes ICMP, Low TTL, SNMP, DNS, and ARP stats
	DECNet Vital Signs	Tabular display includes DRP, NSP, LAT, MOP, and CLNP statistics
Decodes		
	Network Stack Decode	Shows what protocols are running on the network, decodes all fields for each protocol, and displays the entire frame in hex
	FDDI Stack Decode	Decodes SMT and MAC frames on the network
	Apollo Stack Decode	Shows the Ethernet and Apollo Domain protocols running on the network
	AppleTalk Stack Decode	Shows what AppleTalk protocols are running on the network and decodes all fields for each protocol
	ARPA Stack Decode	Shows what ARPA protocols are running on the network and decodes all fields for each protocol
	DECNet IV Stack Decode	Shows what DECNet IV protocols are running on the network and decodes all fields for each protocol
	DECNet IV& V Stack Decode	Shows what DECNet IV and V protocols are running on the network and decodes all fields for each protocol
	ISO Stack Decode	Shows what ISO protocols are running on the network and decodes all fields for each protocol
	LAT Stack Decode	Shows what LAT protocols are running on the network and decodes all fields for each protocol

FDDI Analysis		
	Novell Stack Decode	Shows what Novell protocols are running on the network and decodes all fields for each protocol
	SUN Stack Decode	Shows what SUN protocols are running on the network and decodes all fields for each protocol
	VINES Stack Decode	Shows what Banyan protocols are running on the network and decodes all fields for each protocol
	XNS Stack Decode	Shows what XNS protocols are running on the network and decodes all fields for each protocol
	Brief Network Stack Decode	Decodes a subset of fields of all protocols running on the network and displays the entire frame in hex
AppleTalk	AppleTalk Stack Decode	Shows what AppleTalk protocols are running on the network and decodes all fields for each protocol
	ELAP Decode	Decodes the EtherTalk Link Access Protocol
	AARP Decode	Decodes the AppleTalk Address Resolution Protocol
	DDP Decode	Decodes the Datagram Delivery Protocol
	ATP Decode	Decodes the AppleTalk Transaction Protocol
	RTMP Decode	Decodes the Routing Table Maintenance Protocol
	AEP Decode	Decodes the AppleTalk ECHO Protocol
	ANBP Decode	Decodes the Appletalk Name Binding Protocol
	ADSP Decode	Decodes the AppleTalk Data Stream Protocol
	ZIP Decode	Decodes the Zone Information Protocol which coordinates zone names in AppleTalk networks
Apollo Domain	Apollo Stack Decode	Decodes the Apollo Domain protocols running on the network
Banyan	VINES Stack Decode	Shows what Banyan protocols are running on the network and decodes all fields for each protocol
	VIP Decode	Decodes the Vines Internet Protocol
	VARP Decode	Decodes the Vines Address Resolution Protocol
	VRTP Decode	Decodes the Vines Routing Update Protocol
	VSPP Decode	Decodes the Vines Sequenced Packet Protocol
	VIPC Decode	Decodes the Vines Internet Control Protocol
	VICP Decode	Decodes the Vines Interprocess Communication Protocol
DECNet	DECNet IV Stack Decode	Shows what DECNet IV protocols are running on the network and decodes all fields for each
	DECNet IV & V Stack Decode	Shows what DECNet IV & V protocols are running on the network and decodes all fields for each

FDDI Analysis		
	LAT Stack Decode	Shows LAT protocols running on the network and decodes all fields for each
	DRP Decode	Decodes the DECNet Routing Protocol
	NSP Decode	Decodes the Network Services Protocol
	SCP Decode	Decodes the Session Control Protocol
	DAP Decode	Decodes the Data Access Protocol
	LAT Decode	Decodes the Local Area Transport Protocol
	CLNP Decode	Decodes the Connectionless-Mode Network Protocol
	TP Decode	Decodes the Connection Oriented Transport Protocol
FDDI/LLC	FDDI Stack Decode	Shows MAC and SMT frames on the network and decodes all fields for each protocol
	MAC Decode	Decodes the FDDI MAC protocol
	SMT Decode	Decodes the FDDI SMT protocol
	802.2 Decode	Decodes the 802.2 Protocol
	SNAP Decode	Decodes the Sub-Network Access Protocol
ISO	ISO Stack Decode	Shows what ISO protocols are running on the network and decodes all fields for each protocol
	ES-IS Decode	Decodes the End System Intermediate System Protocol
	CLNP Decode	Decodes the Connectionless Network Protocol
	TP Decode	Decodes the Transport Protocol classes 0 thru 4
	IS-IS Decode	Decodes the Intermediate System to Intermediate System Protocol
Microsoft/ LAN Mngr.	NETBIOS over TCP/UDP Decode	Decodes the NETBIOS protocol
	SMB Decode	Decodes the IBM PC Server Message Block protocol
Novell	Novell Stack Decode	Shows what Novell protocols are running on the network and decodes all fields for each protocol
	IPX Decode	Decodes the Internet Packet eXchange Protocol
	SPX Decode	Decodes the Sequenced Packet eXchange Protocol
	NCP Decode	Decodes the Netware Code Protocol
	Novell RIP Decode	Decodes the Routing Information Protocol
	Novell SAP Decode	Decodes the Service Advertising Protocol
	SNMP Decode	Decodes the Simple Network Management Protocol
SUN	SUN Stack Decode	Shows what SUN protocols are running on the network and decodes all fields for each protocol

FDDI Analysis		
	RPC Decode	Decodes the SUN Remote Procedure Protocol
	NFS Decode	Decodes the Network File System Protocol
	NIS Decode	Decodes the SUN Network Information System protocol
	PMAP Decode	Decodes the SUN Port Mapper Protocol
	Mount Decode	Decodes the SUN Mount Protocol
TCP/IP	ARPA Stack Decode	Shows what ARPA protocols are running on the network and decodes all fields for each protocol
	IP Decode	Decodes the Internet Protocol
	ARP/RARP Decode	Decodes the Address Resolution Protocol
	ICMP Decode	Decodes the Internet Control Protocol
	TCP Decode	Decodes the Transport Control Protocol
	UDP Decode	Decodes the User Datagram Protocol
	Telnet Decode	Decodes the Telnet Protocol
	FTP Decode	Decodes the File Transfer Protocol
	TCP/IP Routing Protocols	Decodes the RIP and IGRP routing protocols
	BOOTP	Bootstrap protocol which is used to boot diskless stations
XNS	XNS Stack Decode	Shows what XNS protocols are running on the network and decodes all fields for each protocol
	IDP Decode	Decodes the Internetwork Datagram Protocol
	SPP Decode	Decodes the Sequence Packet Protocol
Commentators		
	Network Commentator/ FDDI	Provides a high-level report of significant DECNet, TCP/IP IBM LAN Manager, ICMP, Vines, AppleTalk, OSI, and Novell protocol events
	AppleTalk Commentator/ FDDI	Provides a high-level report of significant AppleTalk protocol events
	DECNet Commentator/ FDDI	Provides a high-level report of significant DECNet protocol events
	Novell Commentator/FDDI	Provides a high-level report of significant Novell protocol events
	OSI Commentator/FDDI	Provides a high-level report of significant OSI protocol events
	TCP/IP Commentator/ FDDI	Provides a high-level report of significant TCP/IP protocol events

FDDI Analysis		
	Vines Commentator/FDDI	Provides a high-level report of significant Vines protocol events
Stimulus/Response Tests		
	FDDI Traffic Generator	Sends SMT and MAC frames, line states, and raw symbols on the network
	Novell/FDDI Server List	List up to 500 Novell servers
	Novell/FDDI Srvr Long List	List up to 2000 Novell servers
	SNMP Trap Application	Generate an SNMP trap packet on occurrence of selected events
Novell	Novell/FDDI Nearest Server	Ping configurable server type (in time), nearest server of specified type
	Novell/FDDI Network List	Find addresses and names of remote networks
	Novell/FDDI Node Ping	Ping configurable node address
	Novell/FDDI Server List	List up to 500 Novell servers
	Novell/FDDI Srvr Long List	List up to 2000 Novell servers
	Novell/FDDI Server Ping	Ping configurable server address
	Novell/FDDI View Nodes	List all Novell clients on local segment
TCP/IP	ARP/RARP Request	Verifies connectivity to a node by sending an ARP Request packet to find the physical address for a target host
	PING (Packet InterNet Groper)	Tests whether destinations can be reached by sending an ICMP Echo Request packet and waiting for an ICMP Reply packet
Network Discovery		
	FDDI Station Discovery	Discovers FDDI stations on the network (MAC addresses and network addresses)
	Automatic Vitals Baseline	Find network and physical addresses
	Novell/FDDI Server List	List up to 500 Novell servers
	Novell/FDDI Srvr Long List	List up to 2000 Novell servers
Novell	Novell/FDDI Nearest Server	Ping configurable server type (in time), nearest server of specified type
	Novell/FDDI Network List	Find addresses and names of remote networks
	Novell/FDDI Node Ping	Ping configurable node address
	Novell/FDDI Server List	List up to 500 Novell servers
	Novell/FDDI Srvr Long List	List up to 2000 Novell servers
	Novell/FDDI Server Ping	Ping configurable node address
	Novell/FDDI View Nodes	List all Novell clients on local segment

FDDI Analysis		
Troubleshooters		
	AppleTalk/FDDI Troubleshooter	Run the AppleTalk Commentator/FDDI and Vital Signs
	AppleTalk/FDDI Troubleshooter/Dec	Run the AppleTalk Commentator/FDDI, Vital Signs, and Stack Decode
	DECNet/FDDI Troubleshooter	Run the DECNet Commentator and Vital Signs
	DECNet/FDDI Troubleshooter/ Dec	Run the DECNet Commentator and Vital Signs and the DECNet Stack Decode
	Novell/FDDI Troubleshooter	Run the Novell Commentator and Vital Signs
	Novell/FDDI Troubleshooter/ Dec	Run the Novell Commentator, Vital Signs, and the Novell Stack Decode
	OSI/FDDI Troubleshooter	Run the OSI Commentator/FDDI and Vital Signs
	OSI/FDDI Troubleshooter/ Dec	Run the OSI Commentator, Vital Signs, and Stack Decodes
	TCP/FDDI Troubleshooter	Run the TCP/IP Commentator and Vital Signs
	TCP/FDDI Troubleshooter/ Dec	Run the TCP/IP Commentator and Vital Signs and the ARPA Stack Decode
	Vines/FDDI Troubleshooter	Run the Vines. Commentator and Vital Signs
	Vines/FDDI Troubleshooter/Dec	Run the Vines Commentator, Vital Signs, and Stack Decode
	Monitor	Runs the Network Stack Decode in the Detailed and Summary views
Demo Tools		
	DEMO: FDDI Stats	Runs a demo of the FDDI Summary Stats measurement

Token-Ring Measurements

The following table lists the categories, subcategories, and measurements, and describe the function of each Token-Ring measurement. .

Table 1-3: Token-Ring Analysis

Token-Ring Analysis		
Expert Analyzer		
	Token-Ring Expert Analyzer	Token-Ring top level measurements including protocols, network health, and network utilization
Statistics		
	Token-Ring Summary Stats	Graphical and tabular displays show statistics mostly for the entire network (rather than for any particular stations)
	Token-Ring Station Stats	Graphical display show various statistics for 20 stations
	Protocol Stats	Graphical displays show various statistics for 20 protocols
	Token-Ring Connection Stats	Graphical displays show MAC connection statistics
	IP Subnet Connection Stats	Graphical displays show IP Subnet connection statistics
	Token-Ring Top Talkers	Tabular display lists 50 stations sending the most frames
	T-R Top Error Reporters	Tabular display lists 50 stations reporting the most error frames
	Token-Ring Vital Signs	Tabular display includes code violations, aborts, receiver congestion, errors, beacons, claim tokens, and ring purges
	AppleTalk Vital Signs	Tabular displays show network utilization and stats for DDP, ATP, ADSP, NBP, AARP, RTMP, and ZIP protocols
	DECNet Vital Signs	Tabular display includes DRP, NSP, LAT, MOP, and CLNP statistics
	Novell Vital Signs	Tabular display shows RIP, SAP, Read, Write, Busy Server statistics
	OSI Vital Signs	Tabular display includes CLNP, TP, ESIS, and ISIS stats
	TCP/IP Vital Signs	Tabular display includes ICMP, Low TTL, SNMP, DNS, and ARP stats
	Vines Vital Signs	Tabular display includes VIP, VIPC, VSPP, and VARP stats
Decodes		
	Network Stack Decode	Shows what protocols are running on the network, decodes a subset of fields for each protocol, displays the entire frame in hex
	AppleTalk Stack Decode	Shows what AppleTalk protocols are running on the network and decodes all fields for each protocol
	ARPA Stack Decode	Shows what ARPA protocols are running on the network and decodes all fields for each protocol

Token-Ring Analysis		
	DECNet IV Stack Decode	Decodes DECNet Phase IV protocols running on the network
	DECNet IV & V Stack Decode	Decodes DECNet Phase IV & Phase V protocols running on the network
	IBM Stack Decode	Shows what IBM protocols are running on the network and decodes all fields for each protocol
	ISO Stack Decode	Shows what ISO protocols are running on the network and decodes all fields for each protocol
	LAT Stack Decode	Decodes all LAT protocols running on the network
	Novell Stack Decode	Shows what Novell protocols are running on the network and decodes all fields for each protocol
	SUN Stack Decode	Shows what SUN protocols are running on the network and decodes all fields for each protocol
	VINES Stack Decode	Shows what Banyan protocols are running on the network and decodes all fields for each protocol
	XNS Stack Decode	Decodes all XNS protocols running on the network
	Brief Network Stack Decode	Decodes a subset of fields of all protocols running on the network and displays the entire frame in hex
Token-Ring/LLC	Token-Ring Decode	Decodes the Token-Ring Protocol
	802.2 Decode	Decodes the 802.2 Protocol
	SNAP Decode	Decodes the Sub-Network Access Protocol
	TLAP Decode	Decodes the TokenTalk Link Access Protocol
AppleTalk	AppleTalk Stack Decode	Shows what AppleTalk protocols are running on the network and decodes all fields for each protocol
	TLAP Decode	Decodes the TokenTalk Link Access Protocol
	AARP Decode	Decodes the AppleTalk Address Resolution Protocol
	DDP Decode	Decodes the Datagram Delivery Protocol
	ATP Decode	Decodes the AppleTalk Transaction Protocol
	RTMP Decode	Decodes the Routing Table Maintenance Protocol
	AEP Decode	Decodes the AppleTalk ECHO Protocol
	ANBP Decode	Decodes the Appletalk Name Binding Protocol
	SNMP Decode	Decodes the Simple Network Management Protocol
	ADSP Decode	Decodes the AppleTalk Data Stream Protocol
	ZIP Decode	Decodes the Zone Information Protocol which coordinates zone names in AppleTalk networks

Token-Ring Analysis		
Banyan	VINES Stack Decode	Shows what Banyan protocols are running on the network and decodes all fields for each protocol
	VIP Decode	Decodes the Vines Internet Protocol
	VARP Decode	Decodes the Vines Address Resolution Protocol
	VRTP Decode	Decodes the Vines Routing Update Protocol
	VSPP Decode	Decodes the Vines Sequenced Packet Protocol
	VIPC Decode	Decodes the Vines Internet Control Protocol
	VICP Decode	Decodes the Vines Interprocess Communication Protocol
DECNet	DECNet IV Stack Decode	Shows what DECNet IV protocols are running on the network and decodes all fields for each
	DECNet IV & V Stack Decode	Shows what DECNet IV & V protocols are running on the network and decodes all fields for each
	LAT Stack Decode	Shows LAT protocols running on the network and decodes all fields for each
	DRP Decode	Decodes the DECNet Routing Protocol
	NSP Decode	Decodes the Network Services Protocol
	SCP Decode	Decodes the Session Control Protocol
	DAP Decode	Decodes the Data Access Protocol
	LAT Decode	Decodes the Local Area Transport Protocol
	CLNP Decode	Decodes the Connectionless-Mode Network Protocol
	TP Decode	Decodes the Connection Oriented Transport Protocol
ISO	ISO Stack Decode	Shows what ISO protocols are running on the network and decodes all fields for each protocol
	ES-IS Decode	Decodes the End System Intermediate System Protocol
	CLNP Decode	Decodes the Connectionless Network Protocol
	TP Decode	Decodes the Transport Protocol classes 0 thru 4
	IS-IS Decode	Decodes the Intermediate System to Intermediate System Protocol
Microsoft/ IBM LAN Mngr.	NETBIOS Decode	Decodes the NETBIOS Protocol
	SMB Decode	Decodes the IBM PC Server Message Block Protocol
	NetBIOS over TCP/UDP	Decodes the NetBIOS over TCP/UDP protocol
Novell	Novell Stack Decode	Shows what Novell protocols are running on the network and decodes all fields for each protocol
	IPX Decode	Decodes the Internet Packet Exchange Protocol
	SPX Decode	Decodes the Sequence Packet Exchange Protocol

Token-Ring Analysis		
	NCP Decode	Decodes the Netware Core Protocol
	Novell RIP Decode	Decodes the Routing Information Protocol
	Novell SAP Decode	Decodes the Service Advertising Protocol
	SNMP Decode	Decodes the Simple Network Management Protocol
SNA	IBM Stack Decode	Shows what IBM protocols are running on the network and decodes all fields for each protocol
	SNA Decode	Decodes the Systems Network Architecture Protocol
SUN	SUN Stack Decode	Shows what SUN protocols are running on the network and decodes all fields for each protocol
	RPC Decode	Decodes the SUN Remote Procedure Protocol
	NFS Decode	Decodes the Network File System Protocol
	NIS Decode	Decodes the SUN Network Information System protocol
	PMAP Decode	Decodes the SUN Port Mapper Protocol
	Mount Decode	Decodes the SUN Mount Protocol
TCP/IP	ARPA Stack Decode	Shows what ARPA protocols are running on the network and decodes all fields for each protocol
	IP Decode	Decodes the Internet Protocol
	ARP/RARP Decode	Decodes the Address Resolution Protocols
	ICMP Decode	Decodes the Internet Control Message Protocol
	TCP Decode	Decodes the Transmission Control Protocol
	UDP Decode	Decodes the User Datagram Protocol
	Telnet Decode	Decodes the Virtual Terminal Protocol
	SNMP Decode	Decodes the Simple Network Management Protocol
	FTP Decode	Decodes the File Transfer Protocol
	TCP/IP Routing Protocols	Decodes the RIP and IGRP routing protocols
	BOOTP	Bootstrap protocol which is used to boot diskless stations
XNS	XNS Stack Decode	Shows what XNS protocols are running on the network and decodes all fields for each protocol
	IDP Decode	Decodes the Internetwork Datagram Protocol
	SPP Decode	Decodes the Sequence Packet Protocol
3Com	3Com NBP Decode	Decodes the 3Com-optimized implementation of the NETBIOS Protocol
	SMB Decode	Decodes the Server Message Block Protocol
Commentators		

Token-Ring Analysis		
	Network Commentator/T-R	Provides a high-level report of significant DECNet, TCP/IP IBM LAN Manager, AppleTalk, OSI, Banyan Vines, ICMP, and Novell protocol events
	AppleTalk Commentator/ T-R	Provides a high-level report of significant AppleTalk protocol events
	DECNet Commentator/T-R	Provides a high-level report of significant DECNet protocol events
	Novell Commentator/T-R	Provides a high-level report of significant Novell protocol events
	OSI Commentator/T-R	Provides a high-level report of significant OSI protocol events
	TCP/IP Commentator/T-R	Provides a high-level report of significant TCP/IP protocol events
	Vines Commentator/T-R	Provides a high-level report of significant Vines protocol events
Stimulus/Response		
	T-R Traffic Generator	Sends an LLC frame or one of four MAC packets (Remove Ring Station, Request Ring Station Address, Request Ring Station State, Request Ring Station Attachments)
	Novell/T-R Server List	List up to 500 Novell servers
	Novell/T-R Srvr Long List	List up to 2000 Novell servers
	List All Stations	List all stations attached to the local ring
	SNMP Trap Application	Generate an SNMP trap packet upon selected events
Token-Ring	T-R Traffic Generator	Sends an LLC frame or one of four MAC packets (Remove Ring Station, Request Ring Station Address, Request Ring Station State, Request Ring Station Attachments)
	Identify Active Monitor	Identify the active monitor on the local ring
	List All Bridges	List all bridges attached to the local ring
	List All Stations	List all stations attached to the local ring
	List Config Report Servers	List all config report servers attached to the local ring
	List LAN Managers	List all LAN managers attached to the local ring
	List NETBIOS Stations	List all NETBIOS stations attached to the local ring
	List Novell Stations	List all Novell stations attached to the local ring
	List Ring Error Monitors	List all ring error monitors attached to the local ring
	List Ring Parm Servers	List all ring parameter servers attached to the local ring
	Request Station ID	Tests connectivity to a station on a local or remote ring by sending a Test Command packet and watching for Test Response packets

Token-Ring Analysis		
	Station Adapter Status	Shows information about a station by sending a Request Ring Station Address frame
	Token-Ring Lobe Test	Performs a lobe test on the Internet Advisor LAN
Novell	Novell/T-R Nearest Server	Ping to get nearest server of specified type
	Novell/T-R Network List	Find addresses and names of remote networks
	Novell/T-R Node Ping	Ping specified node to test client reachability
	Novell/T-R Server List	List Novell servers
	Novell/T-R Server List	List up to 2000 Novell servers
	Novell/T-R Server Ping	Ping configurable server address
	Novell/T-R View Nodes	List all Novell clients on local segment
	List Novell Stations	List all Novell stations attached to the local ring
TCP/IP	ARP/RARP Request /T-R	Verifies connectivity to a node by sending an ARP Request packet to find the physical address for a target host
	PING /T-R	Tests whether destinations can be reached by sending an ICMP Echo Request packet and waiting for an ICMP Reply packet
Network Discovery		
	Station Discovery	Discovers T-R stations on the network (MAC and network addresses)
	Audit Network	Runs group of network tests. Results are printed in a report
	T-R Automatic Vitals Baseline	Automatically set baselines for Vitals measurements
	Active Station List	Monitors the neighbor notification process to generate a list of stations on the ring
	Calculate Ring Length	Measures the length (in feet and meters) of an active Token-Ring network
	Novell/T-R Server List	List Novell servers
	Novell/T-R Server Long List	List up to 2000 Novell servers
Token-Ring	Active Station List	Monitors the neighbor notification process to generate a list of stations on the ring
	Calculate Ring Length	Measures length (in feet or meters) of an active T-R network
	Identify Active Monitor	Identify the active monitor on the local ring
	List All Bridges	List all bridges attached to the local ring
	List All Stations	List all stations attached to the local ring
	List Config Report Servers	List all config report servers attached to the local ring
	List LAN Managers	List all LAN managers attached to the local ring

Token-Ring Analysis		
	List NETBIOS Stations	List all NETBIOS stations attached to the local ring
	List Novell Stations	List all Novell stations attached to the local ring
	List Ring Error Monitors	List all ring error monitors attached to the local ring
	List Ring Parm Servers	List all ring parameter servers attached to the local ring
	Request Station ID	Tests connectivity to a station on a local or remote ring by sending a Test Command packet and watching for Test Response packets
	Station Adapter Status	Shows information about a station by sending a Request Ring Station Address frame
	Token-Ring Lobe Test	Performs a lobe test on the Internet Advisor LAN
Novell	Novell/T-R Nearest Server	Ping configurable server type (in time), nearest server of specified type
	Novell/T-R Network List	Find addresses and names of remote networks
	Novell/T-R Node Ping	Ping specified node to test client reachability
	Novell/T-R Server List	List Novell servers
	Novell/T-R Server Long List	List up to 2000 Novell servers
	Novell/T-R Server Ping	Ping configurable server address
	Novell/T-R View Nodes	List all Novell clients on local segment
	List Novell Stations	List all Novell stations attached to the local ring
Screen Snapshots		
	Screen Snapshots	Create your own snapshots using the Screen Snapshot template
	Monitor	Runs the Network Stack Decode in the Detailed and Summary views
	Request Routed Station ID	Request Station Identification with LLC and routing filters
	Request Bridge Routed Station	Request Station Identification with routing filter for bridges
Troubleshooters		
	AppleTalk/T-R Troubleshooter	Run the AppleTalk Commentator/T-R and Vital Signs
	AppleTalk/T-R Troubleshooter/Dec	Run the AppleTalk Commentator/T-R, Vital Signs, and Stack Decode
	DECNet/T-R Troubleshooter	Run the DECNet Commentator and Vital Signs
	DECNet/T-R Troubleshooter/ Dec	Run the DECNet Commentator and Vital Signs and the DECNet Stack Decode

Token-Ring Analysis		
	Novell/T-R Troubleshooter	Run the Novell Commentator and Vital Signs
	Novell/T-R Troubleshooter/ Dec	Run the Novell Commentator, Vital Signs, and the Novell Stack Decode
	OSI/T-R Troubleshooter	Run the OSI Commentator/T-R and Vital Signs
	OSI/T-R Troubleshooter	Run the OSI Commentator, Vital Signs, and Stack Decodes
	TCP/T-R Troubleshooter	Run the TCP/IP Commentator and Vital Signs
	TCP/T-R Troubleshooter/ Dec	Run the TCP/IP Commentator and Vital Signs and the ARPA Stack Decode
	Vines/T-R Troubleshooter	Run the Vines. Commentator and Vital Signs
	Vines/T-R Troubleshooter/ Dec	Run the Vines Commentator, Vital Signs, and Stack Decode
	T-R Stats Troubleshooter	Run the Summary and Station Statistics with errors
	Fault Finder	Run tests to observe, find, and inform network faults
Demo Tools		
	DEMO: 4M T-R Traffic	Generates 4 Mbit Token-Ring traffic on the network for demonstrating other measurements
	DEMO: 16M T-R Traffic	Generates 4 Mbit Token-Ring traffic on the network for demonstrating other measurements

2

Getting Started

What's in this Chapter

This chapter contains procedures for getting started with the HP Internet Advisor LAN. These procedures cover the basic skills that you'll need to use the Internet Advisor LAN.

- Starting the Internet Advisor LAN from Windows 95
- Starting the Internet Advisor LAN from DOS
- Exiting from Internet Advisor LAN
- Setting the Date, Time, and Time Zone
- Setting the Printer
- Using a mouse
- Using the keyboard
- Using the windows interface
- Making selections with the status icons
- Using the online help facility
- Configuring the Internet Advisor LAN to test a network
- Starting a measurement
- Installing an undercradle on the Internet Advisor LAN
- 10 Mbps Ethernet Interface Connections
- Fast Ethernet Interface Connections
- Ethernet LED Display
- Installing (or reinstalling) the operating software

Starting the Internet Advisor from Windows 95

Starting Internet Advisor for the First Time

The first time you start the HP Internet Advisor with software shipped from Hewlett-Packard, Microsoft requires you to provide some information to complete the configuration.

Several dialog boxes prompt you for information such as user name, company name, etc. You can accept the default selections by pressing ENTER.

A Certificate of Authenticity box asks you for an authenticity number. The number you should enter is located on the front cover of the *Introducing Microsoft Windows 95* book shipped with your Internet Advisor. Look for the Product ID number above the bar code label.

To start the Internet Advisor LAN from Windows 95

1. In Windows 95, click on the Start button 

to display the Start menu.

2. Move the pointer over Internet Advisor | LAN Analysis. Then move the pointer to the interface and measurement you want and press **ENTER** or click the left mouse button

   Notice that Ethernet and Fast Ethernet measurements for LAN in DOS are located under the Internet Advisor | LAN Analysis | Utilities menu item. The Ethernet and Fast Ethernet menu items in the Interface Selections part of the menu list start the LAN in Windows application.

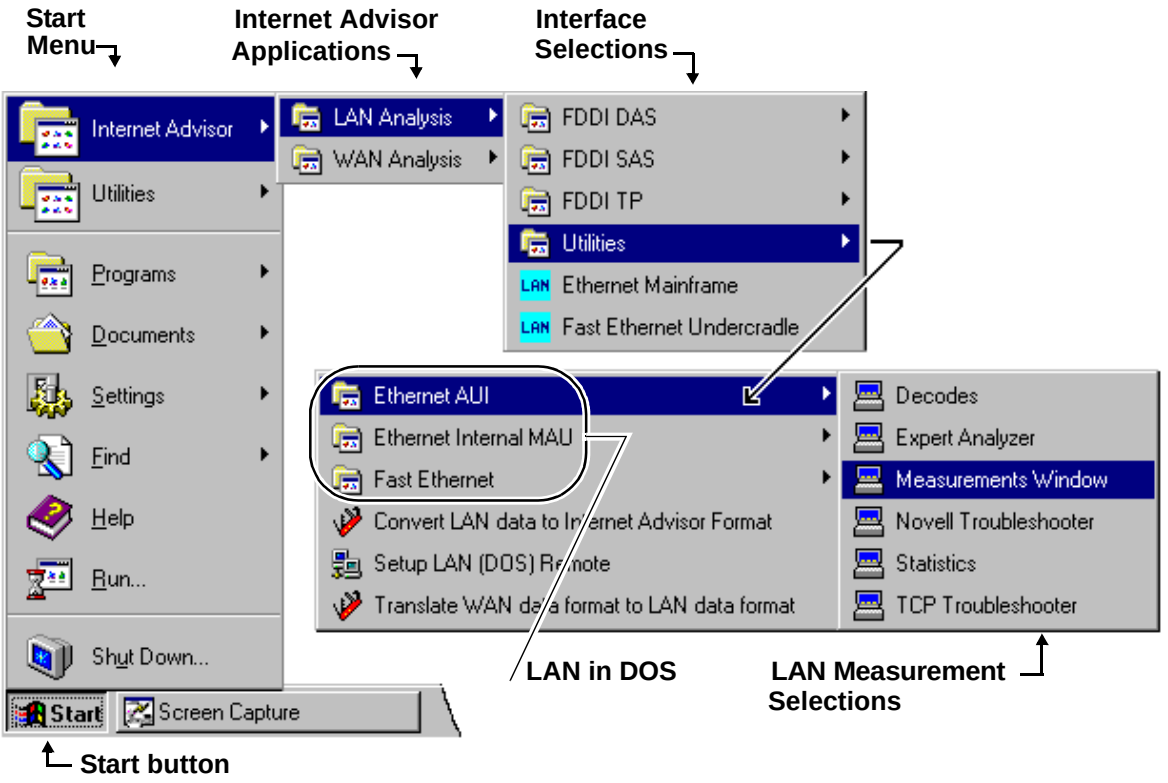


Figure 2-1: Starting Measurement Window on Ethernet AUI Test Port

When the Internet Advisor LAN completes its power-on sequence (the hour glass in the status box goes away), the selected window is opened in the upper right corner of the screen and the Event Log, Setup, Node List, Filters, and Utilities windows are iconized at the bottom of the display.

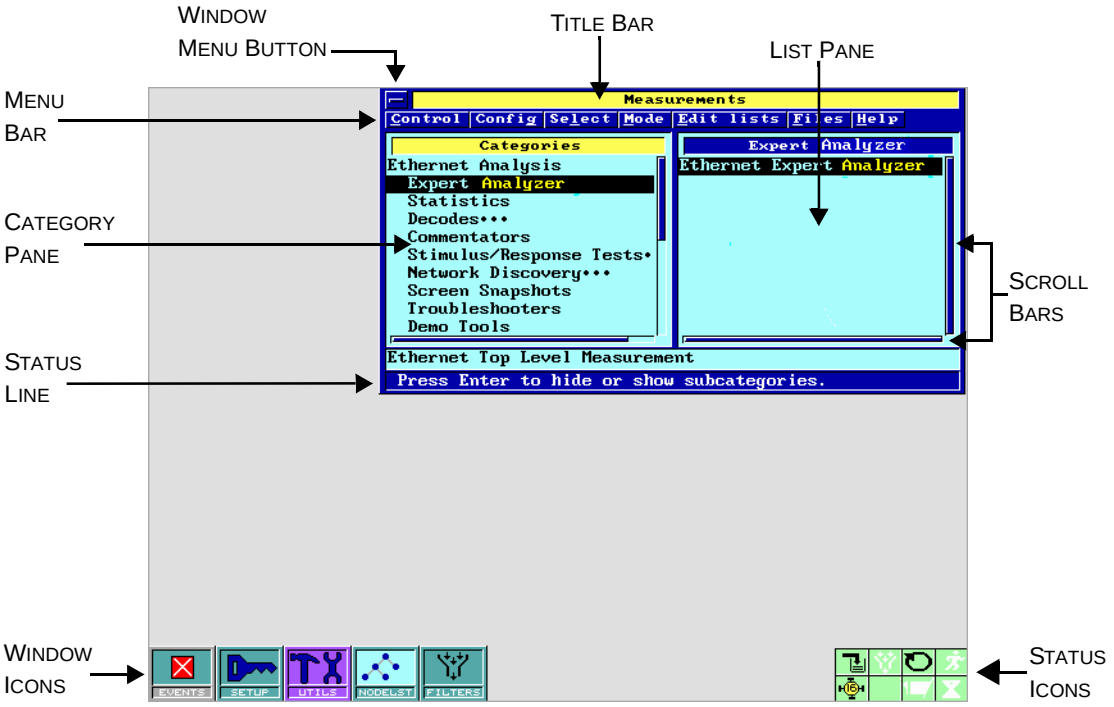


Figure 2-2: Internet Advisor LAN Main Display

Title bar	The title bar is an area at the top of each window that identifies the primary function of the window.
Window Menu button	This is a small graphic button located in the upper left corner of most windows. Clicking on the Window Menu button or pressing **F4** displays the Window Menu.
Window Menu	The Window Menu contains items such as Close, Move, Size, Zoom, and Icon that let you control a window's size and position.
Menu bar	The menu bar is located just below the title bar and contains labels called menu bar items.
Menu bar items	Menu bar items let you access dropdown menus. As you highlight each menu bar item, its dropdown menu appears.
Dropdown menus	Dropdown menus (usually just called "menus") contain one or more items. The items are the individual commands that let you perform specific functions.
Pane	A pane is a partition of a window. All windows have at least one pane. Some panes contain text entry fields (also known as fields or text entry boxes), check boxes, push buttons, and other items. Other panes are called list panes. A list pane contains a list of items you can scroll. Pressing **Enter** or clicking the mouse selects a highlighted item from a list pane.
Scroll bar	The scroll bar indicates what part of the window contents is visible, and allows vertical or horizontal scrolling with a mouse.
Status line	The status line is an area at the bottom of a window that displays prompts, instructions, or comments specific to that window.
Icon	An icon is a small graphic symbol with a short title or picture that represents a measurement window that has been minimized. Icons are displayed in a reserved area at the bottom of the screen.
Status icons	There are eight boxes in the lower right corner of the screen which graphically show the status of the Internet Advisor LAN. In addition, some of the icons open the window that controls their function, and some of the icons select a direct action. For example, with the Ethernet Media Connection icon, clicking the icon toggles the Internet Advisor LAN's interface connection to the network between BNC and AUI. See the section "Making selections with the status icons" later in this chapter. Most of the icons are turned off (a white image is displayed) if the Data Source in the Setup window is NOT Network Under Test. For more information about the status icons, see the section "Making Selections with the Status Icons" later in this chapter.

Starting the Internet Advisor LAN from DOS

If you use the Internet Advisor primarily for LAN applications, you can use an alternate boot process that lets you start the Internet Advisor LAN applications more quickly from a DOS menu than from the Windows 95 Start menu.

To start Internet Advisor from a DOS menu:

3. In Windows 95, click on the Start button  to display the Start menu.

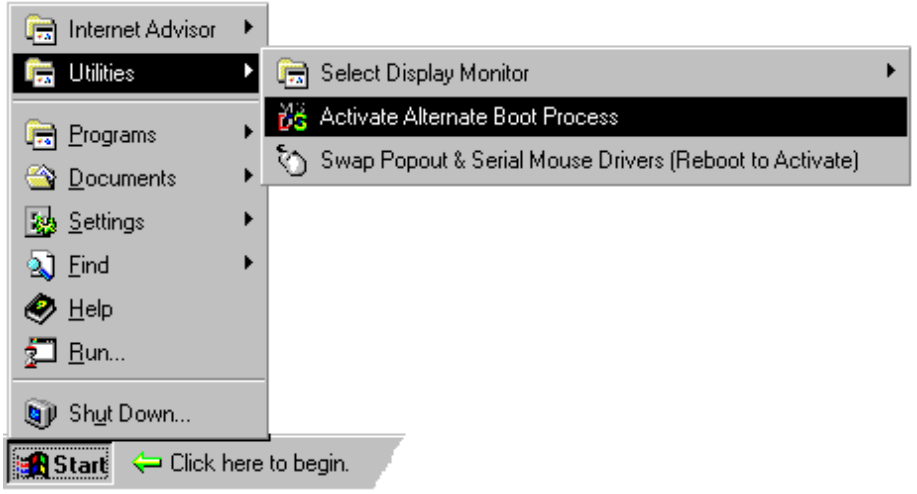


Figure 2-3: Selecting Alternate Boot Process

4. In the Start menu, select Utilities | Activate Alternate Boot Process.

   A prompt tells you that switching to a DOS boot will close any open applications.

5. Select Yes to continue to the alternate DOS boot.

   A prompt describes how to return to Windows 95 from the alternate boot.

6. Press any key to continue to the alternate DOS boot.

   After restarting, the following DOS menu is displayed.

```
MS-DOS Startup Menu
==================
1. Internet Advisor WAN
2. Internet Advisor LAN
3. Windows 95
4. DOS Prompt
Enter a choice:
```

NOTE When you cycle the power, the Internet Advisor LAN will boot to this DOS Startup Menu. To return to using the Windows 95 Start menu, select item 3 in this main DOS menu.

7. Type 2 and press **ENTER**.

The following menu lets you choose a LAN application to start.

```
MS-DOS Startup Menu
==================
1. Ethernet
2. Fast Ethernet
3. Token-Ring
4. FDDI
5. Return to Main Menu
Enter a choice:
```

8. Choose the LAN application you want and press **ENTER**.

Exiting from Internet Advisor LAN

When you exit from an Internet Advisor LAN application, you exit to the current selection for starting from Windows 95 or starting from a DOS menu.

To exit from Internet Advisor:

1. Select the Utilities icon.
2. Highlight the Exit to DOS item.
3. Press **ENTER**.

NOTE

A dialog box warns you that exiting will cause all measurements to be stopped and unsaved data to be lost.
The message about restarting Network Advisor by typing “ADVISOR” at the DOS prompt is no longer effective. You can restart by using either the Windows 95 Start menu or the alternate DOS menu described in the previous sections of this chapter.

4. Press **ENTER** to exit the application.

NOTE

If you exit from a LAN application to the MS-DOS Startup Menu, you will be at the prompt for MS-DOS. To return to the MS-DOS Startup Menu, press CTRL, ALT, DELETE (to reboot the Internet Advisor) or cycle the power.

Setting Date, Time, and Time Zone

You may need to set the Internet Advisor's date, time, and time zone for your location.

To set date, time, and time zone

1. From the Windows 95 desktop, select the Start button 

.
2. Select Settings | Control Panel and then select the Date/Time icon.
3. In the Date/Time tab, set your local date and time.
4. In the Time Zone tab, set your local time zone.

Setting the Printer

Internet Advisor's default printer selection is No Printer. If you want to use a printer, you must select the printer driver and output port.

To select a printer:

1. From the Windows 95 desktop, select the Start button 

.
2. Select Settings | Control Panel.
3. Select the Printers icon.
4. Select the Add Printer icon.
5. Use the Add Printer Wizard window to select the printer driver and port you want to use.

Using a Mouse

You can use a mouse to perform most functions except the entry of text. Anything you can do with a mouse you can also do with the Internet Advisor LAN's keyboard, so a mouse is not required. There is a mouse housed in the Internet Advisor or you can attach and use an external mouse.

The visible indication of the mouse is the mouse cursor. The mouse cursor is represented by different symbols depending on the mode of operation:

- It is an arrow in normal mode.
- It is an hourglass whenever the Internet Advisor LAN is working and cannot accept further keyboard or mouse input.
- It is a vacuum cleaner whenever the Internet Advisor LAN is gathering memory so the memory can be used again.

The following terms describe typical mouse operations. If you use a mouse that has more than one button, you can use any mouse button to perform mouse operations.

Operation	Description
Move or point	Move the mouse to position the mouse cursor on (over) an object.
Click	Press and then release a mouse button.
Double-click	Press and quickly release a mouse button two times.
Press and hold	Press a mouse button and continue to hold the button down instead of releasing it.
Drag	Move the mouse after you have pressed and are still holding down a mouse button.

Using the Keyboard

You can use the keyboard to operate the Internet Advisor LAN. The function keys located at the top of the keyboard let you do common window management functions with one key stroke.

Function Key	Action
F1 - Help	displays general help on the window with focus (the window you are in).
F2 - Next Window	causes the "next" window or icon to receive focus. Windows cycle in the order they were created, not with any relation to their position on the screen.
SHIFT + F2	gives focus to the previous window; in other words, it cycles through the windows in the opposite order.
F3 - Next Pane	cycles focus through the panes in a multiple-pane window.
SHIFT + F3	cycles through the panes in the opposite order.
F4 - Window Menu	causes the Window Menu of the window you are in to dropdown, if the window has a Window Menu button.
F5 - Close Window	closes the window you are in if the window has a Window Menu. **F5** works the same as pressing **F4** (Window Menu) and then **C** (Close).
F6 - Fault Finder	gives focus to the Fault Finder window, if it is opened.
F7 - Event Log	gives focus to the Event Log window, and if the Event Log window is iconized, it is opened.
F8 - Measurements	gives focus to the Measurements window, and if the Measurements window is iconized, it is opened.

F9 - Setup	gives focus to the Setup window, and if the Setup window is iconized, it is opened.
F10 - Utilities	gives focus to the Utilities window, and if the Utilities window is iconized, it is opened.
F11 - Nodelist	gives focus to the Node/Station List window, and if the Node/Station List window is iconized, it is opened.
F12 - Filters	gives focus to the Filters window, and if the Filters window is iconized, it is opened.
ESC - Menu Bar	shifts focus to and from the menu bar of the window with focus. When the menu bar has focus, the first menu bar item is highlighted and its dropdown menu appears. Subsequent keystrokes apply to that dropdown menu or other menu bar items. Pressing **ESC** again takes focus off the menu bar.

Some other important keys are described below. The System Topics online help index contains a topic called “Keyboard Interface” that explains the Internet Advisor LAN's keyboard in more detail.

Keys	Action
Accelerators	each menu bar item and each item in a dropdown menu has one underlined character. When the menu bar has focus, typing the underlined character in a menu bar item selects that menu bar item and displays its dropdown menu. Similarly, when a dropdown menu is displayed, typing the underlined character in an item selects that item.
Arrow keys	the ←, →, ↑, and ↓ arrow keys and the **PgUp** and **PgDn** keys perform several different functions depending where they are used. They can move the highlight between items, move the text entry cursor (I-beam), or scroll information.
CTRL+**ALT**+**DEL**	this combination of keys reboots the Internet Advisor LAN.

Enter	this key selects (performs the default action for) the highlighted item or object. For example, pressing **Enter** starts the highlighted measurement in the Measurements window. Pressing **Enter** after you make a selection for a text entry field, causes the selection to be accepted (as long as it is an allowed selection).
PRTSC	this key prints whatever is on the screen to a printer if you are in the DOS mode. If you are in the Internet Advisor LAN mode, it prints what is on the screen to a printer or a file, depending on the selections you make in the PC Configuration window (a subwindow of the Utilities window). This is useful for printing the results of a measurement.

Using the Windows Interface

The Internet Advisor LAN uses a windowing type of display interface. There can be several windows open at once. The “active” window or the window “with focus” is the one that receives keyboard or mouse input. It is displayed on top of other windows it overlaps, and its title bar is highlighted.

Two of the main window functions you will need to perform are selecting items from dropdown menus and making selections for text entry fields.

Selecting Menu Items

Every window has a menu bar with items. When a menu bar item is highlighted, its dropdown menu appears. The dropdown menu lists items you can use to perform specific functions. Below are some conventions used for menu items.

Keys	Action
Grayed-out item	an item that cannot be selected at the current time is disabled by being grayed-out. Because the Measurements window is a top-level window, it can never be closed so the Close item is grayed-out.
An ellipsis (...)	items that open a new window to extend the functionality of the parent window are marked with an ellipsis.
A right arrow	items that have a cascaded menu (another dropdown menu that lists additional items) are marked by a trailing right arrow. Pressing **Enter** displays the cascaded menu.
A checkmark	items that toggle between one state and another are preceded by a checkmark when they are in effect.

When you choose an item in a menu, the Internet Advisor LAN either performs a command, opens a new window, or asks you for more information with a dialog box.

There are three ways to use the keyboard to select menu items: accelerators (underlined characters that are a quick selection method), the arrow keys, and using a mouse.

The following figure shows a “dropdown menu’ from the Control selection in the menu bar.

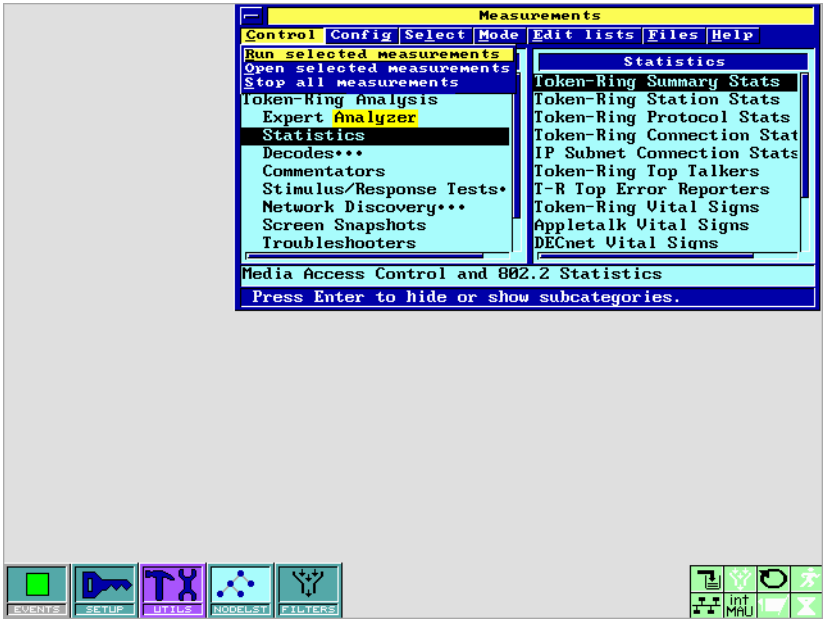


Figure 2-4: Dropdown Menus

Selecting Menu Items with Accelerators

1. Press **ESC**(Menu Bar) to give focus to the menu bar.
2. Press the underlined character of the desired menu bar item to display its dropdown menu (unless you want the first menu bar item; its dropdown menu is automatically displayed when you press **ESC**).
3. Press the underlined character of the desired dropdown item.

Selecting Menu Items with Arrow keys

1. Press **ESC** (Menu Bar) to give focus to the menu bar.
2. Use the ← and → arrow keys to move the highlight to the desired menu bar item and display its dropdown menu.
3. Use the ↑ and ↓ arrow keys to highlight the desired dropdown item.
4. Press **Enter** to select the highlighted item.

Selecting Menu Items with a Mouse

1. Move the mouse cursor so it is on the desired menu bar item.
2. Press and hold a mouse button to display its dropdown menu.
3. Drag the mouse cursor over the desired dropdown item.
4. Release the mouse button to select the item.

Making Selections for Text Entry Fields

Many of the Internet Advisor LAN's windows have two panes:

- A left pane that has text entry fields (also known as fields or text entry boxes), check boxes, push buttons, and other items
- A right pane, called a list pane, that shows choices for the text entry fields

The Autostart Configuration and Setup windows are examples of such windows.

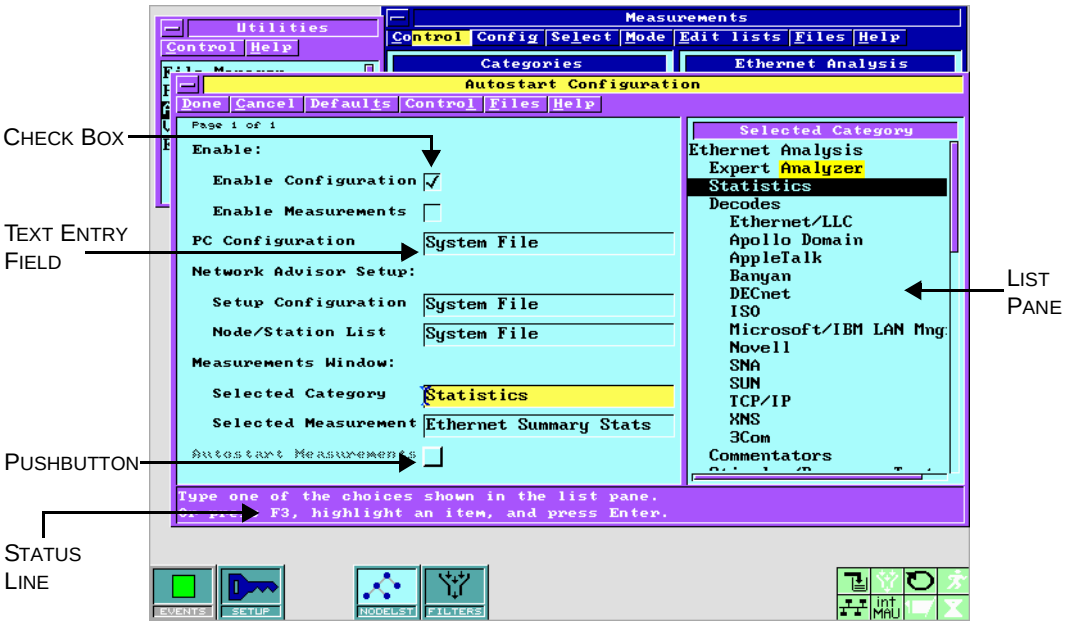


Figure 2-5: List panes and text entry fields

When focus (indicated by the highlight) is in the left pane, you can move focus between the items using the ↑ and ↓ arrow keys. When focus is on an item, the status line at the bottom of the window gives directions on how to make a selection for that item.

For example, when focus is on a text entry field, the status line gives directions according to the type of text entry field.

There are two types of text entry fields:

- Fields that can only contain one of the choices shown in the list pane. An example of this is the Network Interface field in the Setup window.
- Fields that can contain either one of the choices shown in the list pane or a choice of your own not shown in the list pane. An example of this is the Advisor Physical Address field in the Setup window.

You can use the keyboard or a mouse to make a selection for a text entry field.

Using the Keyboard to Select a Choice from a List Pane

1. Press **F3** (Next Pane) until focus is in the left pane.
2. Use the ↑ and ↓ arrow keys to highlight the desired text entry field.
3. Type the first character of a choice shown in the list pane. If an item in the list pane starts with that character, it is highlighted.
4. If there are other items that start with the same character, type enough characters to highlight the particular item you want.
5. Press **Enter**. The choice is put into the text entry field.

OR

1. Press **F3** (Next Pane) until focus is in the left pane.
2. Use the ↑ and ↓ arrow keys to highlight the desired text entry field.
3. Press **F3** (Next Pane) to give focus to the list pane.
4. Use the ↑ and ↓ arrow keys to highlight the desired choice, or type enough characters to highlight the item you want.
5. Press **Enter**. Your choice is put into the text entry field.

Using a Mouse to Select a Choice from a List Pane

1. Move the mouse cursor so it is over the desired text entry field.
2. Click a mouse button to give focus to the text entry field.
3. If the item you want to select from the list pane is visible, move the mouse cursor over the item and click a mouse button once to highlight the item and a second time to put the item into the text entry field.
4. If the item you want to select from the list pane is not visible, move the mouse cursor over the vertical scroll bar and click a mouse button to display a different part of the list. Then click a mouse button once to highlight the item and a second time to put the item into the text entry field.

Typing a Choice of Your Own into a Text Entry Field

Use this procedure only for text entry fields that can contain either one of the choices shown in the list pane OR a choice of your own.

1. Press **F3** (Next Pane) until focus is in the left pane.
2. Use the ↑ and ↓ arrow keys to highlight the desired text entry field.
3. Type your choice into the text entry field.
4. Press **Enter**.

Making Selections with the Status Icons

The status icons in the lower right corner of the screen graphically show the status of the Internet Advisor LAN. Some of the icons open a window that controls their function, and some of the icons select a direct action.

