

Surveyor

User's Guide

Shomiti Systems, Inc.

P/N 750-00163-0001 Rev. B

Trademarks and Copyrights

Shomiti Systems, Surveyor, Explorer, Century 12-Tap, 12-Tap, Century Tap, Century Media Module 1, CMM1, Century Media Module 2, CMM2, Century LAN Analyzer, Packet Blaster plug-in, Remote plug-in, Expert plug-in, Voyager, and Century Tool Kit are trademarks of Shomiti Systems, Inc. Windows '95, Windows NT, Microsoft Mail, and Excel are trademarks of Microsoft Corporation. Pentium is a trademark of Intel Corporation. Magic Packets is a trademark of Advanced Micro Devices. Sniffer is a trademark of Network General, Inc. All other trademarks are those of their respective companies.

Shomiti Software License Agreement

This Software Program and accompanying written materials are proprietary products of Shomiti Systems, Inc., and are protected by copyright laws and international treaties. You must keep the Software Program in strict confidence and treat it like any other copyrighted material. You may not copy the Software, documentation, or associated written materials except as provided below.

License

Subject to the provisions of this License, Shomiti hereby grants to Licensee, a non-exclusive, non-transferable license to use the Software and all documentation and upgrades provided for said Software. The Software may be loaded and executed on a single host computer. Title to the Software shall at all times remain with Shomiti. Licensee may not copy or sublicense such Software, documentation, or other written material, in whole or in part, without prior written consent of Shomiti, except for as provided below.

Term

This License shall become effective upon shipment or other transfer of the designated Software from Shomiti and shall remain in full force and effect in perpetuity, unless terminated pursuant to the provisions of this License. This agreement can be terminated at any time by returning or destroying all copies of the Software and related written materials and documentation and by notifying Shomiti in writing of your termination of the License.

If either party defaults in the performance of any of its obligations thereunder, and such default continues for thirty (30) days after receipt of notice from the non-defaulting party, the non-defaulting party shall have the right to terminate this License immediately by giving written notice. Upon termination of this License, Licensee shall, at Shomiti's request, either return to Shomiti or destroy all copies of the licensed Software and documentation.

Restrictions

Licensee shall have the right to make one backup copy of the Software for use in the event the original Software is damaged. Such License does not convey any right, expressly or by implication, to manufacture, duplicate or otherwise copy or reproduce any of the Software or documentation. Licensee hereby agrees not to trace, decompile or disassemble the Software, or use any other means to identify the source codes of the Software.

Shomiti's Software is commercial computer Software and, together with any related documentation, is subject to the restrictions on US Government use, duplication or disclosure set forth in DOD FAR j2.227-7013(c)(1)(II). Licensee agrees to mark any Software and related documentation that is to be directly or indirectly delivered to any branch or agency of the US Government with the legend set forth below in such manner that it can be readily and visually perceived:

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subdivision (c)(1)(II) of the Rights in Technical Data and Computer Software clause at DOD FAR 52.227-7013

Shomiti Systems, Inc., 1800 Bering Drive, San Jose, CA 95112

Limited Software Warranty

A Shomiti Limited Software Warranty is provided with each Software Product purchased through one of Shomiti's authorized distribution channels. For a period of twelve (12) months from date of shipment, Shomiti warrants Software to conform with Shomiti's published specifications on date of shipment when properly operated in accordance with procedures described in documentation supplied by Shomiti.

Defects in the Software will be reported to Shomiti accompanied by supporting information reasonably requested by Shomiti to verify, diagnose and correct the defect. Shomiti's exclusive obligation with respect to nonconforming Software Product shall be, at Shomiti's option, (a) to replace that copy of the Software with one that conforms to the specifications, or, (b) to use diligent efforts to provide the customer with a correction or workaround of the defect. Shomiti is under no obligation to provide Software updates which contain additional features and enhancements other than defect corrections.

Patent and Copyright Indemnification

Shomiti shall have no liability to the Licensee if any patent or copyright infringement is based upon or arises out of: (1) compliance with designs, plans or specifications furnished by or on behalf of the Licensee as to the Products or services, (2) alterations of the Products or services by the Licensee, (3) failure of the Licensee to use updated Products or services, including error corrections and updates, provided by Shomiti for avoiding infringement, (4) use of Products or services in a manner for which the same was neither designed nor contemplated, or (5) a patent or copyright in which the Licensee or affiliate or subsidiary of the Licensee has any direct or indirect interest by license or otherwise.

Limitation of Liability

Shomiti's liability under or for breach of this license shall be limited to refund of the purchase price actually paid by the Licensee to Shomiti for the specific item causing the damage. In no event shall Shomiti be liable for costs of procurement of substitute goods, loss of profits, or for any special, consequential or incidental damages, however caused, whether for breach of warranty, breach of contract, repudiation of contract, negligence or otherwise.

Forum

This License shall be interpreted in accordance with the laws of the State of California, and exclusive jurisdiction and venue shall lie in the state or federal courts of Santa Clara County, California.

Entirety

These terms and conditions represent the entire agreement between the parties relative to the license of the Software and firmware incorporated in or provided with the designated equipment. Any modification hereto must be embodied in a writing signed by both parties. No modification hereof shall be effected by either party's use of a purchase order, acknowledgment, or other form containing additional or different conditions.

About This Guide

This guide provides descriptions of the software components, features, and capabilities of the Surveyor product, Release 2.4. It also contains detailed tutorials and examples that will enable you to install, configure, and run the Surveyor software.

On-line Help System

We have included an extensive, on-line Help system with the Surveyor software. The on-line Help system contains nearly all the tutorials and instructions contained in this guide *plus* additional examples and tips to help you get the most from your Surveyor. Be sure to browse on-line Help. From any location in the Surveyor program, and with just a few clicks of the mouse, you will find that you can locate the answer to almost any question you might have.

Specific task information is included in the on-line Help system that is not included in this manual.