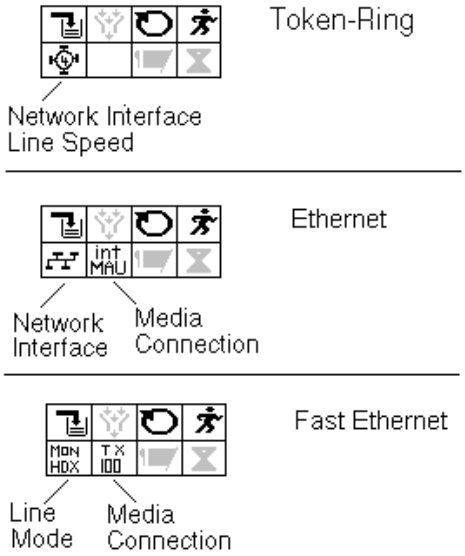


Figure 2-6: Status icons

In Fast Ethernet, the two icons located at the lower left corner have different functions. They identify the Line Mode and Line Speed. These icons are static, they do not toggle or make selections.

Using the Status Icons

The function of each of the status icons is described below.

Data Source

The Internet Advisor LAN can analyze data flowing directly from the network, or postprocess data previously saved in the capture buffer.

The Data Source icon toggles between getting data from the network under test (arrow showing data going into the buffer) and reading data from the capture buffer (arrow showing data flowing out of the buffer).

In Fast Ethernet, the Data Source icon turns red if frames are not captured in the buffer.

Active Capture Filter

When you are testing a network, you can activate a filter to control what frames you save into the capture buffer.

The Active Capture Filter icon is shown as a funnel in bold outline if the following setup conditions are true; otherwise, it is shown in white.

- Network Under Test is selected as the Data Source in the Setup window.

  AND

- A filter is activated in the Capture Filters window.

When you first turn on the Internet Advisor LAN and no filters are activated, the filter icon is white. If you select the filter icon, the Capture Filters window is opened and you can define or activate filters you need.

After you activate a filter, selecting the filter icon toggles the filter between active and inactive.

Capture Buffer Mode

When you are testing a network, you can set the capture buffer to capture data continuously (circularly) or to capture data only until the capture buffer is full.

Selecting the Capture Buffer Mode icon toggles between Continuous and Stop When Full modes.

The continuous Capture Buffer Mode icon is shown as a circle in bold outline when the following conditions are true; otherwise, it is shown in white.

- Network under test is selected as the Data Source in the Internet Advisor LAN's Setup window.

  AND

- Continuous Mode is selected as the Buffer Mode in the Internet Advisor LAN's Setup window.

The linear Capture Buffer Mode icon is shown as a linear list in bold outline when the following conditions are true; otherwise, it is shown in white.

- Network under test is selected as the Data Source in the Internet Advisor LAN's Setup window.

  AND

- Stop When Full mode is selected as the Buffer Mode in Internet Advisor LAN's Setup window.

Measurement Running

The Measurement Running icon looks like a running figure in black if measurement which does not transmit on the network is running. It is shown in red if any measurement which transmits on the network is running. It is shown in white if no measurements are running.

You can stop all running measurements by selecting the black or red running man.

Selecting the white running man has the effect of starting any open measurements. If any measurements are open and Data Source is set to Capture Buffer, you must switch the Data Source to Network Under Test and then select the running man.

Network Interface



For 10 Mbps Ethernet, FDDI, and Token-Ring Internet Advisor interfaces the Network Interface icon shows the type of network being tested. Ethernet is shown as a bus with nodes attached. Token-Ring is shown as a ring with stations attached and it shows a value of 4 or 16 to indicate the line speed in Mbits per second. FDDI is shown as initials representing the Connection Mode and Connection Type, for example, DAS or SAS.

For Fast Ethernet, the Network Interface status icon box shows the Line Mode. See the Line Mode status icon description.

Selecting the Network Interface causes the window containing the interface parameters for the current network testing interface to open. You can then select Internet Advisor LAN setup parameters for the network interface you are using.

The Network Interface icon for Token-Ring is shown in bold outline if these conditions are true; otherwise, it is shown in white.

- Token-Ring is selected as the Network Interface in the Setup window.

  AND

- Network Under Test is selected as the Data Source in the Setup window.
- AND
- Participating in Ring is enabled in the Setup window.

The Token-Ring icon shows an X through the stations and the 4 or 16 if the following setup conditions are true.

- Token-Ring is selected as the Network Interface in the Setup window.

  AND

- Network Under Test is selected as the Data Source in the Setup window.

  AND

- Participate in Ring is NOT enabled in the Setup window.

The Network Interface icon for Ethernet shows several nodes connected to a bus in bold outline if these conditions are true; otherwise, it is shown in white.

- Network Under Test is selected as the Data Source in the Setup window.

  AND

- Ethernet is selected as the Network Interface in the Setup window.

The Network Interface icon for FDDI is shown as the initials of the Connection Mode and Connection Type requested in the FDDI Interface Parameters of the Setup window. If the requested connection is not presently in effect, the initials are shown under a red X.

10 Mbps Ethernet Connector

You can connect the Internet Advisor LAN to a 10 Mbps Ethernet network using the AUI or the 10baseT connector on the network interface module.

If an Ethernet interface is being used, when you select the Ethernet Connector icon, it toggles between AUI and int MAU.

The Ethernet Connector icon shows AUI in bold letters when these conditions are true; otherwise, it is shown in white.

- Network Under Test is selected as the Data Source in the Setup window.

  AND

- AUI is selected as the Media Connection in the Setup window.

The Ethernet Connector icon shows int MAU in bold letters when these conditions are true; otherwise, it is shown in white.

- Network Under Test is selected as the Data Source in the Setup window.

  AND

- int MAU is selected as the Media Connection in the Setup window.

Fast Ethernet Media Connection

When Fast Ethernet is selected as the Network Interface, a non-toggling status icon identifies the current selection in the Media Connection field.

The Media Connection field lets you choose the test port you are using.

With a Fast Ethernet interface module, you can connect the Internet Advisor LAN to a 10 Mbps Ethernet network using the AUI, MII, or TX connectors on the network interface module.

You can also connect the Internet Advisor LAN to a Fast Ethernet network using the MII, TX, or SC connectors on the network interface module.

Depending on which Media Connection you select, the Line Mode and Line Speed fields let you make additional selections about the connection. For example, you can choose between Full Duplex and Half Duplex and between 10 Mbits/sec and 100 MBits/sec.

Fast Ethernet Line Mode

When Fast Ethernet is selected as the Media Interface, a non-toggling status icon identifies the current selection in the Line Mode field.

The Line Mode field identifies whether the Internet Advisor is operating in full duplex or half duplex line mode.

Fast Ethernet Line Speed

The Line Speed field lets you choose whether the Internet Advisor is operating at 10 MBits/sec or 100 MBits/sec. In the Auto Negotiate selections for Media Connection, the Line Mode field and status icon show the negotiated line speed.

FDDI Port State

The FDDI Port State icon shows the real time state of each Internet Advisor LAN port involved in the current interface connection. The port state is reported as wrapped (WP), good connection (OK), or not connected (ISO).

Partial Packet Store

When you are capturing data from a network, you can select to capture only part of each packet. This is referred to as packet slicing or partial packet store.

Selecting the Partial Packet Store icon toggles between enabling and disabling the storage of partial packets.

The Partial Packet Store icon looks like a start flag followed by a frame of data being truncated if the following setup conditions are true; otherwise, it is shown in white.

- Network Under Test is selected as the Data Source in the Setup window.

  AND

- Partial Packet Store is enabled in the Setup window.

User Interface Working

The User Interface Working icon shows the state of the user interface in much the same way as the mouse cursor does. This lets you see the state of the user interface even if you do not have a mouse attached.

The User Interface Working icon is shown as an hour glass in bold outline whenever the user interface is working and cannot accept further keyboard or mouse input; otherwise, it is shown in white.

Selecting the User Interface Working icon has no effect, no action occurs.

Using Online Help

The Internet Advisor LAN has extensive online help. This User's Guide contains step by step instructions for running some of the representative measurements in the Internet Advisor LAN. For detailed instructions on all measurements, use the online help that is present in every window.

There are two main ways to get help:

- Pressing **F1**
- Using the Help dropdown menu

You can press **F1** from any window and get general help for that window. In addition, most windows have the rightmost menu bar item labeled Help.

The first three items in Help menu let you access help for a specific window. The help topics for a specific window include reference information about what the window does, what the menu items do, and what any selections in the window do. There may also be procedural topics that explain how to do something. Windows such as detailed decode windows also have reference information about the protocol.

The last three items in the Help menu access "system topics". These are topics that apply to the Internet Advisor LAN in general, not just to one window.

Using the Help Menu

- To get an alphabetical index or list of all the help topics for the window you are in, select the first menu item (labeled "xxx topics" where "xxx" is the name of the window). Once you are in the index, highlight the topic you want and press **Enter**.

- To get help about the menu bar items and dropdown menus in the window you are in, select the "Menu bar Description" item.

- To get general information about the functions of the window you are in, select the “About This Window” item. This opens the same help topic that pressing **F1** opens.
- To get detailed help about how the Internet Advisor LAN's windows interface works, select the “Using the Windows Interface” item.
- To get detailed help about how the help facility works, select the “Using Help” item. This help topic is more complete than what you are reading here.
- To get an alphabetical index or list of the system help topics, select the “System Topics” item. Once you are in the index, highlight the topic you want and press **Enter**.
- To print all the help topics in the current help window, go to the index of topics and select ‘Print/All Topics’ from the help window menu bar. You can print either to a file or to a printer depending on the configuration selected in the ‘PC Configuration’ in the Utilities window.

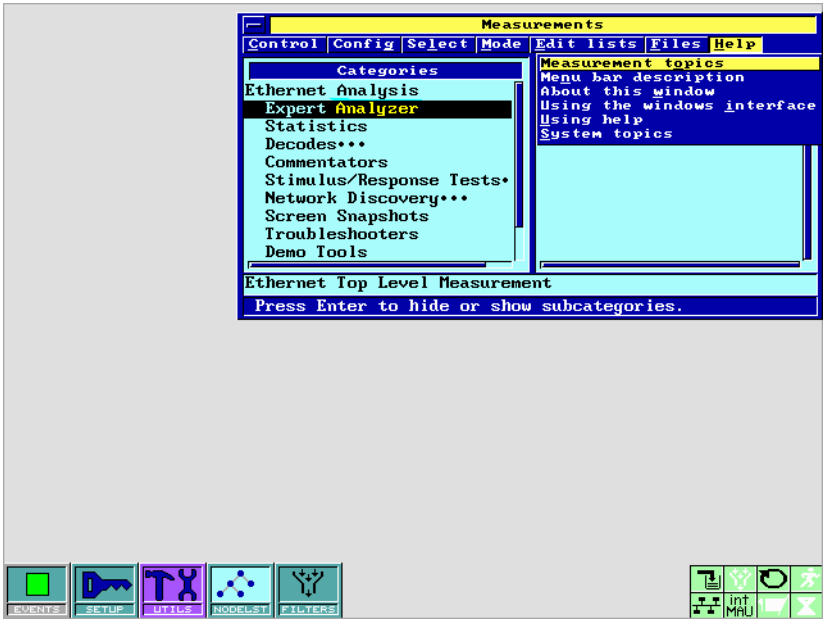


Figure 2-7: Help menu

Setting up to Test a Network

The Setup window lets you control the configuration of the Internet Advisor LAN. The selections you make in the setup window are global selections that affect the way measurements run.

To test a network, rather than to post-process data in the capture buffer or a file, certain setup conditions such as the data source and the type of network interface must be selected before you start any measurements. Other setup conditions, such as whether to use a capture filter, are optional.

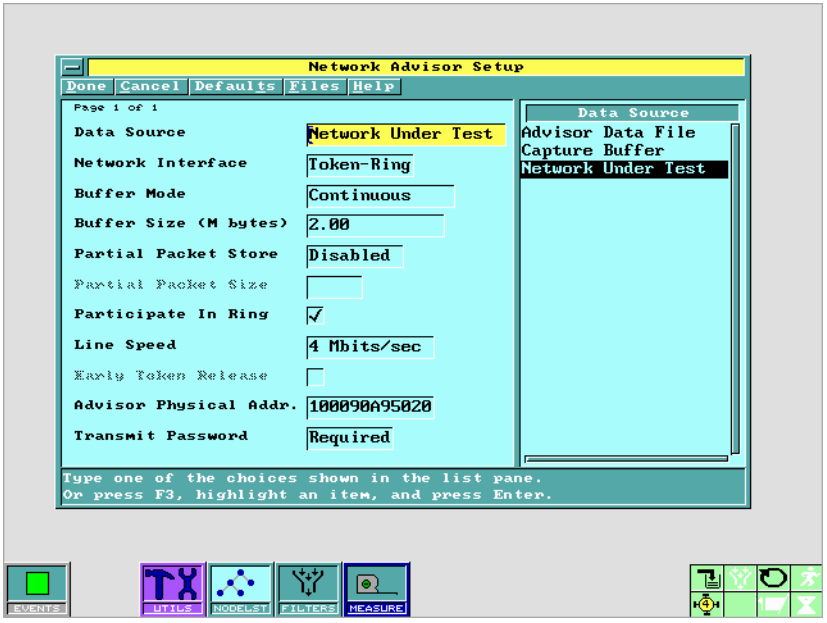


Figure 2-8: Setup window

Set up for a 10 Mbps Ethernet Network

Connect to the Network

1. Connect the Internet Advisor LAN to the network you want to test. Use the appropriate Ethernet connector (AUI, RJ-45, or BNC (Thinlan)) on the side of the Internet Advisor LAN.

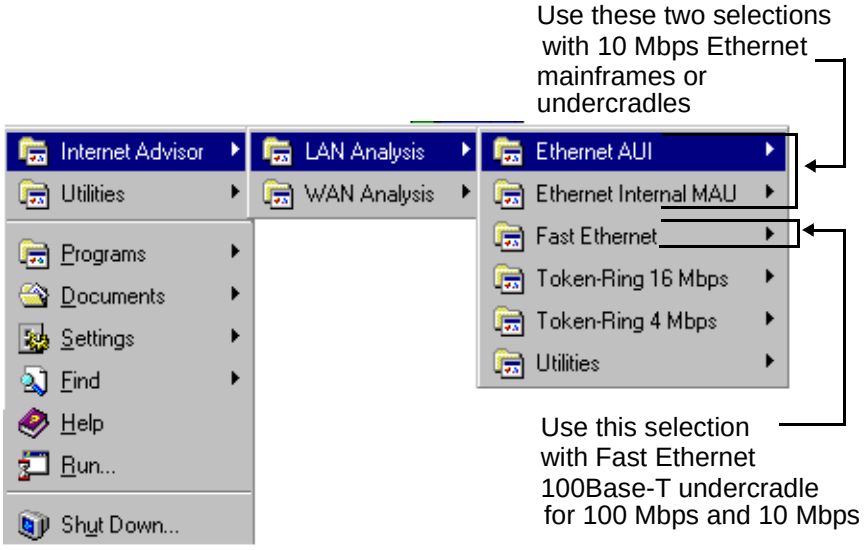


Figure 2-9: Selecting 10 Mbps Ethernet from the Start Menu

Select the Ethernet Network Interface

1. In the Windows 95 Start menu, select Internet Advisor | LAN Analysis | and then select the Ethernet connector you want to use.

   In the Setup window, Ethernet is displayed in the Network Interface field. Either AUI or Internal MAU is displayed in the Media Connection field depending on what you selected in the Start menu.

Select the Media Connection

1. In the Setup window, use the Media Connection field to select the test port you are connecting to the network.

Select the Data Source

1. Select Network Under Test in the Data Source field.

Configure the Capture Buffer

1. Select the buffer mode you want. In ‘Continuous’ mode, data fills the buffer until you stop the measurement, which means that once the buffer is full, newer data overwrites the older data. In ‘Stop When Full’ mode, the measurement stops as soon as the buffer is full.

2. Select the buffer size you want.

3. Select whether or not to use partial packet store (packet slicing). Enabling partial packet store causes the Internet Advisor LAN to capture only the first portion of each packet. This lets you store more packets for a given buffer size.

4. If you enabled partial packet store, select the partial packet size.

Select the Physical Address

1. Use the Internet Advisor LAN's unique physical layer address in the Advisor Physical Addr field, or enter another address. You can use another address if you want to simulate another node.

Save Your Setup

1. Select ‘Save setup/filter changes and Iconize’ in the Done menu to save your selections and iconize the Setup window.

Activate Capture Filters

1. Activate any filters you want to use in Capture Filters window. Chapter 8 explains how to create and activate filters.

Set up for a Fast Ethernet Network (100Base-T)

Connect to the Network

1. Connect the Internet Advisor LAN to the network you want to test using the appropriate Fast Ethernet connector (MII, TX, or FX) on the side of the Fast Ethernet undercradle.

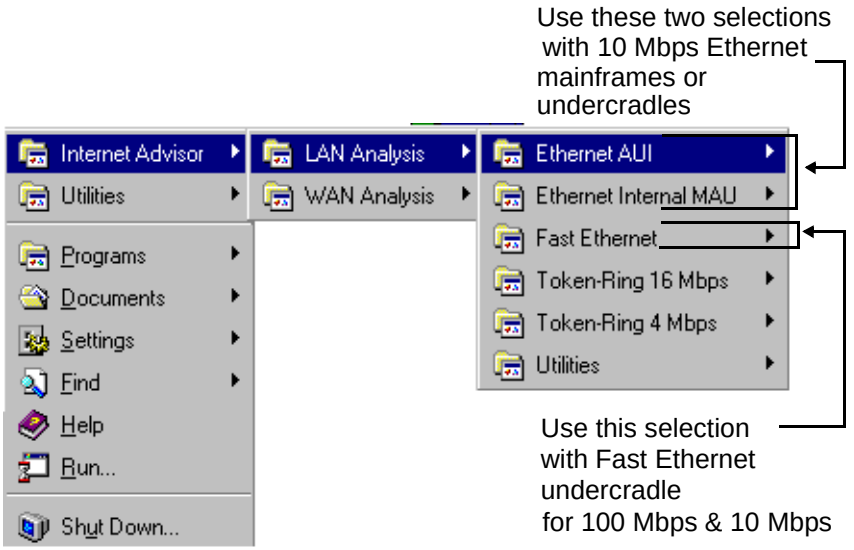


Figure 2-10: Selecting Fast Ethernet from the Start Menu

Select the Fast Ethernet Network Interface

1. In the Windows 95 Start menu, select Internet Advisor | LAN Analysis | Fast Ethernet. After Internet Advisor LAN starts, the Setup window shows Ethernet in the Network Interface field.

NOTE

10 Mbps Ethernet may also be tested with the Fast Ethernet undercradle. You select 10 Mbps Ethernet in the Setup window after you start the Internet Advisor LAN.

Select the Media Connection, Line Mode and Line Speed

1. In the Setup window, use the Media Connection field to select the test port you are connecting to the network.

2. Select the Line Mode you want to use (either half duplex or full duplex).

NOTE

10 Mbps Ethernet typically operates in half duplex (HDX) mode. That is, a node transmits and receives at different times. With Fast Ethernet, the transmit and receive lines can operate in full duplex (FDX) mode where both the transmit and the receive lines are active at the same time for a total throughput of 200 Mbits/sec.

With Monitor Full Duplex selected as the Line Mode, Internet Advisor LAN may not capture at the full 200 Mbit/sec throughput. To see full traffic in one direction, you can select either Hub to Node Only or the Node to Hub Only for Line Mode and the Internet Advisor will capture the full 100 Mb thoughput for the selected line.

3. Select the Line Speed you want to use (either 10 or 100 Mbit/sec).

NOTE

If you choose an Auto Negotiate selection for Media Connection, the Line Mode and Line Speed fields display the negotiated line speed.

Select the Data Source

1. Select Network Under Test in the Data Source field.

Configure the Capture Buffer

1. Select the buffer mode you want. In ‘Continuous’ mode, data fills the buffer until you stop the measurement, which means that once the buffer is full, newer data overwrites the older data. In ‘Stop When Full’ mode, the measurement stops as soon as the buffer is full.

2. Select the buffer size you want.

3. Select whether or not to use partial packet store (packet slicing). Enabling partial packet store causes the Internet Advisor LAN to capture only the first portion of each packet. This lets you store more packets for a given buffer size.

4. If you enabled partial packet store, select the partial packet size.

Select the Physical Address

1. Use the Internet Advisor LAN's unique physical layer address in the Advisor Physical Addr field, or enter another address. You can use another address if you want to simulate another node.

Save Your Setup

1. Select ‘Save setup/filter changes and Iconize’ in the Done menu to save your selections and iconize the Setup window.

Activate Capture Filters

1. Activate any filters you want to use in Capture Filters window. Chapter 8 explains how to create and activate filters.

Set Up for an FDDI Network

Select the Network Interface

1. Connect the Internet Advisor LAN to the network you want to test using the FDDI connectors on the side of the Internet Advisor LAN. See the Internet Advisor Mainframe Features manual for more information. If you are unsure of the state of the ring, connect the Internet Advisor LAN as a single attach station through a concentrator. The A/S/M port on the Internet Advisor LAN attaches to the concentrator's M port. This configuration does not disturb the dual ring, but lets the Internet Advisor LAN run decodes and display Summary Stats.

2. In the Setup window, select FDDI in the Network Interface field.

3. Double-click on the Interface Parameters push button to open the FDDI Parameters window.

4. Select the Connection Mode and Connection Type that describe the way the Internet Advisor LAN is connected to the FDDI ring. For connecting to the concentrator, choose Connection Mode = Station, and Connection Type = Single Attach Station-S.

5. Enter a Target Rotation Time or accept the default of 160 milliseconds.

6. Use the Internet Advisor LAN's unique physical-layer address in the Advisor Physical Addr field, or enter another address.

7. Select 'Accept Changes and Exit' in the Done menu to save your selections and return to the Setup window.

8. The first two icons in the second row of status icons give you information about the state of the connection. The online help topics in this window contain more information about each field.

Select the Data Source

1. Select Network Under Test in the Data Source field.

Configure the Capture Buffer

1. Select the buffer mode you want. In Continuous mode, data fills the buffer until you stop the measurement, which means that once the buffer is full, newer data overwrites older data. In Stop When Full mode, the measurement stops as soon as the buffer is full.

2. Select the buffer size you want.

3. Select whether or not to use partial packet store (packet slicing). Enabling partial packet store causes the Internet Advisor LAN to capture only the first portion of each packet. This lets you store more packets for a given buffer size.

4. If you enabled partial packet store, select the partial packet size.

Activate the Capture Filters

1. Activate any filters you want to use in Capture Filters window. Chapter 8 explains how to create and activate filters.

Save Your Setup

1. Select ‘Save setup/filter changes and Iconize’ in the Done menu to save your selections and iconize the Setup window.

Set Up for a Token-Ring Network

Select the Network Interface

1. Connect the Internet Advisor LAN to the network you want to test using the Token-Ring connector on the side of the Internet Advisor LAN.

2. In the Setup window, select Token-Ring in the Network Interface field. If you are changing the interface selection, a dialog box asks you to confirm loading the new interface.

3. Select whether to participate in the ring or not. If you choose not to participate in the ring, the Internet Advisor LAN passively monitors the network and inserts into the ring, but you cannot perform measurements that transmit such as Traffic Generator or Request Station ID.

4. Select the appropriate line speed depending on the type of network you are connected to.

5. Select whether or not to have early token release. Early token release causes the Internet Advisor LAN to release the token immediately after it transmits the last bit of a frame it is transmitting. You can select early token release only with 16 Mbits per second line speed.

Select the Data Source

1. Select Network Under Test in the Data Source field.

Configure the Capture Buffer

1. Select the buffer mode you want. In Continuous mode, data fills the buffer until you stop the measurement, which means that once the buffer is full, newer data overwrites older data. In Stop When Full mode, the measurement stops as soon as the buffer is full.

2. Select the buffer size you want.

3. Select whether or not to use partial packet store (packet slicing). Enabling partial packet store causes the Internet Advisor LAN to capture only the first portion of each packet. This lets you store more packets for a given buffer size.

4. If you enabled partial packet store, select the partial packet size.

Select the Physical Address

1. Use the Internet Advisor LAN's unique physical-layer address in the Advisor Physical Addr field, or enter another address. You can use another address if you want to simulate another station.

Save Your Setup

1. Select 'Save setup/filter changes and Iconize' in the Done menu to save your selections and iconize the Setup window.

Activate the Capture Filters

1. Activate any filters you want to use in Capture Filters window. Chapter 8 explains how to create and activate filters.

Starting a Measurement

The Measurements window organizes all of the Internet Advisor LAN's measurements. The left pane of the Measurements window, labeled Categories, contains a hierarchy of categories and subcategories. Categories and subcategories contain measurements in much the same way that DOS directories and subdirectories contain files. The category structure organizes related measurements.

There are three top-level categories: Ethernet Analysis, Token-Ring Analysis, and FDDI Analysis. These categories correspond to the three network interfaces you can use with the Internet Advisor LAN.

The right pane of the Measurements window displays measurements. It can either display the list of all measurements regardless of what category they are in, or it can display the measurements in a particular category, depending on which item is active in the Select menu.

1. Make sure the correct network interface is selected in the Setup window for the type of measurement you want to run.

For Example. . . For example, if you want to run an Ethernet measurement, make sure the Network Interface field is Ethernet. Make sure any other setup choices, such as data source and capture filters are selected correctly. Refer to *Setting up to Test a Network*.

2. In the Measurements window, double-click on the measurement you want to run, or

   a. Press **F3** until focus is in the right-hand pane.

   b. Use the ↑ and ↓ arrow keys to highlight the measurement.

c. Press **Enter** or select the Run Selected Measurements item in the Control menu.

Regardless of which method you use, you may need to highlight the category in the left pane that contains the measurement you want to run.

After the measurement is started, a window opens showing the results of the measurement.

You can start more than one measurement at a time by enabling the Select Multiple Measurements item in the Mode menu. When this item is active (indicated by a checkmark), use the **Space Bar** to put a right-pointing arrow in front of all the measurements you want to run simultaneously. Then use the Run Selected Measurements item in the Control menu to start the measurements.

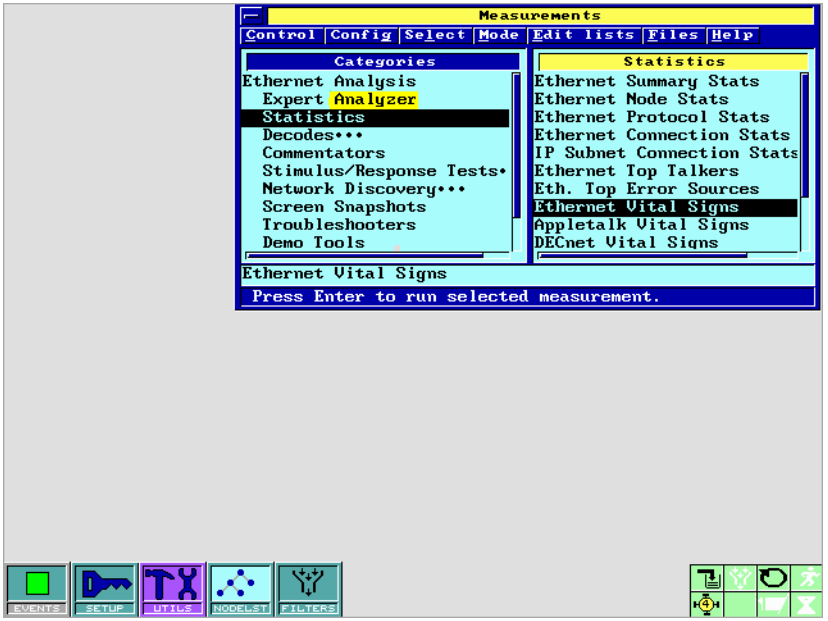


Figure 2-11: Starting a measurement

Some measurements have a Configuration window in which you can specify options or values for some fields. You may want to configure a measurement before you run it. For configurable measurements, use the Control menu to stop the measurement, then select the Config menu to open the Configuration window.

Installations

If you ordered a separate Internet Advisor LAN undercradle for your Internet Advisor, follow the instructions below to attach it, then follow the instructions to install software if you need to.

If you are installing a Fast Ethernet or an FDDI undercradle, you will need to check the power supply source before you install the undercradle.

NOTE

Power Supply Requirement for the J2524A FDDI Undercradle and the J3444A Fast Ethernet Undercradle

You can identify whether your Advisor needs the Power Supply Upgrade Kit J3308A by the serial number on your Internet Advisor.
Internet Advisor's with serial prefix numbers less than 3518 will need the Power Supply Upgrade Kit J3308A installed before you can use the J2524A or J3444A undercradles. Contact your local Hewlett-Packard Sales office for information.

CAUTION

The HP J2524A FDDI Undercradle and the HP J3444A Fast Ethernet Undercradle require the Advisor you attach it to be equipped with an 80 Watt Power Supply.

Attaching an Undercradle to the Internet Advisor LAN

WARNING

Be sure the Internet Advisor is turned off and disconnected from any power source before you begin any assembly or disassembly procedures.

The undercradle contains the hardware needed to run with Hewlett-Packard LAN Internet Advisor. To attach this undercradle to the Internet Advisor, follow these steps:

1. Turn off and disconnect the Internet Advisor from any power source.

2. Remove the two screws from the face plate on the bottom of the Internet Advisor using the wrench provided in the module kit.

3. If the face plate is approximately 1.5” x 4”, save the screws you just removed if you ever want to re-attach the face plate. Install the two short screws (you received in the bundle of parts) in the bottom of the Internet Advisor. After installation of the two short screws, they should be flush with the bottom sheet metal.

CAUTION

It is important to install the two short screws (you received in the bundle of parts) in the bottom of the Internet Advisor if the face plate you removed was 1.5” x 4”.

4. If the face plate is approximately 1” x 4”, save the screws you just removed if you ever want to re-attach the face plate. It is not necessary to install the two short screws (you received in the bundle of parts) into the bottom of the Internet Advisor.

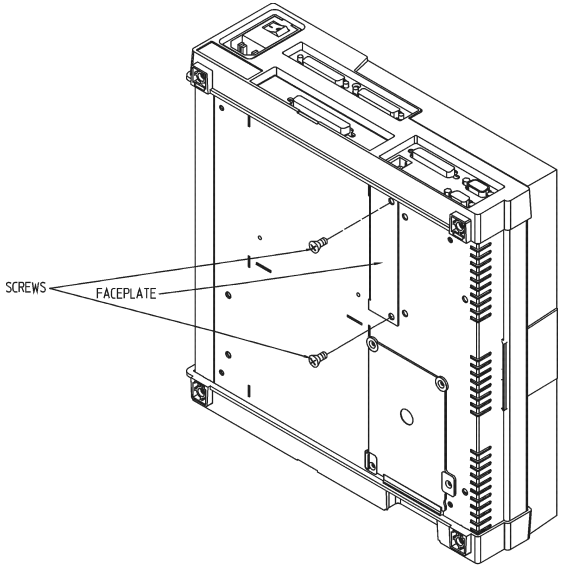


Figure 2-12: Location of Faceplate on Internet Advisor

5. Insert the connector board into the slot uncovered by the face plate.

6. Position the undercradle with the four black feet down and the undercradle connector to your left. Two of the silver tabs should face you.

7. Make sure all four silver tabs are pulled out.

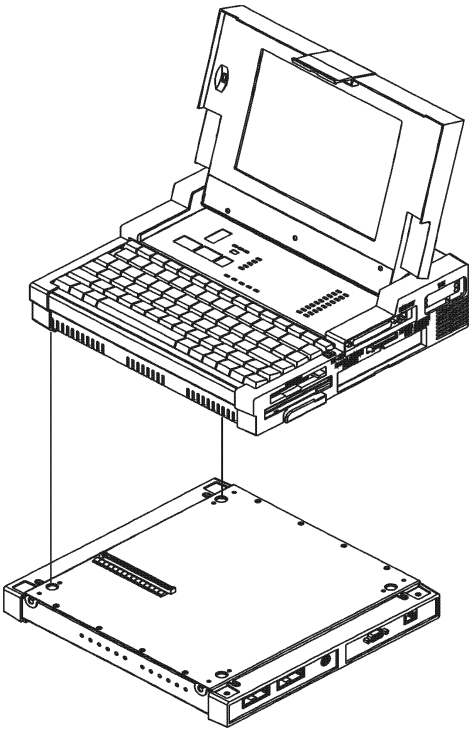


Figure 2-13: Placing the Advisor on an Undercradle

8. Place the Internet Advisor on top of the undercradle, matching the connector on the bottom of the Internet Advisor to the connector on the top of the undercradle.

9. Push in the four silver tabs, locking the undercradle to the Internet Advisor.

Removing the Undercradle from the Internet Advisor

With the Internet Advisor turned off and unplugged:

1. Pull out the four silver tabs on the front and the back of the undercradle.
2. Lift the Internet Advisor away from the undercradle.
3. Remove the connector board from the slot of the Internet Advisor.

Install or Remove Slide-in Interface Modules

To install the slide-in interface module in an undercradle:

1. Slide the module into the opening of the undercradle.

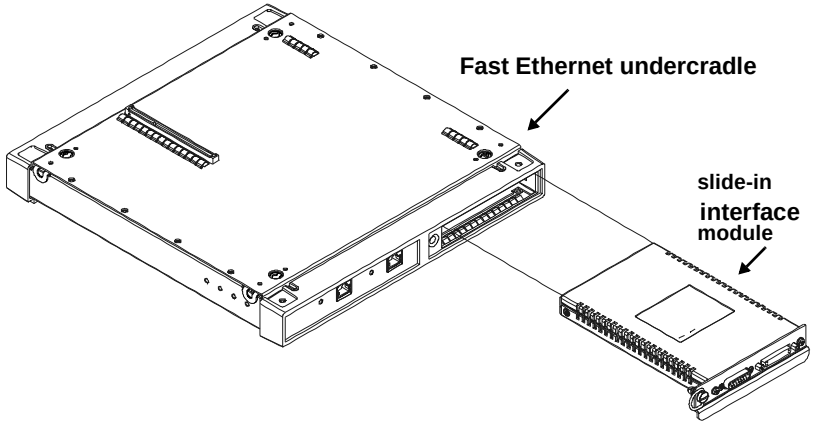


Figure 2-14: Install an Interface Module in an Undercradle

2. Push the slide-in module into place until it seats in the undercradle and then rotate the fastener 1/4 turn to lock the slide-in module in place.

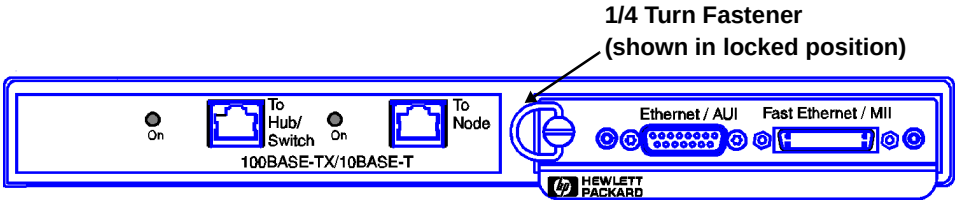


Figure 2-15: 1/4 Turn Fastener on slide-in module

To remove a slide-in interface module from an undercradle:

1. Rotate the fastener 1/4 turn to unlock the slide-in module.
2. Pull on the bottom of the slide-in module's front panel.

   It is not recommended to pull on the 1/4 turn fastener.

10 Mbps Ethernet Interface Connections

The following HP Internet Advisor products have 10 Mbps Ethernet and switched 10 Mbps Ethernet interfaces:

J2306B, J2309B, J2522B, and J2523B.

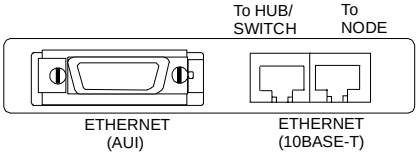


Figure 2-16: 10 Mbps Ethernet Connectors

To connect to an Ethernet segment, you can use either the 15-pin AUI or the RJ-45 connectors. The AUI connector is used for universal Ethernet testing through the use of an external transceiver.

The Ethernet configuration in the Setup window must match the connector type you choose. See the online help in the Setup window for more information.

Connecting as a Node to 10 Mbps Ethernet

Several following figures illustrate connecting the Internet Advisor LAN as a node to an Ethernet network.

Connecting as a Node to an AUI Connector

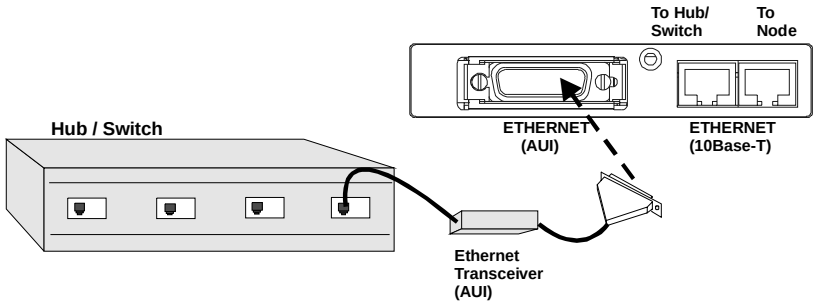


Figure 2-17: Connecting as a Node to AUI

When Internet Advisor LAN is connected at the AUI test port, the Internet Advisor can view traffic it sees at the test port. Internet Advisor can monitor and simulate with this connection.

Connecting as a Node to a Hub/Switch with a RJ-45 Connector

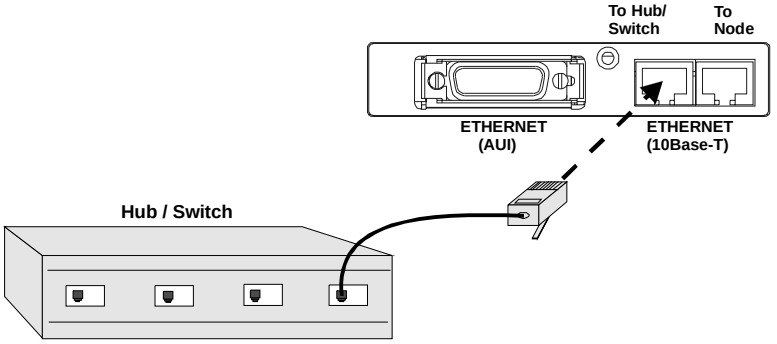


Figure 2-18: Connecting to a hub/switch with a RJ-45 connector

With this connection, the Internet Advisor LAN can monitor activity from the hub/switch directly by using the ‘To Hub’ connection only. The ‘To Node’ connection is not used.

Connecting in Monitor Mode to 10 Mbps Ethernet

The HP Internet Advisor has built-in circuitry that allows testing in a switched 10 Mbps Ethernet environment.

Monitoring Switched 10 Mbps Ethernet

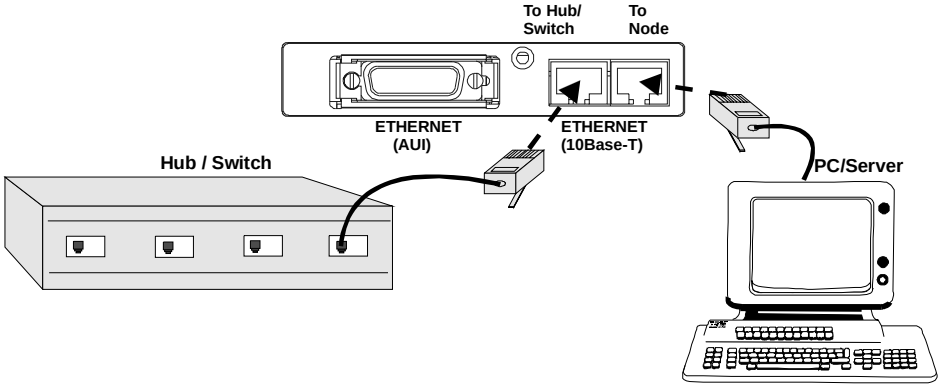


Figure 2-19: Monitoring switched 10 Mbps Ethernet

You can use the two 10 Mbps Ethernet RJ-45 connectors to connect the Internet Advisor into a 10 Mbps switched Ethernet segment for monitoring. The connection labeled ‘To Hub’ is connected to a switch or hub. The connection labeled ‘To Node’ is connected to a node or server.

NOTE

The HP Internet Advisor will not operate properly if you connect it to two different Ethernet segments. Do not connect ‘To Node’ to a hub or a switch.

Fast Ethernet Interface Connections

The HP J3446C Internet Advisor LAN mainframe provides 10 Mbps Ethernet, Fast Ethernet, and switched 10/100 Mbps interfaces. The HP J3447C slide-in module provides the HP J3444C mainframe with a multimode fiber interface with SC connectors.

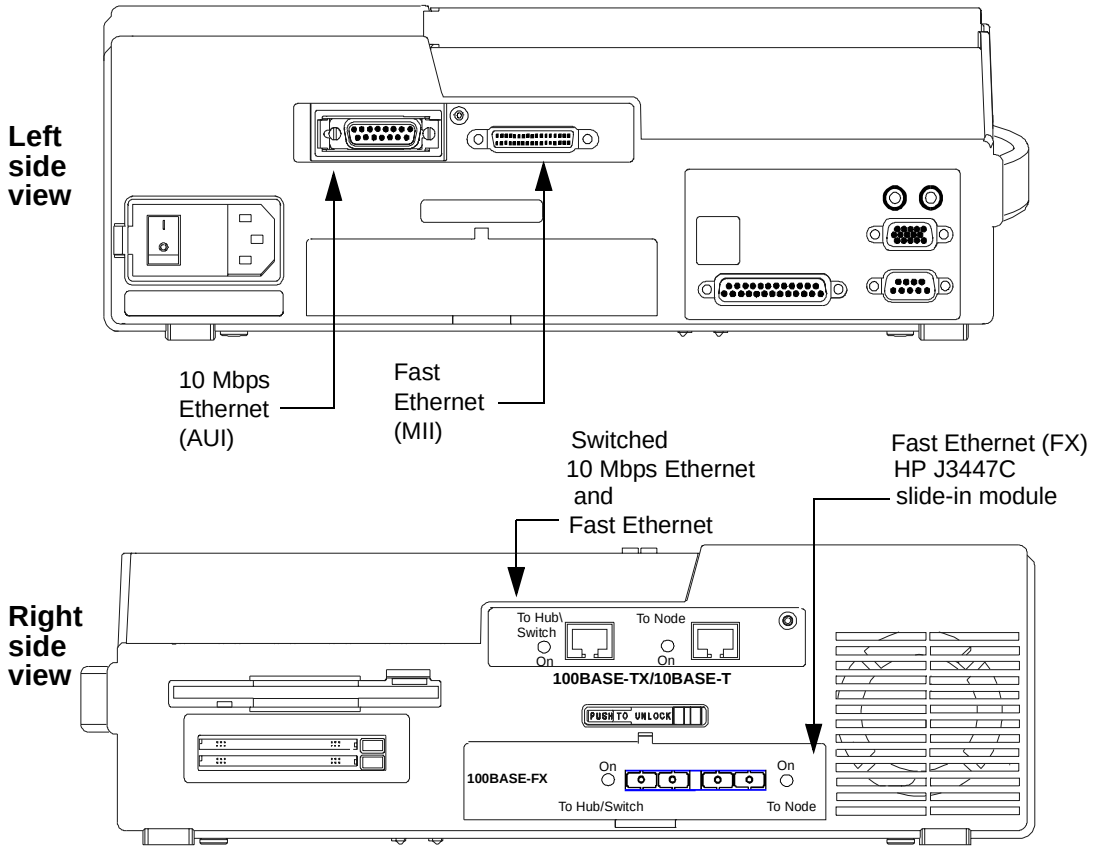


Figure 2-20: HP J3446C Internet Advisor and HP J3447C slide-in module interfaces

The HP J3444A Fast Ethernet undercradle also provides 10 Mbps Ethernet, Fast Ethernet, and switched 10/100 Mbps interfaces. The HP J3445A slide-in module provides the HP J3444A undercradle with a multimode fiber interface with SC connectors.

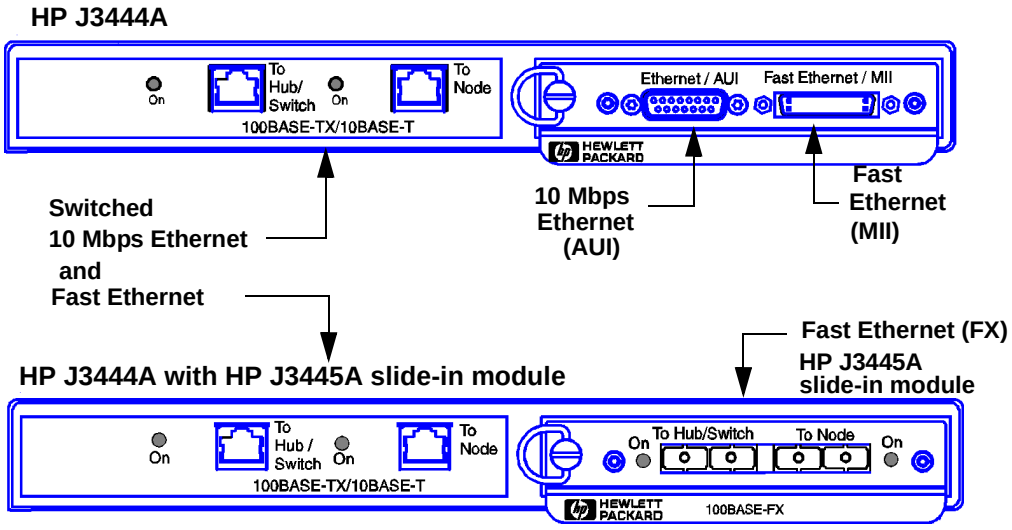


Figure 2-21: HP J3444A/J3445A Undercradle/Slide-in Module 10/100 Mbps Ethernet and Switched Ethernet Interfaces

The Fast Ethernet mainframe and the undercradle each has two RJ-45 ports to allow connection to unshielded twisted pair (UTP) cabling. These ports, labeled ‘To Hub/Switch’ and ‘To Node,’ let you monitor the signal between a node and a hub/switch on a pass-through basis or let you terminate the signal as a node.

The HP J3446C mainframe and the standard HP J3444A undercradle each has an AUI connector and a Media Independent Interface (MII) connector. The AUI connector lets you use an Ethernet transceiver to connect to a 10 Mbps Ethernet network. The MII connector lets you use an external transceiver to connect to other physical interfaces such as T4 and fiber. The MII connector supports auto negotiation between 10 and 100 Mbps.

Connecting as a Node to 10 Mbps Ethernet

Several following figures show how to connect the Internet Advisor LAN as a 10 Mbps Ethernet node using the Fast Ethernet undercradle.

Connecting as a Node with the AUI Connector

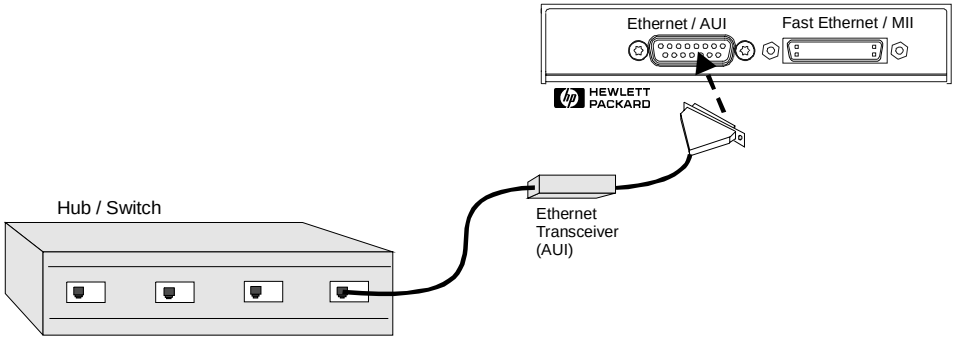


Figure 2-22: Connecting as a node with the AUI connector

With this connection, your Internet Advisor can monitor 10 Mbps Ethernet and simulate 10 Mbps Ethernet data using the LAN applications.

Connecting as a Node with the MII Connector

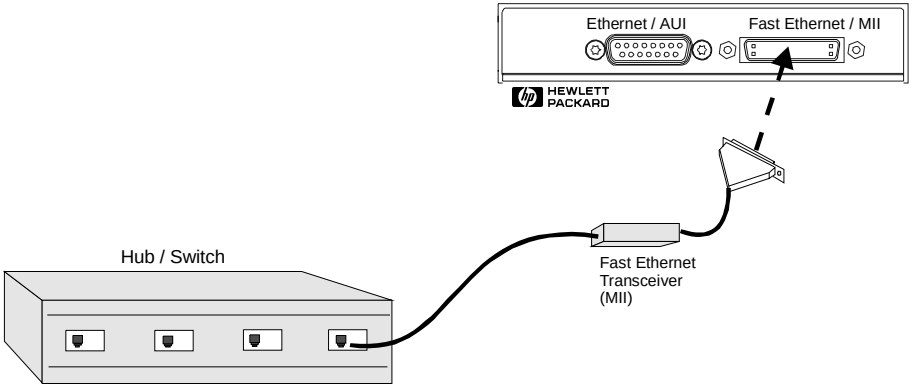


Figure 2-23: Connecting as a node with the MII connector

With this connection, your Internet Advisor can monitor Fast Ethernet and simulate Fast Ethernet data using the LAN applications.

NOTE

You should connect the MII Fast Ethernet Transceiver to the Internet Advisor when the power is off. The Internet Advisor software recognizes the transceiver at power on.
If you connect the transceiver with the Internet Advisor power on, you may be able to select only half duplex operation.

Connecting as a Node to a Hub/Switch with a RJ-45 Connector

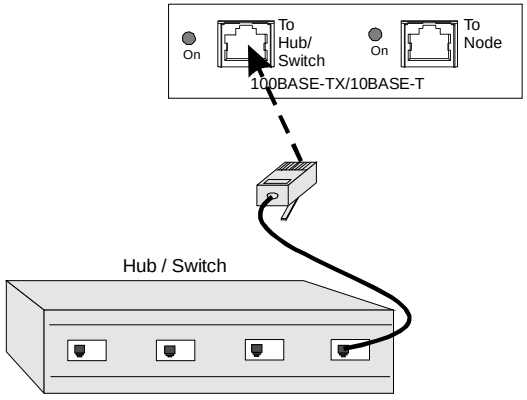


Figure 2-24: Connecting to a hub/switch using a RJ-45 connector

With this connection, the Internet Advisor LAN can monitor activity from the hub/switch directly by using the ‘To Hub’ connection only. The ‘To Node’ connection is not used.

The Auto negotiate selections in the Setup window let you monitor either 10 Mbps or 100 Mbps.

Connecting as a Node to a Hub/Switch with a SC Connector

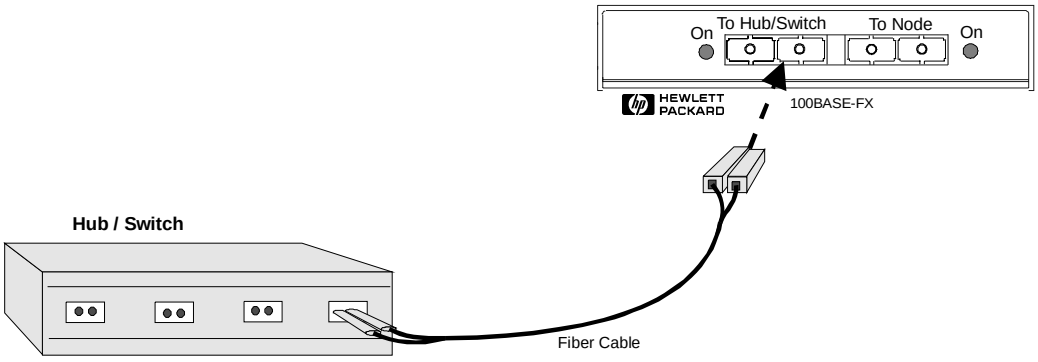


Figure 2-25: Connecting to a hub/switch with a SC connector

With this connection, The Internet Advisor LAN can monitor Fast Ethernet data on multimode fiber (FX) using the LAN applications.

Using the 'To Node' port to Monitor Traffic Between a Node and a Hub/Switch

The next two figures show how to connect the Internet Advisor LAN for monitoring 10/100 Ethernet traffic between a node and a hub/switch. The table below shows the fields you must select in the Setup window.

Table 2-1: Internet Advisor Setup Window Settings

	Setup Window		
Monitor Function	**Media Connection**	**Line Speed**	**Line Mode**
monitor 10 Mb Ethernet in half duplex	TX 10 Mb Ethernet	10	Monitor Half Duplex
monitor 10 Mb Ethernet in full duplex	TX Fast Ethernet	10	any Monitor Full Duplex mode
monitor Fast Ethernet in half duplex	TX Fast Ethernet	100	Monitor Half Duplex
monitor Fast Ethernet in full duplex	TX Fast Ethernet	100	any Monitor Full Duplex mode

TIP: You can not monitor with TX Auto Negotiate selected as the media connection because auto negotiation can only occur between the two end devices. In this mode, the Internet Advisor is only monitoring and cannot participate in the auto negotiate process.

For switched 10/100 Ethernet, Internet Advisor LAN does not perform crossover of transmit/received pairs internally. If this function is required (e.g. connecting two switches together) the crossover function must be done external to the Internet Advisor LAN.