Quick Start

Surveyor includes a Quick Start guide to get you up and running.

Contacting Shomiti Customer Support

There are several ways to contact Shomiti Systems if you need support.

Customer Support Phone	(408) 437-4059
Customer Support FAX	(408) 437-4041
Internet Address	support@shomiti.com
World-Wide Web	http://www.shomiti.com/
Mailing Address	Shomiti Systems, Inc. 1800 Bering Drive San Jose, CA 95112

Table of Contents

About This Guide	iv
On-line Help System	iv
Quick Start	iv
Contacting Shomiti Customer Support	iv

Chapter 1 Introduction

Surveyor Functions	1-2
Protocols Supported	1-4

Chapter 2 Installation

System Requirements	2-1
Installing Surveyor Over Windows 95 or Windows NT	2-2

Chapter 3 Getting Started

The Surveyor System	3-1
Launching Surveyor	3-1
Basic Navigation Tips	3-5
Buttons and Toolbars	3-11
Surveyor Toolbar	3-11
Module Toolbar (Summary View)	3-11
Detail View Toolbar	3-13
Data Views Toolbar	3-15
Capture Filter Toolbar	3-17
Display Filter Toolbar	3-18
Capture View Toolbar	3-19
File Formats	3-22
.CAP Extension – Capture Files	3-22

.NAM Extension – Name Table Files	3-22
.CFD Extension – Capture Filters	3-22
.DFD Extension – View Filters	3-22
.TSP Extension – Transmit Specifications	3-22
Providing a Name Table to Surveyor	3-23

Chapter 4 Configuring Surveyor

Configuring the Interface	4-1
Customizing Views and Windows	4-1
Setting the Monitoring View for a Module	4-2
Configuring Chart Views	4-2
Table Views	4-3
Protocol Color Coding	4-3
Setting Protocol Summary Information in Capture View	4-4
Setting Start of Elapsed Time in Capture View	4-4
Module Settings	4-5
Buffer Size	4-5
Packet Slice	4-6
Capture Buffer	4-6
Modes	4-7
Expert Symptoms	4-7
Expert Thresholds	4-8
System Settings	4-8
Configuring Ports to Scan	4-8
Configuring Remote Communications	4-9
Setting Update Timers	4-10
Configuring Counter Logging	4-11
Configuring Expert Logging	4-11
Configuring Alarms	4-12
Configuring Century 12-Taps	4-13
Setting the COM Port for Century 12-Tap	4-13
Settings for Explorer and Voyager	4-14
Resetting Explorer	4-14
Updating Explorer	4-14
Setting the Voyager Ports for Explorer	4-15

Advanced Configuration	4-17
SURVEYOR.INI File	4-17
Customizing Expert Diagnostic Information	4-17
Assigning Names to Protocols (Monitor)	4-18
Assigning TCP or UDP Ports to Protocol Parsers	4-22

Chapter 5 Resources and Modes

Resource Browser	5-1
Remote vs. Local Resources	5-2
Resource Protection	5-4
Modes	5-5
Synchronized Resources	5-7
Hints and Tips for Resources	5-8

Chapter 6 Views

Summary View	6-2
Detail View	6-5
Using Monitor + Capture Mode in Detail View	6-7
Capture View	6-8
Packet Editor	6-10
Data Views	6-11
MAC Statistics View (Rx)	6-11
MAC Statistics View (Tx)	6-12
Frame Size Distribution View	6-13
Protocol Distribution View	6-14
Utilization/Error View	6-16
Host Table View	6-16
Network Layer Host Table View	6-17
Application Layer Host Table View	6-20
Host Matrix View	6-22
Network Layer Matrix View	6-24
Application Layer Matrix View	6-26
VLAN View	6-28
Address Map View	6-29
Packet Summary View	6-29
Duplicate Address View (Expert only)	6-29
Expert View (Expert only)	6-30

Application Response Time View (Expert only).....	6-33
Hints and Tips for Using Views	6-33

Chapter 7 Capture and Display Filters

Activating Capture and Display Filters	7-2
Filter Parts and Structure	7-2
Structure	7-3
Frame Types	7-4
States.....	7-4
Statements	7-5
Actions.....	7-6
Filter Dialog Boxes	7-6
Filter Modes	7-8
Quick Mode	7-8
Advanced Mode.....	7-10
Filter Examples	7-11
Filter Example, Quick Mode	7-11
Filter Example, Advanced Mode.....	7-14
Rules of the Capture or Display Filter	7-16
Hints and Tips for Using Filters	7-16

Chapter 8 Transmit Specification

Transmit Specifications	8-1
Transmit Specification Dialog Box	8-2
Repeating Frames.....	8-6
Stream Modes	8-7
Bursts	8-8
Transmission Mode	8-8
Specifying Transmit Data	8-9
Packet Editor	8-9
Changing Fields Directly in the Dialog Box	8-10
Using Templates.....	8-11
Transmitting Capture Files	8-12
Transmit Specification Examples	8-12
Transmit Specification Example, Bursts	8-14
Hints and Tips for a Transmit Specification	8-15

Chapter 9 Alarms (Alarm Browser)

Alarm Browser	9-2
Alarm Editors	9-2
Alarm Groups	9-3
Alarms and Alarm Events.....	9-3
Thresholds and Alarms	9-4
Alarm Actions	9-4
Expert Alarms	9-5
Alarm List and Log	9-6
Hints and Tips for Alarms	9-7
Alarm Examples	9-7
Alarm Example, Utilization.....	9-7
Alarm Example, MAC Errors	9-8
Alarm Example, Frame Size	9-8

Chapter 10 Expert System

Expert Overview	10-1
Expert Views.....	10-1
Expert Symptoms and Diagnosis.....	10-2
Expert Alarms.....	10-6
Customizing Expert Diagnostic Information	10-7
Application Response Time.....	10-7
Application Layer	10-8
Excessive ARP	10-8
Excessive BOOTP	10-9
ICMP All Errors.....	10-10
ICMP Bad IP Header	10-11
ICMP Destination Host Access Denied	10-12
ICMP Destination Host Unknown.....	10-13
ICMP Destination Network Access Denied.....	10-14
ICMP Destination Network Unknown	10-15
ICMP Destination Unreachable	10-16
ICMP Fragment Reassembly Time Exceeded.....	10-17
ICMP Fragmentation Needed [D/F set]	10-18
ICMP Host Redirect	10-19
ICMP Host Redirect for TOS	10-20
ICMP Host Unreachable	10-21

ICMP Host Unreachable for TOS	10-22
ICMP Network Redirect	10-23
ICMP Network Redirect for TOS	10-24
ICMP Network Unreachable	10-25
ICMP Parameter Problem	10-26
ICMP Port Unreachable	10-27
ICMP Protocol Unreachable	10-28
ICMP Redirect	10-29
ICMP Required IP Option Missing	10-30
ICMP Source Quench	10-31
ICMP Source Route Failed	10-32
ICMP Time Exceeded	10-33
ICMP Time to Live Exceeded	10-34
NFS Retransmissions	10-35
Transport Layer	10-36
Non Responsive Station	10-36
TCP/IP Frozen Window	10-37
TCP/IP Long Ack	10-38
TCP/IP Retransmissions	10-39
TCP/IP RST Packets	10-40
TCP/IP SYN Attack	10-41
TCP/IP Zero Window	10-42
Network Layer	10-43
Duplicate Network Address	10-43
HSRP Coup	10-44
HSRP Errors	10-44
HSRP Resign	10-45
Illegal Network Source Address	10-46
IP Checksum Errors	10-47
IP Time to Live Expiring	10-48
ISL BPDU/CDP Packets	10-49
ISL Illegal VLAN ID	10-49
Unstable MST	10-50
OSPF Broadcasts	10-51
Network Overload	10-52
RIP Broadcasts	10-53
SAP Broadcasts	10-53
Total Router Broadcasts	10-53
MAC Layer	10-54
Broadcast/Multicast Storms	10-54
Excessive Broadcasts	10-55
Excessive Collisions	10-55

Excessive Multicasts	10-55
Illegal MAC Source Address.....	10-56
New MAC Stations.....	10-57
Overload Frame Rate.....	10-57
Overload Utilization Percentage	10-57
Physical Errors.....	10-58
Total MAC Stations.....	10-59
Hints and Tips for Expert Features	10-60
Summary of Expert Counters and Symptoms.	10-61

Chapter 11 Counters

Packet Counters.....	11-2
Custom Counters.....	11-2
Error Counters	11-2
Expert Counters	11-6
Counter Log File Overview	11-9
Log Directory Structure.....	11-10

Chapter 12 Utilities

Name Table Utility	12-1
Building a Name Table From the Network	12-4
NIS-to-Name-Table Conversion Utility	12-4
Sniffer™ Translator Utility.....	12-5
Get Version Information Utility	12-5
Module Identification Utility (CMM Only)	12-5
Logging Utilities.....	12-6
Export Utilities	12-6
Exporting Packets	12-6
Exporting Tables to CSV Format or Graphs to a Bitmap.....	12-7
Exporting to Optimal CSV Format	12-7
Exporting Counter Log Files to Excel.....	12-8

Appendix A Implementation Profile

Buffers.....	A-1
How Resources Use Buffers.....	A-2
Hardware Dependencies.....	A-5
About NDIS Mode.....	A-7
Captured Packets.....	A-7
Capture Rate / Transmit Speed.....	A-7
Counters.....	A-7
Transmit Specification.....	A-7
NDIS Configuration Options.....	A-8
Set Capture Buffer and Packet Slicing Size.....	A-8

Appendix B Standard Filter Elements

Appendix C Keyboard Shortcuts

Function Keys.....	C-1
From All Windows.....	C-1
From Summary View.....	C-2
From Detail View.....	C-2
From Capture View Window.....	C-2
From the Capture Filter Window.....	C-2

Appendix D Protocol Information

Protocol Reference Documentation.....	D-1
Protocol Display Colors.....	D-4

Appendix E Parser Names

Glossary

Index

List of Figures

- Figure 1. Selecting Ports to Scan for CMM1 and CMM2 Modules 3-2
- Figure 2. Using the Login Dialog Box 3-3
- Figure 3. Selecting a Module Port 3-4
- Figure 4. Selecting the Module Port and Speed 3-4
- Figure 5. Orientation to Summary View 3-5
- Figure 6. Display Detail View for a Resource 3-7
- Figure 7. Capture View of Buffer Contents 3-8
- Figure 8. Display Capture View for a Capture File 3-9
- Figure 9. Remote Host Connections 5-3
- Figure 10. Summary View Window 6-4
- Figure 11. MAC Statistics View (Capture) 6-12
- Figure 12. MAC Statistics View (Transmit) 6-13
- Figure 13. Capture Filter Window and Capture Filter Definition Example 7-12
- Figure 14. Example IF statement Dialog Box, Quick Mode 7-13
- Figure 15. Advanced Mode, Capture Filter Definition 7-14
- Figure 16. Example IF statement Dialog Box, Advance Mode 7-15
- Figure 17. Transmit Specification Dialog Box 8-3
- Figure 18. Transmit Specification Dialog Box, Packet Gaps 8-13
- Figure 19. Transmit Specification Dialog Box, Bursts 8-14
- Figure 20. Alarm Example, Utilization 9-7
- Figure 21. Alarm Example, MAC Errors 9-8
- Figure 22. Alarm Example, Frame Size 9-8
- Figure 23. Expert Overview Table Example 10-2
- Figure 24. Expert Overview Detail Table Example 10-3
- Figure 25. Expert Overview Host Summary Example 10-4
- Figure 26. Expert Analysis Table Example 10-5
- Figure 27. Expert Diagnosis Example 10-6
- Figure 28. Example Name Table Dialog Box 12-2
- Figure 29. Surveyor and Interface A-1
- Figure 30. Surveyor Capture and Real-time Buffers A-4