FAQ

In monitor mode, do I use straight or crossover cables?

Answer: Use the cable you would use for a node to hub/switch connection as one of the cables in monitor mode and then use a straight-through cable for the other connection. The combined cable length for the two connections should not exceed 100 meters.

Monitoring Switched 10 Mbps and Fast Ethernet with RJ-45 Connectors

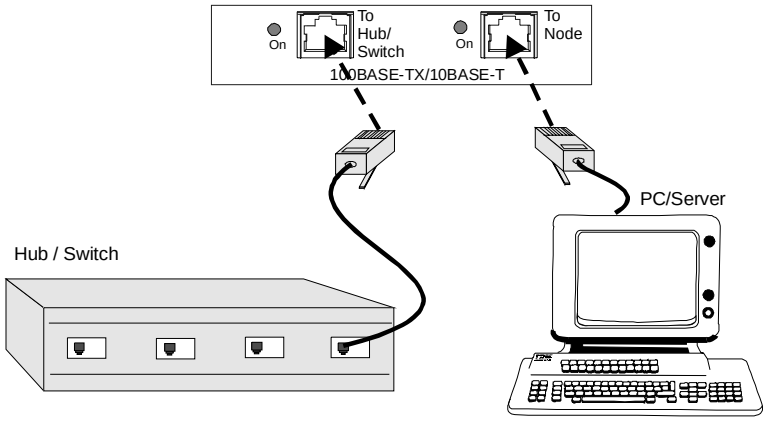


Figure 2-26: Monitoring switched 10/100 Mbps Ethernet with RJ-45 connectors

Monitoring Switched Fast Ethernet with a SC Connector

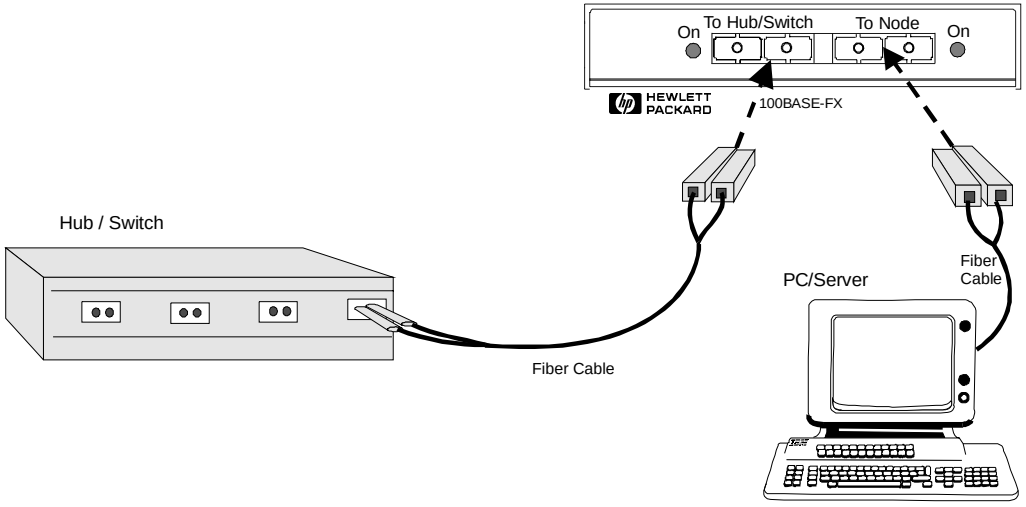


Figure 2-27: Monitoring switched Fast Ethernet with SC connectors

Connecting to a 4/16 Mbps Token-Ring Network

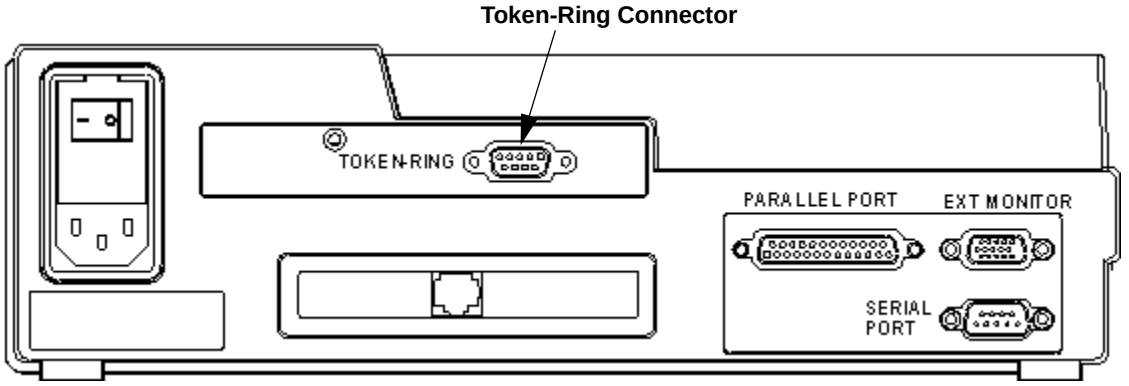


Figure 2-28: Connecting to a Token-Ring network

To connect the HP Internet Advisor to a Token-Ring network, use the 9-pin Token-Ring connector. Make sure the 4/16 Mbps Line Speed parameter in the HP Internet Advisor Setup window matches the line speed of your Token-Ring network.

Ethernet\Fast Ethernet LEDs

LEDs on the Internet Advisor and the Fast Ethernet undercradle identify selections made in the Setup window and Ethernet traffic occurring at the test connector ports.

Selected Interface LEDs

On the Internet Advisor, LEDs identify which Media Connection and Line Mode selections are chosen in the Setup window. You can select one of four different media connections and one of two line modes. The LED state updates when you start a new measurement.

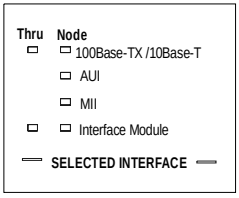


Figure 2-29: Ethernet/Fast Ethernet LEDs

Node	The four LEDs in this column identify the active test port selected by Media Connection field in the Setup window, that the Internet Advisor is connected for node operation, and a measurement is started. The Interface Module LED identifies that the FX (fiber) module is selected.
Monitor/Thru	The two LEDs in this column identify a monitor operation is selected in the Line Mode field in the Setup window. An LED lights when the Internet Advisor is connected for monitoring, and a measurement is started. Monitoring between a node and a hub/switch can only be done at the 100 Base-TX/10 Base-T connectors and the FX fiber connectors.

Ethernet Activity LEDs

On the HP J3446C Internet Advisor and the HP J3444A undercradle, LEDs indicate Ethernet activity occurring at the active test port selected by the Media Connection field in the Setup window.

Figure 2-30: Ethernet Activity LEDs

Receiving from: Hub/Switch	This LED lights when frames are seen at the receive data pins (3, 6) of the To Hub/Switch port. Frames can be present when the Internet Advisor is connected as a node or in monitor mode.
Receiving from: Node	This LED lights when frames are seen at the receive data pins (3, 6) of the To Node port. The To Node port is used only when Internet Advisor is in monitor mode (selected in the Setup window).
Transmit	In the 'Node' mode, this LED lights when Internet Advisor is transmitting frames. For example, Traffic Generator or a Stimulus/Response measurement is running.
Collision	In the 'Node' mode, this LED lights when the Internet Advisor is trying to transmit a frame and a collision is detected. Full Duplex disables collision detection and the LED does not light.

Installing (or reinstalling) the Operating Software

NOTE If you are installing or reinstalling the Internet Advisor LAN software, be sure to save any node list or filter files you have created to a floppy disk before installing the new LAN software.

To install the Internet Advisor LAN software, first remove any attached undercradle and then use the instructions in the *HP Internet Advisor Software Installation Guide* supplied with the Internet Advisor software CD.

An Internet Advisor Software Installation Guide is stored in the cover of the CD case.

3

Running Statistical Measurements

What's in this Chapter

This chapter describes how to use the HP Internet Advisor LAN's various statistical measurements. These measurements show important information about the network's overall performance, and also about particular nodes or stations.

You can run statistical measurements from either the network under test or from frames in the Advisor capture buffer. If you want to replay frames in the capture buffer, use the Control menu of the measurement to switch to the capture buffer, then use the Control menu "Run measurement from Capture Buffer". See the Menu Bar online help in the measurement for more information.

When you are using the Fast Ethernet undercradle, you should not have more than two or three measurement running at one time. Running multiple Fast Ethernet measurements at the same time may cause the Internet Advisor to not capture frames at the full line rate. Expert Analyzer for Fast Ethernet should be run only one measurement at a time.

NOTE

This manual provides detailed information about typical measurements on the Internet Advisor LAN, but does not cover each measurement in every category. Detailed information and step by step instructions for every measurement are provided in the online help topics for each measurement.

- **Ethernet, Fast Ethernet, FDDI, and Token-Ring Summary Stats -** These measurements use graphs, gauges, and pie charts to summarize the network's overall performance. The measurements show the percentage of the network's capacity being used, the number and type of errors occurring, the mix of protocols on the network, and the number of nodes on the network.

  Since the Fast Ethernet undercradle lets you select Line Speed (10/100) and Line Mode (half duplex/full duplex), measurements that display utilization do calculations based on the current line speed and line mode. The list below summarizes the maximum rate (100% utilization).

Speed / Mode		Max Rate (100%utilization)
100 Mbit	-- Half Duplex	100 Mbit
100 Mbit	-- Full Duplex	200 Mbit
10 Mbit	-- Half Duplex	10 Mbit (standard Ethernet)
10 Mbit	-- Full Duplex	20 Mbit

In addition to the data presented in the Summary Stats window, you can get more detailed information by “drilling down” from the Summary Stats measurements to additional windows.

The results of these measurements can be plotted to a graph in the Trends Graphical window, or shown in a tabular format in the Trends Tabular display. You can also log data to disk. See the Files menu bar help for more information.

- **Ethernet Node Stats, FDDI, and Token-Ring Station Stats -**
  These measurements let you follow critical nodes. They graphically show, in either bar char or pie chart form, a variety of statistical information about 20 nodes. For example, the Token-Ring Station Stats measurement can be configured to show the 20 stations sending source routed broadcasts, all stations broadcasts, functional address frames, and source routed frames.

- **Ethernet, FDDI, and Token-Ring Protocol Stats -**
  These measurements chart the top 20 protocols on your network. You can choose to display IP, Novell, or Data Link Layer protocols. For each protocol, the display shows the number of frames, the number of bytes, the number of DLL errors, and the average frame length. See the online help for more information.

- **Ethernet, FDDI, and Token-Ring Connection Stats -**
  These measurements display statistical information for up to 20 connections. The stats shown are relevant to a connection between two nodes depending on the choices selected in the Stats Configuration window.

- **Ethernet, FDDI, and Token-Ring Top Talkers -**
  These measurements let you follow critical nodes. They list up to 50 nodes generating the most frames and how many bytes and frames each node is sending and receiving.

- **Ethernet and FDDI Top Error Sources and Token-Ring Top Error Reporters -** These measurements let you follow critical nodes. They list up to 50 nodes generating the most error frames, the total number of errors each node is generating, and the type of errors each node is generating.
- **Vital Signs**
  These measurements provide a tabular list of significant events. Baseline settings can be configured to trigger the measurements to stop. See the online help in Vital Signs configuration for more information.

The online help for each of these measurements explains the measurements in more detail.

Using the Summary Stats Measurements

The Summary Stats measurements each have three main windows:

- Summary Stats window
- Trends Graphical window
- Trends Tabular window

When you start a Summary Stats measurement from the Measurements window, a Summary Stats window opens. From the Summary Stats window, you can open the Trends Graphical or Trends Tabular windows. If you need additional information, you can “drill down” to more specialized tests from various Summary Stats measurements.

Starting a Summary Stats Measurement

The procedure below is for starting the Ethernet Summary Stats measurement, but the procedure is similar for starting FDDI or Token-Ring Summary Stats measurements also.

1. In the Measurements window, start the Ethernet Summary Stats measurement.

The Ethernet Summary Stats window opens. Graphs, gauges, and pie charts show the results of several individual measurements. This gives you a graphical summary of the activity on the network.

NOTE

Filters can be created in the Capture Filters window to control the capture or exclusion of specified frames or the stopping of a measurement. When a filter is activated, it is in effect for any measurement until you deactivate the filter, either in the Filters window, or by selecting the active filter status icon.

For More Summary Stats Information, you can “drill down” or open more statistics windows by using the following procedure:

1. When you move the mouse over a selected (highlighted) item in the Summary Stats window a magnifying glass appears

2. Click the mouse or press **ENTER** to open another window with additional statistics information.

For Example. . . If the background of the Collisions gauge turns red, this indicates that the number of collisions has exceeded the threshold set in the Collisions Configuration window (which is accessed by using the 'Configure Collisions' item in the Configuration menu). If you click once on the Collisions gauge, its title bar is highlighted and the mouse cursor turns into a magnifying glass. Clicking the mouse again opens the Ethernet Vital Signs measurement. From the Ethernet Vital Signs measurement you can get more detailed information about what type of collisions (local, late, remote, and remote late) are occurring.

. . . . . .

The following Ethernet measurements can be "drilled down" when you :

double-click on	**to open**
Network Utilization graph	Ethernet Top Talkers
Collisions gauge	Ethernet Vital Signs
Errors gauge	Ethernet Top Error Sources
Node Count gauge	Ethernet Node Stats
Bytes/Frame gauge	Ethernet Protocol Stats configured to show frame-length pie chart
Destination Addresses pie chart	Ethernet Node Stats configured to show Ethernet Destination Nodes
Protocols pie chart	Ethernet Protocol Stats
Selected Nodes graph	Ethernet Node Stats
Specific Node in Selected Nodes	Ethernet Node Stats configured to show frames to or from the selected node

NOTE You can perform these same drilldown actions with the keyboard by pressing **F3** until the desired title bar is highlighted, and then pressing **ENTER**.

The following FDDI measurements can be “drilled down” when you :

double-click on	**to open**
Network Utilization graph	FDDI Top Talkers
Frame Type pie chart	FDDI Top Error Sources
Errors gauge	FDDI Top Error Sources
Claim Frames gauge	FDDI Top Error Sources
Beacons gauge	FDDI Top Error Sources
Selected Stations graph	FDDI Station Stats
Specific Station in Selected Stations	FDDI Station Stats configured to show frames to or from the selected station
Destination Addresses pie chart	FDDI Station Stats configured to show Destination Frames and Bytes
LLC Protocols pie chart	FDDI Protocol Stats

The following Token-Ring measurements can be “drilled down” when you :

double-click on	**to open**
Network Utilization graph	T-R Top Talkers
Purges gauge	T-R Top Error Reporters
Soft Errors gauge	T-R Top Error Reporters
Claim Token gauge	T-R Top Error Reporters
Beacons gauge	T-R Top Error Reporters
Stations gauge	T-R Station Discovery configured to show observed stations only
Source Routing pie chart	T-R Source Routed Stations
Selected Stations graph	T-R Station Stats
Specific Station in Selected Stations	T-R Station Stats configured to show frames to or from the selected station
Protocols pie chart	T-R Protocol Stats

The following figures and tables explain what each of the Summary Stats gauges, pie charts, and graphs show, and the online help has additional details.

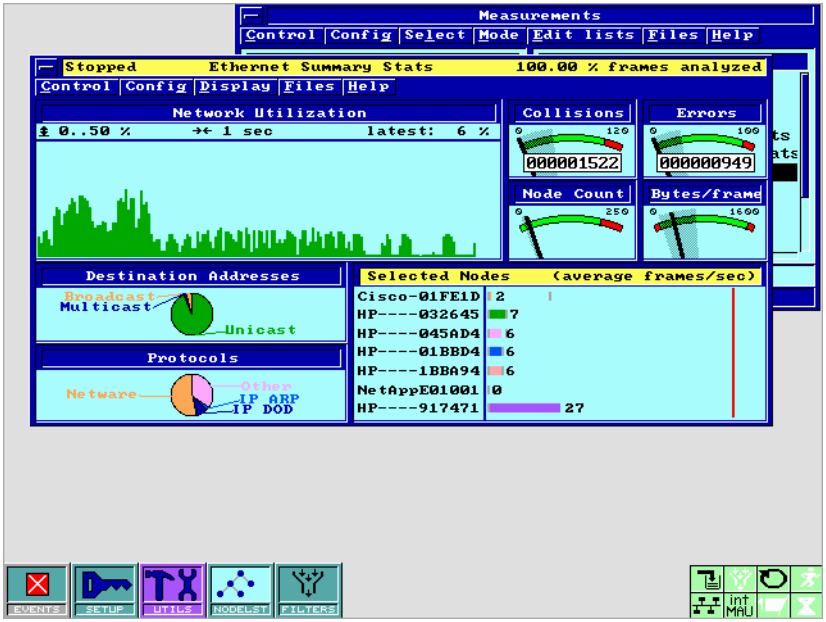


Figure 3-1: Ethernet Summary Stats window

Ethernet Summary Stats Measurement	What the Measurements Show
Network Utilization graph	shows % of network capacity being used during the selected sample period
Collisions gauge	shows number of collisions during the last second; shaded area shows min. and max., counter shows total number since start of test
Errors gauge	shows average number of errors during the last second; shaded area shows min. and max. number since start of test and counter shows total number since start of test
Node Count gauge	needle shows number of nodes that have transmitted during the last 10 seconds; shaded area shows min. and max. number since start of test
Bytes/Frame gauge	needle shows average number of bytes per frame during the last 10 seconds; shaded area shows min. and max. number since start of test
Destination Addresses pie chart	shows average % of broadcast, multicast, and unicast packets during the last 10 seconds
Selected Nodes bar graph	shows traffic generated in frames per second by 7 nodes
Protocols pie chart	shows the distribution of protocols on the network during the last 10 seconds

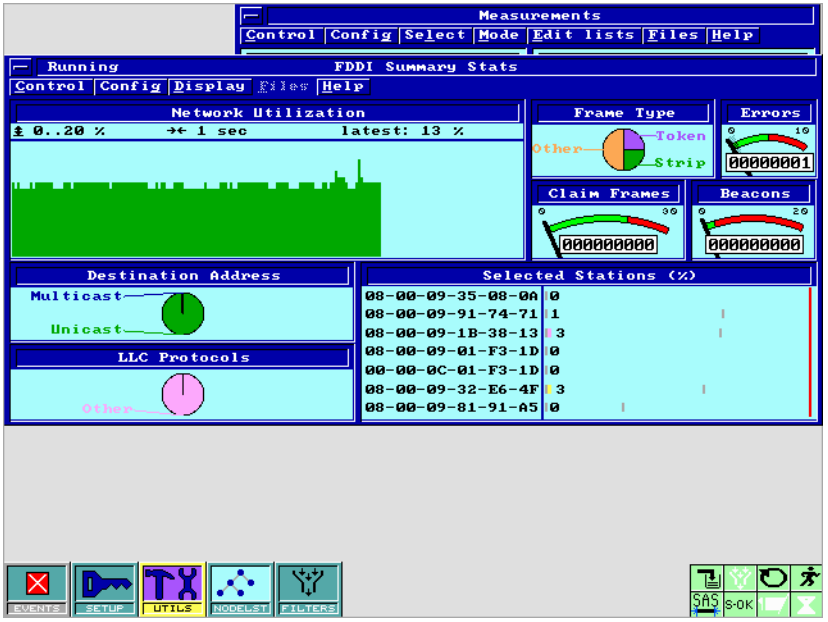


Figure 3-2: FDDI Summary Stats window

FDDI Summary Stats	What the Measurements Show
Network Utilization graph	% of network capacity being used during the selected sample period
Frame Type	pie chart shows mix of frame types on the network. Frame types shown: SMT, LLC, Tokens, Strip, and MAC (Claims and Beacons)
Errors gauge	configured to show the number of any of the five following error types: Bad FCS, Violation Symbol, Error flag set, Preamble too short, PDU too long; or, shows All errors. The needle shows the average number of errors over the last second, the counter, the total number since the gauge was reset
Claims gauge	average number of claims during the last second; shaded area shows min. and max. number since gauge was reset; counter shows total number since gauge was reset
Beacons gauge	average number of beacons during the last second; shaded area shows min. and max. number since gauge was reset; counter shows total number since gauge was reset
Destinations pie chart	mix of destination addresses during last 10 seconds: broadcast, multicast, and unicast
Protocols pie chart	the distribution of protocols on the network during the last 10 seconds
Selected Stations bar graph	shows traffic generated in frames per second by 7 stations

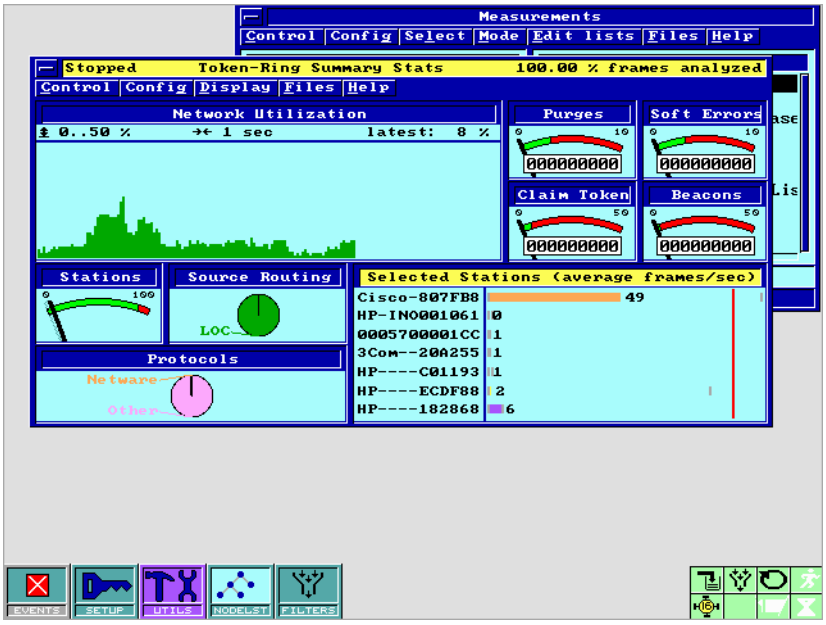


Figure 3-3: Token-Ring Summary Stats window

Token-Ring Summary Stats Measurements	What the Measurements Show
Network Utilization graph	% of network capacity being used during the selected sample period
Purges gauge	number of purges during the last second; shaded area shows min. and max. number since start of test; counter shows total number since start of test
Soft Errors gauge	average number of soft errors during the last second; shaded area shows min. and max. number since start of test; counter shows total number since start of test
Claim Tokens gauge	average number of claim tokens during the last second; shaded area shows min. and max. number since start of test; counter shows total number since start of test
Beacons gauge	average number of beacons during the last second; shaded area shows min. and max. number since start of test; counter shows total number since start of test
Stations gauge	number of stations on ring since the last neighbor notification; shaded area shows min. and max. number since start of test
Source Routing pie chart	local and remote routing patterns during last 10 seconds
Selected Stations bar graph	traffic generated in frames per second by 7 stations
Protocols pie chart	shows the distribution of protocols on the network during the last 10 seconds

Configuring Summary Stats

The Summary Stats windows have a Config menu bar item. Each item in the Configuration menu opens a window for one of the gauges, pie charts, or graphs in the Summary Stats windows.

For Example. . . The 'Configure Network Utilization' menu choice opens the 'Network Utilization Configuration' window. In this window you can change parameters that affect the Network Utilization graph. if you want to look at the level of use on the network, you can set a threshold level. Then, if the level of network utilization exceeds the threshold you specified, you will be notified.

The following procedure is for configuring the Ethernet Summary Stats Node Count gauge, but the procedure is similar for configuring any of the other Ethernet Summary Stats gauges, pie charts, or graphs or any of the FDDI or Token-Ring Summary Stats gauges, pie charts, or graphs.

1. In the Ethernet Summary Stats window, select the Configure Node Count item in the Config menu. The Node Count Configuration window opens.

2. Select a value for the Gauge Range field. This determines the range or maximum reading of the Node Count gauge. For example, if you select 50, the gauge has a range of 0 to 50.

3. Enable or disable the Threshold Enabled check box. This determines whether the value in the Threshold field has an effect.

   If you enable it (indicated by a check mark), the value in the Threshold field is used as a threshold level for the gauge. This causes the threshold to appear as a red area on the gauge. If the number of nodes exceeds the threshold, the gauge background turns red and an event is posted to the Threshold Browser of the Event Log.

4. If you enabled the Threshold Enabled check box, select a value for the Threshold field. The value must be less than the Gauge Range value, since the Gauge Range is the high-end of the gauge.

5. Enable the Clear Gauge check box if you want to reset the Node Count gauge.

6. Select Accept Changes and Exit in the Done menu to save your selections and return to the Summary Stats window. The new configuration is used in the Node Count gauge.

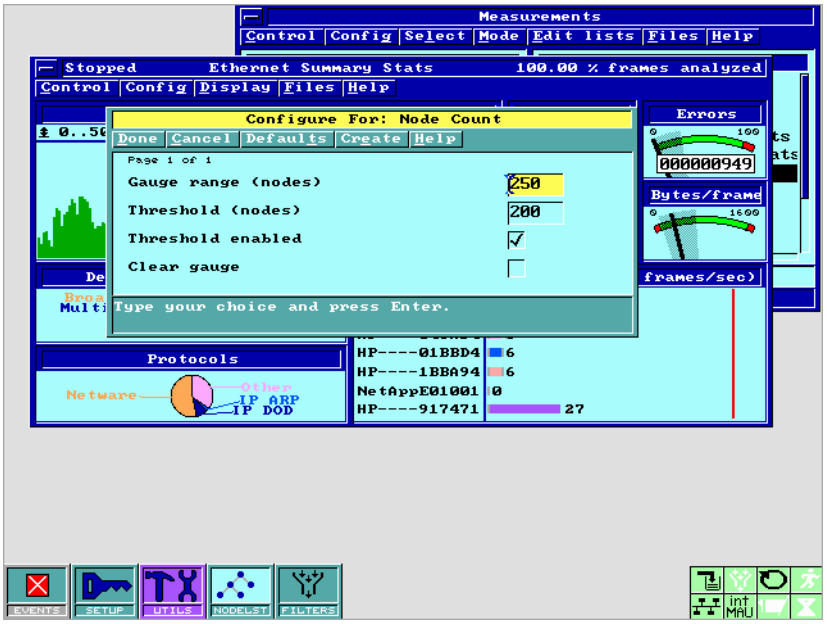


Figure 3-4: Node Count Configuration window

Using the Trends Tabular and Graphical Windows

The Trends Graphical windows let you plot four items against time on one graph. The Trends Tabular windows let you determine the exact value of the same four items at a given time. By using the Trends Graphical and Tabular windows, you can see any correlations in time between the four items.

For example, you can see the minimum, maximum, current, and total number of purges, beacons, claim tokens, and soft errors using the gauges in the Token-Ring Summary Stats window. If you then configure the Token-Ring Graphical and Tabular Trends windows to show purges, beacons, claim tokens, and soft errors, you can see correlations between these four items.

The procedure below is for using the Ethernet Trends Graphical window, but the procedure is similar for using the Ethernet Trends Tabular window or the FDDI or Token-Ring Trends Tabular and Trends Graphical windows.

1. In the Ethernet Summary Stats window, select Display Trends in Graphical Display in the Format menu.

   The Summary Stats window closes, and the Trends Graphical window opens showing the four items last selected in the Trends Configuration window. You can change the configuration so that four different items are shown.

   Each of the four items is graphed on its own scale, which is re-scaled as required. A maximum of 180 samples can be displayed for each item.

   The legend at the top of the Trends Graphical graph shows these things:

   - The leftmost column lists the items that are being graphed.
   - The Legend column shows the color being used for each of the items.
   - The Units column shows the unit of measure being used for each item. For example, “fr/sec” indicates an item is being measured in frames per second.
   - The Scale column indicates the vertical scale being used for each item.

- The Max column shows the maximum value measured for each item.
- The Avg column shows the average value measured for each item.
- The Current column shows the current value measured for each item.

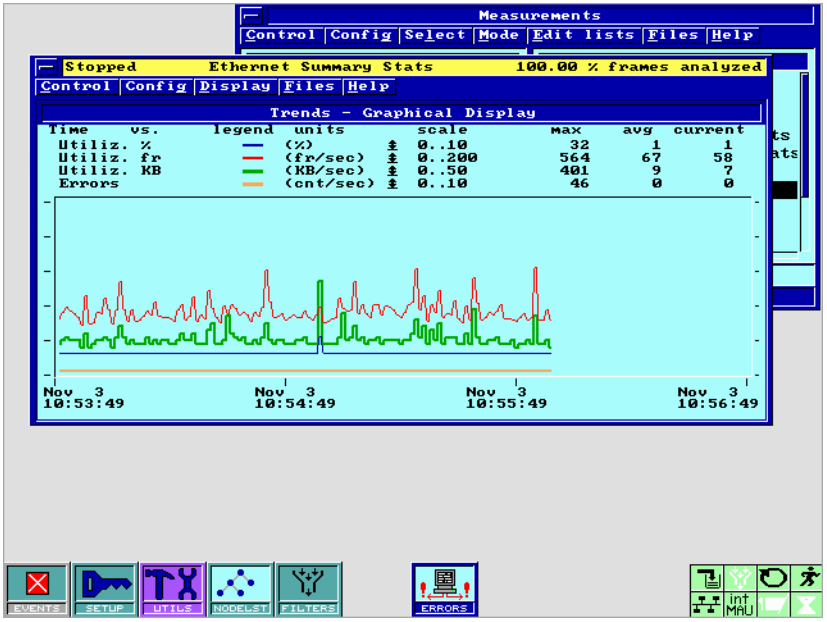


Figure 3-5: Ethernet Trends Graphical window

Configuring the Trends Windows

The Trends Graphical window and Trends Tabular window are implicitly tied together. Therefore, when you use the Trends Configuration window to choose the four items you want to show in one window, the same four items are also used in the other window.

The following procedure is for configuring the Ethernet Trends Graphical and Trends Tabular displays, but the procedure is similar for configuring the FDDI or Token-Ring Trends Tabular and Trends Graphical displays.

1. In any of the three Ethernet Summary Stats windows (Summary Stats, Trends Graphical, or Trends Tabular) select Configure Trends in the Config menu. The Trends Configuration window opens.

2. In the Graph Shows field, select either <user defined> or one of the other items shown in the list pane. This determines what four items are shown in the Trends Graphical and Trends Tabular windows. If you set the Graph Shows field to something other than <user defined>, the Line 1 through 4 fields show the predefined set of items that will be shown in the Trends Graphical and Trends Tabular windows.

   OR

   If you set the Graph Shows field to `<user defined>`, use the Line 1 through 4 fields to select the four items of your choice from the list pane.

   The online help for the Trends Configuration window explains the user defined items and the predefined sets in more detail.

3. Select a sample rate by double-clicking on one of the Sample Rate radio buttons.

4. Select Accept Changes and Exit in the Done menu to save your selections and close the window. The new configuration is now used in the Trends Graphical and Trends Tabular windows.

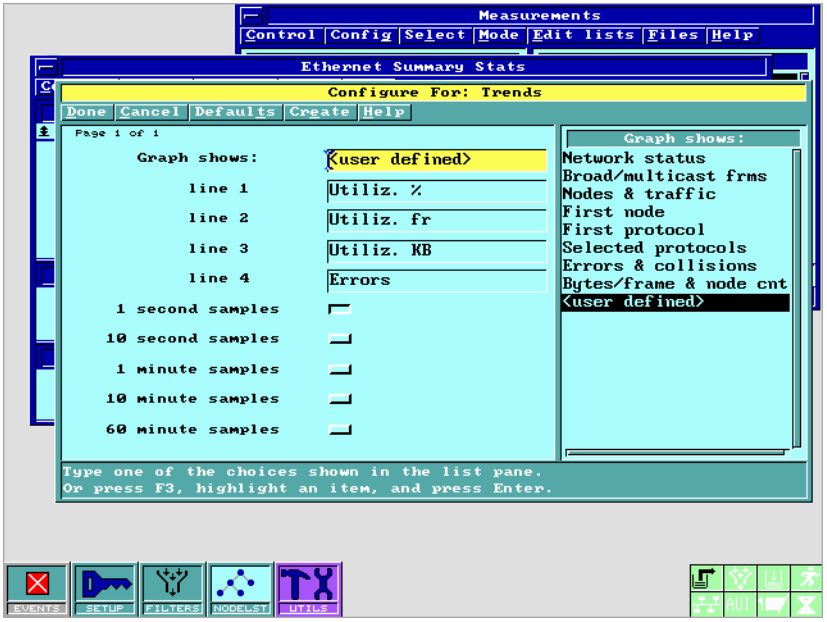


Figure 3-6: Ethernet Trends Configuration window

Using the Top Talkers Measurements

The Ethernet, FDDI, and Token-Ring Top Talkers measurements let you follow critical nodes or stations. They list up to 50 nodes or stations generating the most frames and how many bytes and frames each node or station is sending and receiving.

For Example. . . One way to use the Ethernet Top Talkers measurement is in combination with a capture filter. For instance, you can modify the Basic Ethernet filter by opening the Basic Ethernet Capture Filter window and putting in a router's MAC address in the Station 1 Address field, leaving the Station 2 Address field set to Don't Cares (all Xs), and setting the Traffic Mode field to 'To or From Stn 1'. Then you can activate the filter in the Capture Filters window and run the Ethernet Top Talkers measurement. This will then show you a list of the top stations using that particular router.

Starting a Top Talkers Measurement

The following procedure is for starting an Ethernet Top Talkers measurement, but the procedure is similar for starting the FDDI and Token-Ring Top Talkers measurements.

1. In the Measurements window, start the Ethernet Top Talkers measurement.

   The Ethernet Top Talkers window opens showing a list of up to 50 nodes generating the most traffic. One line of information for each node shows the number of frames and bytes each node has sent and received.

2. Use the ↑ , ↓ , **PgUp**, **PgDn**, **HOME**, and **END** keys to scroll through the list.

The following figure shows you a typical Ethernet Top Talkers display.

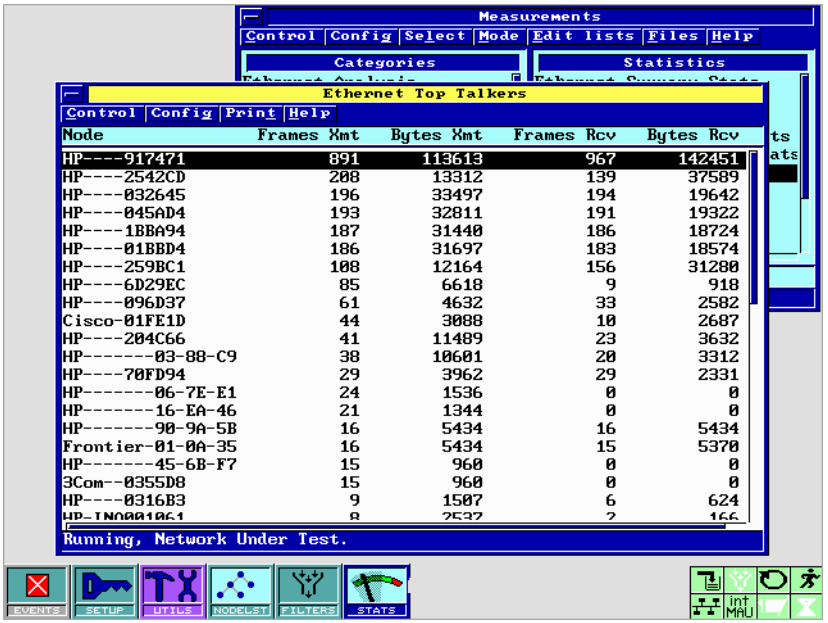


Figure 3-7: Ethernet Top Talkers window

Configuring a Top Talkers Measurement

The following procedure is for configuring the Ethernet Top Talkers measurement, but the procedure is similar for the FDDI and Token-Ring Top Talkers measurements.

1. In the Ethernet Top Talkers window, select Stop all Measurements in the Control menu.

2. Select Configure Measurement in the Config menu. The Ethernet Top Talkers Configuration window opens.

3. Make a selection for the Update Interval field. The Top Talkers measurement runs continuously once you start it, but the choice you make for the update interval determines how often the display is updated with the latest results of the measurement.

4. Select Accept Changes and Exit in the Done menu to save your selection and return to the Top Talkers window. The new configuration is used the next time you start the Top Talkers measurement.

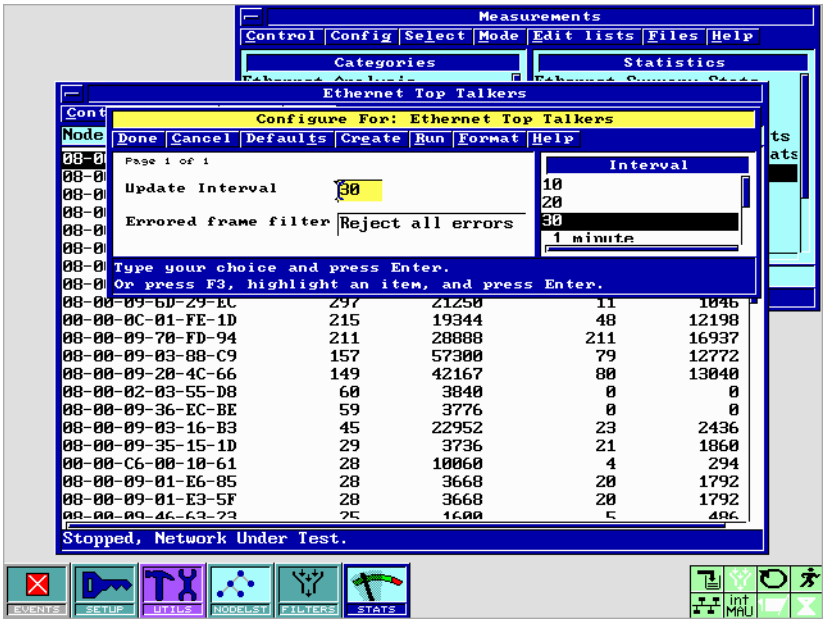


Figure 3-8: Ethernet Top Talkers Configuration window

Using the Top Errors Measurements

The Ethernet and FDDI Top Error Sources and the Token-Ring Top Error Reporters measurements let you follow critical nodes or stations. They list up to 50 nodes or stations generating the most error frames, the total number of errors they are generating, and the type of errors they are generating.

For Example. . . One way to use the FDDI Top Error Sources measurement is in combination with a capture filter. You can modify the Basic FDDI filter by opening the Basic FDDI Capture Filter window and putting in a router's MAC address in the Station 1 Address field, leaving the Station 2 Address field set to Don't Cares (all Xs), and setting the Traffic Mode field to From Stn 1. Then, you can activate the filter in the Capture Filters window and run the FDDI Top Error Sources measurement. This measurement will then show you how may errors and what type of errors this particular router is sending.

Starting a Top Errors Measurement

The procedure below is for starting the Ethernet Top Error Sources measurement, but the procedure is similar for starting the Token-Ring Top Error Reporters measurement.

1. In the Measurements window, start the Ethernet Top Error Sources measurement.

   The Ethernet Top Error Sources window opens showing a list of up to 50 nodes that have reported the most error frames.

   One line of information for each node shows the total number of error frames each node has sent and the type of errors each node has sent since the measurement was started.

A frame is considered to be an error frame if it is a jabber or a misalign, or if it contains an FCS error. A runt may also be considered an error, depending on how you configure the measurement.

The online help for the Top Error Sources measurement defines these errors and gives possible causes.

2. Use the ↑ , ↓ , **PgUp**, **PgDn**, **HOME**, and **END** keys to scroll through the list.

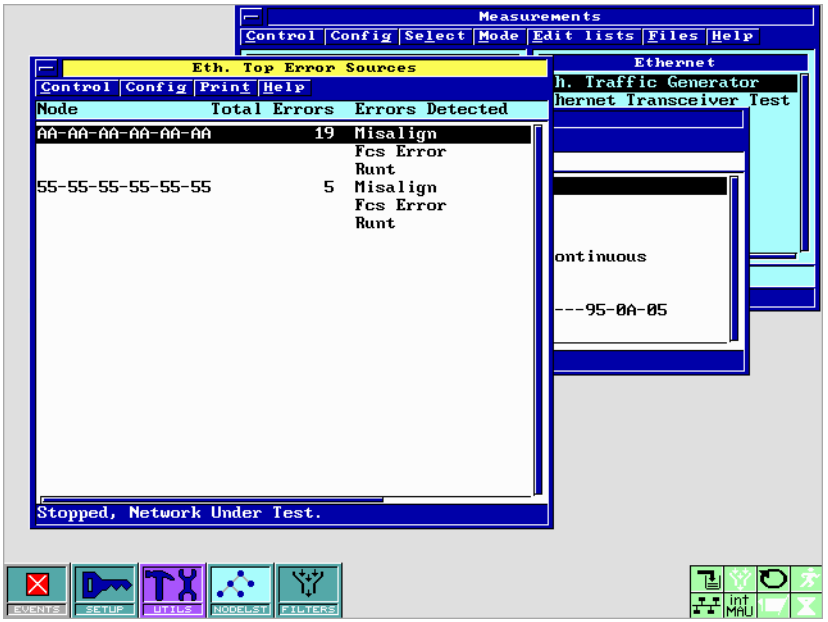


Figure 3-9: Ethernet Top Error Sources window

Configuring a Top Errors Measurement

The procedure below is for configuring the Ethernet Top Error Sources measurement, but the procedure is similar for configuring the FDDI Top Error Sources and the Token-Ring Top Error Reporters measurements.

1. In the Ethernet Top Error Sources window, select Stop Measurement in the Control menu.

2. Select Configure Measurement in the Config menu. The Top Error Sources Configuration window opens.

3. Make a selection for the Update Interval field. The Top Error Sources measurement runs continuously once you start it, but the choice you make for the update interval determines how often the display is updated with the latest results of the measurement.

4. Choose Yes or No in the Ignore Runt Errors field. This determines whether runts are counted as errors.

   If you select ‘Yes’, runts are ignored (they are not counted as errors).

5. Select Accept Changes and Exit in the Done menu to save your selections and return to the Top Error Sources window. The new configuration is used the next time you start the Top Error Sources measurement.

   OR

   Select Run in the Run menu. This saves your selections, returns to the Top Error Sources window, and starts the Top Error Sources measurement using the new configuration.

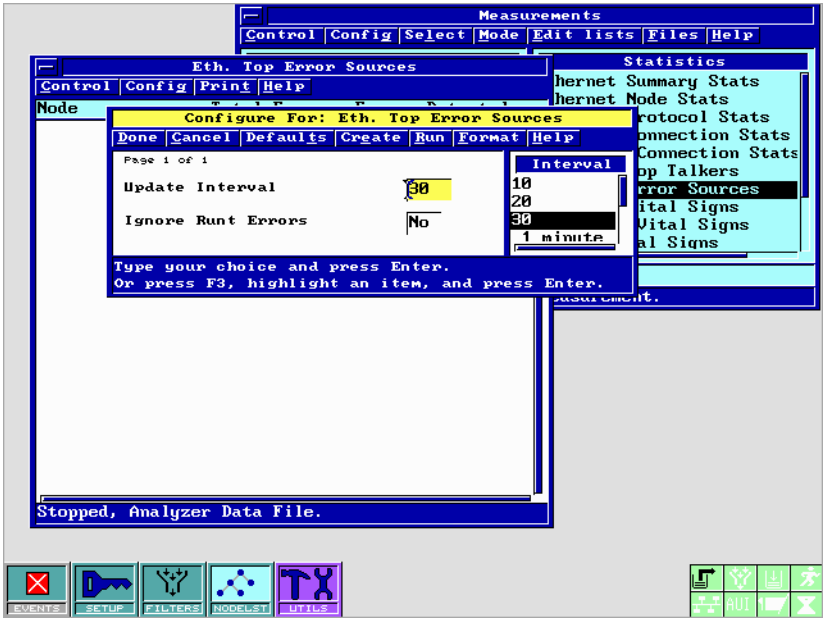


Figure 3-10: Ethernet Top Error Sources Configuration window

Using the Node and Station Stats Measurements

The Ethernet Node Stats and the Token-Ring and FDDI Station Stats measurements let you follow critical nodes or stations. They graphically show you, in either bar chart or pie chart form, a variety of statistical information about 20 nodes or stations.

For Example. . . You can configure the Token-Ring Station Stats measurement to show the 20 stations sending source routed broadcasts, all stations broadcasts, functional address frames, and source routed frames.

When you start the Node Stats or Station Stats measurement from the Measurements window, the bar chart window is displayed. From the bar chart window, you can open the pie chart window.

Starting the Station Stats Measurement

The procedure below is for starting the Token-Ring Station Stats measurement, but the procedure is similar for starting the Ethernet Node Stats and FDDI Station Stats measurements.

1. In the Measurements window, start the Token-Ring Station Stats measurement. The Token-Ring Station Stats Bar Chart window opens showing a list of up to 20 stations.

The left column shown is labeled Station. The Station column shows either the hex MAC address, the station name, or the vendor name of the 20 stations, depending on the format selected in the Station Stats Configuration window.

If a station is remote (that is, it is not on the ring the Internet Advisor LAN is monitoring), it is shown in red (white on a monochrome display). A station is assumed to be remote until it sends a non-source routed frame.

If a station is local (that is, it is on the ring the Internet Advisor LAN is monitoring), it is shown in black. Functional addresses are assumed to be local.

In addition to the Station column, up to five items can be tracked for each station, depending on how you configure measurement. For example, you can configure the measurement to show the 20 stations reporting the most token errors, beacons, claim tokens, purges, and frequency errors.

Information about the items you track is shown numerically and in bar chart form. The online help for the Station Stats measurement gives more information about the items you can track.

If traffic on the network is very high, the acquisition hardware can miss some frames. If this happens, the status line at the bottom of the window shows “X frames missed,” where X is the number of missed frames.

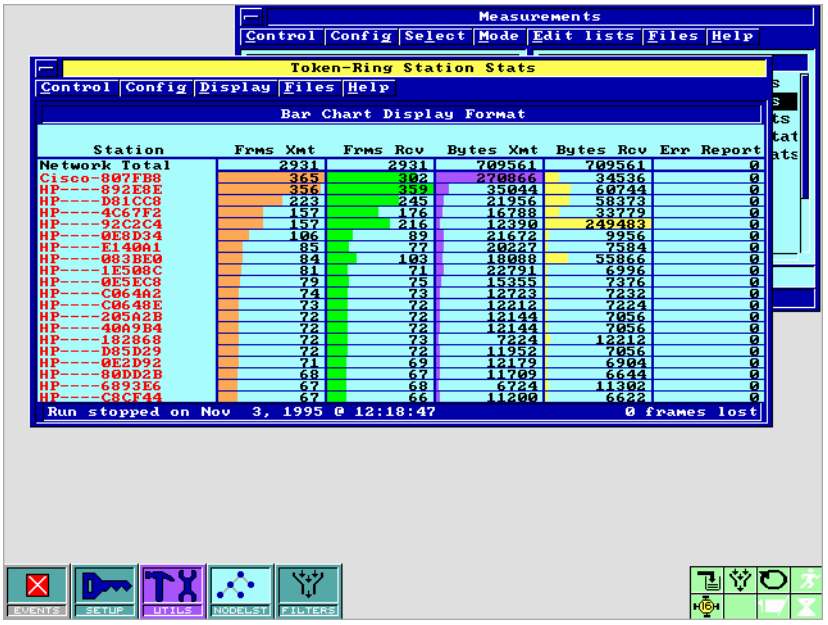


Figure 3-11: Token-Ring Station Stats Bar Chart window

Using the Station Stats Pie Chart Window

The Token-Ring Station Stats Pie Chart measurement uses pie charts to show information about the same items that the Station Stats Bar Chart window is tracking. Up to five pie charts can be displayed, depending on how you configure measurement.

The procedure below is for using the Token-Ring Station Stats Pie Chart window, but the procedure is similar for using the FDDI or Ethernet Node Stats Pie Chart window.

1. In the Token-Ring Station Stats Bar Chart window, select Display in Pie Chart Format in the Display menu. The Station Stats Pie Chart window opens and the Station Stats Bar Chart window closes.

   In each pie chart, the stations are identified by their hex MAC addresses, their station names, or their vendor names, depending on the format selected in the Station Stats Configuration window.

   For each pie chart, if a station contributes less than 2%, its percentage is not shown individually. Its percentage is shown in the “Other Top 20” segment of the pie chart. The “All Other” segment of the pie charts indicates what percentage was contributed by stations that are not in the top 20.

   If traffic on the network is very high, the acquisition hardware can miss some frames. If this happens, the status line at the bottom of the window shows “X frames missed,” where X is the number of missed frames.

2. Use the ↑ , ↓ , **PgUp**, **PgDn**, **HOME**, and **END** keys to scroll through the list.

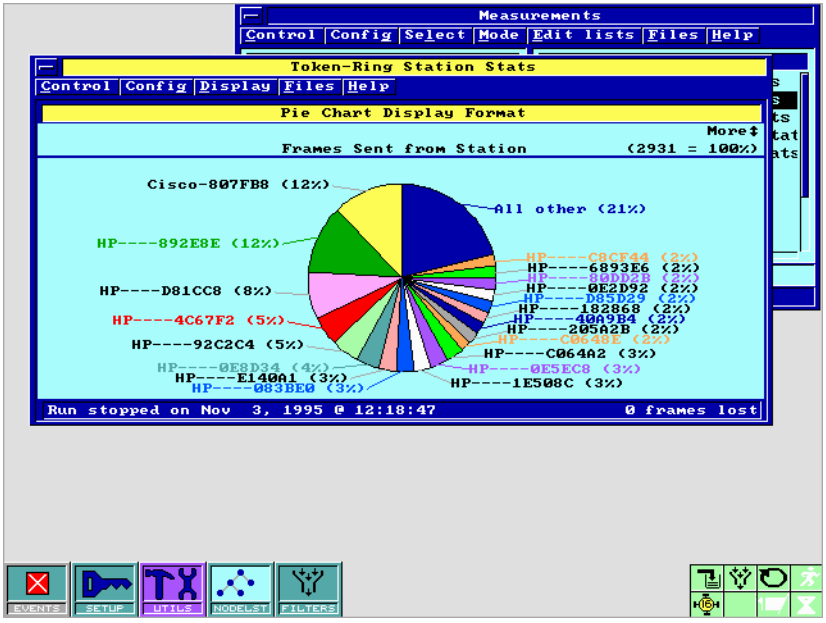


Figure 3-12: Token-Ring Station Stats Pie Chart window

Configuring the Station Stats Measurement

The following procedure is for configuring the Token-Ring Station Stats measurement, but the procedure is similar for configuring the Ethernet Node Stats and FDDI Station Stats measurement.

The configuration selections you make affect the Station Stats Bar Chart and Pie Chart windows.

1. In either of the Station Stats windows (Bar Chart or Pie Chart), select Stop Measurement in the Control menu.

2. Select the item in the Config menu. The Station Stats Configuration window opens.

3. Make a selection for the Display Update Interval field. The Station Stats measurement runs continuously once you start it, but the choice you make for the display update interval determines how often the display is updated with the latest results of the measurement.

4. In the Sort On and Display field, select either <user defined> or one of the other items shown in the list pane. This field determines the "sort criteria." In other words, the item you select in this field determines which 20 stations are tracked.

5. In each of the four Also Display fields, select either <user defined> or one of the other items shown in the list pane.

6. If you set the Sort on and Display field or any of the four Also Display fields to <user defined>, make a selection for that field from the list pane.

   OR

   If neither the Sort on and Display field nor any of the Also Display fields are set to <user defined>, the selection in the <user defined> field has no effect.

7. Double-click on one of the Count Frames radio buttons to determine how frames that match the sort and display criteria are counted.

   a. If you select All Frames, all frames that match the criteria coming from or going to any station are counted.

   b. If you select To (station), only frames that match the criteria and are sent to the station whose address is in the (station) field are counted.

   c. If you select From (station), only frames that match the criteria and are sent from the station whose address is in the (station) field are counted.

   d. If you select To or From (station), only frames that match the criteria and are sent to or from the station whose address is in the (station) field are counted.

NOTE

If you have activated a global capture filter in the Capture Filters window (accessed through the Setup window), the filter also affects which frames are counted.

8. If you selected any radio button other than All Frames, enter an address in the (station) field.

9. Select Accept Changes and Exit in the Done menu to save your selections and close the configuration window. The new configuration is used the next time you start the Station Stats measurement.

   OR

   Select Run in the Run menu. This saves your selections, closes the configuration window, and starts the Station Stats measurement using the new configuration.

Figure 3-13: Token-Ring Station Stats Configuration window

Using the Protocol Stats Measurement

The Protocol Statistics measurement shows you what protocols are running on your network. You can examine one of the following protocol groupings:

- Data Link Layer (DLL)
- IP (ARPA) Stack
- Novell Stack
- AppleTalk Stack
- DECnet stack
- OSI Stack
- Banyan Vines Stack

Each protocol group is described in more detail in its own help topic.

You can select which of these groups to view and set certain parameters pertaining to each group in the Configuration window for this measurement.

Starting a Protocol Stats Measurement

The following procedure is for starting the Ethernet Protocol Stats measurement, but the procedure is similar for starting the Token-Ring or FDDI Protocol Stats measurements.

1. In the measurements window, start the Ethernet Protocol Stats measurement. The Ethernet Protocol Statistics window opens.

The following statistics can be displayed for each protocol group:

- Frames Sent
- Bytes Sent

- DLL Errors - Data Link Layer errors include all physical errors. For example, for Ethernet, the DLL Errors count includes runts, jabbers, bad FCSs, and misaligns.

- Average Frame Length

You can choose to view these statistics as either a bar chart or a pie chart using the Display menu bar items. You can cycle through the pie charts using the ARROW keys and the PAGE keys.

Configuring the Protocol Stats Measurement

The Protocol Stats Configuration window lets you customize the Protocol Stats measurement by selecting parameters such as:

- Which protocols to show (see the "Show Statistics For" help topic)

- Which frames to count within the protocols

- Whether to count all frames or only frames to/from specified addresses

- What display update interval to use

Each configuration field is defined in its own online help topic.

The following fields are available in the Protocol Stats Configuration window:

1. The Show Statistics For field determines how the protocols running on your network are grouped. The choices are:

    a. Data Link Layer - shows protocols based on their Type fields, 802.2 DSAP and SSAP fields, and SNAP fields. These fields indicate the Data Link Layer next protocol. On the second page of the Configuration window, you can choose to further group these frames into the major protocol stacks.

    b. IP (ARPA) Stack - shows protocols based on the IP protocol fields. If the protocol is UDP or TCP, then show protocols based on the Port numbers.

c. Novell Stack - shows protocols based on the Packet Type fields in Novell IPX packets. If the Packet Type is 0, 4, or 17, then also show protocols based on socket numbers.

d. AppleTalk Stack - shows AARP (AppleTalk Address Resolution Protocol) Phase 1 or Phase 2 and AppleTalk Phase 1 or Phase 2 protocols. In addition, if the protocol is AppleTalk Phase 1 or Phase 2, then it shows the higher-level protocols based on the value of the DDP (Datagram Delivery Protocol) type field.

e. Banyan (VINES) Stack - identifies whether Vines Echo and VIP (Vines Internet Protocol) is running on the network. If VIP is found, the Protocol Type field is analyzed. If the VIP Protocol Type field indicates that the next protocol is VIPC (Vines InterProcess Communications Protocol), the higher-level protocols and the port numbers are analyzed and displayed. If the VIP Protocol Type field indicates the next protocol is VSPP (Vines Sequenced Packet Protocol), the higher-level protocols are analyzed and displayed.

f. DECnet Stack - identifies several DECnet protocols. In addition, if DECnet Phase IV or Phase V is found, the higher-level protocols are analyzed and displayed.

g. OSI Stack - shows protocols grouped by the value in the Network Layer Protocol Identifier byte of OSI packets. If this byte's value is 129, which indicates a CLNP (Connectionless Network Protocol) frame, the higher-level protocols are analyzed and displayed.

You can add, remove, or modify the lists of recognized protocols, ports, and numbers. See the online help topic "Modifying the Protocol Names Files" for more information.

2. The Display Update Interval field determines how often the display is updated. For example, if you choose 1 minute, the latest results are displayed every minute.

   This field also determines how frequently data is logged to a file if data logging is enabled. (Data logging is enabled by selecting the "Log Data to ASCII File During Next Run" item in the Files menu of the Protocol Stats window.)

3. In the Sort on and display field, you can select one of the following statistics to be the criteria by which the protocols are sorted. The choice you make determines what is displayed in the second column of the Protocol Stats window.

   a. Frames sent - the second column of the bar chart display shows the protocols sorted by the number of frames sent from each protocol.

   b. Bytes sent - the second column of the bar chart display shows the protocols sorted by the number of bytes sent from each protocol.

   c. DLL Errors - the second column of the bar chart format displays protocols sorted by the number of Data Link Layer errors detected in the frames sent from each protocol.

4. You can also display up to three more statistics from the following. The choices you make determine what is displayed (if anything) in columns 3 through 5 of the Protocol Stats window.

   a. Bytes sent
   b. Frames sent
   c. DLL errors
   d. Average frame length
   e. No Selection

   If you choose No Selection for any or all of these fields, the remaining statistics are redrawn with more resolution on the bar chart display.

5. The Count Frames fields let you control which frames are counted. There are four choices, only one of which can be selected at a time:

   a. All frames- Selecting this causes all frames coming from or going to any protocol to be counted.

   b. To <node>- Selecting this causes only frames sent to the node whose address is in the <node> field to be counted.

   c. From <node>- Selecting this causes only frames sent from the node whose address is in the <node> field to be counted.

   d. To or From <node>- Selecting this causes only frames sent to or from the node whose address is in the <node> field to be counted.

   If you select a count mode other than All Frames, type an address into the <node> field or select an address from the list pane on the right. The list pane shows any addresses which are in the Advisor's node/station list.

NOTE The Count Frames option is a software display filter that only affects which frames are counted by the Protocol Stats

   Instead of (or in addition to) using the Count Frames software display filter, you can activate a hardware capture filter in the Capture Filters window. Activating a capture filter focuses all running measurements on a specific set of frames.

6. The Errored Frame Filter field lets you exclude frames errors. For Ethernet, you can exclude only frames with runt errors, or all frames with errors (including runt frames). Select the Errored Frame Filter field and then use the list pane to select the errored frame condition you want to exclude. The list pane option "Reject runt frames" is useful for excluding collision fragments which may have spurious Ethernet Type fields. When Off is selected, all frames are included in the statistical information.

7. In the Data Link Layer Statistics field, choose one of the following to customize the Data Link Layer Protocol Statistics measurement:

a. Show SAPs and Types - shows protocols based on the value in the Type and SAP fields.

b. Show Protocol Stacks - shows protocols grouped into the major protocol stacks.

8. In the AppleTalk Stack Statistics field, if the Count non-ATalk Frames box is checked, the pie charts and bar charts show AppleTalk frames as a percentage of all frames on the network. If this box is NOT checked, the pie charts and bar charts show counts relative to only the AppleTalk Stack traffic on your network.

9. In the Banyan Stack Statistics field, choose any of the following options to customize the Banyan Vines Stack Protocol Statistics measurement:

   a. Count non-Banyan Frames - if this box is checked, pie charts and bar charts show Banyan Vines frames as a percentage of all frames on the network. If this box is NOT checked, the pie charts and bar charts show counts relative to only the Banyan Vines Stack traffic on your network.

   b. Count Transient Port Frames - Vines transient port numbers range from 512 to 61439. If this box is checked, transient port service frames are counted in addition to well-known port service frames. If the box is NOT checked, frames with transient port numbers are excluded from the total counts, and only frames with well-known port numbers are counted.

   c. Transient Ports Start At - Frames with port numbers equal to or greater than the number entered here are grouped together as transient port frames. The measurement displays frames with port numbers less than the value in this field grouped by their port numbers.

10. In the DECnet Stack Statistics field, if the Count non-DECnet Frames box is checked, the pie charts and bar charts show DECnet frames as a percentage of all frames on the network. If this box is NOT checked, the pie charts and bar charts show counts relative to only the DECnet Stack traffic on your network.

11. In the IP (ARPA) Stack Statistics field, choose any of the following options to customize the IP (ARPA) Stack Protocol Statistics measurement:

    a. Count non-ARPA Frames - if this box is checked, pie charts and bar charts show IP, ARP, and RARP frames as a percentage of all frames on the network. If this box is NOT checked, the pie charts and bar charts show counts relative to only the IP Stack traffic on your network.

    b. Count User Port Frames - if this box is checked, user port service frames are counted in addition to well-known port service frames. If the box is NOT checked, frames with user port numbers are excluded from the total counts, and only frames with well-known port numbers are counted.

    c. User Ports Start At - Frames with port numbers equal to or greater than the number entered here are grouped together as user port frames. The measurement displays frames with port numbers less than the value in this field grouped by their port numbers.

12. In the Novell Stack Statistics field, choose any of the following options to customize the Novell Stack Protocol Statistics measurement:

    a. Count non-Novell Frames - if this box is checked, pie charts and bar charts show IPX frames as a percentage of all frames on the network. If this box is NOT checked, the pie charts and bar charts show counts relative to only the IPX Stack traffic on your network.

    b. Count non-Novell Sockets - Novell socket numbers range from 0451 to 045F hex. If this box is checked, non-Novell sockets are counted in addition to these Novell socket numbers. If this box is NOT checked, frames with socket numbers outside the Novell socket range are ignored.

13. In the OSI Stack Statistics field, if the Count non-OSI Frames box is checked, the pie charts and bar charts show OSI frames as a percentage of all frames on the network. If this box is NOT checked, the pie charts and bar charts show counts relative to only the OSI Stack traffic on your network.

Using the Connection Statistics Measurement

The Connection Statistics measurement displays statistical information for up to 20 connections. The statistics shown are relevant to a connection between two nodes at the MAC layer or the network layer, depending on the selection made in the "Show Statistics For" field of the Connection Stats Configuration window. The following are the choices for the "Show Statistics For" field:

- Data Link Layer - shows MAC-layer connection statistics.
- AppleTalk Stack - shows DDP (Datagram Delivery Protocol) network-layer connection statistics.
- Banyan Vines Stack - shows VIP (Vines Internet Protocol) network-layer connection statistics.
- DECnet stack - shows DRP (DECnet Routing Protocol) network- layer connection statistics.
- IP (ARPA) Stack - shows IP (Internet Protocol) network- layer connection statistics.
- Novell Stack - shows IPX (Internetwork Packet Exchange) network-layer connection statistics.
- OSI Stack - shows CLNP (Connectionless Network Protocol) network-layer connection statistics.

A connection is supposed to be formed if a node sends a frame to another node. The node with the smaller network address is treated as the source and the node with the higher network address is treated as the destination. All the subsequent frames between these two nodes are sent using the same connection.

NOTE

The term 'connection' should not be confused with the same term used in higher-layer protocols (for example, a TCP connection).

Starting a Connection Stats Measurement

The procedure below is for starting the Ethernet Connection Stats measurement, but the procedure is similar for starting other Connection Stats measurements also.

1. In the Measurements window, start the Ethernet Connection Stats measurement.

The Ethernet Connection Stats window opens.

In the Connection Stats window, the leftmost column (Stn 1 Addr) shows the source node. The next column (Stn 2 Addr) shows the destination node for that connection. The Stn 1 and Stn 2 Addr columns show either the hex MAC address, the node name, or the vendor name of the 40 nodes, depending on the format selected in the Connection Stats Configuration window's Format menu.

In addition to the Stn 1 and Stn 2 Addr columns, up to three of the following items can be shown for each connection, depending on the selections made in the "Sort On and Display" and the "Also Display" fields of the Connection Stats Configuration window.

- Frames - This column shows the total number of frames seen between the two nodes involved in each connection. For each connection, this number should be equal to the sum of what is shown in the S. Frames and D. Frames columns.
- Bytes - This column shows the number of bytes transferred between the two nodes involved in the connection.
- Errors - This column shows the number of frames with an error.
- Stn 1 Fr - This column shows the number of frames sent by the source node to the destination node in each connection.
- Stn 2 Fr - This column shows the number of frames sent by the destination node to the source node in each connection.

You can choose to view the connection statistics as either a bar chart or a pie chart using the Display menu bar items. You can cycle through the pie charts using the ARROW keys and the PAGE keys.

Configuring the Connection Stats Measurement

The Connection Stats Configuration window lets you customize the Connection Stats measurement by selecting parameters such as:

- Whether to show MAC-layer or network-layer connection information (see the "Show Statistics For" help topic)
- Whether to enable Subnet Stats for network-layer protocols
- What display update interval to use
- What statistics to show (for example, bytes, frames, errors, and so on)
- Whether to count all frames or only frames to/from specified addresses
- Whether to count errored frames

The following procedure is for configuring the Ethernet Connection Stats measurement, but the procedure is similar for configuring the other Connection Stats measurements.

1. The Show Statistics For field determines whether MAC-layer or network-layer connection information is shown in the Connection Stats window. The choices are:

    a. Data Link Layer - The MAC addresses are taken as the basis for connections between the two nodes in a connection.

    b. AppleTalk Stack - The connections are based on the network layer DDP (Datagram Delivery Protocol) network numbers and Node IDs.

c. Banyan Vines Stack - The connections are based on the network layer VIP (Vines Internet Protocol) network numbers and sub-network number.

d. DECnet Stack - The connections are based on the network layer DRP (DECnet Routing Protocol) Node numbers.

e. IP (ARPA) Stack - The connections are based on the network layer IP (Internet Protocol) addresses.

f. Novell Stack - The connections are based on the network layer IPX (Internetwork Packet Exchange) network and Node numbers.

g. OSI Stack - The connections are based on the network layer CLNP (Connectionless Network Protocol) addresses.

2. The Display Update Interval field determines how often the display is updated. For example, if you choose 1 minute, the latest results are displayed every minute.

   This field also determines how frequently data is logged to a file if data logging is enabled. (Data logging is enabled by selecting the "Log Data to ASCII File During Next Run" item in the Files menu of the Connection Stats window.)

3. The Enable Subnet Stats field checkbox can be enabled only when a network layer protocol stack is selected in the Show Statistics For field. If Data Link Layer is selected in the Show Statistics For field, the Enable Subnet Stats checkbox is disabled.

   When the Enable Subnet Stats checkbox is enabled (marked with a checkmark), the Connection Stats measurement becomes a subnet connection stats measurement instead of a connection stats measurement. Subnet connections stats can show you that one particular group of stations is talking to another group of stations.

   See the online help for more information about the Enable Subnet Stats field.

4. In the Sort on and Display field, you can select one of the following statistics to be the criteria by which the connections are sorted. The choice you make determines what is displayed in the column to the right of the Stn 1 and Stn 2 Addr columns in the Connection Stats bar chart display.

    a. Frames - This causes the column to show the source addresses of the connections sorted by the total number of frames seen between the two nodes in each connection.

    b. Bytes - This causes the column to show the source addresses of the connections sorted by the number of bytes transferred between the two nodes involved in each connection.

    c. Errors - This causes the column to show the source addresses of the connections sorted by the number of Data Link Layer errors detected in the frames sent from the source node.

    d. Stn 1 Fr - This causes the column to show the source addresses of the connections sorted by the number of frames sent by each source (Stn 1) node.

    e. Stn 2 Fr - This causes the column to show the source addresses of the connections sorted by the number of frames received by each source node. In other words, the number of frames sent by the destination nodes (Stn 2) is the sort criteria.

5. You can also display up to two more columns of statistics from the following.

    a. Bytes
    b. Frames
    c. Errors
    d. Stn 1 Fr
    e. Stn 2 Fr

f. <no selection>

If you choose <no Selection> for either or both of the Also Display fields, the remaining statistics are redrawn with more resolution on the bar chart display.

6. The Count Frames field lets you control which frames are counted by the Connection Stats measurement. There are four choices, only one of which can be selected at a time:

   a. All frames- Selecting this causes all frames coming from or going to any node to be counted.

   b. To <node>- Selecting this causes only frames sent to the node whose address is in the <node> field to be counted.

   c. From <node>- Selecting this causes only frames sent from the node whose address is in the <node> field to be counted.

   d. To or From <node>- Selecting this causes only frames sent to or from the node whose address is in the <node> field to be counted.

   e. If you select a count mode other than All Frames, type an address into the <node> field or select an address from the list pane on the right. The list pane shows any addresses in the Advisor's node/station list which are relevant to the protocol selected in the Show Statistics For field.

NOTE

The Count Frames option is a software display filter that only affects which frames are counted by the Connection Stats measurement.

Instead of (or in addition to) using the Count Frames software display filter, you can activate a hardware capture filter in the Capture Filters window. Activating a capture filter focuses all running measurements on a specific set of frames.

7. The Errored Frame Filter field lets you exclude frames with errors from the connection statistics. If this field is set to OFF, error frames are included in the statistics. If this field is set to Reject All Errors, then only frames with no errors are included in the connection statistics.

Using the Vital Signs Measurements

The Vital Signs measurement gives you information about the activity on your network. Some of the Vital Signs provided by the measurement indicate normal and desirable activity. Other Vital Signs indicate the presence of potentially serious errors which should never be present or should be present only in very rare instances.

There are a variety of different Vital Signs measurements for the different interfaces and protocols available in the Internet Advisor LAN.

See the online help for specific information on each of the different Vital Signs measurements.

Starting a Vital Signs Measurement

The procedure below is for starting the Ethernet Vital Signs measurement, but the procedure is similar for starting FDDI or Token-Ring Vital Signs measurements also.

1. In the Measurements window, start the Ethernet Vital Signs measurement.

The Ethernet Vital Signs window opens.

The Vital Signs measurement shows values for each of the Vital Signs under the following column headings:

- Threshold
- Current
- Average
- Peak
- Total

Threshold

The values in the Threshold column are set in the Configuration window for this measurement. For frame and packet counts, the threshold value sets the expected number of frames or packets per second.

If a threshold is exceeded, the Current value is displayed in red (black on monochrome units). You also have the option of logging the event to the Event Log. The Configuration window lets you toggle Threshold Events Logging on or off.

NOTE

Threshold events are only logged as they pass the threshold level. For example, if Utilization % exceeds the threshold for 10 minutes, only 1 entry is made in the Event Log. However, if Utilization % goes up and down, an event is logged each time the threshold is exceeded.

If you configure the measurement to stop when the threshold is exceeded, the Threshold value is displayed in orange to indicate that the measurement will stop if the threshold value is exceeded. Then, if the measurement does stop, a banner tells you all measurements were stopped by the Vital Signs measurement. The stop event is logged to the Instrument log and the threshold event is logged to the Threshold log, even if Event Logging is turned off in the Configuration window.

If you disable a threshold in the Configuration window, the Threshold column displays "disabled".

Current

This is the value measured in the preceding second. If the Current value is greater than the threshold, the Current value is displayed in red (black on monochrome units) to indicate that the threshold has been exceeded.

Average

The Average column shows the average of the last 30 samples for each type of Vital Sign.

Peak

The Peak column shows the highest value for each of the Vital Signs since the start of the measurement.

Total

The Total column shows the total number of each type of frame received since the start of the measurement. For Utilization %, the Total column is not used.

If Vital Signs is run for a long period of time, it is possible for the total counts to roll over (back to 0). This typically happens first with the frame counts and will typically require about 50 days to occur. (Rollover cannot occur in less than 80 hours.)

NOTE Filters can be created in the Capture Filters window to control the capture or exclusion of specified frames or the stopping of a measurement. When a filter is activated, it is in effect for any measurement until you deactivate the filter, either in the Filters window, or by selecting the active filter status icon.

Running Vital Signs from the Network or the Capture Buffer

The Vital Signs display is divided into Network Counts (pre-filter) and Buffer Counts (post-filter), because you can run the measurement using the network or the Capture Buffer as the data source.

When you run the measurement from the network, the vital sign counts are all pre-filter counts. In other words, any capture filters you have activated in the Capture Filters window have no affect on the counts because the counts are tabulated from the frames before they enter the Capture Buffer.

In contrast, when you run the measurement from the Capture Buffer, the vital sign counts are post-filter counts. That is, the counts are derived from the frames in the Capture Buffer so they are affected by filters which include (capture) or exclude frames from the Capture Buffer.

Therefore, if you run the measurement from the network when no capture filters are activated, the counts shown under Buffer Counts will be the same as those shown under Network Counts. However, if you run the measurement from the network when a capture filter is activated, the counts shown under Buffer Counts will NOT be the same as those shown under Network Counts.

If you run the measurement from the Capture Buffer, the Buffer Counts are reset to zero, and then increase as the frames are processed from the Capture Buffer. In addition, the counts shown under Buffer Counts are copied to the Network Counts.

Configuring the Vital Signs Measurement

The Token-Ring Vital Signs Configuration window lets you do the following:

- Control whether thresholds which are exceeded are logged to the Event Log
- Set each Vital Sign threshold value (or accept the default value)
- Enable or Disable threshold monitoring for each Vital Sign
- Set the measurement to stop all running measurements when a threshold is exceeded

The following procedure is for configuring the Token-Ring Vital Signs measurement, but the procedure is similar for configuring the Ethernet and FDDI Vital Signs measurements.

1. In the Token-Ring Vital Signs window, select Stop Measurement in the Control menu.

2. Select the item in the Config menu. The Token-Ring Vital Signs Configuration window opens.

3. Check the Log Threshold Events field to log an event to the Event Log when any enabled threshold is exceeded. To disable all threshold logging, toggle this field so that the checkmark is not displayed.

4. Each Vital Sign threshold (Utilization, Frames, and Bad FCS) can be enabled or disabled. If a threshold is enabled and the threshold is exceeded, the Current value in the Token-Ring Vital Signs window is displayed in red (black on monochrome units). If Log Threshold Events is checked, the event is also logged to the Event Log.

   To enable a Vital Sign threshold, select (double-click) Enabled from the list pane, or press F3, highlight Enabled, and press ENTER. When a threshold is enabled, the threshold value appears in the Threshold column in the main Vital Signs configuration window.

   The default threshold value for each Vital Sign can be edited by typing a new threshold value into the threshold field.

   Each Vital Sign threshold can be enabled or disabled separately. When a threshold is disabled, "Disabled" appears in the Threshold column of the Token-Ring Vital Signs window, the Current value does not turn red in the Token-Ring Vital Signs window if the threshold is exceeded, and no event is logged to the Event Log. The Stop on Threshold field is also grayed-out when a threshold is disabled.

   To disable a Vital Sign threshold, select (double-click) Disabled from the list pane, or press F3, highlight Disabled, and press ENTER.

5. Each Vital Sign has a Stop on Threshold checkbox. Enable (mark with a check) this field to stop all running measurements if the Vital Sign threshold is exceeded. The Vital Sign threshold must be Enabled in order to enable the Stop on Threshold checkbox.

4

Running Decode Measurements

What's in this Chapter

This chapter describes how to use the HP Internet Advisor LAN's various decode measurements. The Internet Advisor LAN provides decodes for many Ethernet, FDDI, and Token-Ring protocols such as 802.2, 802.3/Ethernet, Token-Ring, FDDI MAC, TCP, and IP.

In addition to the individual-layer protocols, there are several "stack" decodes such as ARPA stack, Novell stack, and Vines stack.

The summary stack decodes display a summary of the protocols in each frame. The detailed stack decodes expand each encapsulated protocol in the frame to let you see the frame contents, layer by layer, in one decode window.

Individual layer protocols let you simultaneously monitor close up views of different protocol layers in the same stack.

A complete list of the available decodes is shown in the first chapter.

Decode measurements interpret the data in frames according to a protocol so you can examine the contents of the frames. There are three decode formats:

- **Summary format** - shows a one line overview of each decoded frame
- **Detailed format** - shows what was decoded in each field of each frame
- **Data forma**t - shows the raw hexadecimal data

When you start most decode measurements, a window opens showing the data in the detailed format. From the detailed window, you can open windows that show the same data in the summary format and the data format. The exception to this is stack decodes; they open in the summary format, but you can open the data and detailed formats from the summary window.

For detailed decode windows, there are usually help topics that introduce the protocol and describe the purpose and possible values of each field being decoded.

In network stack decode measurements, you display an entire frame in one window in hex code when Data Decode is selected as the display format.

Decode measurements can use several different data sources:

- **Network Under Test** - Data can be processed real-time as it is being captured from the network.

- **Capture Buffer or File** - Data can be post-processed from the Capture Buffer, an Advisor Data file, or a Decode Result file.

When you start a decode measurement, it processes data coming from whatever data source is currently selected in the Setup window. This can be Network Under Test, Capture Buffer, or Advisor Data File.

You can override the data source selected in the setup window by using the decode configuration window to use a Decode Result File as the data source.

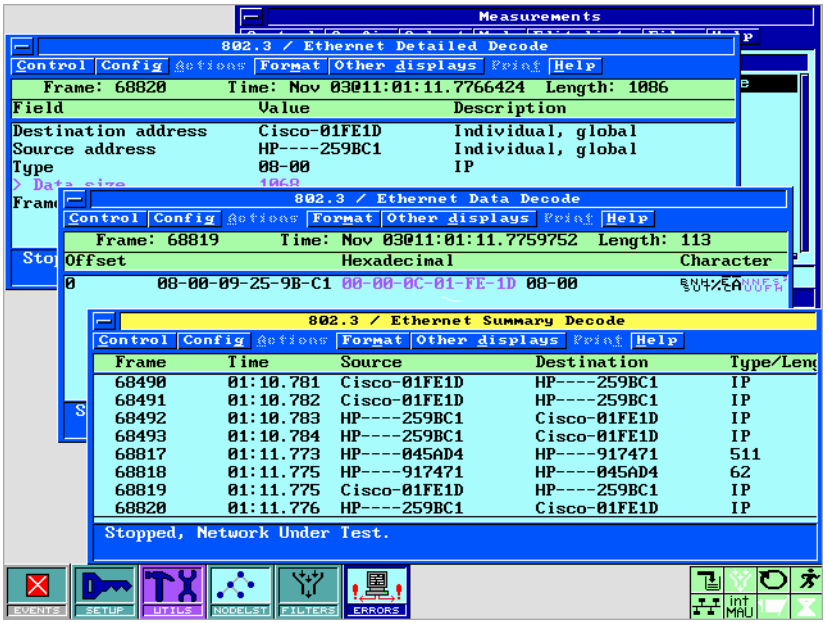


Figure 4-1: Detailed, Data, and Summary decode windows

Using a Decode to Capture Data from the Network

If you want to capture decoded data from the network, the data source must be set to Network Under Test.

If you want to control what data is captured from the network, rather than capturing all data, you can activate a filter in the Capture Filters window. This lets you capture only data of interest, and, because the captured data is temporarily kept in the capture buffer, it uses the capture buffer space more efficiently.

NOTE

When the data source is Network Under Test, frames displayed in the decode window may be only a partial representation of the captured frames. At high traffic levels, the display may lag behind the actual frames. However, all data is stored in the capture buffer.

You can see all captured frames by changing the data source to Capture Buffer.

1. Make sure the data source in the Setup window is Network Under Test.

2. Make sure the network interface in the Setup window is correct for the type network you are connected to.

3. In the Measurements window, start the decode measurement. If the decode you started was an individual decode (rather than a stack decode) a detailed decode window opens showing the decoded data. Refer to the section “Using a Detailed Decode” later in this chapter for a description of what a detailed decode shows.

   If you started a stack decode, a summary window opens. Refer to “Using a Summary Decode” later in this chapter for a description of what a summary decode shows.

4. If you want to pause the display to examine a frame more closely, use the Pause Display item in the Control menu.

5. If you want to see data in the other two formats, use the items in the Other Displays menu. You can have windows for all three formats (detailed, summary, and data) open at the same time.

6. Once you have captured the desired frames, stop the measurement by using the Stop Measurement item in the Control menu.

After you stop the measurement, if you are in a detailed or data decode window, only the last two displayed frames are shown. You can switch the data source to Capture Buffer to see all the frames you captured. Refer to “Post-Processing Data in the Capture Buffer” later in this chapter.

Using a Detailed Decode

Detailed Decodes show the following information:

- **Frame Header** - At the top of the window is a one-line description of the frame currently being decoded. It shows this information:
  - the frame number, preceded by "!" if the frame contains an error
  - the date and time the frame was captured
  - the length in bytes of the frame
- **Field** - This column lists the individual fields being decoded.
- **Value** - This column shows the value decoded for each field.
- **Description** - This column gives additional protocol information. For example, it may describe the meaning of a specific value shown in the Value column.
- **Derived Information** - Some frames are highlighted and preceded by >. This indicates information that the decode derived about a frame. For example, the size of the data for the next protocol layer may be shown this way.

Since each frame in a detailed decode window can have more lines of data than will fit in the window, you can use certain keys to display different parts of the same frame. Refer to "Scrolling Through Data in a Decode Window" later in this chapter. You can also zoom the window.

For detailed decode windows, there are help topics that introduce the protocol and describe the purpose and possible values of each field being decoded.

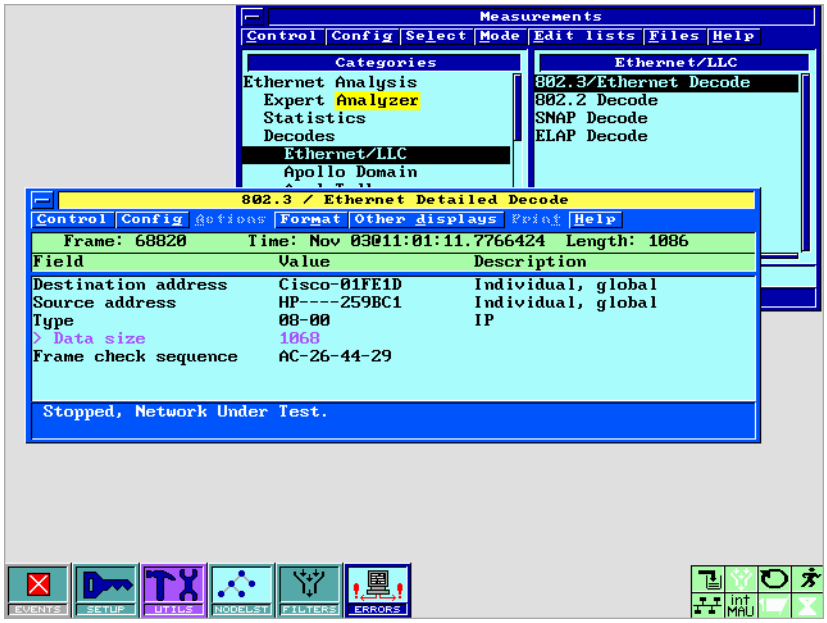


Figure 4-2: 802.3/Ethernet detailed decode window

Using a Data Decode

Data Decodes show the following information:

- **Frame Header** - At the top of the window is a one-line description of the frame currently being decoded. It shows this information:
  - the frame number, preceded by "!" if the frame contains an error
  - the date and time the frame was captured
  - the length in bytes of the frame
- **Offset** - This column is an aid for reading the hexadecimal data. It identifies the byte position of the first byte of data shown in each row of hexadecimal data. Because each row of hex data contains 16 bytes, the offset increases by 16 for each row.
- **Hexadecimal** - This column shows the raw hexadecimal data.
- **Character** - This column shows the data in ASCII or EBCDIC, depending on the data code selected in the decode configuration window.

Different fields are displayed in alternating colors in the hex display for easy correlation with the detailed display.

Since each frame in a data decode window can have more lines of data than will fit in the window, you can use certain keys to display different parts of the same frame. Refer to "Scrolling Through Data in a Decode Window" later in this chapter. You can also zoom the window to see more data.

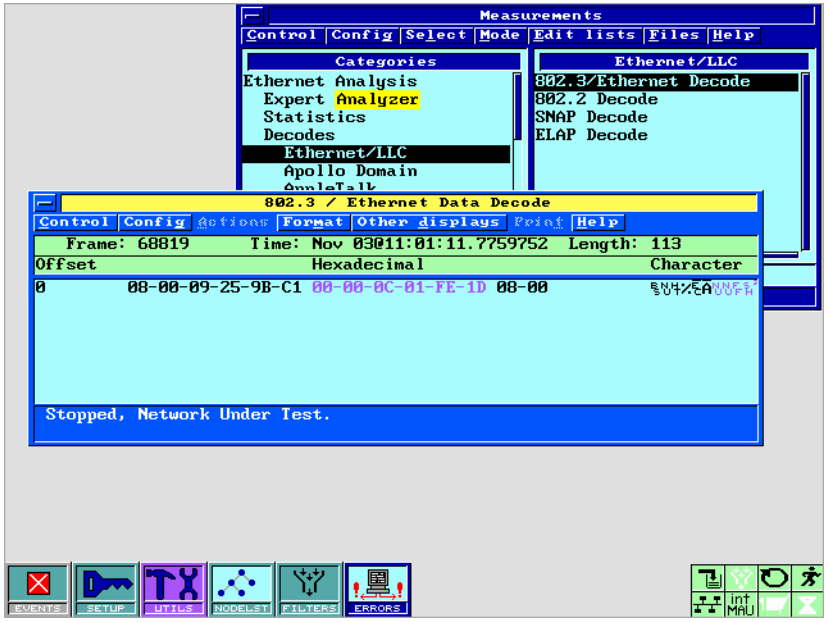


Figure 4-3: 802.3/Ethernet data decode window

Using a Summary Decode

Summary Decodes show the following information:

- Frame number - This column shows the number of each frame, preceded by "!" if the frame contains an error.
- Time - This column shows the date and time the frame was captured. You can select different timestamp resolutions in the decode configuration window. For example, you can choose the month, day, hour format or you can choose the hour, minute, second format.
- Decode-Specific Information - Depending on the protocol being decoded, additional columns show information about the frames. For example, there may be columns that show source and destination addresses.

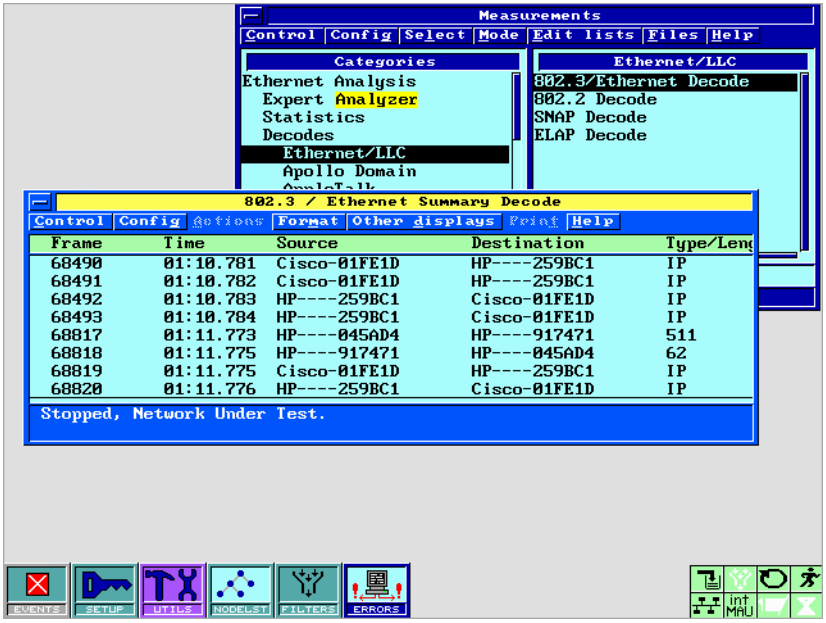


Figure 4-4: 802.3/Ethernet summary decode window

Post-Processing Data in the Capture Buffer

Once you have captured the data you want from the network, you can switch the data source to the capture buffer. This puts you in a post-processing mode in which you can see all the frames that were captured in the buffer.

1. In any decode window, select Switch to Capture Buffer in the Control menu. This stops all running measurements and changes the data source to the capture buffer. This is the fastest way to switch to the capture buffer.

   OR

   Stop the decode using the Stop Measurement item in the Control menu, and then change the Data Source field to Capture Buffer in the Setup window.

Once the data source is Capture Buffer, you can scroll through all the frames. Since each frame in a detailed or data decode window can have more lines of data than will fit in the window, you can use certain keys to display different parts of the same frame. Refer to “Scrolling Through Data in a Decode Window” later in this chapter.

You can also use the items in the Actions menu to mark and display frames that meet certain conditions such as frames with an error or frames that contain certain data. This lets you use the screen to display only frames of interest. Refer to “Marking and Displaying Specific Frames” later in this chapter.

If you want to permanently save the contents of the capture buffer for future use, you can save the data to a file. Refer to “Saving the Capture Buffer to a File” later in this chapter.

Scrolling Through Data in a Decode Window

If you stop or pause a decode when the data source is Network Under Test, you can use the keyboard to scroll through the data to display different frames. You can also scroll through the data when you are post-processing (the data source is Capture Buffer, an Advisor Data File, or a Decode Result File).

Since each frame in a detailed or data decode window can have more lines of data than will fit in the window, you can use certain keys to display different parts of the same frame.

Use These Keys	To Display
HOME	First frame
END	Last frame
↑	Previous frame
↓	Next frame
SHIFT + HOME	Beginning of the current frame in a detailed or data decode
SHIFT + END	End of the current frame in a detailed or data decode
SHIFT + ↑	Previous line of current frame in a detailed or data decode
SHIFT + ↓	Next line of current frame in a detailed or data decode
PgUp	Previous page of the current frame in detailed or data decode
PgUp	Previous page of frames in a summary decode
PgDn	Next page of the current frame in a detailed or data decode
PgDn	Next page of frames in a summary decode
←	10 characters to the left of the window's left edge
→	10 characters to the right of the window's right edge
ENTER	Synchronize frames in other decode windows using same data source

NOTE

When the data source is Network Under Test, the range of scrolling is restricted, and frames displayed may be only a partial representation of the actual frames captured. To see all captured frames, change the data source to Capture Buffer.

Marking and Displaying Specific Frames

When you are in a post-processing mode (for example, when the data source is Capture Buffer), you can use the items in the Actions menu to mark and display frames that meet certain conditions such as frames with an error or frames that contain certain data. This lets you use the screen to display only frames of interest.

You can specify these mark conditions in the Mark Frames window:

- Frames with an error
- Frames with a warning
- Frames containing specific data
- Frames going to or coming from specific addresses

All frames that meet ALL the specified conditions are marked. In other words, the mark conditions you specify are ANDed together.

Marked frames are indicated by an asterisk (*) at the left of the frame number in the decode window.

Once frames are marked, you can use the Display Marked Frames item in the Actions menu to display only the marked frames.

The Menu Bar Description help topic, available in any decode window, describes what the other items in the Actions menu do.

Marking Frames

Because the Mark Frames window ANDs all conditions that are specified in it at any one time, you must make sure you don't specify more than one condition unless you want only frames that meet multiple conditions to be marked.

The procedure below is for marking and displaying only frames meeting all specified conditions. To mark frames that meet one condition or another, use the procedure "Mark Multiple Frame Conditions" later in this chapter.

1. Select the Mark Frames item in the Actions menu of the decode window. The Mark Frames window opens.

2. In the Mark Frames window, enable the Clear Prior Marks check box. This causes any previously marked frames to be unmarked before the new conditions are marked.

3. If you want to mark only the frames in a specified range, specify the range in the Frames From # and To # fields.

4. If you want to mark frames that contain an error and any other specified conditions, enable the Frames With Error check box.

5. If you want to mark frames that contain a warning and any other specified conditions, enable the Frames With Warning check box.

6. If you want to mark frames that contain certain data and any other specified conditions, specify the data in the Frames With Data field. The online help for the Mark Frames window has more information on how to specify the data.

7. If you want to mark frames that meet certain address and traffic mode conditions and any other specified conditions, double-click on the Addresses push button. This opens the Addresses window in which you can specify the addresses and the traffic mode, such as frames coming from or going to a specific address.

8. Select Accept Changes and Exit in the Done menu. This closes the Mark Frames window, unmarks all previously marked frames, and marks the frames that meet all the specified conditions.

9. In the decode window, select Display Marked Frames in the Actions menu. This causes only marked frames to be displayed.

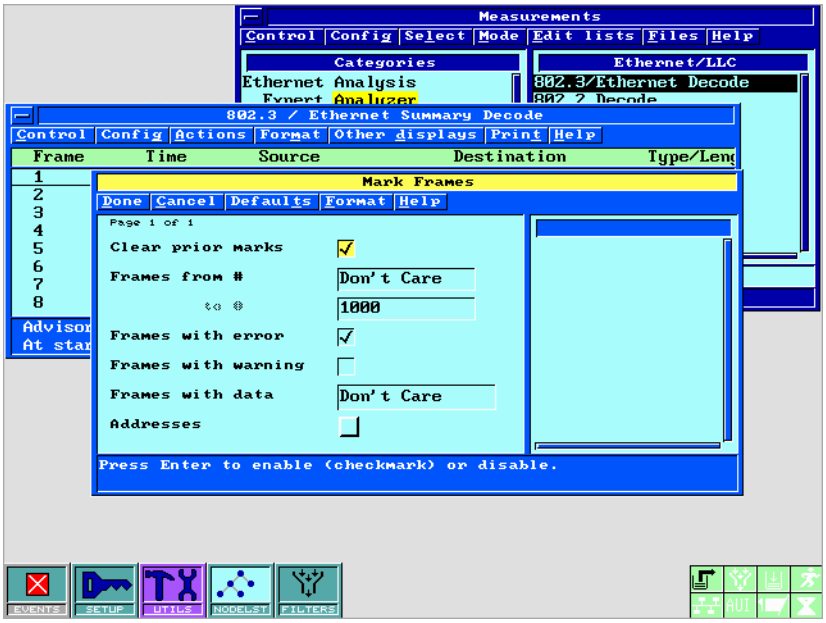


Figure 4-5: Mark Frames window

Mark Multiple Frame Conditions

Because the Mark Frames window ANDs all conditions that are specified in it at any one time, to OR conditions, you must mark frames that meet one condition, and then leave those frames marked while you mark frames that meet the other conditions.

Following is an example of marking all frames that contain errors OR warnings, but the procedure is similar for marking multiple frames for other conditions.

Mark First Condition

1. Select the Mark Frames item in the Actions menu of the decode window. The Mark Frames window opens.

2. In the Mark Frames window, enable the Clear Prior Marks check box. This unmarks any previously marked frames.

3. Enable the Frames With Error check box.

4. Make sure the Frames With Warning check box is disabled (not checked) and the Frames With Data field says Don't Care.

5. Make sure the address conditions specified in the Addresses window are don't cares (all Xs), and the traffic mode is Between Station 1 and Station 2.

6. Select Accept Changes and Exit in the Done menu. The Mark Frames window closes, all previously marked frames are unmarked, and all frames with errors are marked.

Mark Second Condition

1. When the marking is done, go back into the Mark Frames window.

2. Disable the Clear Prior Marks check box. This ensures that the previously marked error frames remain marked.

3. Disable the Frames With Error check box.

4. Enable the Frames With Warning check box.

5. Select Accept Changes and Exit in the Done menu. The Mark Frames window closes and all frames with warnings are marked.

6. In the decode window, select Display Marked Frames in the Actions menu if you want only marked frames to be displayed.

Saving the Capture Buffer to a File

When you capture data from the network, the data is stored temporarily in the capture buffer. If you want to have the data for future use, you must save the contents of the capture buffer to either of two types of files. If you do not do save the data to a file, the data is overwritten the next time you run a measurement.

- **Advisor data file** - If you save the contents of the capture buffer to an Advisor Data file, you can later run different decode measurements using that one file as the data source by selecting Advisor Data File as the data source in the Setup window. This lets you repeatedly post-process the data. This is the preferred method of saving data from the capture buffer.

- **Decode result file** - If you save the contents of the capture buffer to a Decode Result file, all the frames that were processed by the decode measurement are saved. This gives you the ability to repeat viewing a previous measurement's result.

Saving to The Internet Advisor LAN Data File

Save the capture buffer to an Advisor Data File if you want to run several different measurements on the saved data, or if you want to use the capture buffer while post-processing the saved data. There are two ways to save the capture buffer contents to an Advisor Data File, depending on the current data source:

- If the data source is currently Network Under Test, you can use the Save Capture Buffer to Advisor Data File item in the Files menu of the Setup window.

- If the data source is already Capture Buffer, you can use the Save Advisor Data File item in the Actions menu of the decode window.

If the Data Source is Network Under Test

1. Stop the decode by selecting Stop Measurement in the Control menu of the decode window.

2. In the Setup window, select the Save Capture Buffer to Advisor Data File item in the Files menu. This opens a Save File Selector window where you can specify the name of a file in which to save the contents of the capture buffer.

3. Type the drive (if it is different than the current drive), file name and extension (optional) of the file to which you want to save the data. For example, `a:\ethernet.dat` .

4. Select Accept Selection and Exit in the Done menu to close the File Selector window and save to the file.

If the Data Source is Capture Buffer

1. In the decode window, select the Save Advisor Data File item in the Actions menu. This opens a Save File Selector window where you can specify the name of a file in which to save the contents of the capture buffer.

2. Type the drive (if it is different than the current drive), file name and extension (optional) of the file to which you want to save the data. For example, `a:\ethernet.dat` .

3. Select Accept Selection and Exit in the Done menu to close the File Selector window and save the data to the file.

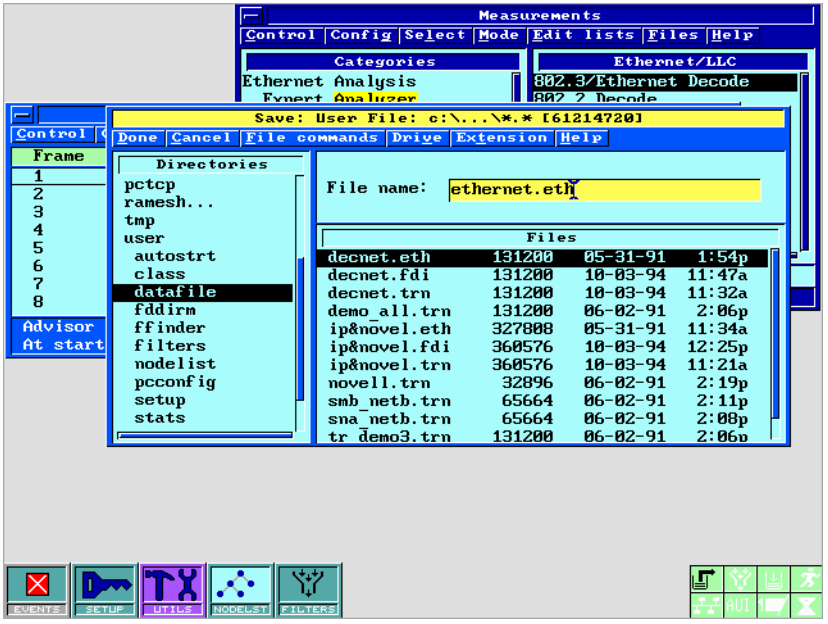


Figure 4-6: Save File Selector window

Saving to a Decode Result File

Save the capture buffer to a Decode Result File if you only want to re-run the current decode on the saved data. To save the contents of the capture buffer to a Decode Result File, you use the Save Decode Result File item in the Actions menu of the decode window. Since the Actions menu is disabled (grayed-out) when the data source is Network Under Test, you may first need to change the data source to Capture Buffer.

1. If the data source is already Capture Buffer, select either Save Decode Result File All Frames or Save Decode Result File Marked Frames in the Actions menu of the decode window. This opens a Save File Selector window where you can specify the name of a file in which to save the contents of the capture buffer.

   OR

   If the data source is Network Under Test, select Switch to Capture Buffer in the Control menu of the decode window, and then select Save Decode Result File All Frames or Save Decode Result File Marked Frames in the Actions menu.

2. Type the drive (if it is different than the current drive), file name and extension (optional) of the file to which you want to save the data. For example, `a:\tokenrng.dat` .

3. Select Accept Selection and Exit in the Done menu to close the File Selector window and save the data to the file.

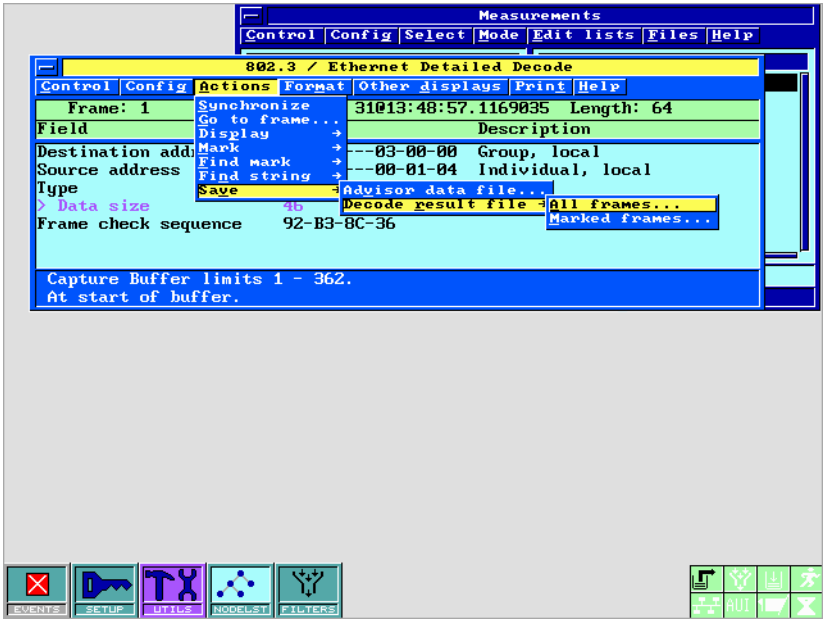


Figure 4-7: Decode with Save Decode Result File menu displayed

Printing a Decode Measurement

After you run a decode measurement, you can print the viewed frames to either a printer or to a file.

In any decode measurement window, the Print menu bar item lets you print either the currently viewed frame, a range of the frames, or all the frames in the capture buffer.

The Print dropdown items act in combination with the display mode selected in the Actions menu. If the current display mode views all frames then all frames (marked and unmarked) can be printed. If the current display mode views only marked frames, then only marked frames can be printed. In all cases, the printed output displays the frames that are being viewed.

The print output goes to either a printer or to a file depending on your selection in the Print Screen Output field of the Utilities/PC Hardware Configuration window.

The Print menu bar item has these commands:

- All Frames- This item prints all viewed frames (marked and unmarked) in the capture buffer.
- Current Frame- In summary decodes, this item prints the frame that is underlined. In detail or data decodes, this item prints the currently viewed frame.
- From # to #- This item prints a range of frame numbers you select. When you select this item, you are prompted to enter the beginning and ending frame numbers for the range of frames you want to print. If you enter the same frame number for the start and end frame, only that one frame is printed.

Remember that printing a large number of frames to a file requires a large amount of disk space (especially for detailed decode and data decode windows). Also, printing a large file to a printer requires a long time period.

5

Running Application Measurements

What's in this Chapter

This chapter describes how to use the HP Internet Advisor LAN's various application measurements. "Applications" are measurements that perform a specific test. Some application measurements transmit onto the network.

NOTE

This manual provides detailed information about typical measurements on the Internet Advisor LAN, but does not cover every measurement in every category.

For detailed information and step by step instructions on any measurement, use the Internet Advisor LAN online help topics for each measurement.

In the Measurement window, the application measurements are organized under these categories:

- Commentator
- Stimulus/Response Tests
- Network Discovery

Following is a partial list of some of the application measurements. For more help on these measurements and any measurements not listed here, open the measurement, then choose the Help menu bar item to see a list of topics for that measurement.

Commentator applications include:

- **Network Commentators** - the Network Commentator measurements for Ethernet, FDDI, and Token-Ring provide a high-level report of significant protocol events that may be preludes to network performance degradation or network failure. The related menus in the Help windows define each protocol event. You can run Commentators on frames captured in the capture buffer using the Control menu Run Measurements from Capture Buffer. You can get more detailed information on the Commentator measurements by "drilling down" (double clicking) on an event.

S***timulus/Response Tests*** include:

- **Ethernet Transceiver Test** - this measurement sends a frame onto an Ethernet network and then checks the capture buffer to see if the frame was captured correctly.

- **TCP/IP ARP Request** - the ARP (Address Resolution Protocol) Request measurement gives you a quick way to verify connectivity to a node. It attempts to find the physical address for a target host on the same physical network to which the Internet Advisor LAN is connected.

- **TCP/IP PING (Packet InterNet Groper)** - the PING measurement lets you test whether destinations can be reached.

- **FDDI Traffic Generator** - this measurement lets you send an LLC frame or a MAC or SMT frame on the network. The FDDI Traffic Generator can also generate line states and raw symbols.

- **Token-Ring Traffic Generator** - this measurement lets you send an LLC frame or one of four MAC packets (Remove Ring Station, Request Ring Station Address, Request Ring Station State, Request Ring Station Attachments) on the network.

- **Token-Ring Lobe Test** - the Lobe Test measurement performs a lobe test on the wiring connecting the Internet Advisor LAN to the ring.

- **Token-Ring Request Station ID** - the Request Station ID measurement tests connectivity to a station on a local or remote ring.

- **Token-Ring Station Adapter Status** - the Station Adapter Status measurement gives you information about a station on the ring.

Network Discovery applications include:

- **Audit Network** - the Audit Network measurement lets the Internet Advisor LAN document the operation of your Ethernet or Token-Ring network for future reference. When you start this measurement, the Internet Advisor LAN runs a number of separate tests. As each test ends, its results are written to a common audit report file.

- **Node Discovery and Station Discovery** - the Discovery measurements let you find all addresses occurring on the local network. The MAC address as well as network layer addresses are found. New ‘observed’ addresses may be added to the node list in the Node/Station List window. You can run Node/Station Discovery on frames captured in the capture buffer using the Control menu Run Measurement from Capture Buffer.