List of Tables

Table 1.	Surveyor Functions 1-2
Table 2.	Surveyor Functions Using Plug-In Modules 1-3
Table 3.	Supported Network and Application Protocols 1-4
Table 4.	Minimum System Requirements 2-1
Table 5.	Default Account Names, Passwords and Privileges 3-3
Table 6.	Hardware Device Properties 4-5
Table 7.	Default Names for Non-WKP TCP Ports 4-21
Table 8.	Default Names for Non-WKP UDP Ports 4-21
Table 9.	Data Views Supported in Primary Windows 6-2
Table 10.	Table Columns for Frame Size Distribution View 6-14
Table 11.	Table Columns for Protocol Distribution View 6-15
Table 12.	Table Columns for Host Table View 6-17
Table 13.	Table Columns for Network Layer Host Table View 6-19
Table 14.	Table Columns for Application Layer Host Table View 6-21
Table 15.	Table Columns for Host Matrix View 6-23
Table 16.	Table Columns for Network Layer Matrix View 6-25
Table 17.	Table Columns for Application Layer Matrix View 6-26
Table 18.	Table Columns for VLAN View 6-28
Table 19.	Table Columns for Address Map View 6-29
Table 20.	Table Columns for Duplicate Address View 6-30
Table 21.	Table Columns for Expert View, Analysis Table 6-31
Table 22.	Table Columns for Expert View, Overview Table 6-31
Table 23.	Table Columns for Detail of Expert Overview Counters 6-32
Table 24.	Table Columns for Application Response Time View 6-33
Table 25.	Expert Alarms 9-6
Table 26.	Summary of Expert Features 10-62
Table 27.	Alphabetical List and Descriptions of Ethernet Error Counters 11-3
Table 28.	Alphabetical List and Descriptions of Token Ring Error Counters 11-5
Table 29.	Alphabetical List and Descriptions of Expert Counters 11-6
Table 30.	NDIS, CMM1 and CMM2 Real-Time Functions A-5
Table 31.	NDIS, CMM1 and CMM2 Capture Functions A-5
Table 32.	NDIS, CMM1 and CMM2 Connectivity A-6
Table 33.	NDIS, CMM1 and CMM2 Transmit Functions A-6

Table 34.	Surveyor Filter Elements and Templates, Ethernet B-1
Table 35.	Standard Filter Elements and Templates, Token Ring B-6
Table 36.	Colors Used to Display Protocols in Surveyor D-4
Table 37.	Parser Names, DLC Suite E-1
Table 38.	Parser Names, Applications and Others E-1
Table 39.	Parser Names, Apple Talk Suite E-2
Table 40.	Parser Names, Banyan Suite E-2
Table 41.	Parser Names, Cisco Suite E-3
Table 42.	Parser Names, DECnet Suite E-3
Table 43.	Parser Names, Fujitsu Suite E-3
Table 44.	Parser Names, IBM Suite E-4
Table 45.	Parser Names, Internet Suite E-5
Table 46.	Parser Names, Internet Next Generation Suite E-6
Table 47.	Parser Names, Netware Suite E-7
Table 48.	Parser Names, PPP Suite E-7
Table 49.	Parser Names, XNS Suite E-8

1 Introduction

Surveyor is a powerful, integrated analyzer plus monitor application for 10/100 Ethernet and 4/16 Token Ring networks. Features such as multi-layer expert analysis, real-time network statistics, 7-layer packet decode and analysis, advanced alarm setting and actions, powerful multi-layer filtering, packet slicing and automatic name table updating provide users with both network analysis and monitoring tools in a single package.

Surveyor incorporates comprehensive real-time monitoring capabilities with the powerful troubleshooting capabilities of a protocol analyzer. These capabilities can function simultaneously, enabling a user to maintain the network using a single multi-purpose tool.

Surveyor monitors local network segments. An optional Remote software module gives Surveyor the capability to monitor remote segments as well.

Surveyor's user interface provides both a comprehensive view of the network as well as the ability to easily drill down to a specific network segment. Surveyor's main window provides a single, user-defined view for each of the segments being monitored. The user determines what information to view for each segment such as network utilization, protocol distribution, host table, etc. In this same window Surveyor enables the user to easily create alarms that monitor multiple segments simultaneously.

To focus on a particular segment the user need only double-click on that segment to unveil Surveyor's monitoring and troubleshooting tools. The user can simultaneously set capture filters, view full 7-layer decodes of captured packets and display multiple real-time MAC, network and application layer statistics in order to quickly understand the status and performance characteristics of the network segment. VLAN breakdowns, MAC, network and application layer matrices, and real-time packet decode summaries provide an extra layer of intelligence.

With the optional Expert plug-in module, Surveyor adds expert analysis and diagnosis of network problems. Potential error conditions are automatically logged. Counters, addresses, protocols, and diagnostic information related to the detected network condition are displayed.

For test and development environments, an optional Packet Blaster software module provides advanced traffic generation and intelligent packet and file editing capabilities.

Surveyor Functions

Surveyor provides you with tremendous flexibility in performing the tasks required to monitor and troubleshoot your network. As your Surveyor expertise grows you will find that the number of ways you can set up and apply the tool are virtually limitless. The basic functions of Surveyor are described in Table 1 below. Table 2 on the next page shows the additional functions available when you add Surveyor plug-in modules.