- **Token-Ring Active Station List** - when you run the Active Station List measurement, the Internet Advisor LAN monitors the neighbor notification process on the ring to generate a list of stations on the ring.

- **Token-Ring Calculate Ring Length** - the Calculate Ring Length measurement attempts to measure (in feet and meters) the ring length of an active Token-Ring network.

Using the Ethernet Transceiver Test

Ethernet Transceiver Test sends a frame onto an Ethernet network and then checks the capture buffer to see if the frame was captured correctly.

Running the Transceiver Test measurement is not an exhaustive test of the network nor the Internet Advisor LAN, but it is an easy way to prove the following:

- The Internet Advisor LAN is connected to the network correctly.
- The Internet Advisor LAN is able to transmit.
- The Internet Advisor LAN is able to receive.
- The network is functioning.

Starting the Ethernet Transceiver Test

1. In the Setup window, make sure the data source is Network Under Test and the network interface is Ethernet.

2. Stop any other running measurements.

   You can do this from the Control menu of the individual measurements, or you can stop all measurements at once by selecting Stop All Measurements in the Control menu of the Measurements window.

3. In the Measurements window, start the Ethernet Transceiver Test measurement. A window opens showing the results of the measurement.

If the Internet Advisor LAN is able to transmit the frame and the capture buffer receives the frame correctly, the measurement displays the message “Frame transmitted. Frame received. Transceiver test passed.”

If the Internet Advisor LAN is able to transmit the frame but the capture buffer does not receive the frame correctly, the measurement displays the message “Frame transmitted. Frame could not be received. Transceiver test failed.”

If the Internet Advisor LAN is not able to transmit the frame, the measurement displays the message “Frame could not be transmitted. Transceiver test failed.”

If the Transceiver Test measurement fails, it may be caused by the connection between the Internet Advisor LAN and the network or by a serious physical problem (for example, a short) on the network. Refer to *What to Do if the Transceiver Test Fails*.

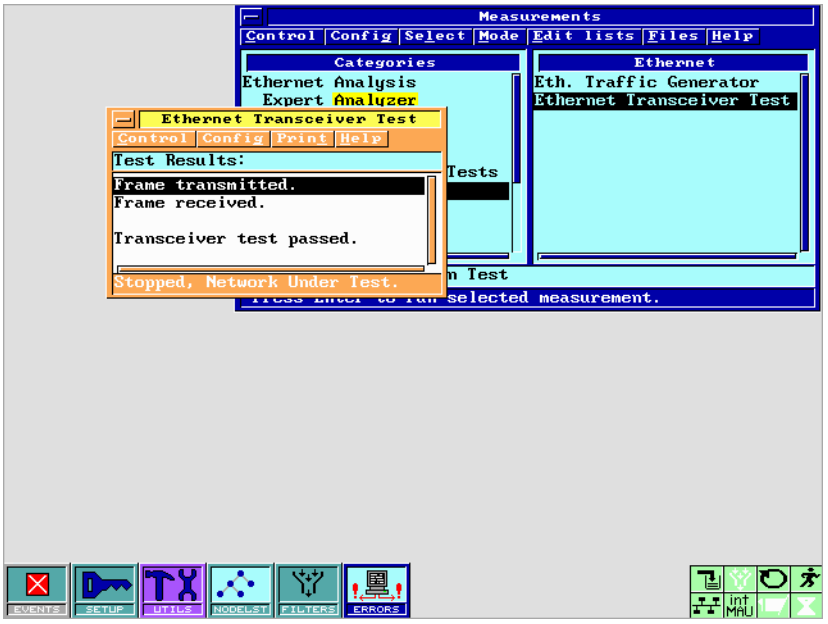


Figure 5-1: Ethernet Transceiver Test window

What to do if the Transceiver Test Fails

Below are some things to check if the Ethernet Transceiver Test fails. In addition, running Fault Finder may provide you with more information.

1. There are two Ethernet connectors on the Internet Advisor LAN: one labeled AUI and one labeled THINLAN. Check that the selection for the media connection in the Ethernet Parameters window (accessed through the Setup window) is correct for the connector you are using.

2. Check the connection between the Internet Advisor LAN and the cable, and make sure that the unused Ethernet connector is not connected to anything.

3. Check the end of the cable connected to the LAN to ensure a solid connection.

4. Check the network for shorts or improper (missing) terminators.

Using the ARP/RARP Request Measurement

The TCP/IP ARP (Address Resolution Protocol) Request measurement in the Stimulus/Response Tests category of the Measurement window gives you a quick way to verify connectivity to a node. It attempts to find the physical address for a target host on the same physical network to which the Internet Advisor LAN is connected.

To do this, the Internet Advisor LAN sends an ARP Request packet to the target host's Internet (IP) address. You supply the target host's Internet address in the ARP Request Configuration window.

The ARP protocol is implemented on most Ethernet networks that run the TCP/IP protocols. The ARP Request measurement is useful on these networks, as well as for networks that run UNIX™ or X-Windows™.

Starting the ARP Request Measurement

1. In the Setup window, make sure the data source is Network Under Test and the network interface is Ethernet.

2. Stop any other running measurements.

   You can do this from the Control menu of the individual measurements, or you can stop all measurements at once by selecting Stop All Measurements in the Control menu of the Measurements window.

3. In the Stimulus/Response Tests category of the Measurements window, start the TCP/IP ARP Request measurement.

   A window opens showing the results of the measurement. You can change certain parameters of the measurement by configuring the measurement.

The results of the ARP Request measurement are displayed in three columns:

- **IP Address** - this column shows the Internet address of the target machine to which the ARP Request packet is sent.

- **Physical Address** - this column shows the resolved address of the target machine. If the Internet Advisor LAN does not receive an ARP Response Packet, the message ‘‘No Response" is displayed.

  If a response is seen (that is, the resolved address is displayed in the Physical Address column), it indicates the interface card hardware and low-level drivers are probably all right.

  Intermittent failures might point to a low-level driver problem, an overloaded node, or excessive broadcast traffic on the network.

  Continuous failures point to a bad interface card, a misconfigured IP address, or a fatal software defect on the node (assuming the ARP protocol is implemented on that node).

  If more than one response is seen, a duplicate IP address might exist on the network or multiple routing paths to the node might exist. Duplicates are labeled.

- **Delay** - this column shows the time between when the ARP Request packet was sent and when the ARP Response packet was received. Long delay times tend to indicate a long routing path to the device or an overloaded node.

When the ARP Request measurement stops, additional statistical information is shown at the bottom of the window:

- The total number of ARP Request packets transmitted
- The total number of ARP Response packets received
- The minimum, average, and maximum times between the ARP Request packets and the ARP Response packets (if any packets were received)

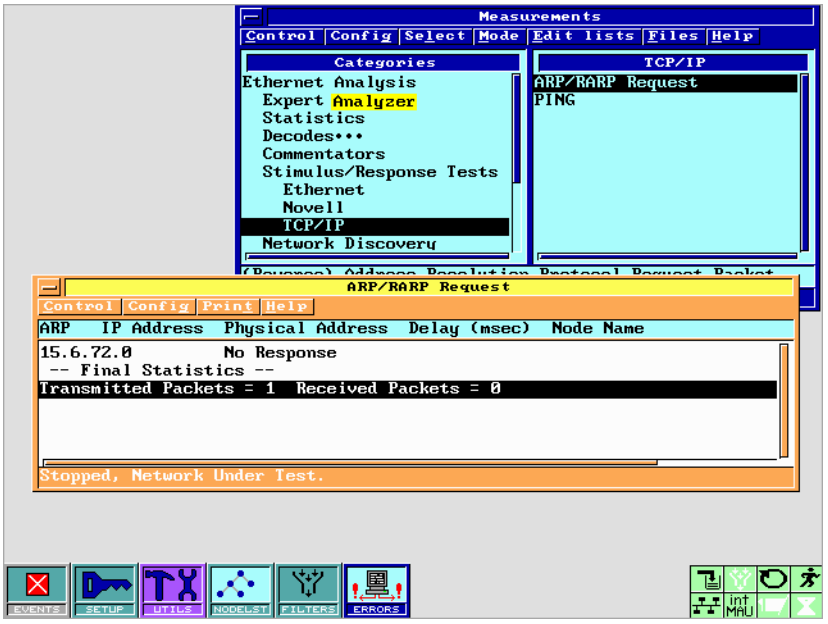


Figure 5-2: ARP Request Window

Configuring the ARP Request Measurement

The Configure Measurement item in the Config menu of the ARP Request window opens the ARP Request Configuration window. From the configuration window, you can change parameters that affect how the measurement runs. For example, you can specify the number of times the ARP Request packet is transmitted and to what target address it is sent.

1. In the ARP Request window, select Stop Measurement in the Control menu.

2. Select Configure Measurement in the Config menu. The ARP Request Configuration window opens.

3. In the Target Address field, specify the internet (IP) address of the host machine you want to test with the ARP Request measurement.

   The items in the Format menu let you enter the address in dot decimal or you can select a node name that is in the Internet Advisor LAN's node/station list from the list pane (if there are any node names that have IP addresses). An example four-byte dot decimal format is - `15.162.48.43`

4. In the Sender Address field, specify the internet address of the Internet Advisor LAN. It is VERY important to configure the Sender Address so it is unique for your network.

5. In the Timeout field, select the amount of time in milliseconds that the ARP Request measurement should wait for an ARP Response packet after it sends an ARP Request packet. Timeout values should be greater than 1000 milliseconds and less than 60,000 milliseconds.

6. In the Number Packets field, select the number of times the ARP Request packet is transmitted. You can enter a number greater than or equal to one, or you can select Continuous from the list pane.

   In the continuous mode, ARP Request packets are transmitted continuously until you stop the measurement. As each ARP Response is displayed, another ARP Request is sent.

7. Select Accept Changes and Exit in the Done menu to save your selections and return to the ARP Request window. The new configuration is used the next time you start the measurement.

   OR

   Select Run in the Run menu. This saves your selection, returns to the ARP Request window, and starts the ARP Request measurement using the new configuration.

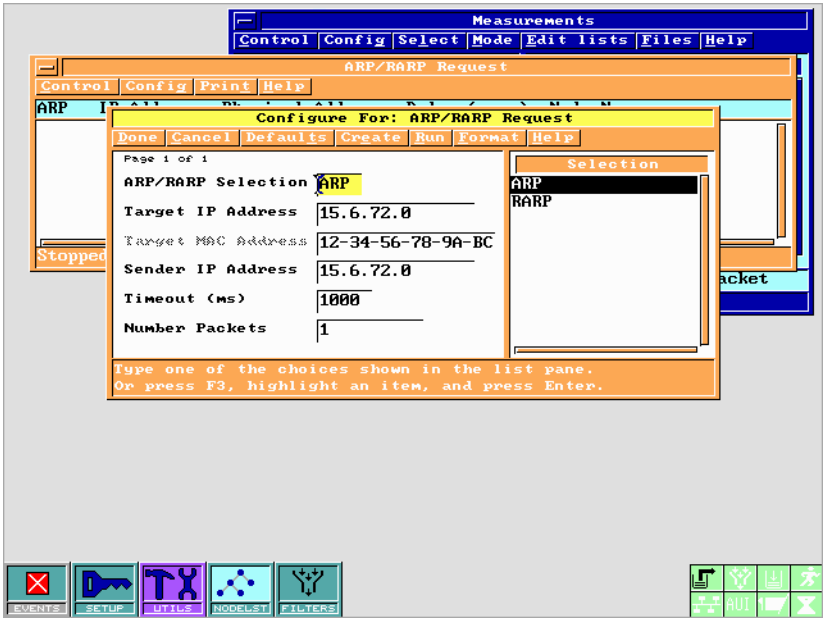


Figure 5-3: ARP Request Configuration window

Using the PING Measurement

The TCP/IP PING (Packet InterNet Groper) measurement lets you test whether destinations can be reached. To do this the Internet Advisor LAN sends out an ICMP Echo Request packet to the target host's Internet (IP) address. You supply the target host's Internet address in the PING Configuration window.

If the Enable Default Routing check box in the PING Configuration window is checked, the Internet Advisor LAN uses the router address in the Default Router IP Address field of the PING Configuration window. Otherwise, the Internet Advisor LAN sends an ARP Request to get the physical address.

Starting the PING Measurement

The PING measurement automatically activates special filters to ensure that it can process all necessary frames. This measurement activates the following filters:

- arp
- ping

These filters can be examined in the list of filters in the Filters window. No other filters should be active when the PING measurement runs. Check the funnel-shaped filter status icon in the lower right screen and be sure it is white before running this measurement.

If another filter is currently active, a message is displayed stating that the automatic filters could not be activated. The results of running without the automatic filters may be misleading.

If another measurement is running when PING is started, the automatic filters cannot be activated. If another measurement is started after the PING measurement, the filters cannot be deactivated. It is best to run the PING measurement when no other measurements are running.

1. In the Setup window, make sure the data source is Network Under Test.

2. Stop any other running measurements. You can do this from the Control menu of the individual measurements, or you can stop all measurements at once by selecting Stop All Measurements in the Control menu of the Measurements window.

3. In the Measurements window, start the PING measurement. A window opens showing the results of the measurement. You can change certain parameters of the measurement by configuring the measurement.

The results of the PING measurement are displayed in five columns:

- **IP Address** - this column shows the Internet address of the target machine to which the ICMP Echo Request packet is sent.

- **Physical Address** - this column shows the resolved address of the target machine. If the Internet Advisor LAN does not receive an ICMP Reply packet, the message ‘‘Address can not be resolved" is displayed.

- **Delay** - this column shows the time between when the ICMP Echo Request packet was sent and when the ICMP Reply packet was received.

- **Length** - this column shows the length in bytes of the received ICMP Reply packet.

- **Sequence** - this column shows the Sequence Number of the received ICMP Reply packet.

When the PING measurement stops, additional statistical information is shown at the bottom of the window:

- the total number of ICMP Echo Request packets transmitted

- the total number of ICMP Reply packets received

- the minimum, average, and maximum times between the ICMP Echo Request packets and the ICMP Reply packets (if any packets were received)

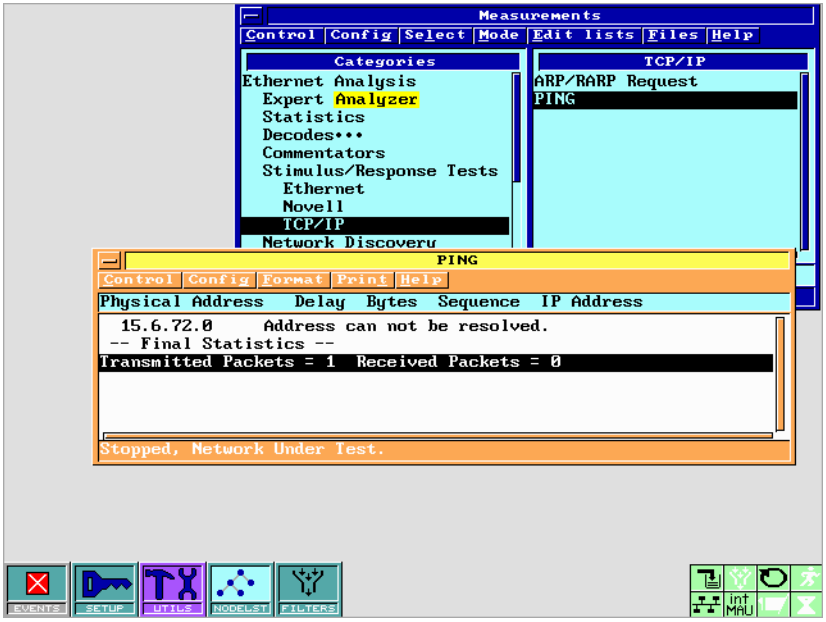


Figure 5-4: PING window

Configuring the PING Measurement

The Configure Measurement item in the Config menu of the PING window opens the PING Configuration window. From the configuration window, you can change parameters that affect how the measurement runs. For example, you can specify the number of times the ICMP Echo Request packet is transmitted and to what target address it is sent.

1. In the PING window, select Stop Measurement in the Control menu.

2. Select Configure Measurement in the Config menu. The PING Configuration window opens.

3. In the Target Address field, specify the internet (IP) address of the host machine you want to test with the PING measurement.

   The items in the Format menu let you enter the target address in dot decimal or hexadecimal format, or you can select a node name that is in the Internet Advisor LAN's node/station list from the list pane (if there are any node names that have IP addresses).

   Example four-byte dot decimal format: `15.6.132.42`
   Example four-byte hexadecimal format: `01-A2-30-2B`
   Example node name format: `brutus`

4. In the Sender Address field, specify the internet address of the Internet Advisor LAN. It is VERY important to configure the Sender Address so it is unique for your network.

   Remember, the items in the Format menu let you enter the address in dot decimal or hexadecimal format, or select a node name from the list pane.

5. In the Packet Data Size field, specify the number of bytes that will be inserted into the data field of the ICMP Echo Request packets. You can enter values between 0 and 1,472.

   The ICMP Echo Request packet is always at least 64 bytes; therefore if the total size of the packet is still less than 64 bytes, the Internet Advisor LAN automatically pads the packet with the correct number of bytes.

6. In the Timeout field, select the amount of time in milliseconds that the PING measurement should wait for an ICMP Reply packet after it sends an ICMP Echo Request packet.

   Timeout values should be greater than 1000 milliseconds and less than 60,000 milliseconds. When you are running the PING measurement across long distances (via a WAN or satellite link, for example) or through many routing hubs, delays may be greater than one second. Use a longer timeout in these cases.

7. In the Number Packets field, select the number of times the ICMP Echo Request packet is transmitted.

   You can enter a number greater than or equal to one, or you can select Continuous from the list pane.

   In the continuous mode, ICMP Echo Request packets are transmitted continuously until you stop the measurement. As each ICMP Reply is displayed, another ICMP Echo Request is sent.

8. Enable or disable the Enable Default Routing check box.

9. If you enabled the Enable Default Routing check box, enter an address in the Default Router IP Address field.

10. Select Accept Changes and Exit in the Done menu to save your selections and return to the PING window. The new configuration is used the next time you start the measurement.

    OR

    Select Run in the Run menu. This saves your selection, returns to the PING window, and starts the PING measurement using the new configuration.

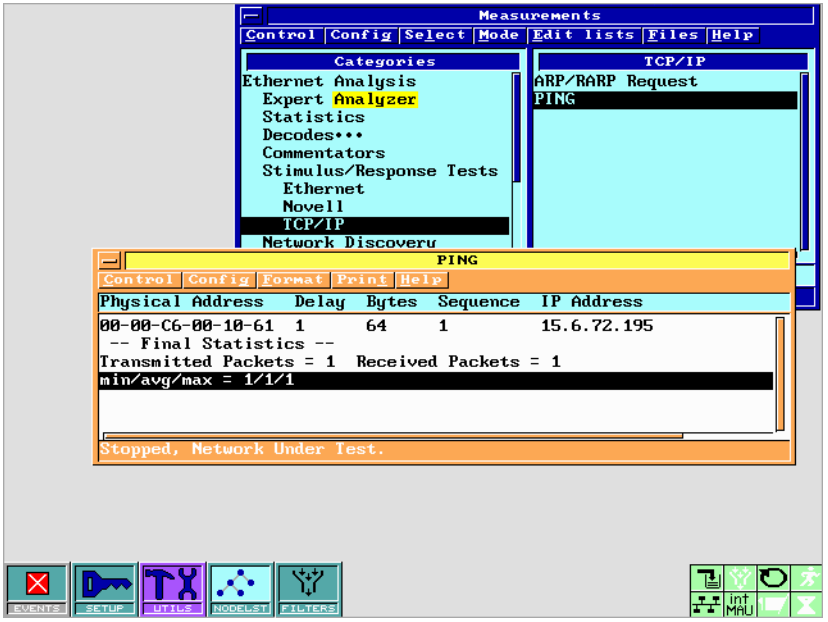


Figure 5-5: PING Configuration window

Using the Active Station List Measurement

When you run the Token-Ring Active Station List measurement, the Internet Advisor LAN monitors the neighbor notification process on the ring to generate a list of stations on the ring.

The Internet Advisor LAN monitors the Active Monitor Present (AMP) and Standby Monitor Present (SMP) frames that are sent between the stations on the ring. The neighbor notification process allows each station to acquire the address of its nearest active upstream neighbor (NAUN).

Starting the Active Station List Measurement

1. In the Setup window, make sure the data source is Network Under Test and the network interface is Token-Ring.

2. In the Measurements window, start the Active Station List measurement.

   A window opens showing the results of the measurement. You can change certain parameters of the measurement by configuring the measurement.

The results of the Active Station List measurement are displayed in four columns:

- **Relative Number** - this column shows the relative position of each station in the ring. This information is used for reference only; it is not derived from the Token-Ring protocol.

- **MAC Address** - this column shows the MAC address of each station in the ring. The first MAC address listed is the address of the Active Monitor.

- **Delay** - the delay time for the Active Monitor is always zero. For all other stations, this column shows the time in milliseconds between when a station sent an SMP and when it saw the last SMP. This lets you see the amount of time it takes for the frames to travel between neighbors.

- **Station Name** - if an address shown in the MAC Address column belongs to the Active Monitor, (Active Monitor) is displayed in this column.

  Otherwise, for each MAC address shown in the MAC Address column, the Internet Advisor LAN attempts to identify the station by its address name or station name (depending on which item is active in the Display Name menu) from the Internet Advisor LAN's node/station list.

  If there is no address name nor station name in the node/station list, the Internet Advisor LAN attempts to identify the station by a vendor name. For example, ‘‘HP----010203".

  If there is no vendor name, the Station Name column is blank.

When the Active Station List measurement stops, you can use the ↑ , ↓ , **PgUp**, and **PgDn** keys to scroll the list.

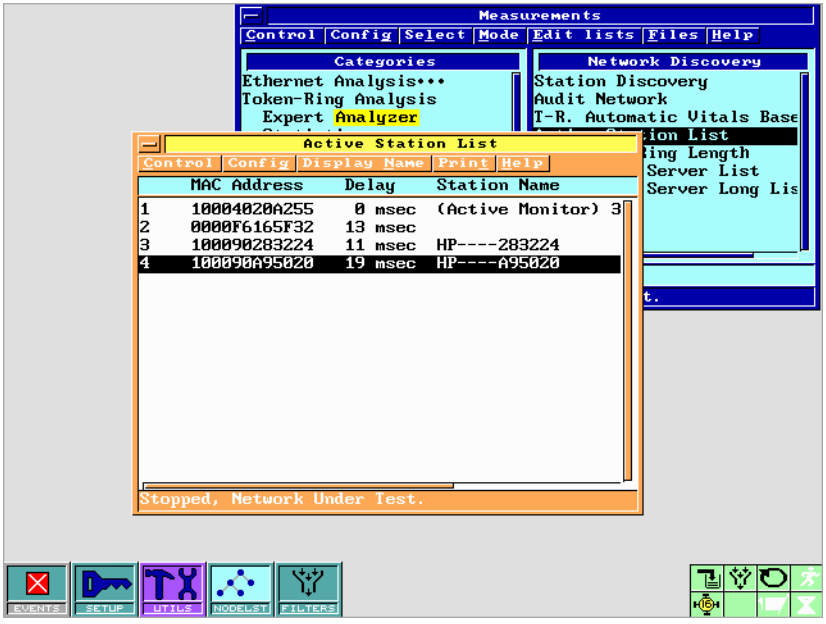


Figure 5-6: Active Station List window

Configuring the Active Station List Measurement

The Configure Measurement item in the Config menu of the Active Station List window opens the Active Station List Configuration window. From the configuration window, you can change parameters that affect how the measurement runs.

For Example. . . You can specify whether the Active Station List measurement should run continuously or only once.

1. In the Active Station List window, select Stop Measurement in the Control menu.

2. Select Configure Measurement in the Config menu. The Active Station List Configuration window opens.

3. In the Timeout field, select the amount of time in seconds that the Internet Advisor LAN should wait before giving up on the neighbor notification process. Timeout values should be greater than 14 seconds.

   A neighbor notification process happens every seven seconds on a healthy network. By waiting at least 14 seconds, you ensure that if the Internet Advisor LAN starts monitoring in the middle of the process it can follow the next process.

4. Enable or disable the Continuous Display check box.

   If you enable it (indicated by a check mark), the Active Station List measurement runs continuously until you stop it. If you disable it, the Active Station List measurement runs only once.

5. Select Accept Changes and Exit in the Done menu to save your selections and return to the Active Station List window. The new configuration is used the next time you start the measurement.

   OR

   Select Run in the Run menu. This saves your selection, returns to the Active Station List window, and starts the Active Station List measurement using the new configuration.

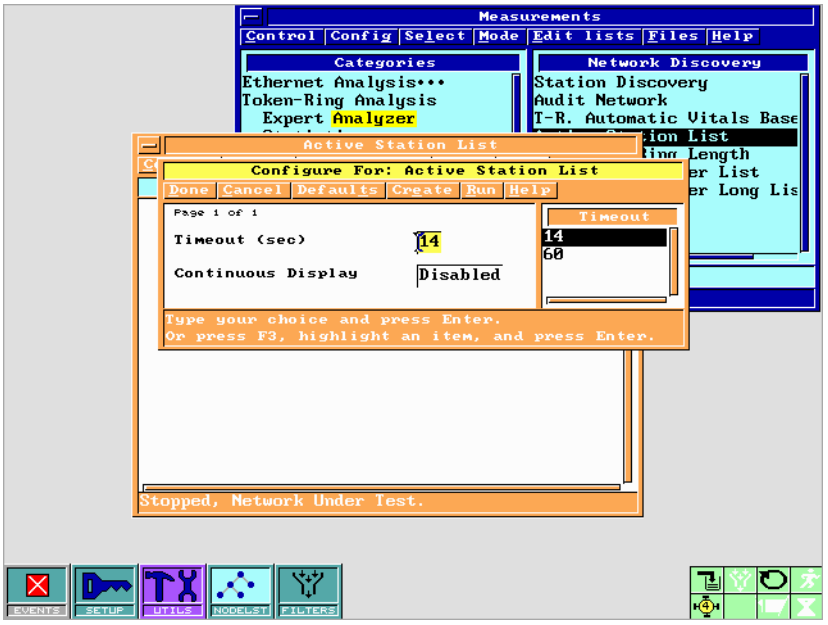


Figure 5-7: Active Station List Configuration window

Using the Calculate Ring Length Measurement

The Token-Ring Calculate Ring Length measurement attempts to measure (in feet and meters) the ring length of an active Token-Ring network. To do this, the Internet Advisor LAN uses two values:

- The velocity propagation delay (VPD) of the network
- The number of stations in the ring

The Internet Advisor LAN uses a VPD that corresponds to the cable type you specify in the Cable Type field of the Calculate Ring Length Configuration window.

To determine the number of stations in the ring, the Internet Advisor LAN follows the Neighbor Notification process.

Starting the Calculate Ring Length Measurement

1. In the Setup window, make sure the data source is Network Under Test and the network interface is Token-Ring.

2. In the Token-Ring Parameters window (accessed through the Advisor Setup window), make sure the Participate in Ring check box is enabled.

3. Stop any other running measurements.

   You can do this from the Control menu of the individual measurements, or you can stop all measurements at once by selecting Stop All Measurements in the Control menu of the Measurements window.

4. In the Measurements window, start the Calculate Ring Length measurement.

   A window opens showing the results of the measurement. You can change certain parameters of the measurement by configuring the measurement.

If the Internet Advisor LAN is unable determine the VPD or the number of stations in the ring before the timeout period specified in the Calculate Ring Length Configuration window, it displays the message ‘‘Network conditions prevented calculation. Please try again." Refer to “What to Do if the Measurement Fails or Is Inaccurate” in the next section for more information.

If the Internet Advisor LAN can calculate the ring length, the following results are shown:

- **Calculated Ring Length** - the calculated ring length is shown in meters and feet. The calculation is accurate to + or - 200 feet provided the following are true:
  - The Internet Advisor LAN can accurately determine the number of stations in the ring.
  - All stations in the ring participate in the Neighbor Notification process.
  - The cable type selected in the Ring Length Configuration window is correct.
- **Inserted Station Coun**t - this shows the number of stations that the Internet Advisor LAN determined are in the ring. If you suspect the inserted station count is wrong, refer to *What to do if the measurement fails or is inaccurate*.
- **Token Rotation Time** - the Token Rotation Time is the time between back-to-back tokens on the network. In other words, it is the velocity propagation delay on the network. It is NOT the average time it takes for a station to get a token.
- **Selected Cable Type** - this shows the cable type that is currently selected in the Cable Type field of the Calculate Ring Length Configuration window.
- **Local Addresses** - this shows whether there are any locally administered addresses on the network. If there are no locally administered addresses, the message “Not Present” is displayed.

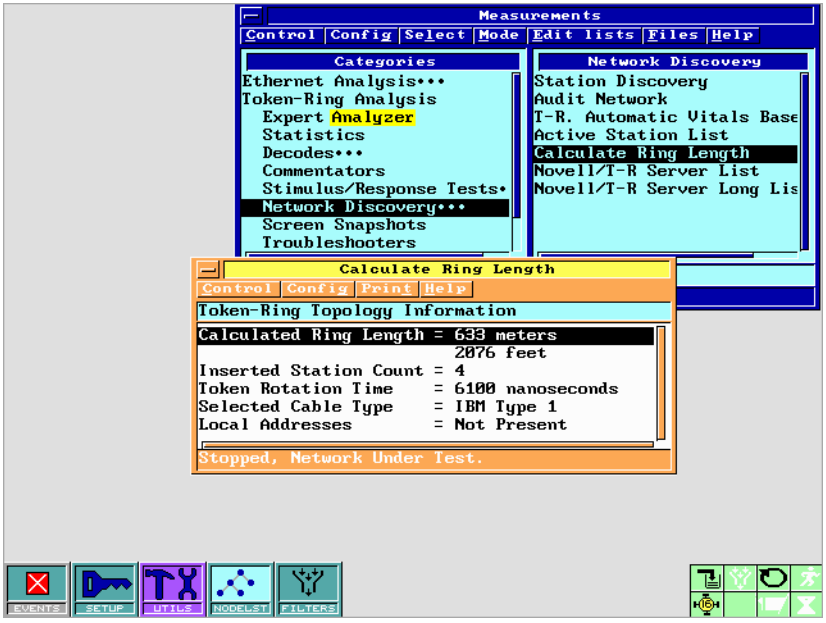


Figure 5-8: Calculate Ring Length window

What to Do if the Measurement Fails or Is Inaccurate

If the Ring Length or Inserted Station Count Seems Wrong

To accurately measure the ring length, the Calculate Ring Length measurement uses two values: the velocity propagation delay (VPD) of the network and the number of stations in the ring.

The Internet Advisor LAN determines the number of stations by following the Neighbor notification process. The determined number of stations could be incorrect if the Neighbor Notification process is preempted by a station inserting or de-inserting.

The number of stations could also be wrong if there is a break in the line causing the Neighbor Notification process to be abruptly terminated. In this case, the Internet Advisor LAN may think there are less stations in the ring than there really are. This results in an apparent ring length that is much greater than the actual ring length.

If either of these values cannot be determined or are inaccurate, the measurement fails or is inaccurate. Below are some possible solutions.

1. Make sure the correct cable type is specified in the Cable Type field of the Ring Length Configuration window.

2. Run the measurement again to make sure the Internet Advisor LAN determines the correct number of stations in the ring.

If Network Conditions Prevented Calculation

If the Internet Advisor LAN is unable to determine the VPD or the number of stations in the ring before the timeout period specified in the Ring Length Configuration window, it displays the message ‘‘Network conditions prevented calculation. Please try again." One possible cause is that the network traffic is so high the Internet Advisor LAN could not see two back-to-back tokens during the calculation. Below are some possible solutions.

1. Try running the measurement again.

2. If the measurement still fails, try changing any or all of the following items and then run the measurement again:

    a. Increase the timeout value in the Calculate Ring Length Configuration window.

    b. Increase the capture buffer size in the Capture Buffer Control window (accessed through the Setup window).

    c. Enable partial packet store (packet slicing) in the Capture Buffer Control window, and set the partial packet size to a relatively low number (for example, 48 bytes).

Configuring the Calculate Ring Length Measurement

The Configure Measurement item in the Config menu of the Calculate Ring Length window opens the Calculate Ring Length Configuration window. From the configuration window, you can change parameters that affect how the measurement runs. For example, you can specify the type of cable used in the network.

1. In the Calculate Ring Length window, select Stop Measurement in the Control menu.

2. Select Configure Measurement in the Config menu. The Calculate Ring Length Configuration window opens.

3. In the Cable Type field, select the appropriate cable type for the ring you are testing.

   The measurement assumes the network has the one type of cabling specified in the Cable Type field. The measurement does not account for mixed cable types. If your network has more than one type of cable, choose the type there is the most of. The resulting ring length calculation will not be extremely accurate if the VPDs are different, but you can get an idea of the ring length.

   The online help for the Calculate Ring Length Configuration window describes each of the possible cable types.

4. In the Timeout field, select the amount of time in seconds that the Internet Advisor LAN should wait before giving up on the Neighbor Notification process.

   The Internet Advisor LAN follows the Neighbor Notification process to determine the number of stations in the ring. Timeout values must be greater than 14 seconds.

   A Neighbor Notification process happens every seven seconds on a healthy network. By waiting at least 14 seconds, you ensure that if the Internet Advisor LAN starts monitoring in the middle of the process it can follow the next process.

5. Select Accept Changes and Exit in the Done menu to save your selections and return to the Calculate Ring Length window. The new configuration is used the next time you start the measurement.

   OR

   Select Run in the Run menu. This saves your selection, returns to the Calculate Ring Length window, and starts the Calculate Ring Length measurement using the new configuration.

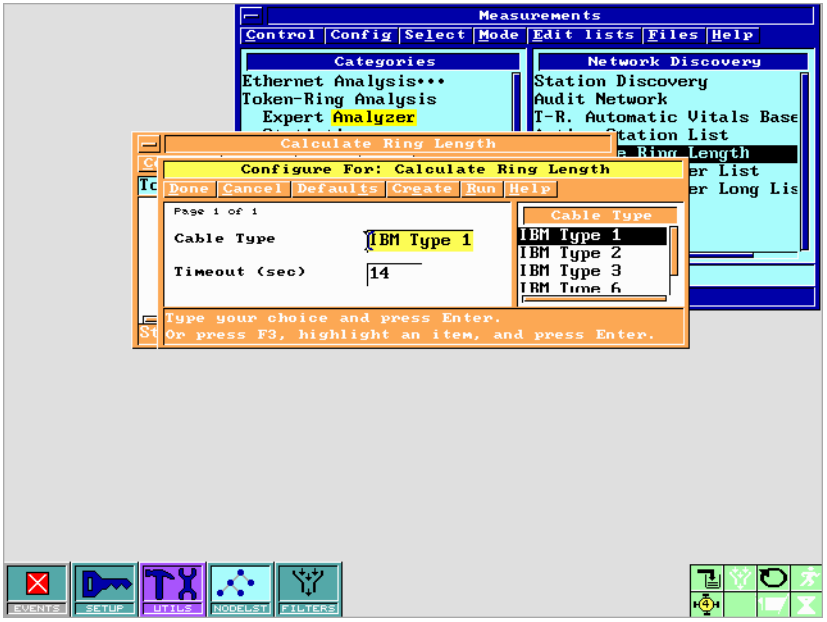


Figure 5-9: Calculate Ring Length Configuration window

Using the Request Station ID Measurement

The Token-Ring Request Station ID measurement tests connectivity to a station on a local or remote ring. To do this, the Internet Advisor LAN sends out a Test Command packet to the station. You supply the station's MAC address in the Request Station ID Configuration window.

For the Test Command packet, the Internet Advisor LAN uses source routing to send an 802.2 "test" message as a single-route broadcast. This message is forwarded by source routing bridges. The response is sent back as all-routes broadcast so the Internet Advisor LAN sees a Test Response packet from each possible route.

Starting the Request Station ID Measurement

1. In the Setup window, make sure the data source is Network Under Test and the network interface is Token-Ring.

2. In the Token-Ring Parameters window (accessed through the Advisor Setup window), make sure the Participate in Ring check box is enabled.

3. In the Measurements window, start the Token-Ring Request Station ID measurement.

   A window opens showing the results of the measurement. You can change certain parameters of the measurement by configuring the measurement.

The results of the Request Station ID measurement tell you this information:

- **MAC Address** - this column shows the MAC address of the station to which the Test Command packet is sent.

- **Delay** - this column shows the time between when the Test Command packet was sent and when a Test Response packet was received. If the Internet Advisor LAN does not receive a response ‘‘No Response Returned" is displayed.

- **Routing** - this column shows whether the station is on a local or remote ring.

- **Duplicate** - if two different stations respond to the Test Command packet, duplicate addresses may exist on the network.

  If you supplied a MAC address in the MAC Address field of the Request Station ID Configuration window, ‘‘Duplicate" indicates that the Internet Advisor LAN saw the MAC address on different rings.

  If you supplied a functional address in the MAC Address field of the Request Station ID Configuration window, you should ignore the ‘‘Duplicate" label because each ring could have a station that responded to that functional address, and it is not really a duplicate MAC address.

When the Request Station ID measurement stops, additional statistical information is shown at the bottom of the window:

- The total number of Test Command packets transmitted

- The total number of Test Response packets received

- The minimum, average, and maximum times between the Test Command packets and the Test Response packets (if any packets were received)

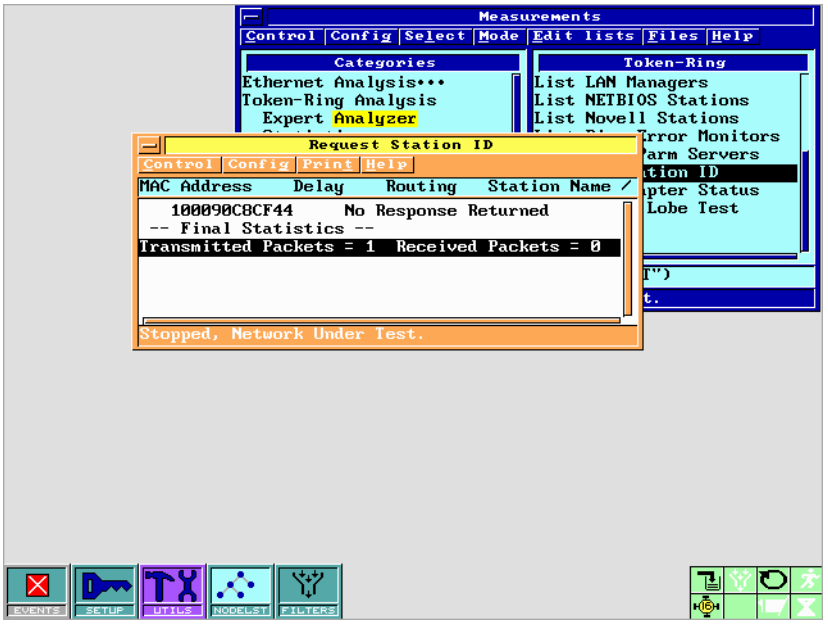


Figure 5-10: Request Station ID window

Configuring the Request Station ID Measurement

The Configure Measurement item in the Config menu of the Request Station ID window opens the Request Station ID Configuration window. From the configuration window, you can change parameters that affect how the measurement runs. For example, you can specify the MAC address you want to test.

1. In the Request Station ID window, select Stop Measurement in the Control menu.

2. Select Configure Measurement in the Config menu. The Request Station ID Configuration window opens.

3. In the MAC Address field, specify the MAC address of the station you want to test with the Request Station ID measurement.

   The items in the Format menu let you enter the MAC address in hexadecimal format or you can select a station name that is in the Internet Advisor LAN's node/station list from the list pane (if there are any station names that have Token-Ring addresses).

   You can also enter a hexadecimal functional address. If you enter a functional address, you should ignore any packets that are labeled as duplicates because each ring could have a station that responds to the functional address.

   Example six-byte hexadecimal format: `01A2302B1122`
   Example six-byte hexadecimal functional format: `C00000000001`
   Example station name format: `brutus`

4. In the Timeout field, select the amount of time in milliseconds that the Request Station ID measurement should wait for a Test Response packet after it sends a Test Command packet.

   Timeout values should be greater than 1000 milliseconds.

5. In the Number Packets field, select the number of times the Test Command packet is transmitted.

   You can enter a number greater than or equal to one, or you can select Continuous from the list pane.

   In the continuous mode, Test Command packets are transmitted continuously until you stop the measurement. As each Test Response is displayed, another Test Command is sent.

6. Select Accept Changes and Exit in the Done menu to save your selections and return to the Request Station ID window. The new configuration is used the next time you start the measurement.

   OR

   Select Run in the Run menu. This saves your selection, returns to the Request Station ID window, and starts the Request Station ID measurement using the new configuration.

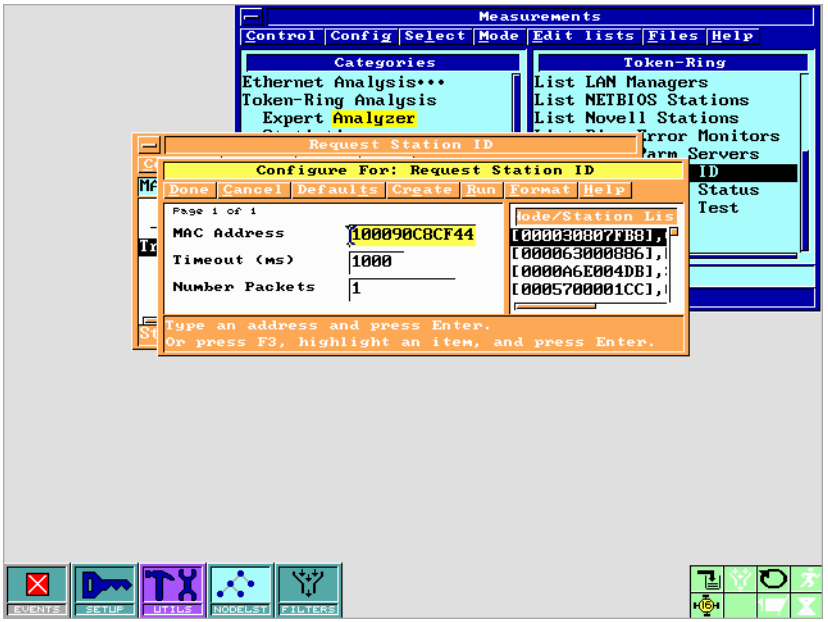


Figure 5-11: Request Station ID Configuration window

Using the Station Adapter Status Measurement

The Token-Ring Station Adapter Status measurement gives you information about a station on the ring. To do this, the Internet Advisor LAN sends out a Request Ring Station Address frame to the station. You supply the station's MAC address in the Station Adapter Status Configuration window. The addressed station should return a frame containing its adapter status.

This MAC frame will not be forwarded by source-routed bridges.

Starting the Station Adapter Status Measurement

1. In the Setup window, make sure the data source is Network Under Test and the network interface is Token-Ring.

2. In the Token-Ring Parameters window (accessed through the Setup window), make sure the Participate in Ring check box is enabled.

3. In the Measurements window, start the Station Adapter Status measurement.

   A window opens showing the results of the measurement. You can change certain parameters of the measurement by configuring the measurement.

The results of the Station Adapter Status measurement tell you this information:

- **MAC Address and Time** - the MAC address of the station to which the Request Ring Station Address frame is sent is displayed. Next to it, the time it took for the Internet Advisor LAN to receive a Report Ring Station Address frame is displayed. If the Internet Advisor LAN does not receive a response, ‘‘No Response Returned" is displayed and no other information is displayed.

- **NAUN** - the address of the Nearest Active Upstream Neighbor is displayed.

- **Physical Location** - the four-byte assigned physical location of the station is displayed.
- **Group** - the four-byte group address recognized by this station is displayed.
- **Functional Address** - the four-byte functional address is displayed.
- **Station Function** - the type of Token-Ring functions the station is performing are listed. For example, if the station is the Active Monitor, ‘‘Active Monitor" is displayed.

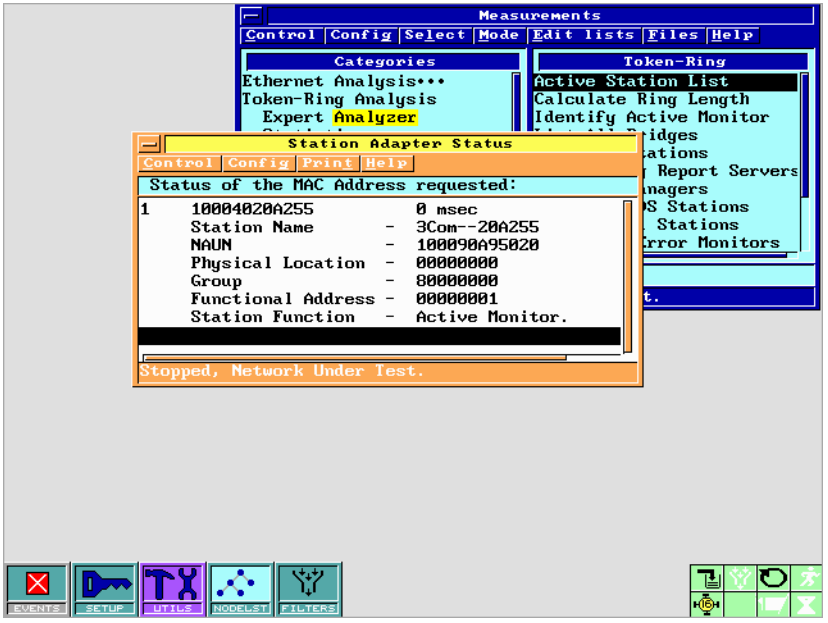


Figure 5-12: Station Adapter Status window

Configuring the Station Adapter Status Measurement

The Configure Measurement item in the Config menu of the Station Adapter Status window opens the Station Adapter Status Configuration window. From the configuration window, you can change parameters that affect how the measurement runs.

For Example. . . You can choose the specific MAC address you want to test.

1. In the Station Adapter Status window, select Stop Measurement in the Control menu.

2. Select Configure Measurement in the Config menu. The Station Adapter Status Configuration window opens.

3. In the MAC Address field, specify the MAC address of the station you want to test with the Station Adapter Status measurement.

   The items in the Format menu let you enter the MAC address in hexadecimal format or you can select a station name that is in the Internet Advisor LAN's node/station list from the list pane (if there are any station names that have Token-Ring addresses). You can also enter a hexadecimal functional address.

   Example six-byte hexadecimal format: `01A2302B1122`
   Example six-byte hexadecimal functional format: `C00000000001`
   Example station name format: `brutus`

4. In the Timeout field, select the amount of time in milliseconds that the Station Adapter Status measurement should wait for a Report Ring Station Address frame after it sends a Request Ring Station Address frame.

   Timeout values should be greater than 1000 milliseconds.

5. Select Accept Changes and Exit in the Done menu to save your selections and return to the Station Adapter Status window. The new configuration is used the next time you start the measurement.

   OR

   Select Run in the Run menu. This saves your selection, returns to the Station Adapter Status window, and starts the Station Adapter Status measurement using the new configuration.

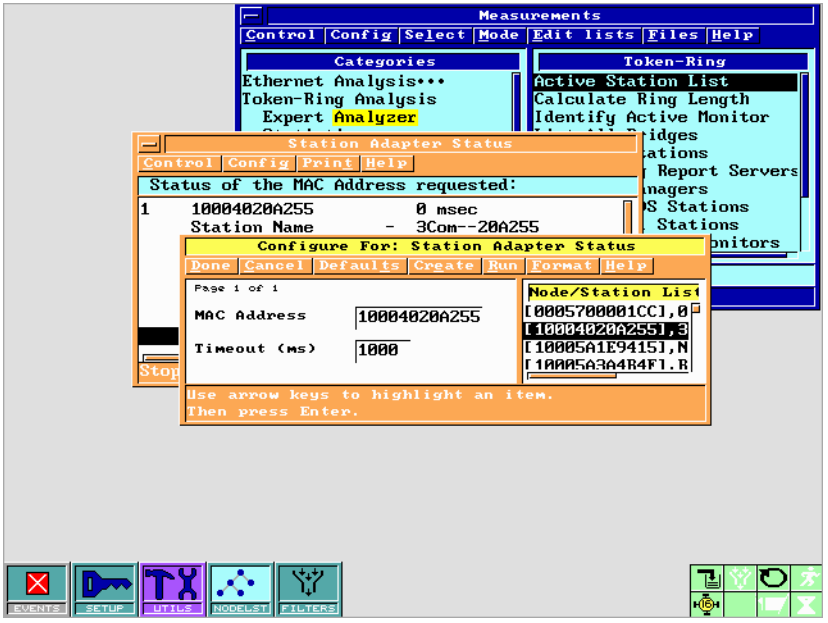


Figure 5-13: Station Adapter Status Configuration window

Printing Node Discovery and Station Discovery Measurements

The Node Discovery and Station Discovery measurements in the Ethernet, FDDI, and Token-Ring network interfaces let you write the discovery results to either a printer or a file.

The Print menu bar item in both of these measurements lets you print either all displayed nodes/stations or only selected nodes/stations. The Format and the Node/Station List menu bar items let you control what nodes/stations are displayed in the measurement window.

1. Open either the Node Discovery or the Station Discovery measurement window.

2. Use the Display menu bar items to set up which discovered nodes are displayed.

3. Run the discovery measurement.

4. (Optional) After the measurement ends, use the Node/Station List menu bar item to select the nodes/stations you are interested in.

5. Select either the Print All Displayed Records item or the Print Selected Records item in the Print menu.

   The measurement result is written to either a printer or a file depending on your selection in the Print Screen Output field of the PC Hardware Configuration window (accessed from the Utilities window).

Using the Network Commentator Measurements

The Network Commentator measurements for Ethernet, Token-Ring, and FDDI provide high-level reports of significant protocol events that may be preludes to network performance degradation or network failure.

From the Network Commentator display, you can get more specific information by “drilling down” on certain measurements.

You can customize Commentator and Vitals measurements to test for certain conditions on your network. You can set up the filters to search for specific events, and then rename the measurement and save it so you can use it again. See the online help for more information about setting up filters and renaming measurements.

Starting a Commentator Measurement

1. The Commentators can run either from the frames on the Network Under Test or from frames in the Capture Buffer. Set the Data Source using the Advisor Setup window or the Control menu of the Commentator.

2. You may want to set some configurable event parameters in the Configuration widow of the Commentator before starting the measurement. Use the Config menu button to go to the Configuration window.

3. Select which events you want to comment on. See the online help in the Configuration window for more information.

4. Start the Commentator measurement from the Control menu.

The Network Commentator window lists information about important events on the network. The online help for the Network Commentator window describes the meaning of each of these events in more detail.

You can easily get more detailed information about a particular event in the Network Commentators display by double clicking the mouse on an event. This "drill down" capability lets you see more information quickly. Press **F5** to return to the main Network Commentator display.

For Example. . . Moving the mouse cursor over the first line of an event and then double-clicking opens the help text for that event. The help text describes the event, and if the event is a Warning or an Alert, and it offers advice on how to resolve the problem.

Moving the mouse cursor over any part of an event and double-clicking causes one of the following things to occur:

- If you are running the Commentator from the Capture Buffer, and the frame which caused the event is in the Buffer, the appropriate decode measurement is opened displaying that frame so you can see the content of the frame.
- If you are running the Commentator from the Capture Buffer, but the frame which caused the event is NOT in the Buffer, a message is displayed.
- If you are running the Commentator from the network, the appropriate decode measurement is opened and it is started so that you can capture traffic from the network.

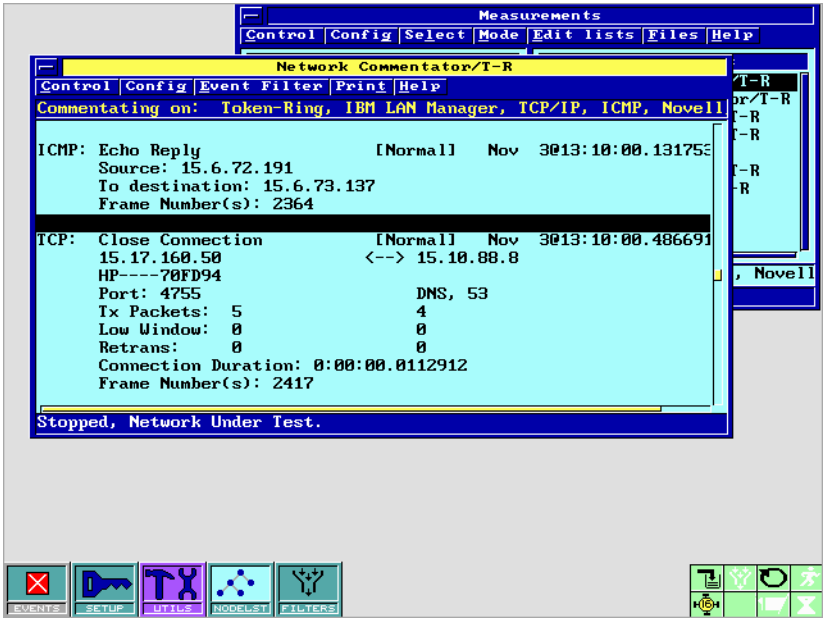


Figure 5-14: Network Commentator Window

Using the Lobe Test Measurement

The Token-Ring protocol specifies that a station be able to perform a lobe test on itself to check the loop of wiring between the station and the relay in the MAU (Multistation Access Unit). The Token-Ring Lobe Test measurement performs a lobe test on the Internet Advisor LAN.

Starting the Lobe Test Measurement

1. Make sure the network interface in the Setup window is Token-Ring.

2. Stop any other running measurements.

   You can do this from the Control menu of the individual measurements, or you can stop all measurements at once by selecting Stop All Measurements in the Control menu of the Measurements window.

3. In the Measurements window, start the Token-Ring Lobe Test measurement. A window opens showing whether the test passed or failed.

When you start the Lobe Test, the Internet Advisor LAN is removed from the ring if it is currently inserted in the ring.

After the lobe test, the Internet Advisor LAN remains de-inserted from the ring regardless of its initial insertion status.

The online help for the Lobe Test window describes what a lobe test is and conditions under which the Lobe Test is run automatically.

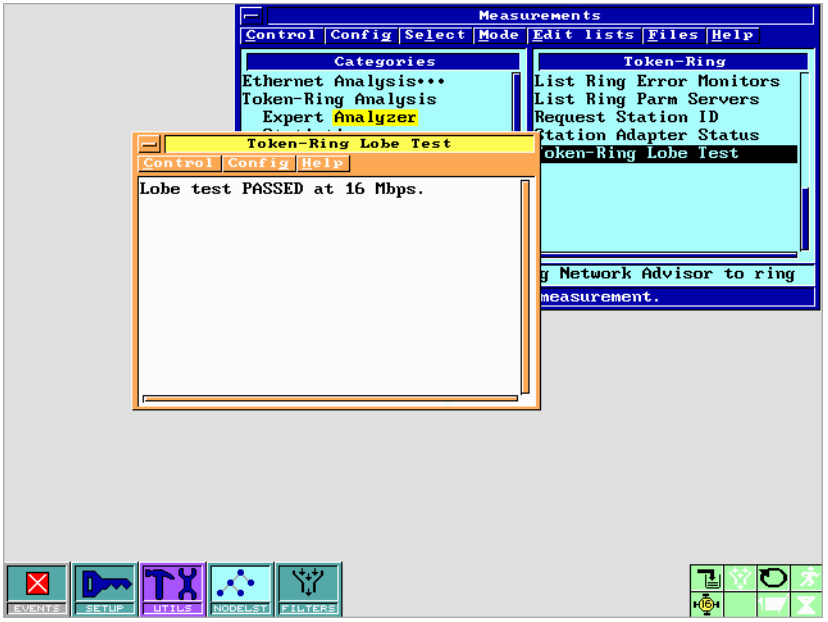


Figure 5-15: Token-Ring Lobe Test window

Using the Token-Ring and Ethernet Traffic Generator Measurements

The Token-Ring and Ethernet Traffic Generator measurements for the Internet Advisor LAN are similar enough to be described in the same section. The FDDI Traffic Generator measurement is described in the following section.

The Traffic Generator measurements let you duplicate frame content and traffic conditions on the network to help solve problems. This section describes how to use the Token-Ring Traffic Generator, but the setup and use of the Ethernet Traffic Generator is similar.

The Token-Ring Traffic Generator measurement lets you transmit frames with an LLC frame format or choose from four MAC packets (Remove Ring Station, Request Ring Station Address, Request Ring Station State, Request Ring Station Attachments).

You can test either a device or a system to determine the limits of network hardware or protocol implementations by increasing the amount of traffic they handle, or by inducing perturbations on the network. You can also find the limits of a device or a group of stations for handling congestion or errors.

Starting the T-R Traffic Generator Measurement

NOTE

In order to protect your network, all measurements which transmit on the network can be set up to require a password. The Internet Advisor LAN is shipped with the password set to **advisor**. You may change the password or disable it. See the online help in the Setup window for more information.

1. In the Setup window, make sure the data source is Network Under Test and the network interface is Token-Ring.

2. In the Token-Ring Parameters window (accessed through the Setup window and the Interface Parameters subwindow), make sure the Participate in Ring check box is enabled.

3. Stop any other running measurements.

   You can do this from the Control menu of the individual measurements, or you can stop all measurements at once by selecting Stop All Measurements in the Control menu of the Measurements window, or you can select the active running figure icon.

NOTE

After starting the traffic generator, you can also run decodes and summary stats, but don't run applications that transmit on the network such as Active Station List.

4. In the Measurements window, select Stimulus/Response Tests under Token Ring Analysis, then open the T-R Traffic Generator measurement.

   If you choose to run the measurement from the Stimulus/Response Tests pane, you will be asked whether you want to run the measurement on the network. If you select Yes, the measurement will run with the current configuration. If you want to specify your own configuration, select No and proceed to the configuration task.

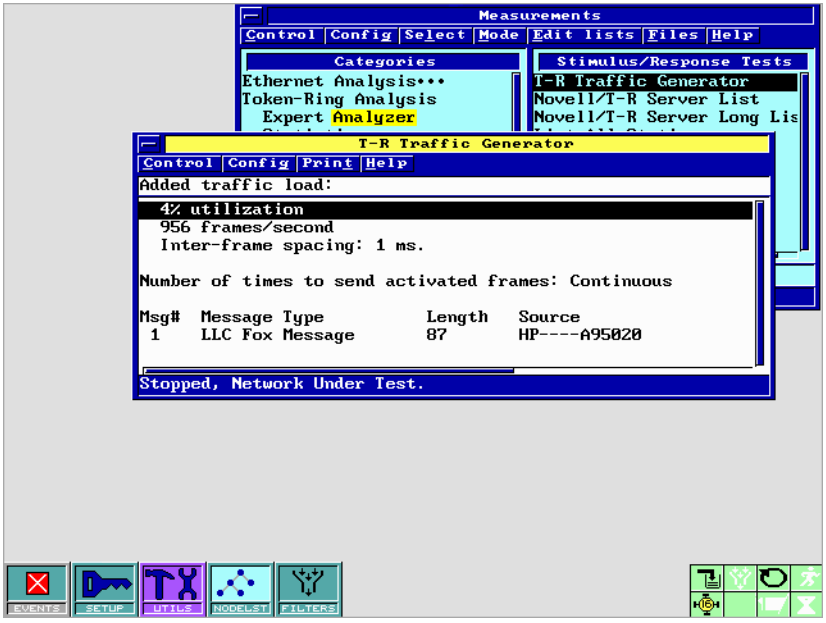


Figure 5-16: Traffic Generator window

Saving Your Configuration as a New Measurement

If you know you will want to use the same measurement configuration again, you can create a new measurement that is listed in the Stimulus/Response Tests pane. You can then open this measurement and set up the configuration.

1. In the Traffic Generator window, select Config in the menu bar, then select Configure Measurement.

   In the Configure window, select Create in the menu bar, then select Create New Measurement.

2. Give your measurement a name and add a comment.

3. Select Accept Changes and Exit in the Done menu of the Create New Measurement window.

4. Select Accept Changes and Exit in the Done menu of the Configure window.

5. Select Accept Changes and Exit in the Done menu of the Traffic Generator window. The new measurement is saved and its name is displayed in the Stimulus/Response Tests list pane of the Measurement window.

6. Open the new measurement from the Stimulus/Response Tests list pane and make the configuration changes you want.

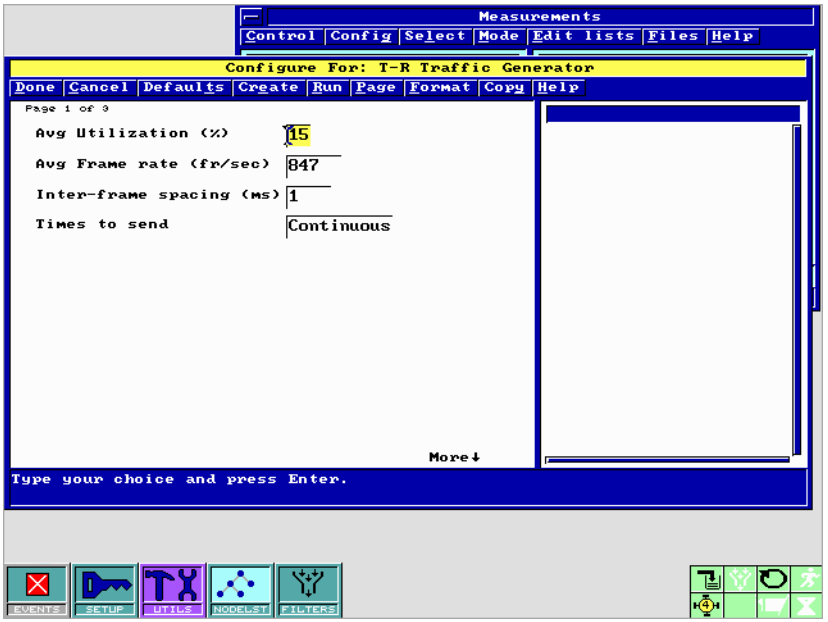


Figure 5-17: Configure for Traffic Generator window

Configuring the Token-Ring Traffic Generator Measurement

In the Configure Measurement window you will be able to:

- Control the number of frames, frequency of transmission and percent utilization of the network.
- Edit frame content and choose which messages are active.
- Edit data bytes or choose random data for the frames.

You can activate up to 32 messages to be transmitted by the Traffic Generator. A message is a frame that has its contents specified in the Traffic Generator. A message can be any of the predefined message types, or a frame you have copied from the capture buffer, or a frame you have modified or created.

If you know you will use the measurement parameters you are setting up only during this session, you can edit the T-R Traffic Generator measurement, run your test, and then cancel the changes and exit when you are done.

If you think you may reuse a traffic generator configuration several times, you may want to use the preceding procedure "Saving your configuration as a new measurement", and then use the steps below to edit that new measurement for your test conditions.

To begin configuring the Traffic Generator, select Config in the menu bar of the T-R Traffic Generator window (or from the traffic generator measurement you have created). Select Configure Measurement to open the Configure window. There are three pages of parameters in this window in which you do the following tasks:

1. Setup network traffic conditions

    a. In the Avg. Utilization field, specify the percentage of the network’s capacity to be used under the current configuration. The average utilization of the network is a function of frame rate, inter-frame spacing, and frame length.

b. In the Avg. Frame Rate field, specify in frames/second, the average number of frames to be transmitted.

c. In the Inter-frame Spacing field, specify in milliseconds the amount of time between transmitted frames.

   When you modify any of the preceding three fields, the values for the other two fields are automatically recalculated and updated.

d. In the Times to Send field, specify how many times the activated messages should be transmitted. You can enter an integer value to send the frame a specific number of times, or you can select Continuous to send the frames continuously until you stop the measurement.

2. Edit and activate messages

   a. Select the Next Page item in the Page menu or press **PgDn** to see the message parameters.

   b. The Activate Messages check box is used to activate or deactivate any of the messages. To activate a message, select the check box to enable it, then in the right pane, select the message numbers you wish to activate. An arrow appears to the left of each selected message number. The selected messages are transmitted when you run the measurement. To deactivate all but message 1, select the check box again.

   c. Edit the Message # field to the message you want to enter values for. All field values are saved to the message currently being configured, that is, the message corresponding to the number in the Message # field.

   d. The Message Type field allows you to select from a list of predefined message types. A predefined message includes values for all fields on this page, but the fields may be customized. The 32 predefined messages are initially defaulted to the LLC Fox Message type. You may also use the Message Type field to label messages you've created.

e. The Frame Length field specifies how many bytes are in this message. When you use a predefined message type, the correct length will be filled in, although you may modify the frame length by editing this field.

   When the Frame Length field is modified, the values of Avg. Utilization, Avg. Frame Rate and Inter-frame Spacing fields are automatically recalculated and updated. To get maximum network utilization, choose Maximum as a value for the Frame Length field.

NOTE The total length of all activated messages must not exceed 32 Kilobytes.

f. The Source and Destination Address fields let you specify addresses for the source and destination of the frame.

   The items in the Format menu control whether the address is displayed in hex or as a station name that is in the Internet Advisor LAN's node/station list from the list pane (if there are any station names that have Token-Ring addresses).

   If the most-significant bit of the source address is 1 (you enter between 8 and F as the left most character of the Source Address), then source routing is used. The online help describes more about using source routing.

g. In the FCS Type field, specify whether the frame will have a good or bad Frame Check Sequence.

   If you choose to have a good FCS, the FCS value is automatically calculated, and the FCS Value field is grayed out.

   If you chose to have a bad FCS in the FCS Type field, specify the bad FCS value in the FCS Value field.

h. In the Priority field, specify what priority the frame should have.

i. The Frame Format field shows whether this frame is an LLC or MAC format frame. If you change the format, the message type may change to match the format you have indicated.

3. Specify the data bytes of the message

   a. Select the Next Page item in the Page menu or press **PgDn** to see the rest of the configurable parameters.

   b. Enabling the Random Data field check box fills in each of the data byte fields with a random character. The Pad Type field will be set to Random and the Pad Value will also contain random characters.

   c. If you want to specify your own data, edit Frame fields 15 through 78.

   d. The Pad Type field allows you to select among Random, Incremental and User-defined pad data. Choose the online help topic Pad Type for more information.

4. Select Accept Changes and Exit in the Done menu to save your selections and return to the Traffic Generator window. The new configuration is used the next time you start the measurement.

   OR

   Select Run in the Run menu. This saves your selection, returns to the T-R Traffic Generator window, and starts the T-R Traffic Generator measurement using the new configuration.

Copying a Message

You can create new messages easily by copying the field values from an already defined message or from a frame in the capture buffer. The Copy menu item copies into the message you are currently editing from the message or frame you specify.

To copy from the capture buffer, the data source must be set to Capture Buffer. You can use the control menu in the Traffic Generator window to switch to the capture buffer if it is not currently the data source.

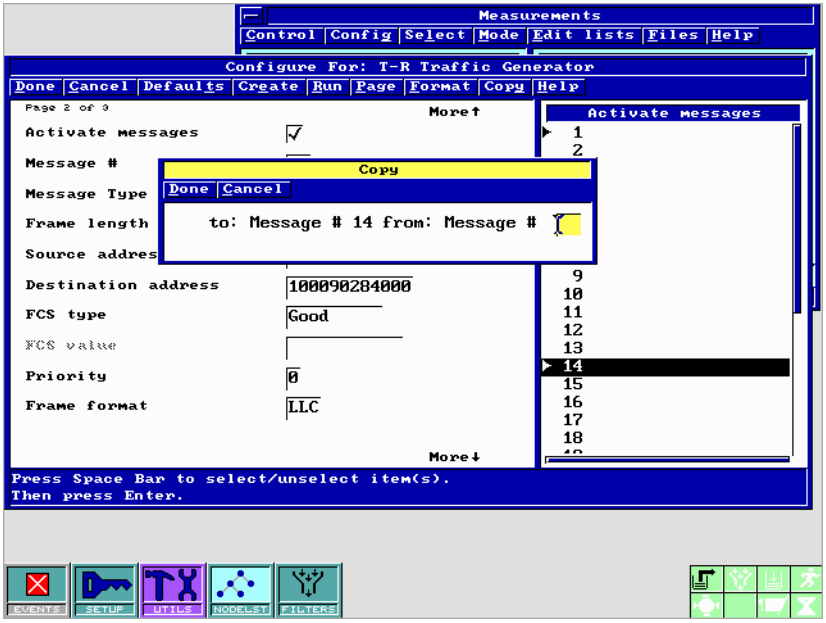


Figure 5-18: Copy message from Capture Buffer window

Using the FDDI Traffic Generator Measurement

The FDDI Traffic Generator measurement provides a full range of choices to accommodate research and development engineers who use the Internet Advisor LAN in a controlled environment. However, generating traffic is potentially hazardous to the health of your network. It is possible to choose options that will make various timers expire and cause the network to claim. Users not involved in device testing and development should use caution when generating traffic.

NOTE

In order to protect your network, all measurements which transmit on the network can be set up to require a password. The Internet Advisor LAN is shipped with the password set to **advisor**. You may change the password or disable it. See the online help in the Setup window for more information.

The FDDI Traffic Generator measurement is found in the Stimulus/Response Tests section under FDDI Analysis in the Measurements window. The Traffic Generator can transmit frames, generate line states, and generate raw symbols to test either a device or a network.

Starting the FDDI Traffic Generator Measurement

1. In the Setup window, make sure the data source is Network Under Test and the network interface is FDDI.

2. In the Measurements window, select Stimulus/Response Tests under FDDI Analysis, then open the FDDI Traffic Generator measurement.

If you choose to run the measurement from the Stimulus/Response Tests pane, you are asked whether you want to run the measurement on the network. If you select Yes, the measurement runs with the current configuration. If you want to specify your own configuration, select No and proceed to the configuration task.

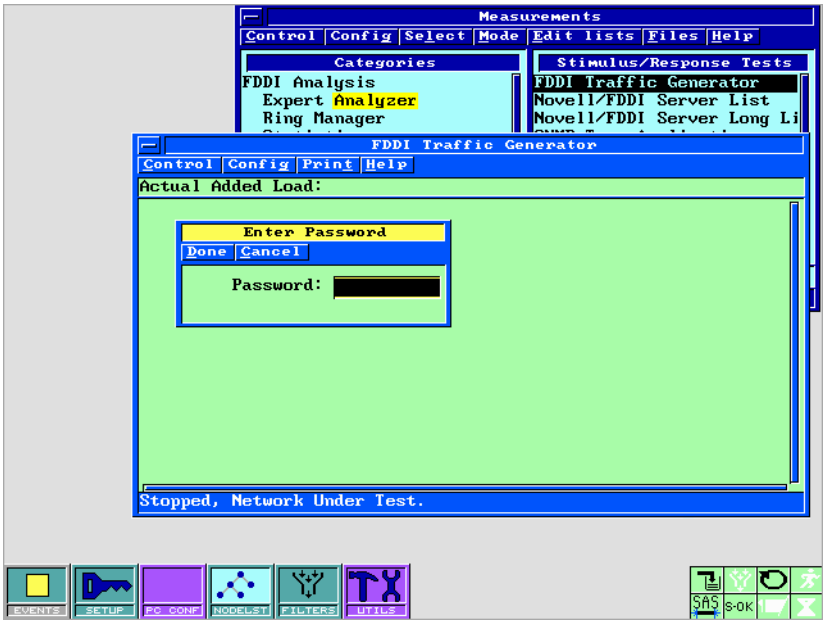


Figure 5-19: FDDI Traffic Generator window

Saving Your Configuration as a New Measurement

If you know you will use the same measurement configuration again, you can save the configuration by creating a custom measurement that is listed in the Stimulus/Response Tests pane. You can then open this measurement and set up the configuration. To create a custom measurement, follow the steps below.

1. In the Traffic Generator window, select Config in the menu bar, then select Configure Measurement. Or, if you have not opened the Traffic Generator window, you can choose Config from the Measurements window to Configure the selected measurement.

   In the Configure window, select Create in the menu bar, then select Create New Measurement.

2. Give your measurement a name and add a comment.

3. Select Accept Changes and Exit in the Done menu of the Create New Measurement window.

4. Select Accept Changes and Exit in the Done menu of the Configure window.

5. Select Accept Changes and Exit in the Done menu of the Traffic Generator window.

   The new measurement is saved and its name is displayed in the Stimulus/Response Tests list pane of the Measurement window.

6. Open the new measurement from the Stimulus/Response Tests list pane and make the configuration changes you want.

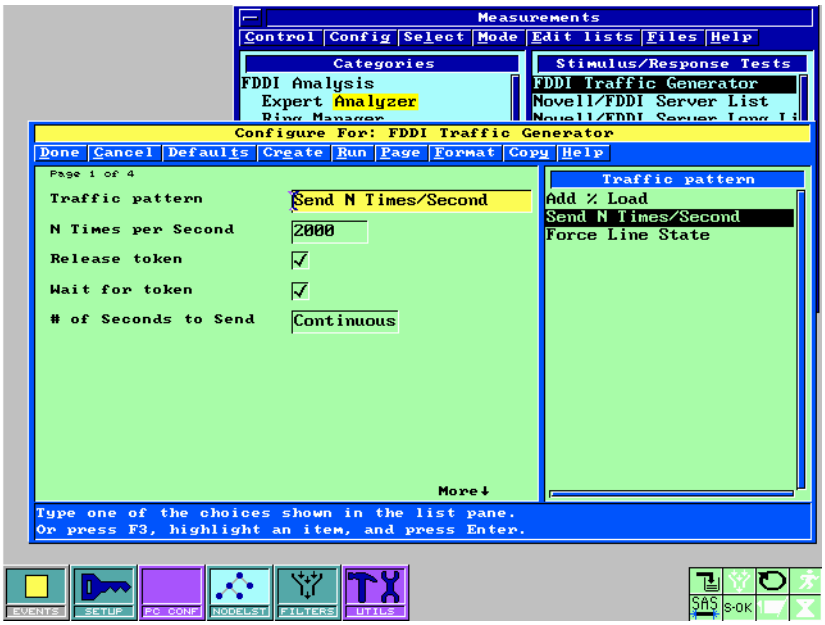


Figure 5-20: Configure for FDDI Traffic Generator window

Configuring the FDDI Traffic Generator Measurement

In the Configure Measurement window you can:

- Set up traffic patterns
- Specify a line state
- Activate and edit predefined messages to send on the network
- Set up to transmit raw symbols

You can activate up to 32 messages to be transmitted by the Traffic Generator. A message is a frame that has its contents specified in the Traffic Generator configuration fields. A message can be any of the predefined message types, a frame you have copied from the capture buffer, or a frame you have modified or created.

If you know you will use the measurement parameters you are setting up only during this session, you can edit the FDDI Traffic Generator measurement, run your test, and then cancel the changes and exit when you are done.

If you think you may reuse a Traffic Generator configuration, you may want to use the preceding procedure "Saving your configuration as a new measurement", and then follow the steps below to edit that new measurement for your test conditions.

To begin configuring the Traffic Generator, select Config in the menu bar of the FDDI Traffic Generator window (or from the traffic generator measurement you have created). Select Configure Measurement to open the Configure window. There are four pages of parameters in this window in which you do the following tasks:

1. Select a traffic pattern

    a. The Traffic Pattern field lets you choose among three patterns:

        - Add a percent load to the network
        - Transmit the activated messages a certain number of times per second
        - Force a line state

Your choice for Traffic Pattern affects the label of the next field on this page.

b. If you choose Add % Load, the second field becomes % Load. Enter an integer from 1 to 100.

c. If you choose Send N Times/Second, the second field becomes N times per Second. Enter an integer between 1 and 15,000 to specify a value for N. The number of packets transmitted each second will be N times the number of activated messages.

d. If you choose Force Line State, the second field becomes Line State. Use the list pane to select the line state to be transmitted.

e. The Wait for Token checkbox should be activated unless you want to test error conditions on the network by transmitting before capturing the token. Be aware if you do not wait for the token, the ring may claim. Wait For Token is grayed out if the Traffic Pattern is Force Line State.

f. The Release Token checkbox should be activated unless you want to test error conditions on the network by causing a valid transaction (TVX) timer to expire. Be aware if you do not release the token, the ring may claim. Release Token is grayed out if the Traffic Pattern is Force Line State.

g. In the # of Seconds to Send field, (or # of Times to Send if Traffic Pattern is Force Line State) specify the duration of time the activated messages should be transmitted (or specify how many times to transmit the specified line state).

   You can enter an integer between 1 and 65,535 for the duration of transmission, or you can select Continuous to transmit the frames continuously until you stop the measurement.

2. Edit message fields and activate messages

   a. Select the Next Page item in the Page menu or press **PgDn** to see the message parameters.

b. The Activate Messages field lets you quickly activate and deactivate messages. Activated messages are transmitted when the measurement is run. To activate a message, use the list pane to select message numbers you wish to activate. To deactivate all messages except message 1, select the checkmark in the Activate messages field and click on it.

c. Edit the Message # field to the message you want to enter values for. You can enter values for up to 32 messages.

d. The Message Name field lets you select from a list of predefined messages, including SMT and LLC messages. You can use the Message Name field to label messages you've created.

e. The Frame Control field can signal an SMT Info frame, Beacon frame, Claim frame, User Defined frame, LLC Asynchronous frame, or an LLC Synchronous frame. Select one of these from the list pane.

f. The Data Length field specifies how many bytes are in this message. When you use a predefined message, the correct length is filled in, although you may modify the data length by editing this field.

g. The Source Address field lets you specify the address of the sending node. You can enter an address other than the Internet Advisor LAN physical address. However, since the sending node is responsible for removing the frame, the address should exist on the ring. If the address does not exist on the ring, the frame will not be removed until the next ring reconfiguration event.

h. The Destination Address field lets you specify the address of the destination node. Note: the destination address should exist on the ring. Transmitting to non-existent addresses can cause the ring to fill up with unstripped frames.

   The items in the Format menu control whether the address is displayed in hex or as a station name that is in the Internet Advisor LAN's node/station list from the list pane (if there are any station names that have FDDI addresses).

i. The Preamble Symbols field lets you specify the symbols to appear in the preamble to the frame. Idle symbols are the default.

j. The Starting Delimiter Symbols field lets you specify the symbols to be used as the starting delimiter. The JK symbol pair is the default.

3. Edit the data bytes of the message

   a. Select the Next Page item in the Page menu or press **PgDn** to see the rest of the configurable parameters.

   b. For predefined messages, bytes 14 through 77 are filled in for you. If you want to specify your own data, you may edit these fields.

   c. The Pad Symbol Pair is 00 by default, but you may edit it.

   d. The Violation symbol value can be selected from the list pane.

4. Edit the Frame Status field

   a. Select the Next Page item in the Page menu or press **PgDn** to see the rest of the configurable parameters.

   b. In the FCS Type field, specify whether the frame has a good or bad Frame Check Sequence.

      If you choose to have a bad FCS in the FCS Type field, specify a value in the FCS Value field.

      If you choose to have a good FCS, the FCS value is automatically calculated, and the FCS Value field is grayed out.

   c. The Terminate Symbol field lets you specify a termination symbol. For a valid frame, this field should be T, but any other FDDI symbol is accepted for the Raw Symbol mode.

d. The EAC Symbols Field lets you specify values for the Error Detect Indicator, Address Recognized Indicator, and Frame Copied Indicator respectively. They can each be specified as Set(S), Reset(R), or None(0).

e. The Additional Symbols field lets you add up to six additional FDDI symbols.

Select Accept Changes and Exit in the Done menu to save your selections and return to the Traffic Generator window. The new configuration is used the next time you start the measurement.

OR

Select Run in the Run menu. This saves your selection, returns to the FDDI Traffic Generator window, and starts the FDDI Traffic Generator measurement using the new configuration.

Using Raw Symbol Mode

Sometimes it may be helpful in device testing to transmit symbols that do not necessarily form a valid frame. You can set up the Traffic Generator so that it functions as a raw symbol generator by following these steps:

1. On the first page of the Configuration window, choose the Traffic Pattern Send N Times/Second.

2. Enter a number for N.

3. Enter a value for # of Seconds to Send.

4. On the second page of the Configuration window, set the Data Length field to 0.

5. Enter FDDI symbols to be transmitted in any or all of the following fields:

   - Preamble Symbols
   - Starting Delim. Symbols
   - Violation Symbol
   - EAC Symbols
   - Termination Symbols
   - Additional Symbols

6. When you run the measurement, the Internet Advisor LAN generates the symbols in these fields for the specified duration of time.

Copying a Message

You can create new messages easily by copying the field values from an already defined message or from a frame in the capture buffer. The Copy menu item copies into the message you are currently editing from the message or frame you specify.

When copying from another message, all fields are copied. When copying from the capture buffer, the following fields are not copied: preamble symbols, starting delimiters, and EAC symbols. The values for these fields come from the configuration page of the Traffic Generator.

To copy from the capture buffer, the data source must be set to Capture Buffer. You can use the control menu in the Traffic Generator window to switch to the capture buffer if it is not currently the data source.

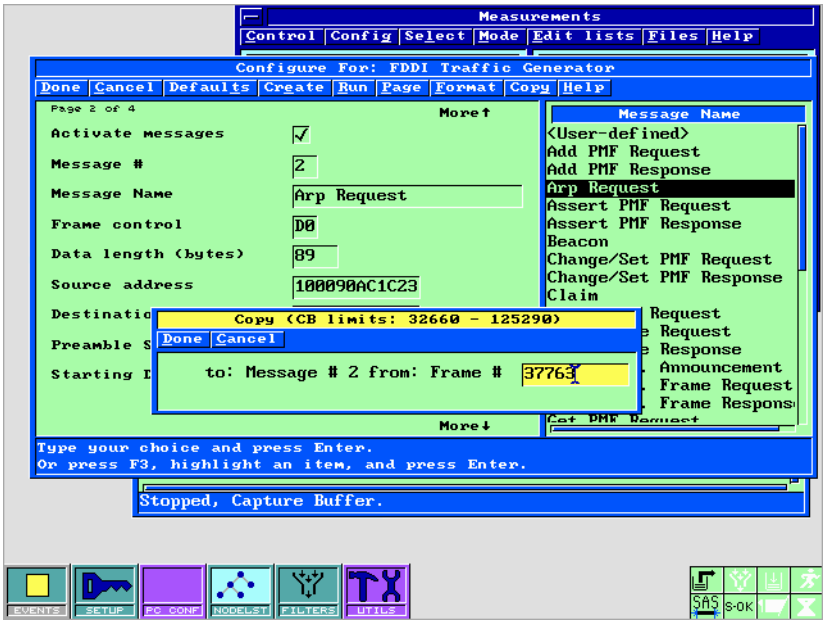


Figure 5-21: Copy message from Capture Buffer window

Using the FDDI Ring Manager Measurement

The FDDI Ring Manager gives you a complete view of the status, topology, and events on your FDDI ring. The main Ring Manager window is divided into three sections:

- Ring Status
- Logical or Physical Ring Map
- Status Bar

Each section is documented in online help topics in the Ring Manager window. See chapter 12 “FDDI Ring Manager” for more information.

Ring Status

In the Ring Status section, you see at a glance whether the ring is wrapped or twisted or functioning normally. You can see which station won the right to set the token rotation time and other token rotation statistics. You can see the network utilization as a percentage, as the number of frames per second, and as the number of kilobytes per second.

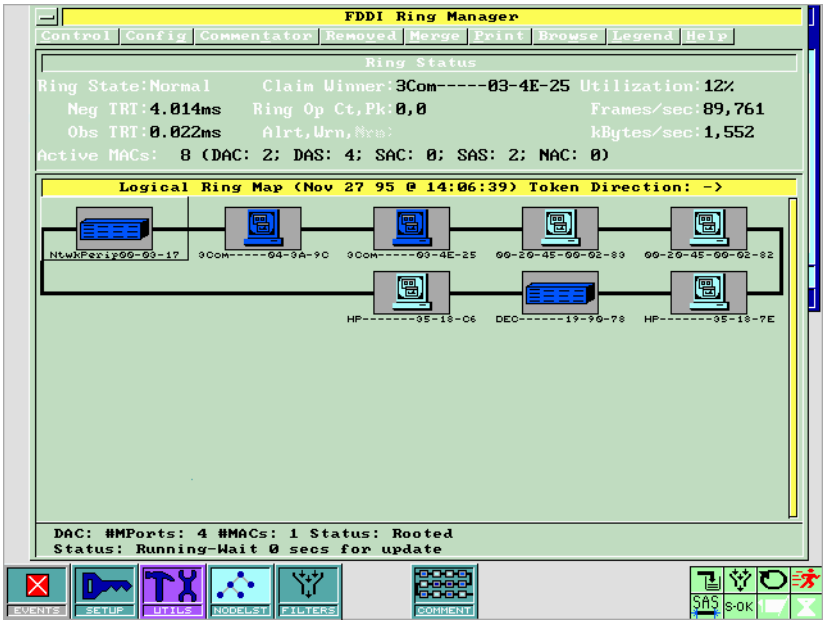


Figure 5-22: The FDDI Ring Manager window

Ring Map

The Ring Map shows the stations on your ring either in the order of the token path (Logical Ring Map) or the physical connection order (Physical Ring Map). You can switch between Logical and Physical views of the ring in the Configuration window.

Status Bar

The Status Bar gives a summary description of the highlighted station in the Ring Map and notifies you of the time to wait for an update when the Ring Manager is running.

M-port Connections and Station Information Windows

Highlight and select any node in the Ring Map. If the node is a concentrator, it opens to the M-port connections map for that concentrator. In the M-ports connections map, you see all the nodes which are connected to that concentrator. The "Concentrator" menu bar item opens a Station Information window for the concentrator.

If you highlight and select a station node, it opens a Station Information window. For each MAC in the station, this window lists connection information, timer values, port status, and link error information. The online help in the Station Information window gives details for each field.

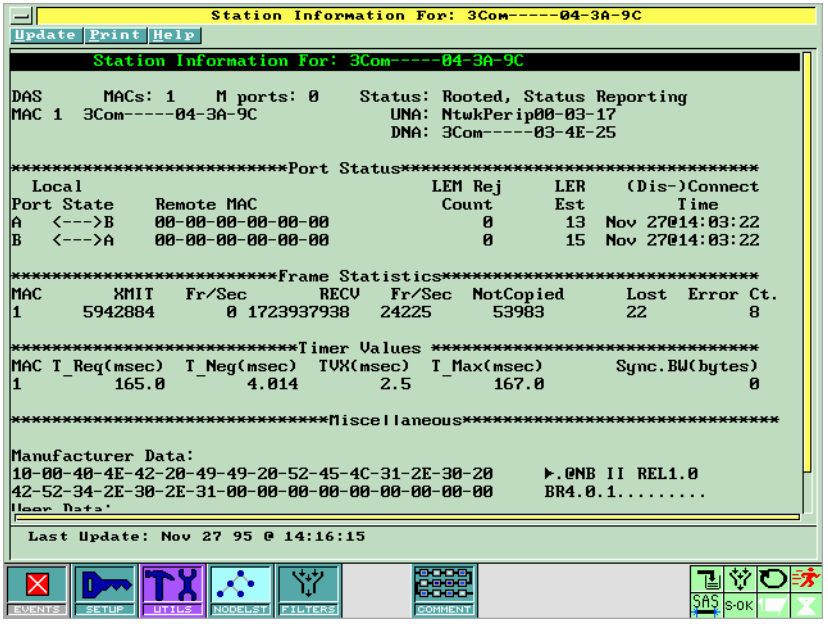


Figure 5-23: The Station Information window

The Ring Manager Commentator

The Ring Manager Commentator chronicles ring events such as stations inserting or leaving the ring, address anomalies, twisted or wrapped ring, and events that may cause a twisted or wrapped ring. The Ring Manager Commentator runs automatically when the Ring Manager is started.

The Commentator events are classified as Alert, Warning, or Normal. You can specify the level of events you want to see in the Ring Manager configuration window.

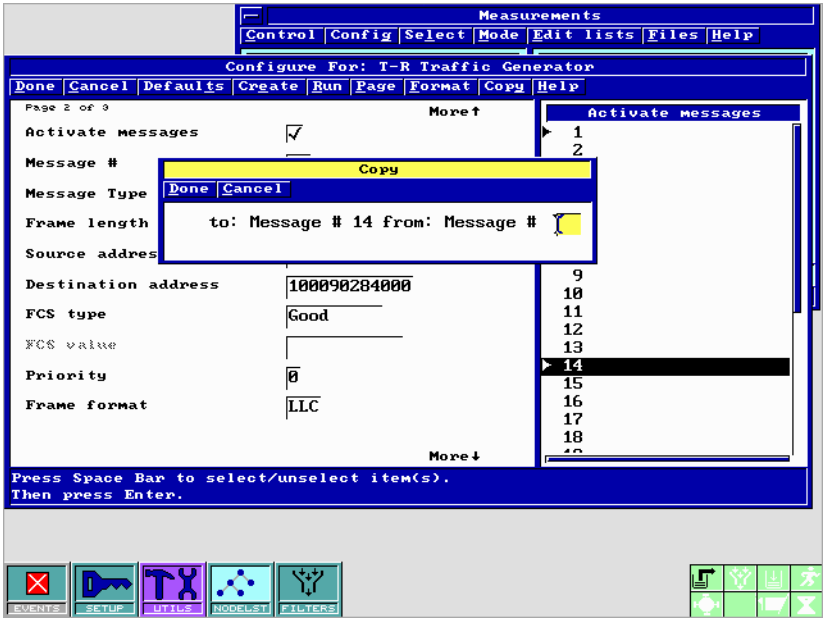


Figure 5-24: The Ring Manager Commentator window

Changing Event Levels

You can change the level of an event (from Alert to Warning, for example) by changing the file -

```
C:\ANALYZER\BUNDLES\FDDI\FDDINMPC.NLS
```

To change this file, you must exit the Internet Advisor LAN to the DOS environment. Use the DOS EDIT command or any other text editor to change the classification of events. For more information, see the topic "Changing the Level of Events" in the Commentator help window.

Opening the Commentator

The Ring Manager Commentator is started automatically when the Ring Manager is started. To view the Commentator window, either select the Comment icon, or use the Commentator menu bar item in the Ring Manager menu bar.

Use the online help in the Ring Manager Commentator window to see explanations for events reported in this window.

Building an FDDI Node List

As a shortcut to creating a node list for your FDDI ring, you can add any selected FDDI node in the Ring Map to the Internet Advisor LAN node list. Use the Merge command in the Ring Manager menu bar to open the Add window of the Node List. The FDDI address is already entered for you. Enter a node name and a node type to complete the Node List entry. The new node name is available the next time the Ring Manager is started.

Use the Format menu bar item of the Ring Manager Configuration window to display stations in hexadecimal format or by node names. The Address Format field in the Setup window determines whether hexadecimal addresses are in canonical or MSB format.

Starting the Ring Manager

1. In the Setup window, make sure the data source is Network Under Test. The first status icon in the lower right of the screen shows a data arrow filling up a buffer when the data source is Network Under Test.

2. Stop any other running measurements. If another measurement is running when you start the Ring Manager, a message informs you that the Ring Manager cannot run. This is because the Ring Manager includes an automatically activated SMT filter and a filter cannot be activated while another measurement is running.

3. In the Measurements window, select the FDDI Ring Manager.

   The Ring Manager Commentator starts automatically and then iconizes. The Ring Manager window opens and displays a map of your FDDI ring. The view of your ring depends on the Ring Manager configuration.

Configuring the Ring Manager

The Configure Measurement item in the Config menu of the Ring Manager window opens the configuration window. From the configuration window, you can change the following parameters to affect how the measurement runs.

- **Access Mode** - The Ring Manager gets information about your ring in either Passive or Active mode. Select either Active or Passive from the list pane.

NOTE The Ring Manager measurement must be stopped in order to change the Access Mode.

  - **Passive Mode:** the Internet Advisor LAN receives and analyzes Neighbor Information Frames (NIFs). The Ring Manager does not transmit any frames on the network.

- **Active Mode:** the Ring Manager transmits and receives Station Information Frames (SIFs). You can control the frequency of the SIF requests using the Update Interval field.

- **Ring View** - You can change the view of your ring to either Logical (token path) or Physical (trunk ring connections). Select either Logical or Physical from the list pane so that it is displayed in the Ring View field. When the Access Mode is Active, you can switch between Logical and Physical views of the ring without stopping the Ring Manager.

  - **Logical View -** The logical view of the ring shows every station on the token path in the order in which the token is passed. The Access Mode can be either Active or Passive for the logical view. When the Ring Manager is in Passive Mode, the Internet Advisor LAN does not transmit frames requesting station information. The available station information is limited to the information in NIFs.

  - **Physical View -** The physical view of the ring presents stations in the order of physical connections. The Access Mode must be Active for the physical view of the ring. The FDDI backbone ring is displayed on the first screen. The nodes on the backbone ring (also known as the trunk ring) are usually concentrators and servers. The stations connected to the concentrators' M ports are displayed by selecting the concentrator to expand it to its M Ports window. If the M Ports window contains other concentrators, they can also be expanded by selecting them.

- **Build Map From NIFs -** In Active Access Mode and Logical Ring View, you also have the option of selecting this field. When this field is enabled, the Ring Manager uses Neighbor Information Frames (NIFs) instead of Station Information Frames (SIFs) to build the Ring Map.

  This option is available because some manufacturers of FDDI nodes have not yet fully implemented SIF capabilities. SIF abnormalities can cause the ring discontinuity symbol (??) to appear on your map. Many of these discontinuities may be resolved if you enable this selection.

  The detailed station information that is available on SIFs is still displayed when possible if Build Map From NIFs is enabled.

When you choose to build the Ring Map from NIFs, the update interval is fixed at 45 seconds.

This field is grayed out in Passive Access Mode and in Active Access Mode for the Physical Ring View.

- **Update Interval** - This field controls the frequency of SIF requests sourced by the Ring Manager. This field can be edited when the Access mode is Active. When the access Mode is Passive, the update interval is set to 35 seconds and this field is grayed out.

- **Start Map From** - Select an entry from the list pane as the starting node for the ring map. The default is any rooted station. If the Address format in the Format menu is Hex, you can enter an address in this field.

- **Show the Following Events** - These fields control which events are reported in the Ring Manager Commentator. Select the box (so that the check mark is displayed) beside the events you want to see in the Commentator.

  To stop reporting on events at a particular level, select the check mark so that the box is blank.

6

Using The Expert Analyzer

What's in this Chapter

The Expert Analyzer measurements for Ethernet, Fast Ethernet, Token-Ring, and FDDI provide a top-level overview of a network's health. To do this, the Expert Analyzer automatically opens and runs specialized versions of other Internet Advisor LAN measurements:

Regular Measurement	Special Version Run by Expert Analyzer
Ethernet Vital Signs	Ethernet Expert Analyzer Vital Signs
Network Commentator/Eth.	Ethernet Expert Analyzer Commentator (also called Ethernet Network Commentator)
Node Discovery	Ethernet Expert Analyzer Node Discovery
Ethernet Protocol Stats	Ethernet Expert Analyzer Protocols

These measurements gather data from the network and present it to the Expert Analyzer measurement, which displays the data in graphical and numerical form.

When the Expert Analyzer measurement is running, a new sample is taken from the network every 10 seconds and the display is updated. (However, the Expert Analyzer Node/Station Discovery measurement can fall behind if there are a lot of new nodes.)

In addition to the data presented in the Expert Analyzer window, you can get more detailed information by "drilling down" from the Expert Analyzer window to additional windows where you can get more detailed information. When the cursor is over an item where you can drill down, it changes into a magnifying glass. To drill down you merely double-click the mouse, or you can use the items in the Display drop-down menu.

Moving the mouse cursor over the first line of a description or over the blank line between descriptions turns the mouse cursor into a question mark. Double-clicking here opens the help text fro that Alert or Warning.

NOTE

The specific measurements or help text which Expert Analyzer opens when you drill down are described in the online help topics under the heading "Drilling Down to Get More Detailed Information."

Network Health and Network Utilization Graphs

In the top half of the Ethernet and Fast Ethernet Expert Analyzer window are two graphs that show you information about the general health of the network and network utilization.

These graphs show the following:

- An overview of the Network Health is shown graphically in blue from the top of this area.
- An overview of the Network Utilization is shown graphically in green from the bottom of this area.

Alerts, Warnings, and bad frames are reported to the Expert Analyzer by the Expert Analyzer Vital Signs and the Expert Analyzer Commentator measurements. Alerts and Warnings are significant network events which may indicate problems that could lead to network performance degradation or network failure. Alerts are more serious than Warnings. The Network Health percentage is calculated for each sampling period using this formula:

100%-X(%per Alert)-Y(%per Warning)-Z(%bad Frames)

The default values used in this formula are X=10, Y=3, and Z=1. However, you can change these values in the Expert Analyzer Configuration window so that the Network Health % is calculated using values that are typical of the traffic conditions on your network. Network Health is defined to be zero if the formula produces a negative number.

If the Show Threshold checkbox is enabled in the Expert Analyzer Configuration window, then a horizontal dotted line appears in the graph area to indicate the Network Health threshold level (which is also set in the Expert Analyzer Configuration window). This lets you easily see when the threshold is exceeded.

The Network Utilization graph provides an overview of the total activity on the network in frames per second. This provides a context for interpreting the results of the other Expert Analyzer statistics.

Above the two graphs, these things are shown:

- The scale of the vertical axis of both the graphs is displayed (for example, 0 to 100%). The Network Health graph is always scaled at 0 to 100%.

  The Network Utilization graph is either autoscaled or scaled at 0 to 100%, depending on whether the Network Utilization Graph Autoscale item in the Expert Analyzer Configuration window is enabled (marked with a check). If this item is enabled, the graph is autoscaled according to the peak utilization rate so the Network Utilization graph does not overwrite the Network Health graph.

  If the Network Utilization Graph Autoscale item in the Expert Analyzer Configuration window is not enabled, the Network Utilization graph is scaled at 0 to 100%.

- The scale of the horizontal axis of both graphs is shown (30 minutes).

- The lowest and latest Network Health percentages and the highest and latest Network Utilization percentages are shown.

Statistics, Warnings, and Alerts

In the bottom half of the Expert Analyzer window various statistics are displayed:

- Depending on what is selected in the "First Column Shows" field of the Expert Analyzer Configuration window, the column next to the "Protocols" column, which is called the First Column, can show one of these items:
  - The number of bytes sent by each protocol (Bytes)
  - The number of frames sent by each protocol (Frames)
  - The percentage of available network bandwidth taken by each protocol (% Utiliz)
  - The number of bytes per second sent by each protocol (Bytes/sec)
  - The frames per second sent by each protocol (Frames/sec)

  You can change what is shown in this column in two ways:

  - First, you can use the Config menu bar item to open the Expert Analyzer Configuration window, where you can change what is selected in the First Column Shows field.
  - Or, you can double-click on the title of this column. When the mouse cursor is over the right half of the title, it becomes a right arrow. Double-clicking here cycles forward through the possible choices. Similarly, when the mouse cursor is over the left half of the title, it becomes a left arrow. Double-clicking here cycles backwards through the possible choices.
- In the Stations column, the number of stations running each protocol is shown, and the MAC Level number indicates the total number of MAC-level stations on the network.

- In the Warnings and Alerts columns, the number of Warning and Alert events generated for each protocol in the Expert Analyzer Commentator and Expert Analyzer Vital Signs measurements are shown. Alerts and Warnings are significant network events which may indicate problems that could lead to network performance degradation or network failure. Alerts are more serious than Warnings.

In all columns, the number shown for the Network Total equals the total of all other items in that column.

If a cell in any of these columns is blank, this means that none of that particular item has been seen since the Expert Analyzer measurement was started.

Drilling Down to Get More Detailed Information

You can easily get more detailed information from Expert Analyzer by double-clicking the mouse on various items in the Expert Analyzer window. When the mouse cursor is over an area from which you can "drill down," it turns into a magnifying glass.

NOTE

If you drill down to another screen, you can press F5 to close the drill-down screen and return to Expert Analyzer. You can also use the Close item, which is accessed by clicking on the Window Menu Button in the upper left corner of the drill-down screen.

Double-Clicking on this	causes this
Network Health/Network Utilization graph area	The Node Stats/Station Stats measurement is started. It shows statistical information for up to 20 of the most active nodes on the network.

Double-Clicking on this in the Protocols Column	causes this
Network Total in the Protocols column	The Expert Analyzer Protocols measurement is started. It shows Frames, Bytes, DLL (Data Link Layer) Errors, and Average Frame Length for all protocol stacks.
A non-grayed protocol in the Protocols column	The Expert Analyzer Protocols measurement is started. It is configured to show what is relevant for that particular protocol.
Other Protocols in the Protocols column (if it isn't grey)	The Ethernet Expert Analyzer Protocols measurement is started. It is configured to show MAC statistics for DDL Types or SAPs (Service Access Points).

In the following table, "First Column" refers to the column immediately to the right of the "Protocols" column. What is shown in the First Column depends on how the First Column Shows field in the Expert Analyzer Configuration window is configured

Double-Clicking on this in the First Column	causes this
The Network Total number in the First Column	The Expert Analyzer Vital Signs measurement is started.
The Other Protocols number (if there is one) in the First Column	The Expert Analyzer Vital Signs measurement is started.
The MAC Level number (if there is one)	The Expert Analyzer Vital Signs measurement is started.
Any other non-blank number in the First Column	The Vital Signs measurement for that protocol is started.

Double-Clicking on this in the Stations Column	causes this
The Network Total number in the Stations column	The Expert Analyzer Node/Station Discovery measurement is started. It is configured to show all observed nodes.
The Other Protocols number (if there is one) in the Stations Node Discovery column	The Expert Analyzer Node/Station Discovery measurement is started. It is configured to show all observed nodes/stations which have sent traffic that does not contain a network address or that contains a network address that the Expert Analyzer does not recognize.
The MAC Level number (if there is one)	The Expert Analyzer Node/Station Discovery measurement is started.
The Routers number (if there is one) in the Stations column	The Expert Analyzer opens a list which describes all the routers that have been discovered
Any other non-zero number in the Stations column	The Expert Analyzer Node/Station Discovery measurement is started. It is configured to show all observed nodes that have sent traffic using a network address for the selected protocol.

Double-Clicking on this in the Warnings Column	causes this
The Network Total number (if there is one) in the Warnings column	The Network Total Event Summary window is opened. This is a list that shows the types of Warnings and the number of each type of Warning that has been received from the Expert Analyzer Commentator measurement or the Expert Analyzer Vital Signs measurement. From the Network Total Warning Event Summary window you can drill down one level to get more detailed information on a particular Warning type, or you can drill down two levels to get either a decode measurement or help text that describes why a Warning was generated and what to do to resolve the problem. See the online help topic "Drilling Down to Get More Information on Warnings" for more information (for example, the meaning of "!" in the leftmost column, and when to single-click or double-click to drill down)
The MAC Level number (if there is one) in the Warnings column	The MAC Level Warning Event Summary window is opened. This summary list works the same as the Network Total Warning Event Summary described above.
Any other non-zero number in the Warnings column	A Warning Event Summary window for the selected protocol or for routers is opened. This summary list works the same as the Network Total Warning Event Summary described above.

Double-Clicking on this in the Alerts Column	causes this
The Network Total number (if there is one) in the Alerts column	The Network Total Alert Event Summary window is opened. This is a list that shows the types of Alerts and the number of each type of Alert that has been received from the Expert Analyzer Commentator measurement or the Ethernet Expert Analyzer Vital Signs measurement. From the Network Total Alert Event Summary window you can drill down one level to get more detailed information on a particular Alert type, or you can drill down two levels to get either a decode measurement or help text that describes why an Alert was generated and what to do to resolve the problem. See the help topic "Drilling Down to Get More Information on Alerts" for more information (for example, the meaning of "!" in the leftmost column, and when to single-click or double-click to drill down).
The MAC Level number (if there is one) in the Alerts column	The MAC Level Alert Event Summary window is opened. This summary list works the same as the Network Total Alert Event Summary described above.
Any other non-zero number in the Alerts column	An Alert Event Summary window for the selected protocol or for routers is opened. This summary list works the same as the Network Total Alert Event Summary described above.

For Example. . . If you run Expert Analyzer and the number "3" is shown in the Warnings column for the Network Total row, then selecting the Warnings/Network Total item in the Display menu would open the Network Total Warning Event Summary window, just as double-clicking on the "3" with the mouse would. Then, from the Network Total Warning Event Summary window, you could use the keyboard to drill down to more detailed information on each type of Warning by using the ARROW keys to highlight the Warning type of interest and then pressing ENTER.

. . . . . .

Expert Analyzer Menu Bar

The menu bar in the Expert Analyzer window contains the following selections:

- Control
- Config
- Display
- Files
- Print
- Help

Control Menu

The Control menu has these items:

- Run Measurement/Stop Measurement
- Pause Display
- Switch to Capture Buffer
- Run Measurement From Capture Buffer
- Run Measurement From Network
- Run Open Measurements From Network

Run Measurement/Stop Measurement

The first item in the Control menu toggles between Run Measurement and Stop Measurement. Selecting Run Measurement starts the Expert Analyzer measurement. Selecting Stop Measurement stops the Expert Analyzer measurement.

Pause Display

The second item in the Control menu is always disabled (grayed-out).

Switch to Capture Buffer

If the data source in the Setup window is NOT already Capture Buffer, this item lets you change to Capture Buffer without going into the Setup window. This is a much faster and easier way to change the data source.