Table 1 Surveyor Functions

<i>Function</i>	<i>Description</i>
Capture	Capture data from a network and place it in the memory space (buffer) on a Century Media Module (hardware card). Surveyor lets you create and save special capture filters that direct Surveyor to capture only the information you want to view and analyze.
Capture View	Look at the data in a way that is useful for network analysis and troubleshooting. Surveyor lets you create and save special viewing filters. You use these filters to display only the information you want to analyze. The data can be viewed in numerous ways and from different perspectives. Display of the data can be either as graphical charts or row-and-column tables.
Save	Move captured data from a module memory buffer to a storage device on the Surveyor host PC. Surveyor enables you to store captured data onto your hard drive for later viewing, analysis, or transmission.
Log	Record counter information. Surveyor enables you to capture all byte, frame, and error counter values compiled during the capture or transmission of data.
Monitor	Real-time views for data seen on a network segment. The data can be viewed in numerous ways and from different perspectives. Display of the data can be either graphical charts or row-and-column tables.
Settings Alarms	Alarms can be set to flag network conditions. Actions can be performed when alarms are triggered.

Table 2. Surveyor Functions Using Plug-In Modules

<i>Function</i>	<i>Description</i>
Remote Functions (Require Remote plug-in)	All data collection and data management functions described in Table 1 are available from other devices in a distributed network.
Transmit (Requires Packet-Blaster plug-in)	Send data to a network. Surveyor lets you see what happens to your network under precisely controlled conditions. You can play back streams of captured data or you can transmit edited data. You can edit a stream of captured data by changing the sequence of the packets, deleting or adding (inserting) packets, creating bad packets, eliminating all packets of a certain type (protocol) and so on. Surveyor also gives you complete control of when, how fast, how long, and how often it transmits the data you want to send over the network.
Expert Analysis (Requires Expert plug-in)	Expert analysis starts with the automatic logging of possible problems. Expert data views display counters, addresses, protocols, and diagnostic information related to the detected network condition. Expert alarms can be set to flag network error conditions. Actions can be performed when alarms are triggered.

Protocols Supported

Table 3 lists the network and application protocols that Surveyor can encode/decode. For a listing of protocol specifications and information, refer to Appendix C.

Table 3. Supported Network and Application Protocols

<u>MAC Layer</u>	<u>IPX/SPX Suite</u>	<u>TCP/IP Suite</u>	<u>TCP/IP Suite, Cont.</u>
IEEE 802.2 (LLC)	Diagnostic	ARP	SMTP
IEEE 802.3	IPX	BGP (Version 4)	SNMP
Ethernet II	IPX EIGRP	BOOTP	TCP
IEEE 802.5	IPX PING	DHCP	TELNET
Loopback	IPX WAN	DNS	TFTP
SNAP	NBCAST	EGP	UDP
	NCP	FTP	UNIX Remote Services (lpr, rcp, rexec, login, rsh)
	NDP	GGP	
<u>Bridge Protocols</u>	NetBOIS	Gopher	WebNFS
IEEE 802.1D (Spanning Tree)	NLSP	HTTP	XDR
IEEE 802.1P	Packet Burst	HTTPS	XDMCP
IEEE 802.1Q VLAN	SAP	ICMP	Xwindows
	Serialization	IGMP	
<u>Cisco Suite</u>	SPX	IMAP	<u>Banyan Vines Suite</u>
CDP	SPXII	IMSP IP	VARP
DISL	Watchdog	LDAP	VICP
EIGRP		NetBIOS	VIP
HSRP	<u>DECnet Phase IV</u>	MIME	VIPC
IGRP	CTERM	MOUNT	VRPC
ISL	DAP	NFS	VRTP
VTP	DRP	NIS	VSSP
	FOUND	NNTP	
<u>IP Multicast Suite</u>	LAT	NTP	<u>Oracle Suite</u>
DVMRP	LAVC	OSPF	TNS (TCP/IP only)
IGMP	MOP	POP3	
MOSPF	NICE	PORT MAPPER	<u>Sybase Suite</u>
PIM-DM	NSP	RADIUS	TDS (TCP/IP only)
PIM-SM		RARP	
RSVP	<u>Microsoft</u>	RIP (Version 2)	
RTCP	NMPI	RPC	
RTP	SMB		
	SMB+ (CIFS)		

Table 3. Supported Network and Application Protocols

<u>AppleTalk Phase2</u>	<u>IPng</u>	<u>IBM Suite</u>	<u>XNS</u>
AARP	DHCPng	NetBEUI	Echo Protocol
ADSP	ICMPng	NetBIOS	Error Protocol
AEP	IDRPng		IDP
AFP	IPng	<u>SNA Protocol Suite</u>	NetBOIS over SSP
ASP	OSPFng	3270	PEP
ATP	RIPng	FDC	RIP
AURP	RSVPng	FID2	SSP
DDP		FM	
DDP EIGRP	<u>PPP Suite</u>	NC	<u>Applications</u>
LAP	PPPCHAP	SC	cc:Mail
NBP	PPPIPCP	XID	Lotus Notes
PAP	PPPIPX		
RTMP	PPPLCP	<u>Fujitsu Suite</u>	<u>Other</u>
ZIP	PPPNBFCP	FNA	Shomiti RSP
		LNDFC	(Remote Server Protocol)

2 Installation

System Requirements

The minimum system requirements for installing and running the Surveyor 2.4 software are shown in the table below.

Table 4. Minimum System Requirements

CPU	Pentium @ 100Mhz
Operating System Software	Windows 95 or Microsoft Windows NT 4.0 (with administrative privileges
Random Access Memory (RAM)	16MB (Windows 95) 32MB (Windows NT 4.0)
Video Display	800x600 or higher (SVGA)
Network Adapters	Century Media Module 1 (CMM1), Century Media Module 2 (CMM2), NDIS-compatible Ethernet adapter, or NDIS-compatible 4/16 Token Ring adapter card. <ul style="list-style-type: none">■ CMM1 or CMM2 boards require an available ISA slot.■ 10/100 Fast Ethernet Adapter Cards require a NDIS enhanced 16/32 bit driver.
Disk Space	15MB of free disk space. An additional 1MB is required for the Packet Blaster plug-in or Remote plug-in. An additional 2MB is required for the Expert plug-in.

Installing Surveyor Over Windows 95 or Windows NT

Begin by installing any local Century Media Modules and/or Ethernet adapter cards. Century Media Modules are packaged separately from the Surveyor software. Multiple modules may be installed in a single PC. *See the guide that comes with each Century Media Module for installation, set-up, and connection instructions.*

Perform the following steps to install the Surveyor software and to set up your PC to run the Surveyor software:

1. If you have previous versions of Century LAN Analyzer or Surveyor, remove those versions using the Windows Uninstall Wizard. The Uninstall Wizard should be available from the same menu where you installed the previous software version.

If you have created any Name Tables, Capture Filters, or Capture Files using a version older than 2.0, these files will not be deleted when you Uninstall the previous version. If you are installing into the same directory as the old version and you want to save these files, you must move these files to a new directory before you begin the new installation. Transmit Specifications from previous versions of Century LAN Analyzer are not compatible with Surveyor 2.0 or higher.

2. Install the Surveyor software.

Place Installation Diskette #1 in your diskette drive.

- a. Run A:\SETUP from the installation diskette. Approximately 15MB of free disk space is required to install the Surveyor software. Some additional disk space is required for each plug-in you install.
 - b. Follow the installation program instructions to install the software.
 - c. The installation software creates a program group called Shomiti Surveyor unless you choose to install in a different location. The program group contains the icon for launching Surveyor software. Other than making sure that the proper port is set for the Century Media Module, no configuration is required.
3. If you have purchased the Surveyor Remote, Packet Blaster, or Expert plug-ins, install these plug-ins now.
 - a. Place Installation Diskette #1 in your diskette drive.
 - b. Run A:\SETUP from the installation diskette. 1MB of free disk space is required to install a plug-in.
 - c. Follow the installation program instructions to install the software.
 4. Connect any local Century Media Modules or Ethernet adapters to the network.
 - a. For Century Media Modules, use a transceiver to connect to the 10/100Mbps Ethernet MII port, or directly connect to the 10/100BASE-T RJ45 port.
 - b. For the MII port, the speed can be set to 10Mbps or 100Mbps, or the port can be set to automatically detect the speed from the network.

NOTE: Be sure to note the base memory (port) address of each CMM module you install. The port address is required to configure Surveyor on start-up.

5. If you are going to use Surveyor to access remote resources, make sure the Surveyor software is installed at the remote host and the remote resources are connected to the network.

3 Getting Started

The Surveyor System

A complete Surveyor system consists of Surveyor software and at least one Century Media Module or NDIS-compatible Ethernet adapter. Multiple devices can be installed in the local host PC.


With the Remote plug-in you have access to other PCs containing NDIS adapters, Century Media Modules (CMMs), or other devices such as Explorer or Century 12-Tap. All remote devices must be properly installed before they can be accessed by Surveyor.

Launching Surveyor

You will need the base memory address of each port where you installed a Century Media Module 1 (CMM1) or Century Media Module 2 (CMM2). This information is necessary to configure Surveyor.

Perform the following steps to set up your environment and launch the Surveyor software:

1. Launch the Surveyor program.

Double-click on the  icon in the Shomiti Surveyor group or other group where you installed the Surveyor application.

2. The first time you launch Surveyor it displays the **System Settings** dialog shown in Figure 1 on the following page. You use this dialog box to tell surveyor which ports to scan to access the CMM1s and CMM2s you have installed on your system.

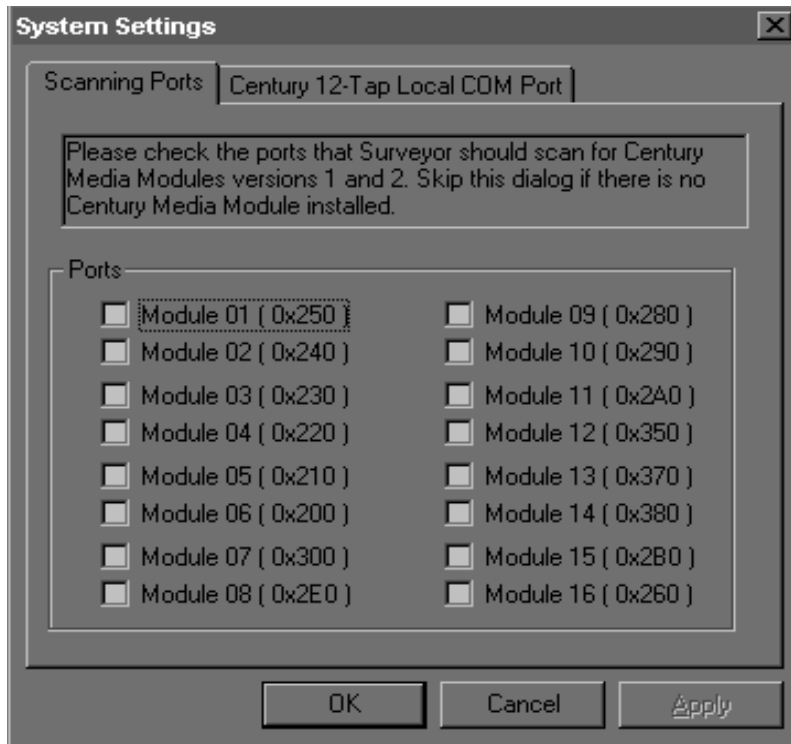


Figure 1. Selecting Ports to Scan for CMM1 and CMM2 Modules

Click the check box opposite the Module number that corresponds to base memory address of each port on which you have installed a CMM1 or CMM2. Do not select ports for devices other than CMM1s or CMM2s. Click **OK**.

You can change the ports to be scanned at any time. Select the **System Settings...** option of the **Configuration** menu to display the **System Settings** dialog box.