After you select this item, any currently running measurements are stopped and the data source is changed to Capture Buffer. Once the data source is Capture Buffer, you are in a post-processing mode so you can analyze the data in the Capture Buffer.

This item is disabled (grayed-out) if the data source is already Capture Buffer.

Run Measurement From Capture Buffer

When there are frames in the Capture Buffer, you can use them as the source of information for this and other measurements. This lets you re-examine a network situation or replay frames which you may have captured at a time when you were not observing the Advisor.

The data source must be Capture Buffer before you can choose Run Measurement From Capture Buffer. Then you can use the Run Measurement From Capture Buffer/All Frames item to run the Expert Analyzer using the frames in the Capture Buffer.

The Frame(s) and Next items in the Run Measurement From Capture Buffer menu are disabled.

Run Measurement From Network

If the data source in the Setup window is not already Network Under Test, this item lets you change to Network Under Test without going into the Setup window. This is a much faster and easier way to change the data source.

After you select this item, the data source is changed and the Expert Analyzer measurement is started.

This item is disabled (grayed-out) if the data source is already Network Under Test.

Run Open Measurements From Network

This item works like the Run Measurement From Network item except that in addition to making the data source Network Under Test and starting the Expert Analyzer measurement, it also starts any other open measurements.

This item is never disabled, even if the data source is already Network Under Test, because there may be other open, but stopped measurements. Using this item is a fast way to run all open measurements regardless of the current data source setting.

Configuring the Expert Analyzer

When you select item in the Config menu, a Configuration window for the Expert Analyzer measurement is opened where you can set parameters for the Expert Analyzer.

For Example. . . You can control such things as what is shown in the first column of the Expert Analyzer and how many Warnings and Alerts are saved by the Expert Analyzer. In this window you can also configure parameters for many of the other measurements that Expert Analyzer runs, such as Ethernet and Fast Ethernet Expert Analyzer Commentator and Ethernet and Fast Ethernet Expert Analyzer Vital Signs.

Displaying the Drill-Down Actions using the Keyboard

The Display menu and its submenus contain items that let you perform with the keyboard the same "drill-down" actions you can perform by clicking on parts of the Expert Analyzer window with a mouse.

For Example. . . For example, if you run Expert Analyzer and the number "3" is shown in the Warnings column for the Network Total row, then selecting the Warnings/ Network Total item in the Display menu would open the Network Total Warning Event Summary window, just as double-clicking on the "3" with the mouse would.

Then, from the Network Total Warning Event Summary window, you could use the keyboard to drill down to more detailed information on each type of Warning by using the ARROW keys to highlight the Warning type of interest and then pressing ENTER.

Expert Analyzer Files

The Files menu contains these items:

- Write Data from Previous Run to ASCII File ...
- Log Data to ASCII File During Next Run...

These items let you log Expert Analyzer information to a file. The data is logged in a CSV (Comma Separated Variable) format. The CSV file can then be read into a spreadsheet program such as Microsoft Excel, or it can be examined with a text editor.

When you use either of these items, the File Manager window opens to let you select the path and file name you want to use. The File Manager window defaults to showing only files with a .CSV extension. Use the Extension menu if you want to change this default.

Both of these items are disabled (grayed-out) if the measurement is currently running.

Write Data From Previous Run to ASCII File

This item lets you save Expert Analyzer data, which has already been collected, to a file.

Log Data to ASCII File During Next Run

This item writes data to a file as the Expert Analyzer measurement is running, so choose this option before you start the Expert Analyzer measurement. The data is logged to disk each time the display is updated.

If power goes off while logging is on, all samples written before the power outage are saved in the log file. Data logging is turned off automatically when the measurement is stopped.

NOTE Logging data as it is being gathered can cause other interactions with the Advisor to slow down since the computer CPU time must be shared.

Printing Expert Analyzer Files

The Print menu contains these items:

- Print Brief Report
- Print Report with Alerts
- Print Report with Alerts and Warnings

These items let you print the results displayed in the Expert Analyzer window. The output goes to either a printer or to a file, depending on the settings in the PC Hardware Configuration window (accessed from the Utilities window).

If the PC Hardware Configuration window is set up to print to a file, when you use any of these Print items, the File Manager window opens so you can specify the path and file name. The File Manager window defaults to showing only files with a .CSV extension. Use the Extension menu if you want to change this default.

If you print to a file, you can then examine the file with a text editor. For example, you can exit the Advisor (by selecting "Exit to DOS" in the Utilities window). If you are using the Windows 95 start, use the DOS Prompt icon. If you are using the alternate DOS menu boot, then you can select the DOS prompt item. After you get to DOS, then use a MS-DOS editor to open the file.

You can use the Print items while the Expert Analyzer is running, so they are never disabled (grayed-out).

Print Brief Report

This item prints the results shown in the bottom half of the Expert Analyzer window.

Print Report with Alerts

This item prints the results shown in the bottom half of the Expert Analyzer window, and it also prints descriptions of any Alerts that were reported.

Print Report with Alerts and Warnings

This item prints the results shown in the bottom half of the Expert Analyzer window, and it also prints descriptions of any Alerts and Warnings that were reported.

Expert Analyzer Online Help

Use the Online Help menu items to access help topics.

Tips for Using the Expert Analyzer

There may be times when you run Expert Analyzer and you get a very large number of many kinds of Warnings and/or Alerts. This tells you that there is a potentially serious problem on the network.

In such situations, you may want to exercise some control over when events are reported to the Expert Analyzer so that you can focus on other aspects of the problem. There are three things you can do:

- You can turn off the reporting of particular Warning and/or Alert events.
- You can change the threshold for a particular event so that it is not reported as often.
- You can turn off an entire category of events (for example, all TCP/IP events).

Turning Off a Particular Event

To turn off a particular kind of event, do the following:

1. Open the Expert Analyzer Configuration window by using the Config menu.
2. Highlight the checkbox that controls the category in which the particular event you want to turn off resides. For example, if you want to turn off the IP Low Time-To-Live event, highlight the TCP/IP checkbox.
3. In the list pane on the right, click on the particular event you want to turn off. When an event is disabled (turned off), there is no arrow in front of it in the list pane. Or, to use the keyboard to disable the event, press F3, use the ARROW keys to highlight the event, press the SPACE BAR, and then press F3 again.

Changing the Threshold for a Particular Event

To change the threshold for a particular event, do the following:

1. Open the Expert Analyzer Configuration window by using the Config menu.

2. Highlight the threshold field for the particular event you are interested in.

For example, the value in the IP Low TTL Value field (under the TCP/IP Events category) controls when an IP Low Time-To-Live Warning is generated. This Warning is generated if a frame is detected which has a TTL less than the value specified in the Configuration window's IP low TTL Value field.

3. Enter an appropriate number in the threshold field.

Turning Off an Entire Category of Events

To turn off an entire category of events, do the following:

1. Open the Expert Analyzer Configuration window by using the Config menu.

2. Highlight the checkbox that controls the category of events you want to turn off. For example, if you want to turn off the reporting of all TCP, IP, RIP, IGRP, and OSPF events, highlight the TCP/IP Events checkbox.

3. Click on the checkbox so that no checkmark is displayed in it. Or, to use the keyboard to disable the category, press ENTER until no checkmark is displayed.

Sizing the Expert Analyzer Window

You can size the Expert Analyzer measurement by clicking on the Size item in the Window Menu. Or, using the keyboard, you can press F4 and then S (for Size), and then use the ARROW keys to change the size. Press ENTER to redraw the window to its new size.

NOTE If you size the window too small, numbers may not be shown in the cells in the bottom half of the window if there is not enough room for them to be displayed. If you make the window larger, the numbers will then be displayed again.

Drilling Down to Get More Information on Warnings

In the Expert Analyzer window, if you double-click on a number in a cell of the Warnings column (or if you use the Warnings item in the Display menu), a Warning Event Summary window opens.

The Warning Event Summary window lists the types of Warnings and the number of each type of Warning that the Expert Analyzer has received from the Ethernet or Fast Ethernet Expert Analyzer Commentator measurement or the Ethernet or Fast Ethernet Expert Analyzer Vital Signs measurement.

NOTE The Retain Description For Warnings field in the Expert Analyzer Configuration window determines the total number of Warnings that the Expert Analyzer saves before it overwrites the earliest saved Warnings. If the Expert Analyzer receives more than this number of Warnings, the Warning Event Summary window will not have descriptions for the Warnings which were overwritten.

In the Warning Event Summary window, the Count column shows the total number of each type of Warning, and the Prot column shows the protocol for each type of Warning. The Description column shows the name of each type of Warning.

In addition, any event type which caused the Network Health graph to go beneath the threshold (which is set in the Expert Analyzer Configuration window), is marked by an exclamation point (!) in the first column. This lets you identify which type of event(s) caused the graph to cross the threshold.

If you click once on a highlighted Warning type or twice on a non-highlighted Warning type, a Warning Event Detail window opens which shows the details of that type of Warning.

NOTE

When you double-click on a non-highlighted Warning type, the first click highlights (selects) the Warning type and the second click drills down. Therefore, you only need to click once, not twice, to drill down from a Warning type that is already highlighted (for example, the first Warning type in the list).

The details shown in the Warning Event Detail window include the source address for the node that sent the frame which caused the Warning, along with other relevant information. In addition, any individual event which caused the Network Health graph to go beneath the threshold is marked by an exclamation point (!) in the first column. This lets you identify which individual event(s) caused the graph to cross the threshold.

In the Warning Event Detail window, moving the mouse cursor over the first line of the Warning description, or over the blank line between Warning descriptions, turns the mouse cursor into a question mark. Double-clicking here (or single-clicking if the area is already highlighted) opens the help text for that Warning. The help text describes when the Warning is generated (that is, what caused the Warning), and it offers advice on how to resolve the problem.

When the mouse cursor is over any other part of the Warning description, it turns into a magnifying glass. Double-clicking here (or single-clicking if the area is already highlighted) causes one of the following things to occur:

- If you are running the Expert Analyzer from the Capture Buffer, and the frame which caused the Warning is in the Buffer, the appropriate decode measurement is opened displaying that frame so you can see the contents of the frame.
- If you are running the Expert Analyzer from the Capture Buffer, but the frame which caused the Warning is NOT in the Buffer, a message is displayed.
- If you are running the Expert Analyzer from the network, the appropriate decode measurement is opened and it is started so that you can capture traffic from the network.

Drilling Down to Get More Information on Alerts

In the Expert Analyzer window, if you double-click on a number in a cell of the Alerts column (or if you use the Alerts item in the Display menu), a Alert Event Summary window opens.

The Alert Event Summary window lists the types of Alerts and the number of each type of Alert that the Expert Analyzer has received from the Ethernet or Fast Ethernet Expert Analyzer Commentator measurement or the Ethernet or Fast Ethernet Expert Analyzer Vital Signs measurement.

NOTE

The Retain Description For Alerts field in the Expert Analyzer Configuration window determines the total number of Alerts that the Expert Analyzer saves before it overwrites the earliest saved Alerts. If the Expert Analyzer receives more than this number of Alerts, the Alert Event Summary window will not have descriptions for the Alerts which were overwritten.

In the Alert Event Summary window, the Count column shows the total number of each type of Alert, and the Prot column shows the protocol for each type of Alert. The Description column shows the name of each type of Alert.

In addition, any event type which caused the Network Health graph to go beneath the threshold (which is set in the Expert Analyzer Configuration window), is marked by an exclamation point (!) in the first column. This lets you identify which type of event(s) caused the graph to cross the threshold.

If you click once on a highlighted Alert type or twice on a non-highlighted Alert type, an Alert Event Detail window opens which shows the details of that type of Alert.

NOTE

When you double-click on a non-highlighted Alert type, the first click highlights (selects) the Alert type and the second click drills down. Therefore, you only need to click once, not twice, to drill down from an Alert type that is already highlighted (for example, the first Alert type in the list).

The details shown in the Alert Event Detail window include the source address for the node that sent the frame which caused the Alert, along with other relevant information. In addition, any individual event which caused the Network Health graph to go beneath the threshold is marked by an exclamation point (!) in the first column. This lets you identify which individual event(s) caused the graph to cross the threshold.

In the Alert Event Detail window, moving the mouse cursor over the first line of the Alert description, or over the blank line between Alert descriptions, turns the mouse cursor into a question mark. Double-clicking here (or single-clicking if the area is already highlighted) opens the help text for that Alert. The help text describes when the Alert is generated (that is, what caused the Alert), and it offers advice on how to resolve the problem.

When the mouse cursor is over any other part of the Alert description, it turns into a magnifying glass. Double-clicking here (or single-clicking if the area is already highlighted) causes one of the following things to occur:

- If you are running the Expert Analyzer from the Capture Buffer, and the frame which caused the Alert is in the Buffer, the appropriate decode measurement is opened displaying that frame so you can see the contents of the frame.
- If you are running the Expert Analyzer from the Capture Buffer, but the frame which caused the Alert is NOT in the Buffer, a message is displayed.
- If you are running the Expert Analyzer from the network, the appropriate decode measurement is opened and it is started so that you can capture traffic from the network.

List of Possible Warning and Alert Events

Following is a list, categorized by protocol, of all the possible Warnings and Alerts the Expert Analyzer can receive from the Commentator and the Vital Signs measurements.

If you would like to read the online help text for events that are not reported to the Expert Analyzer, you can do this by opening the Expert Analyzer Commentator measurement and using the topics item in its Help menu to access the list of Commentator help topics. Then select the help topic for the protocol category that contains the event you are interested in.

For Example. . . For example, if you are interested in the ICMP Source Quench event, select the ICMP Miscellaneous Events topic. From the help window that then opens, you can use the Related menu to open the help for the Source Quench event.

Events Reported from the Expert Analyzer Commentator

The following events can be reported for the Ethernet, Fast Ethernet, Token-Ring, and FDDI Expert Analyzer measurements. Specific events for the different versions of the Expert Analyzer are listed later in this chapter.

NOTE

"A" denotes an Alert, "W" denotes a Warning, and “N” denotes a Normal event.

* denotes that there is more than one event in this category, but at least one of the events is a Warning or Alert.

ICMP Miscellaneous Warning and Alert Events:

W ICMP Source Quench
W ICMP Time To Live Expired
A ICMP Fragment Lost
A ICMP Parameter Problem
A ICMP Option Missing

ICMP Destination Unreachable Warning and Alert Events:

W ICMP Unreachable Port
A ICMP Admin Prohib Host
A ICMP Admin Prohib Network
A ICMP Fragmentation Needed

A ICMP Isolated Source Host
A ICMP Source Route Failed
A ICMP Unknown Host
A ICMP Unknown Network
A ICMP Unreachable Host
A ICMP Unreachable Host and TOS
A ICMP Unreachable Network
A ICMP Unreachable Network and TOS
A ICMP Unreachable Protocol Service

ICMP Redirect Warning Events:

W ICMP Host and TOS Redirect
W ICMP Host Redirect
W ICMP Network and TOS Redirect
W ICMP Network Redirect

Novell Warning and Alert Events:

W Novell: Delay- Dup Service Req
* Novell: Open File Events
* Novell: Create File Events
W Novell: Slow File Transfer
* Novell: General Service Events
A Novell: Down File Server
* Novell: Nearest Service Events

Novell Burst Mode Warning and Alert Events:

W Novell: Burst Mode Read File Error
W Novell: Burst Mode Write File Error
W Novell: Burst Mode Slow File Transfer

IP Warning and Alert Events:

W IP: Low Time-To-Live
A IP: Zero Time-To-Live
A IP: Broadcast Storm
A IP: Duplicate Address

TCP/IP Warning and Alert Events:

W TCP: Reset Connection
W TCP: Excessive Retransmission
W TCP: Low Window

OSI Warning and Alert Events:

W OSI CLNP Low Lifetime
A OSI CLNP Zero Lifetime
W OSI CLNP Error PDU
W OSI TP Connection Rejected
W OSI TP Connection Aborted
W OSI TP Excessive Retransmission
A OSI TP Low Credit
W OSI TP Slow Transfer Rate
W OSI TP Error PDU

AppleTalk Warning and Alert Events:

A DDP Destination Unreachable
W DDP Hop Count Exceeded
W ATP Excessive Retransmission
W ASP Session Reject
W ASP Slow Transfer Rate
W ADSP Connection Denied
W ADSP Slow Transfer Rate

W ADSP Excessive Retransmission
W ADSP Low Window
W PAP Printer Busy

Banyan Vines Warning and Alert Events:

W VIP Low Hop Count
A VIP Broadcast Storm
A VIP Duplicate Address
W VSPP Low Window
W VSPP Excessive Retransmission
W VIPC Excessive Retransmission

DECnet Routing Protocol (DRP) Warning and Alert Events:

W DRP Return to Sender Packet
W DRP High Visit Count
W DRP Duplicate Network Address
W DRP Incorrect Hello Timer

DECnet Network Service Protocol (NSP) Warning and Alert Events:

W NSP Connection Rejected
W NSP Connection Aborted
W NSP Excessive Retransmitted Connect Initiates
W NSP Excessive Retransmissions
A NSP Flow Control Stop Data Message

DECnet Local Area Transport Protocol (LAT) Warning and Alert Events:

W LAT Virtual Connection Reject
W LAT Service Connection Reject
W LAT Excessive Retransmissions

DECnet Data Access Protocol (DAP) Warning and Alert Events:

W DAP File Open Error
W DAP File Close Error
W DAP Slow File Transfer

DECnet Phase V (DECV) Warning and Alert Events:

W DECV CLNP Low Lifetime
A DECV CLNP Zero Lifetime
W DECV CLNP Error PDU
W DECV TP Connection Rejected
W DECV TP Connection Aborted
A DECV TP Low Credit
W DECV TP Excessive Retransmission
W DECV TP Error PDU
W DECV TP Slow Transfer Rate

Router Warning and Alert Events:

W RIP: Router Change
W IGRP: Router Change
W OSPF: Designated Router Change
W OSPF: Neighbor Change
W OSPF: Incorrect Hello Time
W OSPF: Router Change
W OSI ES-IS Redirect
W OSI ES-IS Low Holding Time

W OSI ES-IS High Holding Time
W OSI IS-IS Low Holding Time
W OSI IS-IS High Holding Time
W RTMP Router Change
W VRTP Router Change
A VICP Exception Notification
W DRP Level 1 Router Change Message
W DRP Level 2 Router Change Message
A ZIP Zone Diameter Exceeded

Oracle Warning and Alert Events:

W TNS Connect Refused
W TNS Marker
N TNS Connect Redirect
W TNS Slow Server Response
W TNS Short Dead Conn Detect Time
A TNS Excessive Denied Logons
W TNS Dedicated Server Request

Ethernet and Fast Ethernet Specific Expert Analyzer Events

Ethernet and Fast Ethernet MAC Level Warning and Alert Events:

W Bad FCS
W Broadcast Frames
W Dribble Frames
W Frames (Network)
W Frames (Buffer)
W Jabbers
A Jabbers w/bad FCS
A Late Collisions
W Local Collisions

W Misaligns
W Missed Frames
W Multicast Frames
W Remote Collisions
A Remote Late Collisions
W Runts
W Runts (w/good FCS)
W Utilization % (Network)
W Utilization % (Buffer)

Token-Ring Specific Expert Analyzer Events

LAN Manager Warning and Alert Events:

A L-M: Beaconing
A L-M: Beaconing Recovered
W L-M: Bridge Performance Exceeded
W L-M: Error Rate Decaying
W L-M: Non-Isolating Exceeded
W L-M: Pre-Weight Exceeded
A L-M: Receiver Congested
A L-M: Receiver Congested Ended
W L-M: Weight Exceeded

Token-Ring Warning and Alert Events

W T-R: Active Monitor Error
A T-R: Beacon
A T-R: Beaconing
A T-R: Catastrophic Error
W T-R: Failed Insertion
W T-R: Failed Neighbor Notification
W T-R: Monitor Contention

W T-R: Ring Purging
W T-R: Ring Resetting
W T-R: Soft Error
A T-R: Streaming Beacons

Token-Ring MAC Level Warning and Alert Events:

W Aborts (Network)
W Aborts (Buffer)
A Beacons
W Burst Errors
W Claim Tokens
W Code Violations(Network)
W Code Violations(Buffer)
W Frames (Network)
W Frames (Buffer)
W Line Errors
W Missed Frames
W Receiver Congestion
A Ring Purges
W Soft Errors
W Utilization (Network)
W Utilization (Buffer)
W Bad FCS
W Tokens

FDDI Specific Expert Analyzer Events

LAN Manager Warning and Alert Events:

A L-M: Beaconing
A L-M: Beaconing Recovered
W L-M: Bridge Performance Exceeded

W L-M: Error Rate Decaying
W L-M: Non-Isolating Exceeded
W L-M: Pre-Weight Exceeded
A L-M: Receiver Congested
A L-M: Receiver Congested Ended
W L-M: Weight Exceeded

FDDI MAC Level Warning and Alert Events:

NOTE The following events can be warnings or alerts.

Utilization %
Frames
Tokens
LLC Frames
Claims
Beacons
Stripped Frames
Void Frames
Other Frames
Bad FCS
Violations
E Bit Set
PDU Too long
Token Rotation Time

7

Using the Event Log

What's in this Chapter

This chapter describes the Event Log. The Event Log is a file on the Internet Advisor's hard disk that provides high visibility of "events" occurring on the network and in the Internet Advisor LAN. Events are occurrences that are especially significant or noteworthy.

Events are saved to the file in a linear manner. Events are logged to the file until the file is full. Then as a new event is logged, the oldest event is removed and its space is reused for the newest event.

The Event Log window and its subwindows let you view events. There are six categories of events:

- **Protocol events** - Examples of protocol events include a connection was established or a protocol violation occurred.
- **Threshold events** - An example of a threshold event is that the number of collisions exceeded a threshold.
- **Topology events** - Examples of topology events include a ring insertion occurred or a node was unreachable.
- **Fault events** - Examples of fault events include a broadcast storm occurred or there is a bad cable.
- **Instrument events** - Examples of instrument events include measurements started or stopped and a log of system problems.
- **All events** - This category includes all of the other categories.

In the Event Log window, there is a box called an indicator light for each category. The indicator lights change color to indicate the occurrence and severity of events in a given category. The indicators always show the most severe level that has occurred in each category. There are three levels of severity:

- **No events or normal events** - These events are indicated by green on a color display and dark gray on a monochrome display.
- **Warning events** - These events are indicated by yellow on a color display and light gray on a monochrome display.

- **Alert events** - These events are indicated by red with a white X on a color display and black with a white X on a monochrome display.

To view (browse) all the events in a given category, you can go to a dedicated subwindows for that category.

The Event Log can be turned on (activated) or off (deactivated). While it is on, all events are stored. While it is off, only instrument events are stored. You can also clear the Event Log.

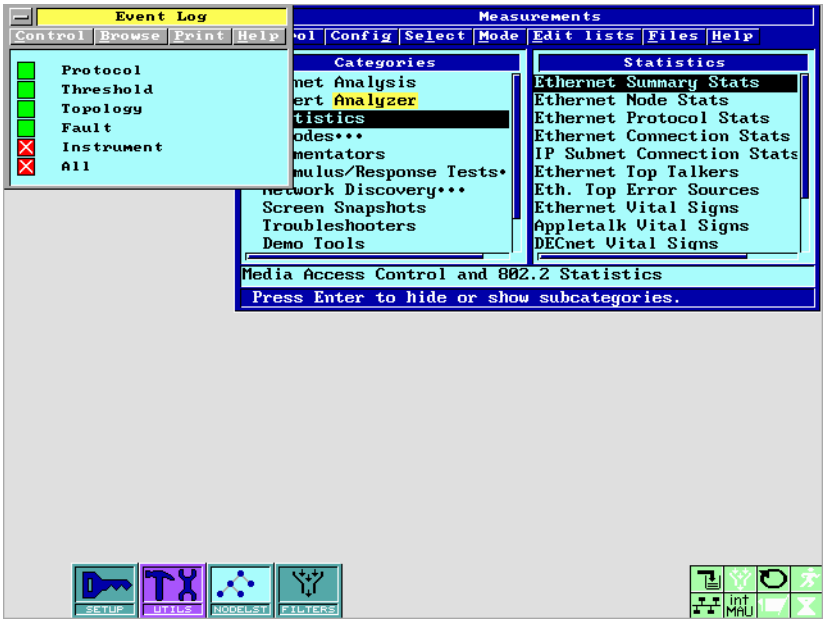


Figure 7-1: Event Log window

Activating, Deactivating, and Clearing the Event Log

The Event Log can be turned on (activated) or turned off (deactivated). The default mode for the Event Log is on. While it is on, all events are stored. While it is off, only instrument events are stored.

You may want to turn the event log off if you want to reduce the number of events written to the Event Log. You can also clear the Event Log.

- To activate the Event Log, select Activate Event Log in the Control menu of the Event Log window. This turns the Event Log on.
- To deactivate the Event Log, select Deactivate Event Log in the Control menu of the Event Log window. This turns the Event Log off.
- To clear the Event Log, select Clear Event Log in the Control menu of the Event Log window. This clears all the events from the Event Log file.

Browsing Events

To browse (view) all the events in a given category, you can go to a dedicated window for that category.

1. In the Event Log window, click on the indicator light for the particular type of events you want to browse (Protocol, Threshold, Topology, Fault, Instrument, or All). This opens the browser window for that category of events.

   OR

   Select the appropriate item in the Browse menu.

In the browser window, a description is displayed for each event along with the date and time each event occurred. The severity of each event is indicated by A (alert), W (warning), or N (normal).

Using the Acknowledge menu, you can acknowledge all events or events of a certain severity. Acknowledging events clears them from the browser window. It also affects the color of the indicator light for that category of events in the Event Log window. The online help for the browser windows describes how to acknowledge events.

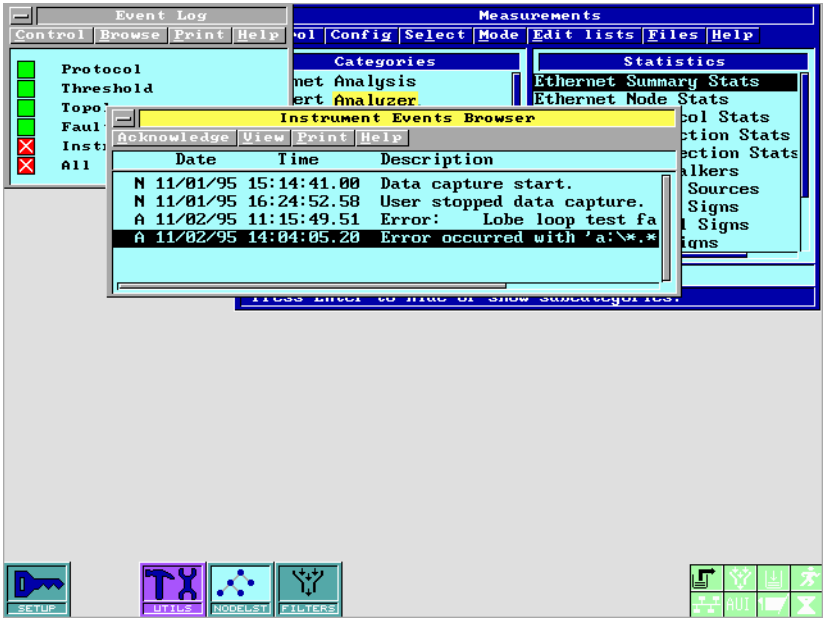


Figure 7-2: Events Browser window

Printing Events

The Print menu bar item lets you print information in the Event Log. You can select the format for the data to be printed, and you can choose what type of events you want to print.

Selecting the Text Format

You can print out Event Log data in either ASCII or CSV (Comma Separated Variable) format. Only one of the two formatting types can be selected, and the active item is indicated by a checkmark.

Using the Text formatting option will produce a printout in ASCII.

Using the CSV formatting option will print the file in comma-separated variable format which is acceptable to most spreadsheet programs.

Printing Different Types of Events

Using the three include items, you can control whether all the Alert, Warning, and Normal events in the Event Log file are printed. You can select any combination of the three to be printed; the active items are indicated by a checkmark next to the item.

For Example. . . All categories of events of the selected items are printed. For example, if you select Alert Events, all protocol, threshold, topology, fault, and instrument Alert events are printed. To print only a specific category of Alert events, open the Browser window for that category and use its Print menu. For instance, to print only protocol Alert events, open the Protocol Events Browser window by selecting Browse Protocol Events in the Browse menu, and then use the Print menu in the Protocol Events Browser window.

When you select the Print item, the event types you selected are printed in the format you selected. The output goes to either a printer or to a file depending on the settings in the PC Hardware Configuration window (accessed from the Utilities window).

8

Using the Capture Filters window

What’s in this Chapter

This chapter describes how to create, customize, and activate filters in the Filters window.

The purpose of filters is to control which frames the Internet Advisor LAN captures or excludes when you are testing a network. Filters can also be used to stop the Internet Advisor LAN when a specified frame is encountered on the network.

The Internet Advisor LAN comes with basic Ethernet, FDDI, and Token-Ring filters. It also contains basic filters for many protocols such as IP, VIP, IPX, DDP, DRP, and TCP.

To create a new filter, you can modify one of the provided filters and save the changes to a new filter name.

To enable a filter, you activate it using the Control menu in the Capture Filters window.

You can tell when a filter has been activated by looking at the status icons in the lower right corner of the display. When the data source is Network Under Test and a filter is activated, the top-row, second-from-left status icon (in the lower right corner of the screen) is a black funnel. If no filter is active, the funnel is white.

Creating a Filter

The following procedure can be used for creating Token-Ring, FDDI, or Ethernet filters.

1. Open the Capture Filters window either by double selecting the Filters window icon or by pressing **F12**.

2. In the list pane, highlight a filter you want to use as a template.

   A filter must be deactivated before it can be modified. Use the Control menu if you need to deactivate a filter. If this is the first user defined filter, you can use the Basic filter. The status line area at the bottom of the window briefly explains what the filter does.

3. Select the Filter item in the Modify menu. A new Capture Filter window opens to let you modify the highlighted filter.

4. If you want to capture or exclude traffic coming from or going to a particular address, enter the hex address in the Station 1 Address field, or select a node/station name from the list pane.

   If you do not want to specify an address condition, leave the field as "don't care" (all Xs).

5. If you want to specify a second address condition, repeat the previous step for the Station 2 Address field.

6. In the Traffic Mode field, select the direction of traffic you want to capture or exclude.

7. Enable or disable the Frame Attributes check box. If you enable it (indicated by a check mark), you can control what frames are captured or excluded based on whether they have certain attributes.

   In the FDDI Capture Filter window, you can also enable or disable the Frame Types check box to control filtering on frame types.

   To select an attribute, click on the attribute in the list pane. A mark is shown next to a selected attribute. You can select multiple attributes.

8. In the Filter Action field, select a filter action. There are three choices:

   - Capture Matched Frames causes frames that meet all the other specified conditions to be captured.
   - Exclude Matched Frames causes frames that meet all the other specified conditions to be excluded (not captured).
   - Stop When Frame Matched causes any running measurements to be stopped when a frame occurs that meets all the other specified conditions.

9. If you want to capture or exclude frames that contain specific data in the first 48 bytes of the data field of a packet select Next Page in the Page menu or press **PgDn**. Enter the values in the Data Byte fields.

10. Select Save to New Filter in the Save menu to save your selections. A window opens that asks you to name the new filter.

11. Type a name for the new filter, and press **ENTER**. This copies the filter to the new name and then returns to display the filter you were editing.

12. Select Cancel Changes and Exit in the Done menu. This cancels the displayed values and keeps the original values for the current filter.

13. If you want to activate the new filter, scroll to the bottom of the filters list pane and highlight the new filter name, then select the Activate item in the Control menu.

14. Select Accept Changes and Exit in the Done menu to implement your changes and exit from the filters window.

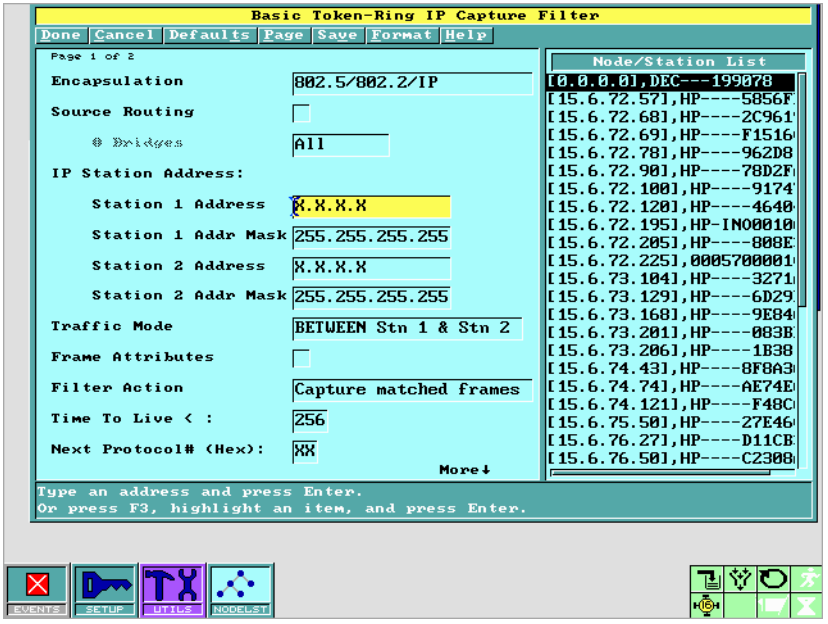


Figure 8-1: Basic Token-Ring Capture Filter window

Activating a Filter

In order to use a filter, you must "activate" it in the Capture Filters window.

1. In the list pane, highlight the filter you want to activate.

2. Select Activate Filter in the Control menu. This displays the filter in the Active Filters pane.

3. Repeat steps 2 and 3 to activate additional filters.

4. Select Accept Changes and Exit in the Done menu to save your selections and return to the Setup window. The activated filters are used whenever you start any measurements.

5. Once you activate a filter or group of filters, selecting the filter status icon (second from the left, on the top row) toggles the filters between active and inactive.

The online help describes how to deactivate and delete filters.

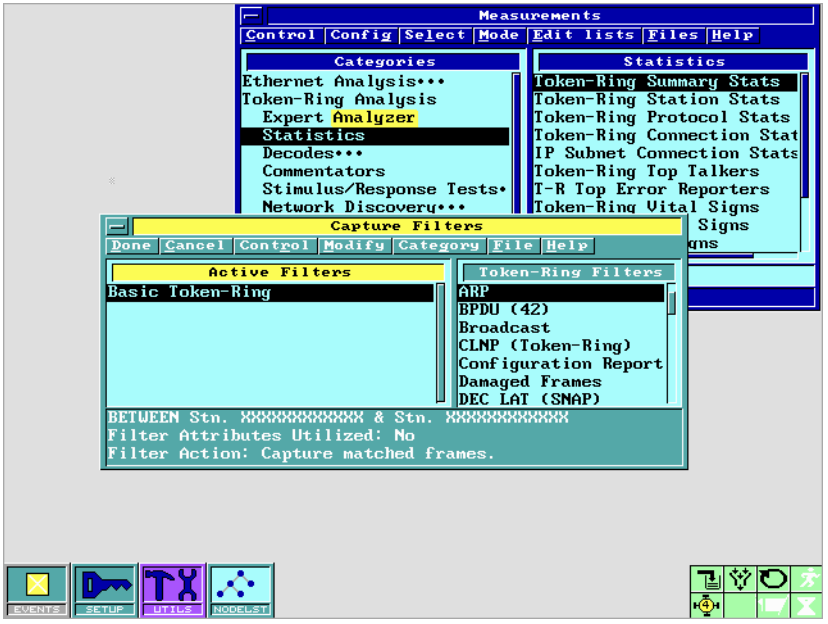


Figure 8-2: Capture Filters window with an activated filter

9

Using the Node/Station List Window

What's in this Chapter

In the Node/Station List window, you can create a node list (symbolic name table) so you can use meaningful names rather than hexadecimal addresses to identify the nodes or stations on your network.

The node list is a global database that can be used by the Internet Advisor LAN's measurements to provide name/address mapping.

For each node, you can identify the general type of node, add comments about the node, and identify address information about the node.

Refer to chapter 11, "Converting trace data and node list files" for more information on converting trace data files and node list files from other LAN analyzers for use in the Internet Advisor LAN.

The Node List Panes

The Node List window is divided into three panes:

- Node/Stations
- Information For:
- Addresses For:

The Node/Station list pane shows the list of node names in the current node list.

The Information For: pane shows information about the highlighted node in the node list. The following information is shown:

- Node/Station Name
- Node Type
- Comments

The Addresses For: pane shows address information for the highlighted node in the node list. The following address information is shown:

- Address
- Protocol Layer
- Address Name
- Cable ID

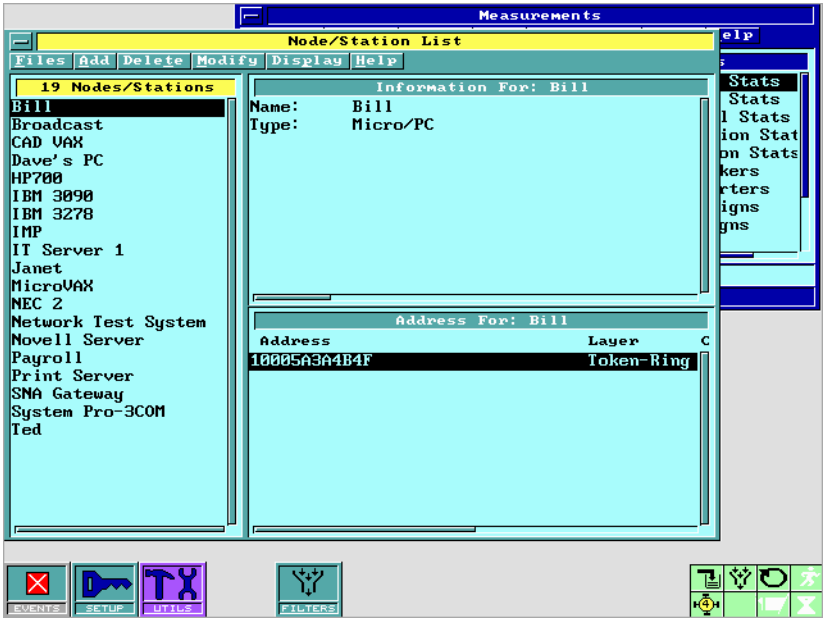


Figure 9-1: The Node List Window

Adding a Node to the Node List

The procedure below summarizes the actions for adding a new node to the node list.

1. Press **ESC** (Menu Bar).
2. Press **A** (Add).
3. Press **N** (Add a Node to the Node List). A new window opens that prompts you to enter the new node name you want to add to the node list.
4. Type the new node name you want to add to the node list. Press **ENTER**.
5. Select the Protocol Layer Field and choose a protocol name from list pane.

6. Select the Address field and enter the address.

7. Enter a Cable Id and a Comment if desired.

8. To add another node, select Save from the menu bar and then Save and Add Another.

9. To exit the window, select Done from the menu bar and then Accept Changes and Exit.

10. To Cancel changes, select Cancel from the menu bar and then Cancel changes and exit or Cancel changes.

Modifying Node Information

You can modify the Node/Station Name, Node Type, and Comment fields for a node already in the node list. Use the Modify menu bar item, and the appropriate choice for node or address.

As a shortcut to opening the node modification window, double-click on the node or address in the Node/Station list pane or the Addresses For: pane.

Modifying Address Information

You can modify the Address, Protocol Layer, Address Name, and Cable ID fields for a node already in the node list. Either double-click the address in the Addresses For: pane, or use the menu bar item Modify to open the Address Editor window.

Printing the Node List

You can print the node list from the Node Discovery or Station Discovery measurement. Follow the steps below:

1. Open the Discovery measurement.

2. Use the Node/Station list menu in the Discovery measurement to reinitialize from the node/station list.

3. Use the Print menu to print the measurement.

Online Help for the Node List Window

The online help for the node list window explains every field in the Node List window, and every action available in the menu bar. In addition, there are topics explaining:

- How to delete nodes and addresses from the node list
- How to save a node list to a file
- How to load a node list into the Internet Advisor LAN

10

Using the Advisor’s Utilities

What's in this Chapter

This chapter describes how to use the utilities provided in the Internet Advisor LAN's Utilities window. These utilities provide functionality not directly related to running measurements. Some of the utilities listed below have additional descriptions in this chapter.

- **File Manager** - lets you perform common file management tasks such as copying, deleting, printing, and renaming files, and creating and deleting subdirectories.

- **PC Configuration** - lets you control whether the internal LCD display or an external display is used. It also lets you control whether the **PRTSC** key is disabled or sends output to a printer or a file, and whether the screen is blanked after a period of mouse or keyboard inactivity.

- **Autostart** - lets you automatically control the Internet Advisor LAN's configuration and automatically run measurements.

- **Version Information** - shows you what version of software and hardware your Internet Advisor LAN has.

- **Install Application** - displays a list of available applications that may be installed. Select an application to display dialog boxes that guide you through the installation.

- **Proxy Port Setup** - lets you support decodes and protocol statistics for non-standard proxy ports. Network fire walls may use non-standard "proxy ports," especially for the World Wide Web. Select this item to display dialog boxes that prompt you for the proxy port information. After a proxy port is setup, the decodes display the specified protocol on the specified proxy port.

- **Exit to DOS** - lets you leave the Internet Advisor LAN mode and go to either Windows 95 or to the alternate DOS boot menu.

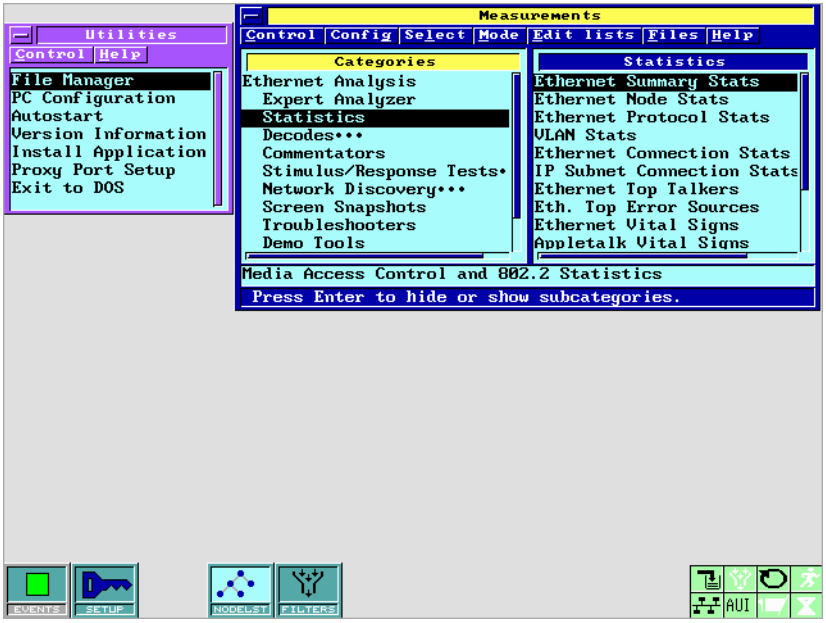


Figure 10-1: Utilities window

Using File Manager

File Manager lets you perform common file management tasks such as copying, deleting, printing, and renaming files, and creating and deleting subdirectories.

When you open the File Manager window, its title bar indicates which disk drive is displayed. It also indicates (in brackets) how many bytes are left on the drive.

The left pane of the window, labeled Directories, shows the directories on the drive. Directories that contain subdirectories are shown with a trailing ellipsis (**...**). Clicking expands the subdirectory structure.

The right pane, labeled Files, shows the files in the highlighted directory.

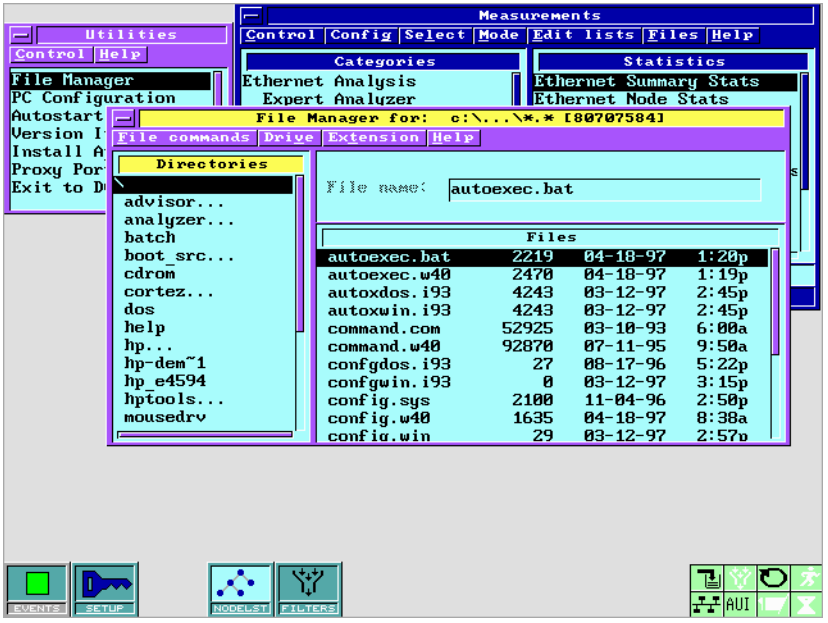


Figure 10-2: File Manager window

Copying, Deleting, and Renaming Files

The following procedure is for copying a file, but the procedure is similar for deleting a file or renaming a file.

1. In the Utilities window, select File Manager. The File Manager window opens.

2. If the file you want to copy is on another drive, select the appropriate drive in the Drive menu.

3. If the file you want to copy is not in the highlighted directory, click on the appropriate directory in the Directories pane. You may first need to click on the vertical scroll bar in the Directories pane to display more directories.

4. In the Files pane, click on the file you want to copy.

5. Select Copy a File in the File Commands menu. A new window opens in which can specify the name of the destination file.

6. Type the destination drive (if it is different from the current drive), the destination file name, and an extension (optional). For example, `a:\myfile.doc` or `newfile`.

7. Press **ENTER** to copy the file.

   OR

   To cancel the copy function, select Cancel Selection and Exit in the Cancel menu.

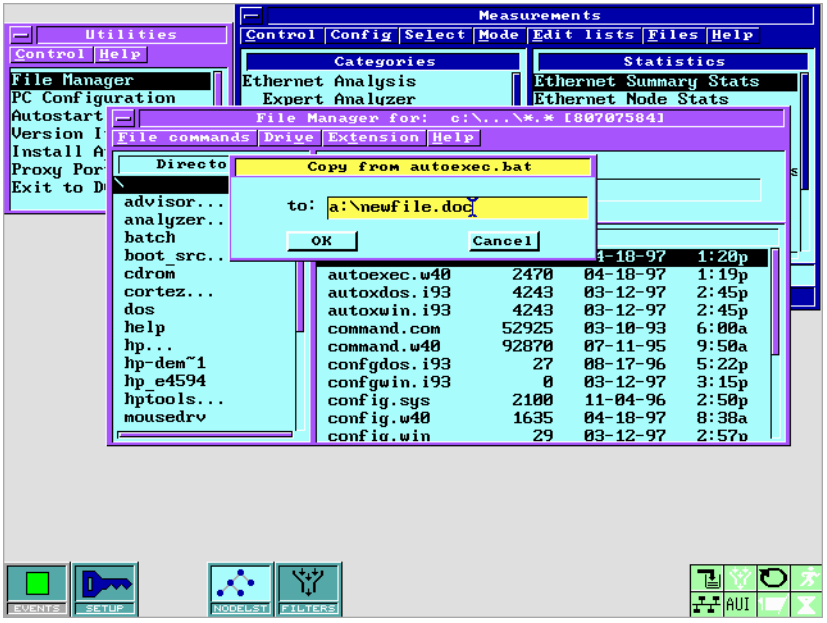


Figure 10-3: Copy a File window

Printing a File

You can print a file to a printer connected to the Internet Advisor LAN's parallel port or serial port 2.

If you have a serial printer connected to the serial port 2, before you use the procedure below, make sure you have re-routed the output of the parallel port (LPT1) to the serial port 2 (COM2) through a statement in your autoexec.bat file such as `MODE LPT1:=COM2`. To do this, exit to DOS from the Utilities window. If you are using the Windows 95 start, use the DOS Prompt icon to get to DOS. If you are using the alternate DOS menu boot, then you can select the DOS prompt item. After you get to DOS, then use a MS-DOS editor to open the file. See "Exiting from Internet Advisor LAN" in this chapter for information on exiting to DOS, and "Using the ED editor" in chapter 11 for information on ED.

NOTE

Capture buffer data files and decode result files are binary files and must be converted to ASCII file format before they can be printed. Use the Data File Conversion Program in the DOS utility named CONV.

Refer to "Converting Trace Data and Node List Files" in chapter 11 for a procedure to convert files.

1. In the Utilities window, select File Manager. The File Manager window opens.
2. If the file you want to print is on another drive, select the appropriate drive in the Drive menu.
3. If the file you want to print is not in the highlighted directory, click on the appropriate directory in the Directories pane. You may first need to click on the vertical scroll bar in the Directories pane to display more directories.
4. In the Files pane, click on the file you want to print.
5. Select the Print a File item in the File Commands menu. The file is printed in ASCII format.

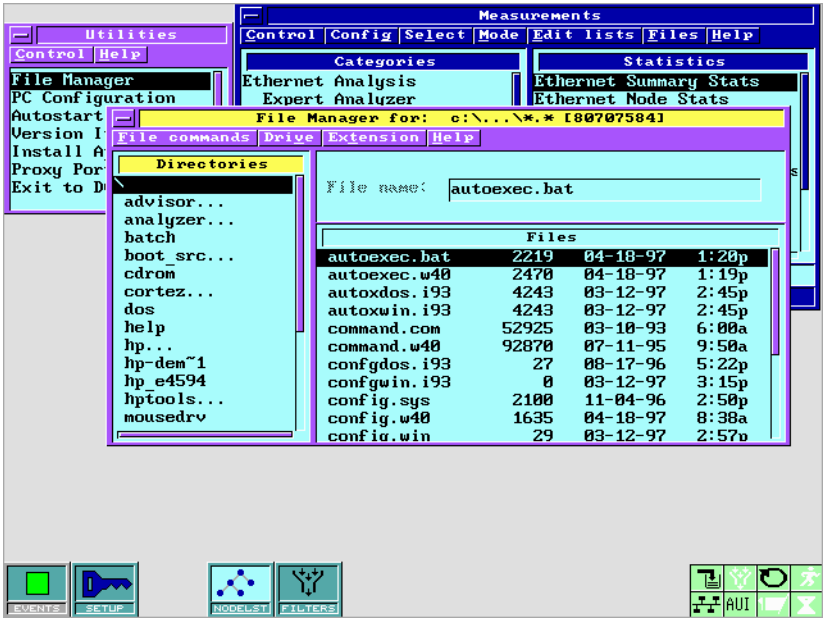


Figure 10-4: File Manager window

Using PC Configuration

PC Configuration lets you control whether the internal LCD display or an external display is used. It also lets you control whether the **PRTSC** key is disabled or sends output to a printer or a file, and whether the screen is blanked after periods of keyboard or mouse inactivity.

The online help for the PC Configuration window contains topics not covered in this chapter, such as using the items in the Files menu to save the values in the PC Configuration window to the system PC Config file or to a user file.

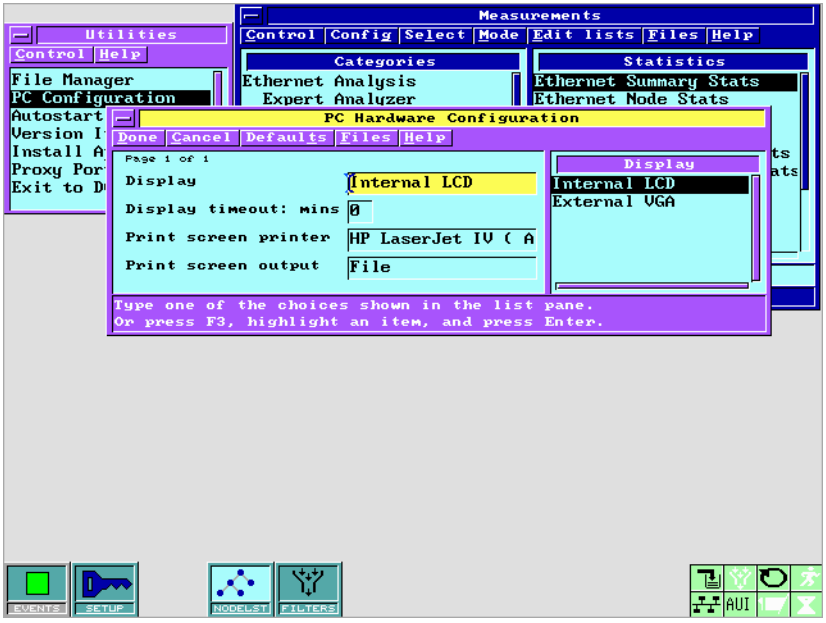


Figure 10-5: PC Configuration window

Using an External Display with the Internet Advisor LAN

The Internet Advisor LAN has an External VGA port that allows you to connect an External VGA display.