3. If you have the Remote plug-in, Surveyor displays the **Login** dialog box shown in the figure on the following page.



Figure 2. Using the Login Dialog Box

Surveyor provides two default accounts, **guest** and **su**. Table 5 shows the password and privileges associated with these accounts. Choose an account, complete the dialog box, and click **OK**.

Table 5. Default Account Names, Passwords and Privileges

<i>Default Account Name</i>	<i>Password</i>	<i>Privileges</i>
guest	public	full
su	manager	super-user

Normally, you can use either account to access all remote resources. If a remote resource will not permit access with either of these accounts, then get the user name and password from the resource owner and establish an account on that resource. To access a remote resource, you must have an account and password set up on the remote system containing the resource or use the remote system's guest account.

You can also password-protect local resources. See the section called "Protecting Local Resources" in the "Resources and Modes" chapter.

4. Select a Century Media Module or Ethernet adapter.

From the Resource Browser, click on the button that corresponds to the Century Media Module or Ethernet adapter that you want to control with the Surveyor software. The resource can be local or remote. A monitor window appears for the Century Media Module or Ethernet adapter you select.

5. If you selected a Century Media Module, select the port.

From the **Module** menu, choose **Interface** to set the port. Figure 3, on the following page, shows the **Module** menu and the **Interface** pop-up menu. On Board RJ45 selects the 10/100BASE-T port.

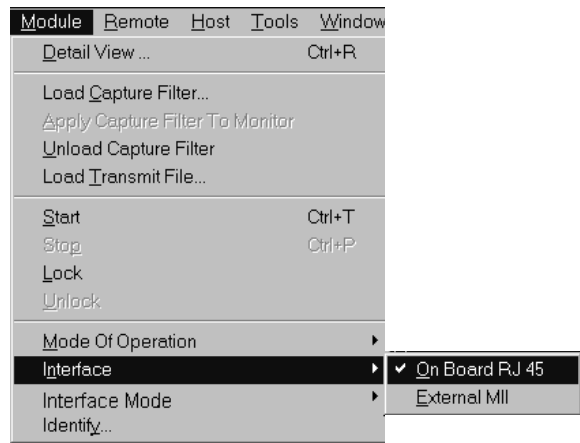


Figure 3. Selecting a Module Port

The MII port requires a 3rd party transceiver to connect to other Ethernet media types such as fiber, coaxial, and twisted-pair cable.

6. If you selected a Century Media Module, select the MII mode and speed.

From the **Module** menu, choose **Interface Mode** to set the port. The figure below shows the **Module** menu and the **Interface Mode** pop-up menu.

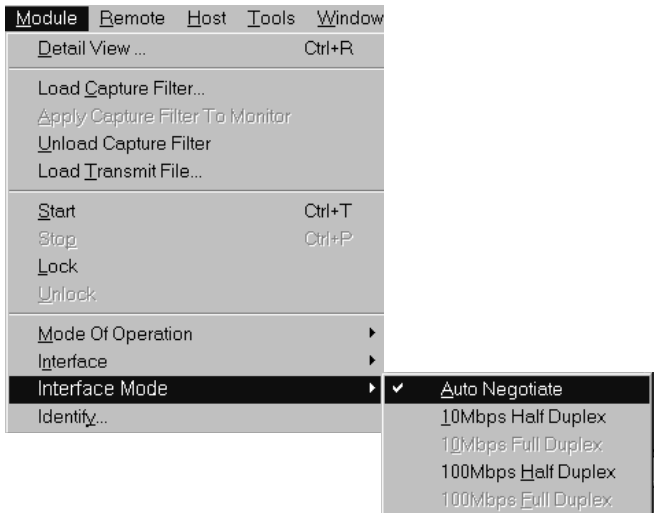


Figure 4. Selecting the Module Port and Speed

Auto Negotiate mode places the resource in auto-detection (10Mbps or 100Mbps) mode. The interface mode can also be set to only one speed. For CMM2s, the mode can also be set to Full Duplex.

After you have selected the port, speed, and MII mode for a Century Media Module you can begin using Surveyor.

Basic Navigation Tips

There are three main windows in Surveyor:

- Surveyor Main Window (Summary View)
- Detail View Window
- Capture View Window

Summary View is used primarily for monitoring, as it shows a single view of many different resources. It also contains the docking windows for selecting resources (Resource Browser), setting alarms (Alarm Browser), and viewing system messages (Message window). The figure below shows the **Summary View** window.