The procedure below is for changing from the internal display to an external display, but the procedure is similar for changing back to the internal display.

1. Connect your External VGA display to the rear panel Internet Advisor LAN connector labeled “Ext Monitor” using the cable supplied with your display.

2. In the Utilities window, select PC Configuration. The PC Configuration window opens.

3. Select External Display in the Display field.

4. Close the PC Configuration window to activate your selection. A dialog box is displayed that asks you to confirm the switch to the external display.

5. Select Yes to switch to the external display. The internal display goes blank, and, if the external display is connected correctly and is functional, a dialog box appears on the external display.

6. If the dialog box appears on the external display, press ‘‘Y" to complete the change. Once you switch to an external display, you are prompted on the internal display to reconfirm using the external display whenever you turn the Internet Advisor LAN's on. This gives you the option of returning to the internal display in case the external display is removed before you switch back to the internal display.

   OR

   If the dialog box does NOT appear on the external display, press ‘‘N" to abort the process and return to the internal display.

7. Then, recheck the connection between the Internet Advisor LAN and the external display, make sure the external display is on, and try again.

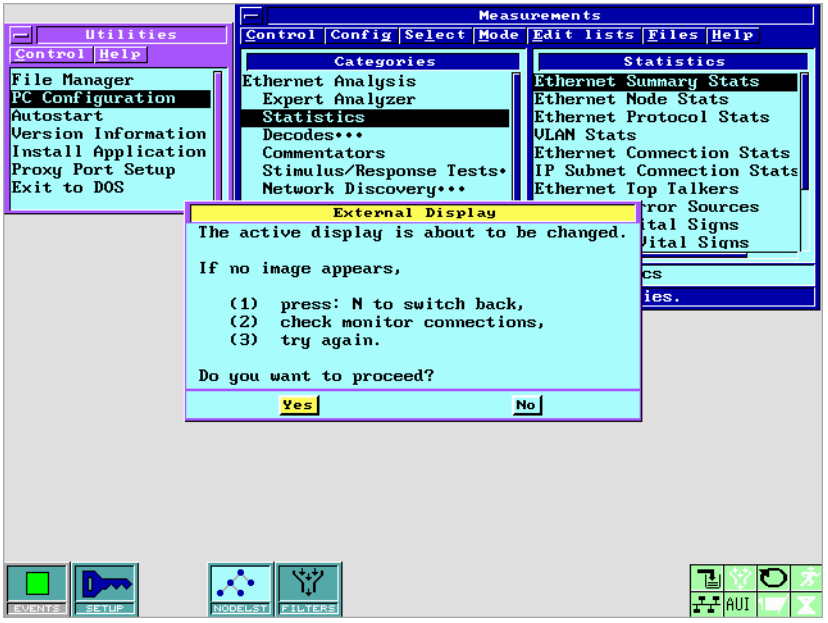


Figure 10-6: Switching to an external display

Printing a Screen to a Printer

You can use the **PRTSC** key to print the Internet Advisor LAN's screen to a printer or a file. This is useful for printing the results of a measurement.

The following procedure is for printing a screen to a printer, but the procedure is similar for printing a screen to a file.

Note that this procedure applies only when you are in the Internet Advisor LAN mode, not when you are in DOS. Also, it assumes you already have a printer connected to the Internet Advisor LAN's parallel port or serial port 2.

If you have a serial printer connected to the serial port 2, before you use the procedure below, make sure you have re-routed the output of the parallel port (LPT1) to the serial port 2 (COM2) through a statement in your autoexec.bat file

such as `MODE LPT1:=COM2`. To do this, exit to DOS from the Utilities window. If you are using the Windows 95 start, use the DOS Prompt icon to get to DOS. If you are using the alternate DOS menu boot, then you can select the DOS prompt item. After you get to DOS, then use a MS-DOS editor to open the file. See "Exiting to DOS" in this chapter for information on exiting to DOS, and "Using the ED editor" in chapter 11 for information on ED.

1. In the Utilities window, select PC Configuration. The PC Configuration window opens.

2. In the Print Screen Printer field, select the type of printer you have connected. The type of printer you select determines how the data is formatted.

   The online help for the PC Configuration window has a help topic that gives more detail on the choices for Print Screen Printer.

   You can use a printer driver other than those supplied with the Internet Advisor LAN by selecting User Print Screen Driver.

3. In the Print Screen Output field, select Printer.

4. Close the PC Configuration window to save and activate your selections.

5. Press the **PRTSC** key whenever you want to print what is shown on the display. A window appears that prompts you to confirm that you want print.

6. Select Yes to print.

   OR

   Select No to abort printing.

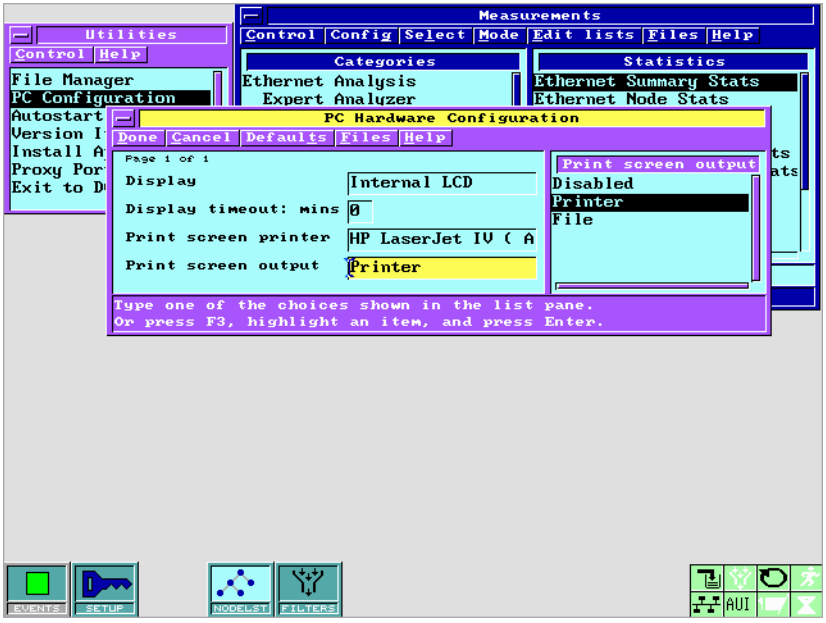


Figure 10-7: Preparing to use the PRTSC key

Using the Screen Saver

1. In the Utilities window, select PC Configuration. The PC Configuration window opens.

2. In the Display Timeout field, select the number of minutes of keyboard or mouse inactivity that must pass before the screen is blanked.

   You may enter any value from 0 to 99 minutes. If you choose 0, the display is always on.

   If a key is not pressed before the timeout value expires, the video output is shut off.

3. Close the PC Configuration window to save and activate your selections.

4. When the screen is blanked, press a key such as the ←, →, ↑, and ↓ arrow keys and the **PgUp** and **PgDn** keys to bring the display back. Pressing such a key is safe whereas pressing some other keys, for example **ENTER**, may initiate an unwanted action.

Using Autostart

There are two windows that let you perform "autostart" functions: the Autostart Configuration window and the Autostart Measurement window. There are two main "autostart" functions:

- **Automatically controlling the Internet Advisor LAN's configuration** - for example, you can control what files are used to load values into the PC Configuration window and the Setup windows, and you can cause a specific measurement to be highlighted in the Measurements window so you can run the measurement by just pressing **ENTER**.

- **Automatically running one or more measurements** - if you run more than one measurement, all the measurements must be for the same network interface (that is, they must be all Ethernet measurements, or all FDDI measurements, or Token-Ring measurements).

Autostart functions are performed whenever any of these five conditions occur:

- You turn the Internet Advisor LAN on.

- You reboot the Internet Advisor LAN by simultaneously pressing the **CTRL+ALT+DEL** keys.

- You return to the Internet Advisor LAN mode from the DOS environment.

- You change the network interface selected in the Setup window and there is an autostart file for that network interface.

- You use the Run Autostart item in the Control menu of the Autostart Configuration window.

When you open the Autostart Configuration window, the values shown in the Autostart Configuration and Autostart Measurements windows are determined by one of the system Autostart files. There are actually three system Autostart files: one associated with each of the Ethernet, FDDI, and the Token-Ring network

interfaces. Whenever you make new selections in these windows and you save your selections, the new selections are saved to the appropriate system Autostart file.

The online help for the Autostart Configuration window contains additional topics not covered in this chapter, such as using the items in the Files menu to save the values in the Autostart Configuration and Autostart Measurements windows to a system Autostart file or to a user file.

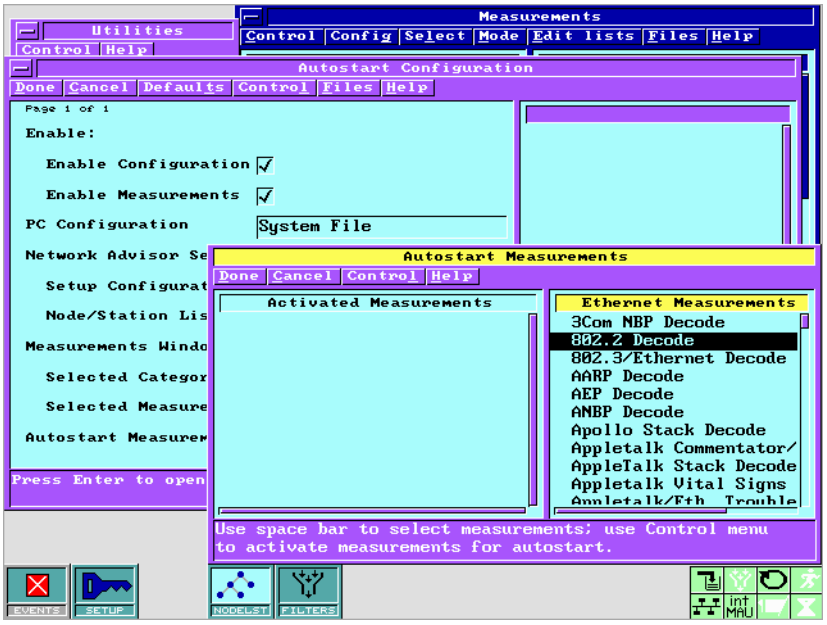


Figure 10-8: Autostart Configuration and Autostart Measurement windows

Automatically Configuring the Internet Advisor LAN

1. In the Utilities window, select Autostart. The Autostart Configuration window opens.

2. Select the Enable Configuration check box by clicking on it until a checkmark appears.

3. To control what files are used to load values into the PC Configuration and the Setup windows, do the following:

    a. In the PC Configuration field, choose either the system PC Configuration file or a user file to load values in the PC Configuration window.

    The system file contains the values that were in the PC Configuration window the last time you closed it or used the Save to System PC Config File item in the Files menu.

    If you have previously saved the values in the PC Configuration window to a user file using the Save to User PC Config File item in the Files menu of the PC Configuration window, you can select User File. When you do, a Load File Selector window opens in which you can specify the user file from which you want to load the PC Configuration window.

    b. Similarly, in the Setup Configuration and Node/Station List fields, select whether to use system files or user files.

    The Setup Configuration choice controls what file is used to load values into all setup windows except the Node/Station List window.

4. To control what category and measurement are highlighted in the Measurements window, do the following:

    a. In the Selected Category field, select the category that contains the measurement you want to be highlighted.

b. In the Selected Measurements field, select the measurement you want to be highlighted.

5. Select the Accept Changes and Exit item in the Done menu. This saves your selections to an Autostart system file for the current network interface.

For example, if Ethernet is currently selected as the network interface in the Setup window, the next time any of the five autostart conditions occur when Ethernet is the network interface, this configuration is loaded.

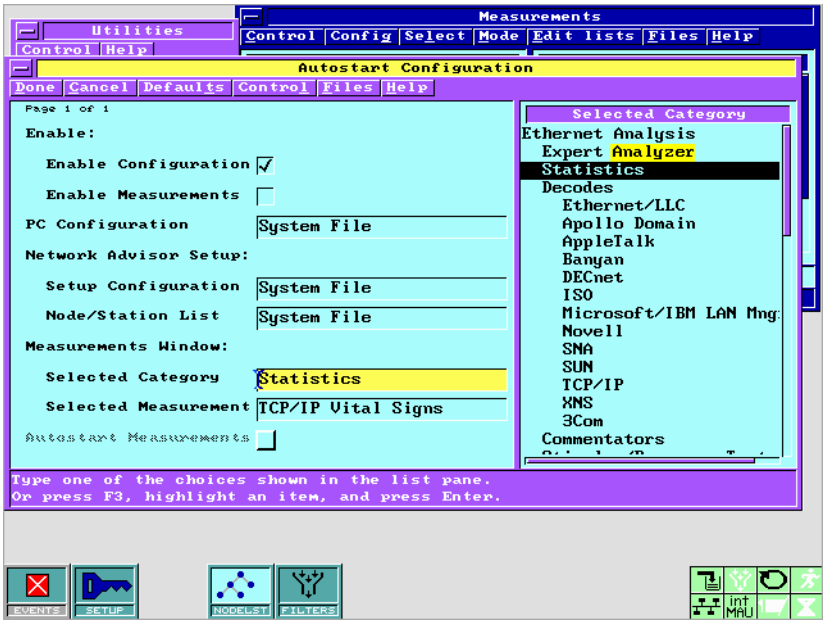


Figure 10-9: Autostart Configuration window

Automatically Running Measurements

In addition to automatically configuring the Internet Advisor LAN, you can automatically run the measurements that you activate in the Autostart Measurements subwindow.

If you activate more than one measurement, all the measurements must be for the same network interface (that is, they must be all Ethernet measurements, or all FDDI measurements, or all Token-Ring measurements). The measurements are run in the order in which they appear in the Activated Measurements pane of the Autostart Measurements window. There may be resource conflicts among measurements.

The procedure below is for selecting and activating the measurements you want to be run upon autostart, but the procedure is similar for deactivating measurements. The online help for the Autostart Measurements window has a topic that describes how to deactivate measurements.

Select Autostart Configuration

1. In the Utilities window, select Autostart. The Autostart Configuration window opens.

2. Enable the Enable Configuration check box by clicking on it until a checkmark appears. This enables Autostart Configuration and causes the Enable Measurements check box to be no longer grayed-out.

3. Enable the Enable Measurements check box by clicking on it until a checkmark appears. This causes the Autostart Measurements push button at the bottom of the window to be no longer grayed-out.

4. Make any autostart configuration selections you want such as specifying user or system files to load into the PC Configuration window, the Setup window and its subwindows, and the Node/Station List window. This is discussed in more detail in the procedure "Automatically configuring the Advisor".

Select Autostart Measurements

1. Open the Autostart Measurements window by double-clicking on the Autostart Measurements push button at the bottom of the Autostart Configuration window. All the measurements that work with the network interface selected in the Setup window are listed.

2. In the right-hand pane, click on a measurement you want. A mark appears in front of the measurement. Clicking on an item again deselects it.

3. Repeat the previous step to select as many measurements as you want.

4. Select Activate Selected Measurements in the Control menu. All the selected measurements are added to the Activated Measurements pane.

5. Select Accept Changes and Exit in the Done menu. This saves your selections and closes the Autostart Measurements window.

6. Select Accept Changes and Exit in the Done menu. This closes the Autostart Configuration window and saves the autostart configuration, so that the next time one of the five autostart conditions occurs, the configuration is loaded and the measurements are run.

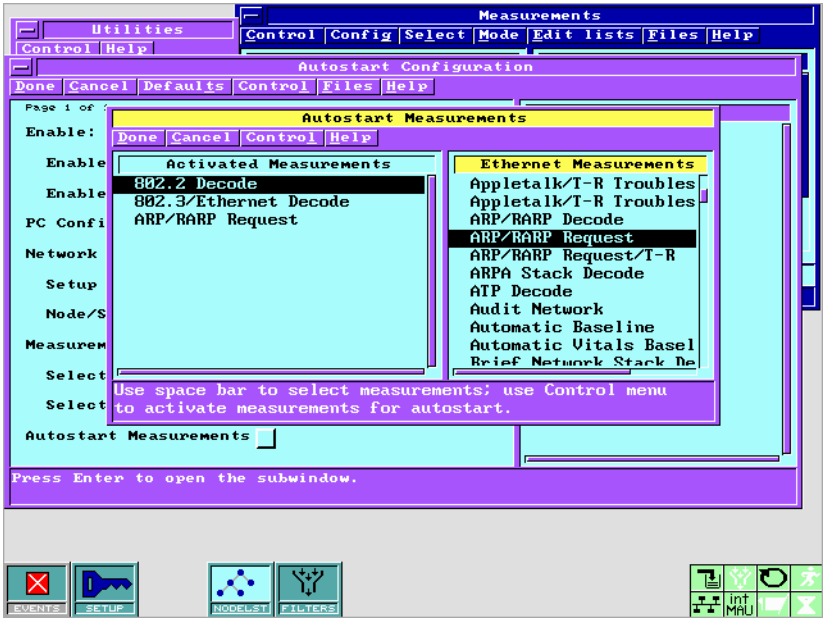


Figure 10-10: Autostart Measurements window

Exiting From Internet Advisor LAN

When you exit from an Internet Advisor LAN application, you exit to the current selection for starting from Windows 95 or starting from a DOS menu.

To exit from Internet Advisor:

1. In the Utilities window, select Exit to DOS.

NOTE

A dialog box warns you that exiting will cause all measurements to be stopped and unsaved data to be lost.
The message about restarting Network Advisor by typing "ADVISOR" at the DOS prompt is no longer effective. You can restart by using either the Windows 95 Start menu or the alternate DOS menu described in chapter 1.

2. Select Yes to exit.

   OR

   Select No to abort exiting.

11

Using Utilities in DOS

What's in this Chapter

This chapter describes how to use the additional utilities that run from DOS.

- ED (A Program Text Editor)
- ProComm® communications program
- Various files that convert trace data and node lists
- Xircom® pocket adapter
- Xlate

Using the ED Editor

DOS provides the text editor, EDIT, that you can use to create and edit text files. EDIT has online help that explains how to use EDIT.

In addition to EDIT, the Internet Advisor LAN comes with a text editor called ED - A Program Text Editor. This is a full screen text editor whose basic operation lets you create and edit text files. The ‘ed.doc’ file explains how to use ED.

Displaying the ED Manual

1. From the Utilities window, exit to DOS.

   If you are using the Windows 95 Start, use the DOS Prompt icon to display the DOS prompt. If you are using the alternate DOS menu, select the DOS Prompt item.

2. At the `C:` prompt, type the following -

   `TYPE C:\UTILS\ED.DOC | MORE` and then press **ENTER.**

Printing the ED Manual

1. Connect a printer to the Internet Advisor LAN.

2. From the Utilities window, exit to DOS.

   If you are using the Windows 95 Start, use the DOS Prompt icon to display the DOS prompt. If you are using the alternate DOS menu, select the DOS Prompt item.

3. At the `C:` prompt, type the following -

   `PRINT C:\UTILS\ED.DOC and then press` **ENTER.**

Using ProComm

The Internet Advisor LAN provides an evaluation copy of the industry-standard communications program ProComm. ProComm lets you communicate with other computers or the HP Bulletin Board Service (BBS). You must have a working modem and modem cable properly installed for this utility to work.

The ‘procomm.doc’ file explains how to use ProComm. This is a long file (over 110 pages).

Displaying the ProComm Manual

1. From the Utilities window, exit to DOS.

   If you are using the Windows 95 Start, use the DOS Prompt icon to display the DOS prompt. If you are using the alternate DOS menu, select the DOS Prompt item.

2. At the `C:` prompt type the following -

   `TYPE C:\UTILS\PROCOMM\PROCOMM.DOC | MORE` and then press **ENTER.**

Printing the ProComm Manual

1. Connect a printer to the Advisor.

2. From the Utilities window, exit to DOS.

   If you are using the Windows 95 Start, use the DOS Prompt icon to display the DOS prompt. If you are using the alternate DOS menu, select the DOS Prompt item.

3. At the `C:` prompt type the following -

   `PRINT C:\UTILS\PROCOMM\PROCOMM.DOC` and then press **ENTER.**

Using ProComm with the HP Bulletin Board Service

The free BBS (Bulletin Board Service) is designed to help you solve your networking problems faster. It contains a library of utilities and application notes for Hewlett-Packard customers. It also contains the latest product information.

Connect your modem cable to either Serial Port 1 or Serial Port 2 on the Internet Advisor LAN rear panel. Refer to the ProComm and modem manuals for more information on modem cabling and communications operations.

In the U. S., the BBS phone number is 1-719-531-4523.

The communications parameters for the BBS are:

- 1200, 2400, or 9600 bits per second
- 8 data bits
- no parity
- 1 stop bit

Introducing ProComm

ProComm is licensed from DATASTORM TECHNOLOGIES, INC.

This is a shareware, “try before you buy” copy of ProComm. DATASTORM has created it to benefit end-users by allowing you to evaluate Procomm before committing your hard earned dollars.

Please be aware that Procomm is not free software, nor is it in the public domain. ProComm is a fully copyrighted works protected to the full extent of U.S. and international copyright laws. This copy of ProComm is a licensed evaluation copy. Registration is not included.

Converting Trace Data and Node List Files

With the Internet Advisor LAN, you can import and export trace data and node lists from other HP systems and from competitive monitoring systems.

The Internet Advisor LAN lets you import trace data from the following devices:

- Hewlett-Packard 4972A
- Network General Sniffer network analyzer
- Novell LANalyzer
- FTP Software LANwatch

The Internet Advisor LAN supports exporting trace data to ASCII file format.

The Internet Advisor LAN supports importing node lists from the following devices:

- Hewlett-Packard 4972A MAC & IP
- Hewlett-Packard LANprobe MAC & IP
- Network General Sniffer network analyzer MAC & IP
- Novell LANalyzer MAC
- UNIX host

The Internet Advisor LAN supports exporting node lists to the following devices:

- Hewlett-Packard 4972A MAC & IP
- Hewlett-Packard LANprobe MAC & IP

Importing or Exporting Trace Data or Node Lists

WARNING If you import a node list file, it replaces the existing node list in the Internet Advisor LAN, so you may want to first save the Internet Advisor LAN's node list to a file before you use the "nlconv.exe" file.

1. From the Utilities window, exit to DOS.

   If you are using the Windows 95 Start, use the DOS Prompt icon to display the DOS prompt. If you are using the alternate DOS menu, select the DOS Prompt item.

2. At the `C:` prompt, type `CD \UTILS` and then press **ENTER**.

3. Type one of the following file names to perform a conversion. Then press **ENTER**:

`CONV`	CONV provides a node list conversion program and a data file conversion program. Refer to the ‘‘Using the CONV Utility" section for tips about using this utility to convert file formats. NodeList Conversion Program Converts node lists from ASCII, HP 4972A, UNIX host, HP ProbeView, Network General Sniffer network analyzer, and Novell LANalyzer to Internet Advisor LAN format. Also converts Internet Advisor LAN node list files to ASCII format. Data File Conversion Program Converts data files from the HP 4972A, Network General Sniffer network analyzer, FTP Software Inc. LANwatch, and Novell LANalyzer to Internet Advisor LAN format. Also converts Internet Advisor LAN data files to ASCII format.
`LPTO72`	Converts an HP Probeview data file to an HP 4972A data file.
`7XDIR`	Shows the directory of an HP 4972A formatted disk on the Internet Advisor LAN.
`7XLOAD`	Copies a file from an HP 4972A formatted disk to the Internet Advisor LAN's hard disk.

`7XSTORE` Copies a file from the Internet Advisor LAN's hard disk to an HP 4972A formatted disk.

You will be prompted to enter the source and destination drive names, path names, and file names for the location of the imported or exported file(s).

There is a short read.me file in the \UTILS directory with instructions on how to use the utilities.

Using the CONV Utility

The CONV utility lets you convert a node list and data file from other LAN protocol analyzers to the Internet Advisor LAN format. Node lists and data files can also be converted to ASCII format.

1. Display a DOS prompt.
   You can do this from the Windows 95 Start menu by selecting either the Programs | MS-DOS Prompt or by selecting the Utilities | Alternative Boot Process to make the Internet Advisor boot to a DOS menu.

2. CD to C:\UTILS.

3. At the C:\UTILS> prompt, type `CONV` to see the options available.

4. More detailed help is available in the C:\UTILS\CONV.DOC file. Use a text editor to view the file.

Using the Internet Advisor LAN as a Network Station

You can use the Internet Advisor LAN as a network station on an Ethernet or Token-Ring network by using a Xircom Ethernet Pocket Adapter™ or Xircom Token-Ring Pocket Adapter™. These adapters connect to the Advisor via the parallel port. The Internet Advisor LAN is factory-configured with a unique physical address (shown in the Advisor Physical Addr field of the Setup window). You can use this address or substitute the address of one of your stations.

To connect the pocket adapter to the Internet Advisor LAN and a network:

1. Turn off the Advisor.
2. Connect the pocket adapter to the Internet Advisor's parallel port.
3. Connect the pocket adapter's BNC connector (Ethernet) or DB9 connector (Token-Ring) to the network.
4. Plug the AC adapter cable into the small round socket at the rear of the pocket adapter.
5. Plug the supplied AC adapter into any standard electrical outlet.
6. Turn on the Advisor.
7. From the Utilities window, exit to DOS.

   If you are using the Windows 95 Start, use the DOS Prompt icon to display the DOS prompt. If you are using the alternate DOS menu, select the DOS Prompt item.
8. Refer to the Xircom Pocket Ethernet Adapter or Xircom Pocket Token-Ring Adapter manual for software configuration and diagnostics.

Xircom Ethernet Pocket Adapter is a trademark of Xircom, Inc.
Xircom Token-Ring Pocket Adapter is a trademark of Xircom, Inc.

12

Using the FDDI Ring Manager

What's in this Chapter

This chapter is intended to get you started using the FDDI Ring Manager. It includes overview information, step by step instructions, and an example of using the Internet Advisor LAN FDDI Ring Manager to troubleshoot a common network problem.

Introduction to the FDDI Ring Manager

The FDDI Ring Manager is a network management application for the Hewlett-Packard Internet Advisor LAN that gives you automated ring monitoring and network troubleshooting in one integrated window. The graphical user interface displays the actual nodes on your ring.

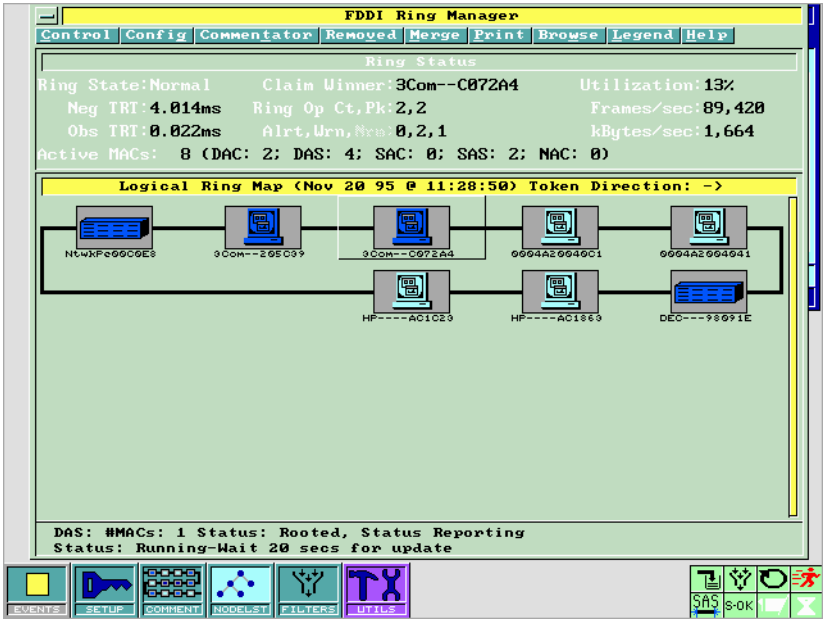


Figure 12-1: The FDDI Ring Manager application interrogates each station on the FDDI ring using the SMT protocol.

At a glance, you can see whether the ring is wrapped, twisted, or functioning normally. You can see detailed information for any node and navigate through the topology of the network using simple point-and-click actions.

How the Ring Manager works

The FDDI Ring Manager gathers information about your network in either *passive mode* or *active mode*.

Passive Mode

In passive mode, the Internet Advisor LAN sits quietly on the network compiling information from the Neighborhood Information Frames (NIFs) that each FDDI node sends on the ring. The Ring Manager analyzes the NIFs to build a map of the token path on the ring. The Ring Manager also formats the NIF information for easy understanding.

When you are looking at your ring in passive mode, the ring map and station information update every 35 seconds.

Active Mode

In active mode, the Internet Advisor LAN interrogates each node on the ring with Configuration and Operation Status Information Request Frames (SIFs). The Ring Manager analyzes the SIF responses to build a database of connection, configuration, and operation information. The information available in active mode is much more extensive and detailed than the information available via passive monitoring of NIFs.

The ring map and station information update interval is user-configurable in active mode.

The Internet Advisor LAN FDDI Ring Manager consists of four interrelated functions to give you a complete description and analysis of your FDDI ring:

- Ring Status
- Ring Map
- Detailed Station
- Ring Commentator

Ring Status

The top section of the FDDI Ring Manager window is the Ring Status section. It provides high level indicators that show the current state of your ring at a glance. With a quick look at the Ring Status section, you see immediately whether the ring is stable and functioning normally or if there are problems on the network.

In addition, you can see the network performance and throughput as a utilization percentage, as frames per second, or as kilobytes of data per second. The Ring Status section gives you the following information:

- **Ring State** - Tells you if the ring is in a normal, twisted, or wrapped state.
- **Negotiated TRT** - Shows the value of the negotiated token rotation time.
- **Observed TRT** - This is the actual time interval between successive tokens.
- **Active MACs** - Shows the number of MACs of each FDDI station type that were active on the ring during the last update interval. The station types are:
  - DAC (Dual Attach Concentrator)
  - DAS (Dual Attach Station)
  - SAC (Single Attach Concentrator)
  - SAS (Single Attach Station)
  - NAC (Null Attach Concentrator)
- **Claim Winner** - This is the MAC address of the station that won the claiming process during last update interval. This information is available only when the Ring Manager is running in active mode.
- **Network Traffic** - Shows the current level of network traffic displayed as a percentage of total bandwidth, and also in frames/second and kilobytes/second.
- **Ring Op Statistics** - This is the number and peak rate of ring initialization in any 5 second interval since the start of the Ring Manager measurement.
- **Commentator Events** - This section shows which event levels are configured for display in the FDDI Commentator: Alert, Warning, or Normal. Counts of each event level are also displayed here.

The Ring Map

The next section of the FDDI Ring Manager window is the Ring Map. This map is a graphical view of your ring topology with different node icons to represent the different device types on the ring. In addition to device type information, colors are used to communicate the status of each device:

- **Blue** - trunk (dual ring backbone) ring station
- **Cyan** (light green-blue) - node connected to the ring through a concentrator
- **Yellow concentrator** - shows a problem in the sub-tree of the concentrator
- **Yellow station** - shows this node has detected frame errors on the ring
- **Red** - indicates an alert level problem with this node

Highlight any node using the keyboard arrow keys or a simple mouse click to see a summary description in the status line at the base of the Ring Map. Selecting a highlighted node opens a window displaying detailed station information.

You have a choice of mapping your ring according to either a *logica*l or a *physical* view of the network.

Logical View

The logical view of your ring shows the token path through all of the active Media Access Control (MAC) elements on the ring. This view is useful for seeing the entire network and the path of the token as it passes from station to station. When the FDDI Ring Manager is configured in passive mode, the logical view is the only view possible. You can also select the logical view in active mode to see detailed station information.

Physical View

The physical view of the ring shows the order in which the network nodes, such as stations, concentrators, bridges, etc., are attached to each other to form the FDDI network. The ring topology is displayed hierarchically in the physical view. The top level of the hierarchy shows the stations on the backbone (trunk) ring. Stations attached to concentrators can be viewed by selecting the concentrator to open the M-port connections map for that concentrator.

This expanded view shows every station connected to the concentrator. If one of the M-port connections is another concentrator, that concentrator can also be expanded to its M-ports connections map. Thus you can examine a tree topology network at any desired level. Station information for a concentrator itself is displayed using the "Concentrator" menu item.

Ring Manager Configuration

The Ring Manager configuration window lets you control the ring view and the access mode of the Ring Manager, and set the level of event reporting in the FDDI Commentator.

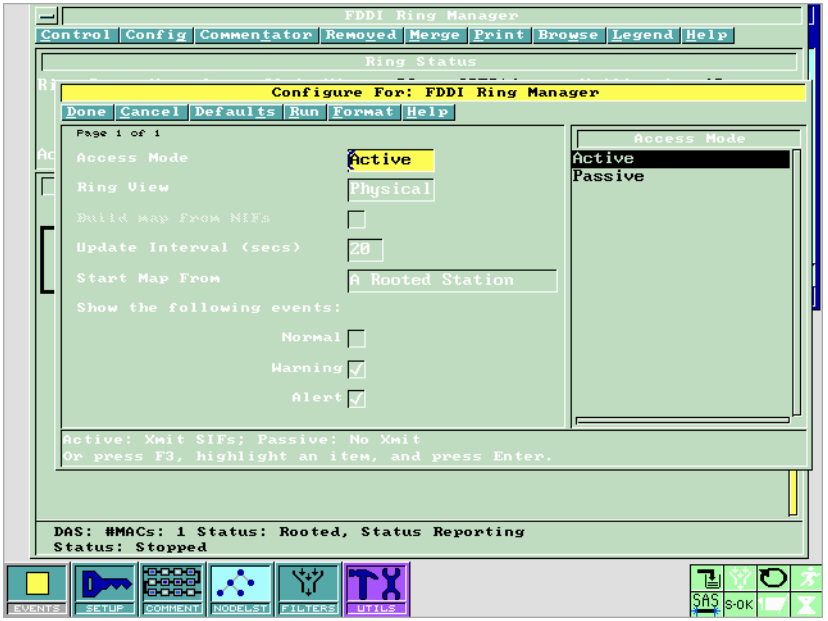


Figure 12-2: You can configure the FDDI Ring Manager and the events to report in the Commentator.

- **Access Mode** - defines the manner in which the FDDI Ring Manager accesses the network.
  - Passive - In this mode, the Ring Manager monitors NIF frames on the network. Passive access mode is used for the logical ring view only.
  - Active - In this mode, the Ring Manager transmits and monitors SIF frames on the network. Active access mode can be used for either a logical or physical view of the ring.
- **Ring View** - specifies whether the view of the ring is logical or physical.
  - Logical - The ring map shows the token path through every MAC on the ring.
  - Physical - The ring map shows the physical connections between all nodes on the ring.
- **Update Interval** - defines the time interval between updates to the FDDI Ring Manager windows. This is also the time interval for rebuilding the ring topology. In passive access mode, this interval is fixed at 35 seconds. In active access mode, the interval may be set from as low as 20 seconds up to 990 seconds in increments of 5 seconds. The update interval determines how frequently the Internet Advisor LAN transmits SIF requests on the ring to get station configuration and operation information.
- **Start Map From** - specifies the node to start the map of the ring. This facilitates convenient analysis by anchoring the graphical display of the ring map to the node of your choice. The node list is displayed in the configuration window so that you can easily select the station you want to see first. Or, if the address format is set to hex, you can enter an address directly into this field. The ability to specify the first node of the map also serves as a means for locating a specific station on the map.
- **Show the Following Events** - these boxes control the level of events reported in the FDDI Ring Manager Commentator. Check the boxes next to the events you want to see logged and interpreted in the FDDI Commentator.

Station Information

The FDDI Ring Manager provides detailed station information for every node on your FDDI network. To see a display of any node's station information, point at the node on the Ring Map and double-click to open it.

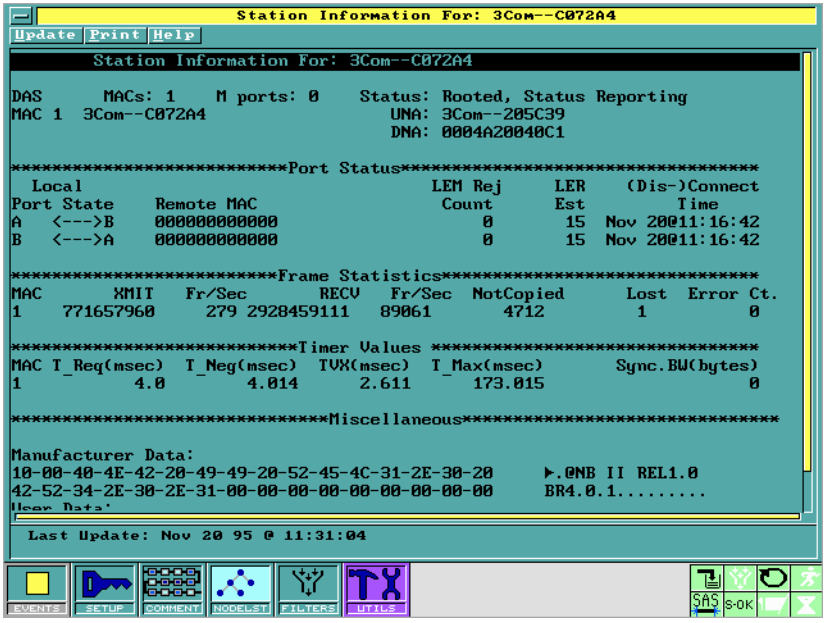


Figure 12-3: Detailed Station Information is available when the Ring Manger is running in active mode

In active access mode, the station information window consists of five sections: Station Description, Port Status, Frame Statistics, Timer Values and Miscellaneous.

- **Station Description** - This section reports the station type, the number of MACs in the station, number of M ports, and the upstream and downstream neighbor addresses of the station.

- **Port Status** - This section shows the connection state between each local port and its remote port, the link error monitor reject count for each port, the link error estimate for each port, and the time the port connected or disconnected from the ring.

- **Frame Statistics** - This section shows frames transmitted, received, not copied, or lost for each MAC in this station.

- **Timer Values** - This section shows the station's requested token rotation time, the negotiated token rotation time, the valid transmission timer setting, the maximum token rotation time, and any allocated synchronous bandwidth.

- **Miscellaneous** - This section shows connection policies for this station, any user data, and the SMT version implemented on this station.

Ring Commentator

The FDDI Ring Commentator provides a real-time commentary on all significant events occurring on the ring. These include events that lead to changes in ring topology, indicate a problem on the ring (or conditions that might lead to a problem), and are likely to be of interest to a network administrator.

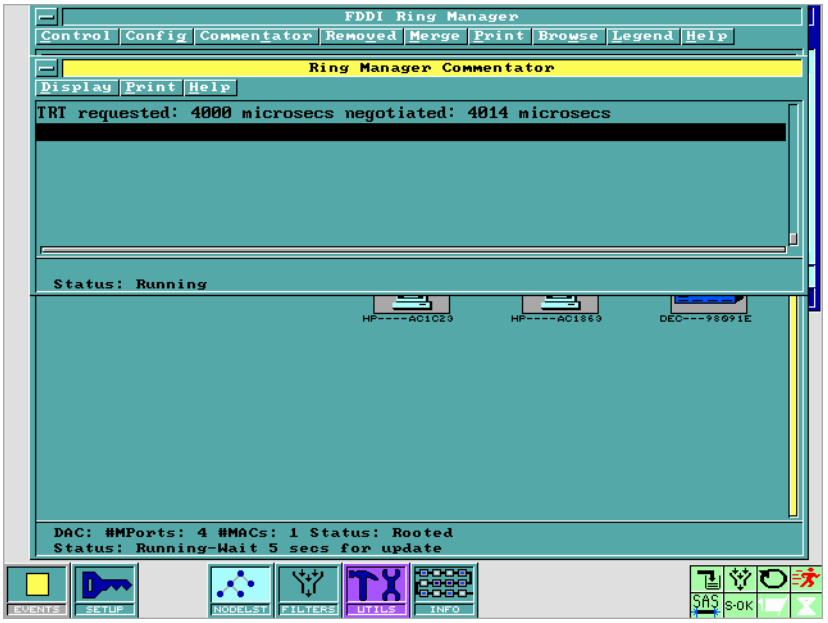


Figure 12-4: The FDDI Ring Manager Commentator

The FDDI Ring Commentator runs automatically whenever the FDDI Ring Manager is started. The FDDI Commentator categorizes events as Alerts, Warnings, or Normal. You can change the default levels in a configuration file to control event reporting. The online help for the Commentator explains how to do this.

The events in the Commentator window are collected across multiple runs of the FDDI Ring Manager. The Commentator window is cleared when the Ring Manager is closed or the Internet Advisor LAN software is exited. You can save the contents of the Commentator by printing the measurement to a file or to the printer.

Getting Started with the FDDI Ring Manager

The graphical map in the Ring Manager can help you keep track of who is where on the ring. The map also shows where the ring is wrapped or twisted if one of these problems occurs. The Station Information windows give you detailed node statistics: port connections, timer values, and frame counts. The Ring Status section at the top gives a concise summary of the state of the network and network performance. The FDDI Commentator shows you a history of interesting events on your ring.

Attaching the Internet Advisor LAN to the ring

The Internet Advisor LAN can be attached at any point in the FDDI network, but it is recommended that you attach it at an M-port of a concentrator. Use the following steps to attach the Internet Advisor LAN to a concentrator:

1. In the Setup window, open the Interface Parameters push button window
2. Select the appropriate Media Connection: Fiber or Copper.
3. Set the Connection Mode field to Station.
4. Set the Connection Type field to Single Attach Stn-S (SAS). You may also connect to a concentrator using the DAS connection type if you wish.
5. Select the Done, Accept Changes and Exit menu.
6. In the main Setup window, you may also want to select the addresses format. Addresses can be displayed in either Canonical or MSB format. Canonical format is more familiar to Ethernet users, MSB format is more common for Token-Ring users.
7. Select "Done, Save Changes and Iconize" in the main Setup window menu.

8. Attach an S-MIC cable from the Internet Advisor LAN's A/S/M-port to an M-port of a concentrator. The port status icons in the lower right screen should signal that the S connection is OK. If you are using the DAS connection type, one port is OK, the other is shown as Wrapped.

9. Start the Ring Manager by double clicking FDDI Ring Manager in the measurements window.

The FDDI Ring Manager default configuration is a logical ring view using active mode. This means that the Internet Advisor LAN queries the stations on the network for information and displays the map of the network based on the token path. The level of events reported in the FDDI Commentator is set to Alerts and Warnings by default. You can change any of the defaults in the Configuration window. If you want to change the access mode from active to passive, stop the Ring Manager measurement before you open the Configuration window.

Looking at the Ring Manager, you see that the window is divided into two main sections with a status bar at the bottom of the window. The Ring Status section at the top of the window gives you a summary description of the network showing the number of active MACs, the Ring State, the network performance, and what events are currently reported in the Commentator.

The Ring Map section shows you the devices types and the status of each device on your ring. You can open any icon to a Station Information window for a station node or to an M Port Connections window for a concentrator. The "Concentrator" menu item in the M-Port Connections window shows detailed station information for the concentrator.

If any station leaves the ring for any reason, you can examine it in the Removed MACs window. Use the "Removed" menu item in the FDDI Ring Manager window to open the Removed MACs window. The station information for the removed MAC shows the state of the nodes when they left the ring.

The status bar at the bottom of the window shows a summary station description for the currently highlighted node in the Ring Map. The second status line shows whether the measurement is running and how long until the next update of Ring Manager information.

You can open the Ring Manager Commentator window using the Commentator menu in the Ring Manager window, by selecting the Commentator icon.

Each window that you open has its own Help menu. Use the first Help menu, Topics, to see a list of detailed information about the function and contents of that window.

Troubleshooting Network Problems

The following scenario is given as an example of how to use the FDDI Ring Manager to troubleshoot a common network problem.

Bob, one of the users on your network, has called to say he can't connect to the server. You have a 15 node backbone (trunk) ring with 150 nodes connected by concentrators.

You bring up the FDDI Ring Manager measurement on your Internet Advisor LAN. Glancing at the Ring Status section, you see that the Ring Op count is high.

In the Physical Ring view of the Ring Map and you can see that the connections to the server are good. The Ring Map shows one of the concentrators is yellow signaling that there is a problem in its subtree. You select that concentrator to open its M-port connections map. Bob's node is connected to this concentrator and it is shown in red. You open that node to its Station Information window. The Port Status section shows you that the Link Error Monitor (LEM) Reject count is very high. This tells you that Bob's node has repeatedly been removed from the ring due to link errors.

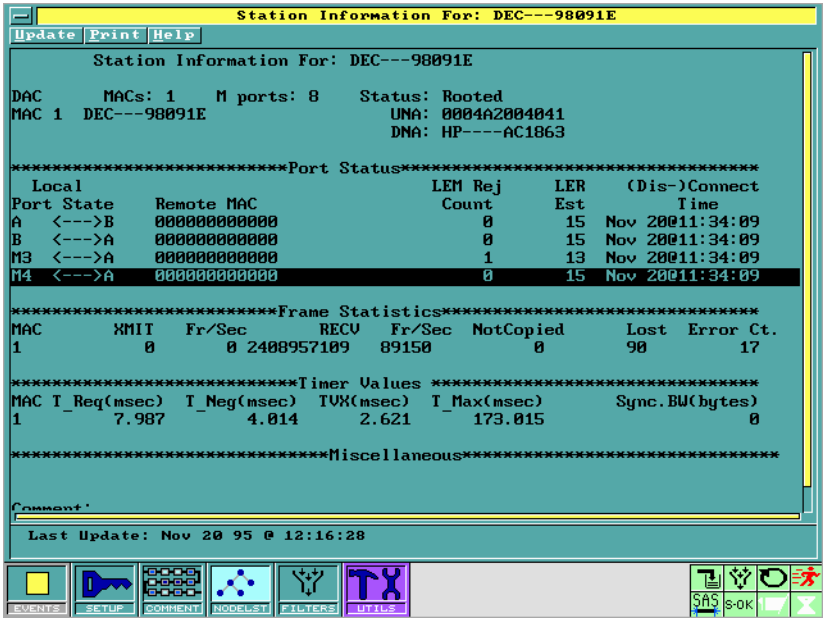


Figure 12-5: Bob's node has a high LEM Reject count

The Station Information window Port Status section shows which M-port is connected to Bob's node. You go to the concentrator and check the cable connections. They are seated correctly. You decide to switch Bob's connection to an unused M-port. A check of the Station Information window shows that the connection is now good.

Now you suspect that the M-port board may be bad. To prove this, you swap the M-port board with a spare that you have and reconnect Bob's node. The connection is good. The Internet Advisor LAN FDDI Ring Manager has helped you isolate the problem quickly.

Summary

The Ring Map showed you exactly where to look for an answer to the common question: "Why can't I connect to the server?"

The yellow concentrator icon was a signal that the problem lay somewhere in the tree structure beneath that concentrator. Opening the concentrator, the M-port Connections map showed Bob's node in red to isolate the problem further. The Station Information window for Bob's node showed which port to check on the concentrator. When you connected Bob to a different M-port, the Station Information window for Bob's node showed that the connection was now good. From this information you were able to deduce that the problem was the M-port board. You and the Hewlett-Packard Internet Advisor LAN FDDI Ring Manager make a great team!

The Ring Discontinuity Symbol

If you see the ring discontinuity symbol, [??] in Active Access Mode, it can mean that your network uses FDDI equipment that has not yet fully implemented the FDDI Station Management (SMT) Standard for Station Information Frames (SIFs). Active Access mode relies on proper SIF responses from each FDDI node to build the physical and logical ring maps.

To address this issue, an option has been added to the Ring Manager Configuration window to specify that the map be built from Neighbor Information Frames which are widely implemented in accordance with the SMT Standard.

When you check the "Build Map From NIFs" field on the Configuration page, you can get the detailed Station Information available in Active Access Mode, and also see a logical ring map with fewer or no discontinuity symbols.

The "Build Map From NIFs" option is only available in Active Access Mode with Logical Ring View. When "Build Map From NIFs" is enabled, the Update Interval is set at 45 seconds and cannot be changed.

Physical Ring View is still available in Active Access mode. On a network with new FDDI equipment, the physical map often works well. However, if the physical map shows many ring discontinuity symbols ([??]), changing the configuration to "Logical Ring View" and "Build Map From NIFs" can resolve many of these discontinuities.

Glossary

Glossary Terms

Accelerators

Each menu bar item and each item in a dropdown menu has one underlined character. When the menu bar has focus, typing the underlined character in a menu bar item selects that menu bar item and displays its dropdown menu.

Similarly, when a dropdown menu is displayed, typing the underlined character in an item selects that item.

Active pane

Some windows have more than one pane. When there are multiple panes, only one pane is active at a time. The active pane receives any keyboard or mouse input, and, if the active pane has a title bar, it is highlighted (white on the standard LCD display and yellow on a color display).

Active window

The active window is the window that has the ability to accept input from the keyboard or a mouse. The active window is displayed on top of any other windows it overlaps and its title bar is highlighted (white on the standard LCD display and yellow on a color display). Only one window is active at a time.

Check box

A small graphical device that is either on (enabled) or off (disabled). On is indicated by a checkmark. An example is the Enable Configuration check box in the Autostart Configuration window.

De-iconize

To return a window to its previous size and position after it has been iconized.

Dialog box

A box that is used to display messages or to ask you for additional information.

Dropdown items

The individual items or commands in a dropdown menu that let you perform specific functions.

Dropdown menu

Dropdown menus (usually just called "menus") contain one or more items. The items are the individual commands that let you perform specific functions.

Focus

The object that has the ability to receive keyboard or mouse input is said to have focus or to be active. See Active Window and Active Pane.

I-beam

A special text marker that is shown in text entry panes and text entry fields. The I-beam marks the position where new text can be inserted or deleted.

Icon

A small graphic symbol with a short title or picture that identifies a window that has been shrunk. Icons are displayed in a reserved area at the bottom of the screen.

Iconize

To cause a window to become an icon. Iconizing a window that contains a running measurement does not cause the measurement to stop or to lose data, and an iconized window continues to post events to the Event Log.

Label

A text field that you cannot edit.

List pane

A pane that contains a list of items you can scroll. Pressing **ENTER** or clicking the mouse selects a highlighted item from a list pane.

Menu

See Dropdown Menu.

Menu bar

Located just below the title bar, the menu bar contains labels called menu bar items.

Menu bar items

Menu bar items let you access dropdown menus. As you highlight each menu bar item, its dropdown menu appears.

Mouse cursor

When a mouse is attached to the Internet Advisor LAN, the visible indication of the mouse is the mouse cursor. The mouse cursor is represented by different symbols depending on the mode of operation. Mouse cursor symbols include:

- an arrow in normal mode
- an hourglass whenever the Internet Advisor LAN is working and cannot accept further keyboard or mouse input
- a vacuum cleaner whenever the Internet Advisor LAN is gathering memory so the memory can be used again

Pane

A pane is a partition of a window. All windows have at least one pane. Some panes contain text entry fields (also known as fields or text entry boxes), check boxes, push buttons, and other items. Other panes are called list panes. See List Panes.

Push button

A small graphical device that invokes some action when "pressed" by clicking the mouse or pressing **ENTER**. Examples of the actions a push button can perform are opening another window or displaying more choices.

Radio button

One of a group of toggle buttons, of which only one can be on at a time.

Scroll bar

A bar that indicates what part of the window contents is visible, and allows vertical or horizontal scrolling with a mouse.

Status icons

Eight boxes in the lower right corner of the screen which graphically show the status of the Internet Advisor LAN. Most of the status icons show Setup window selections.

Status line

An area at the bottom of a window that displays prompts, instructions, or comments specific to that window.

Subwindow

Windows you can access from another window are sometimes called subwindows. For example, from the Setup window you can go to several subwindows such as the Node/Station List subwindow.

Text entry field

A field into which you can type text. The or box I-beam is used to indicate text entry fields. There are actually two kinds of text entry fields:

- Fields that can only contain one of the choices shown in the list pane. An example of this is the Network Interface field in the Setup window.

- Fields that can contain either one of the choices shown in the list pane or a choice of your own not shown in the list pane. An example of this is the Advisor Physical Address field in the Setup window.

Text entry pane

A pane into which you can type text. An example is a pane in which you can enter comments. The I-beam is used to indicate text entry panes.

Title bar

An area at the top of each window, that identifies the primary function of the window.

Unzoom

To return a zoomed or expanded window to its original size and position.

Window

A window is a graphic object with a border, title bar, menu bar, one or more panes, and dropdown menus.

Window Menu

The Window Menu contains items such as Close, Move, Size, Zoom, and Icon that let you control a window's size and position.

Window Menu button

A small graphic button located in the upper left corner of most windows. Clicking on the button or pressing **F4** (Window Menu), displays the Window Menu.

Zoom

To expand a window so it fills the display.

Index

D

E

F

G

N

O

P

R

S

T

U

V

W

X