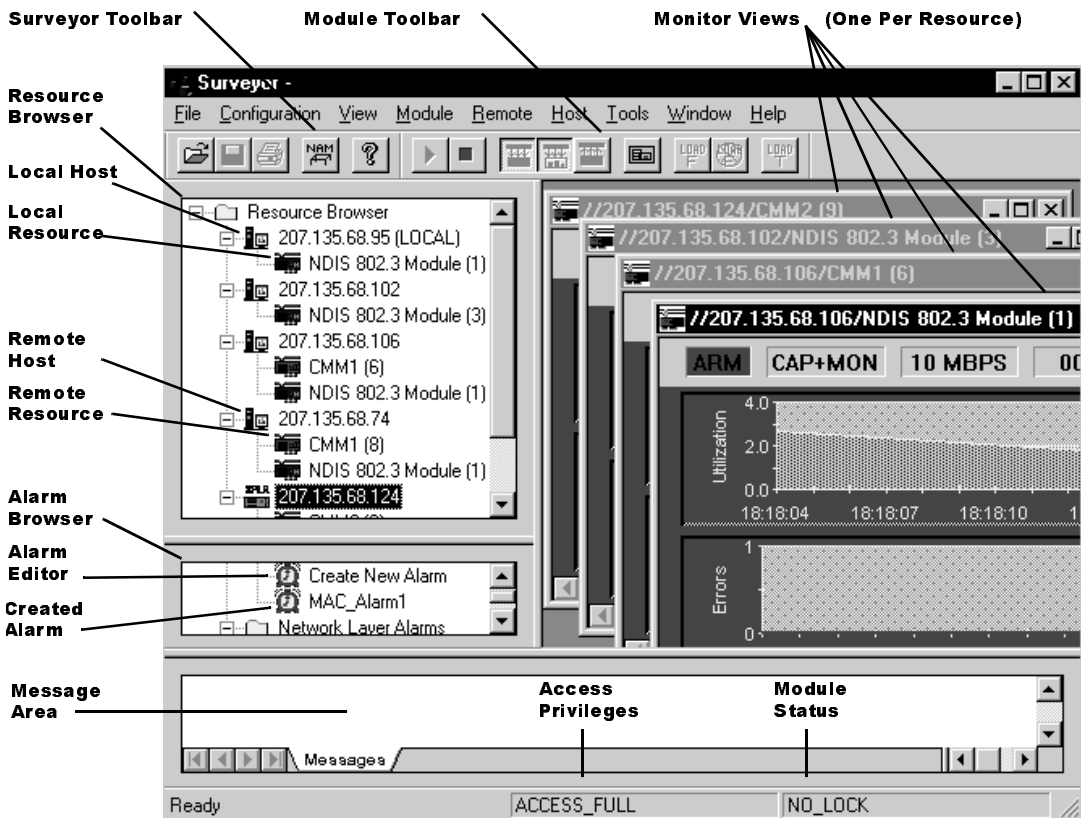



Figure 5. Orientation to Summary View

Detail View is primarily for analyzing data from a single resource. You can look at the data from Detail View in many different ways.

To display a resource in Detail View, click on (highlight) the resource icon in the Resource Browser. Press the  button to display Detail View for the resource. See Figure 6, on the following page, to see the **Detail View** window.

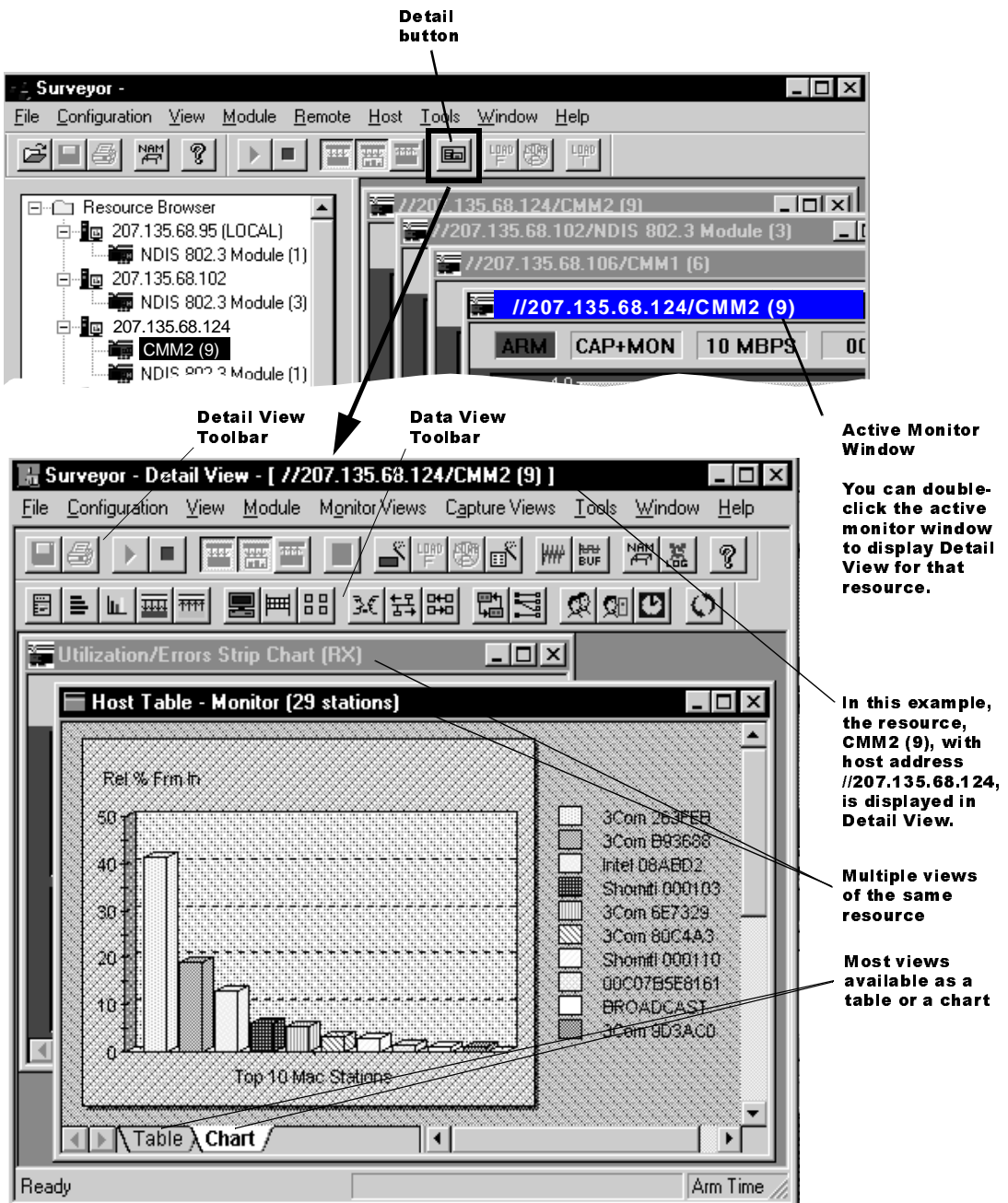


Figure 6. Display Detail View for a Resource


Once you have data to analyze, press  from Detail View to bring up Capture View. Capture View provides full decode of data in a capture buffer. Capture View opens as a window within Detail View.

Figure 7 shows Capture View when accessed from Detail View. The contents of the capture buffer are displayed in the **Capture View** window. Capture View has its own toolbar so you can view captured data in many different ways.

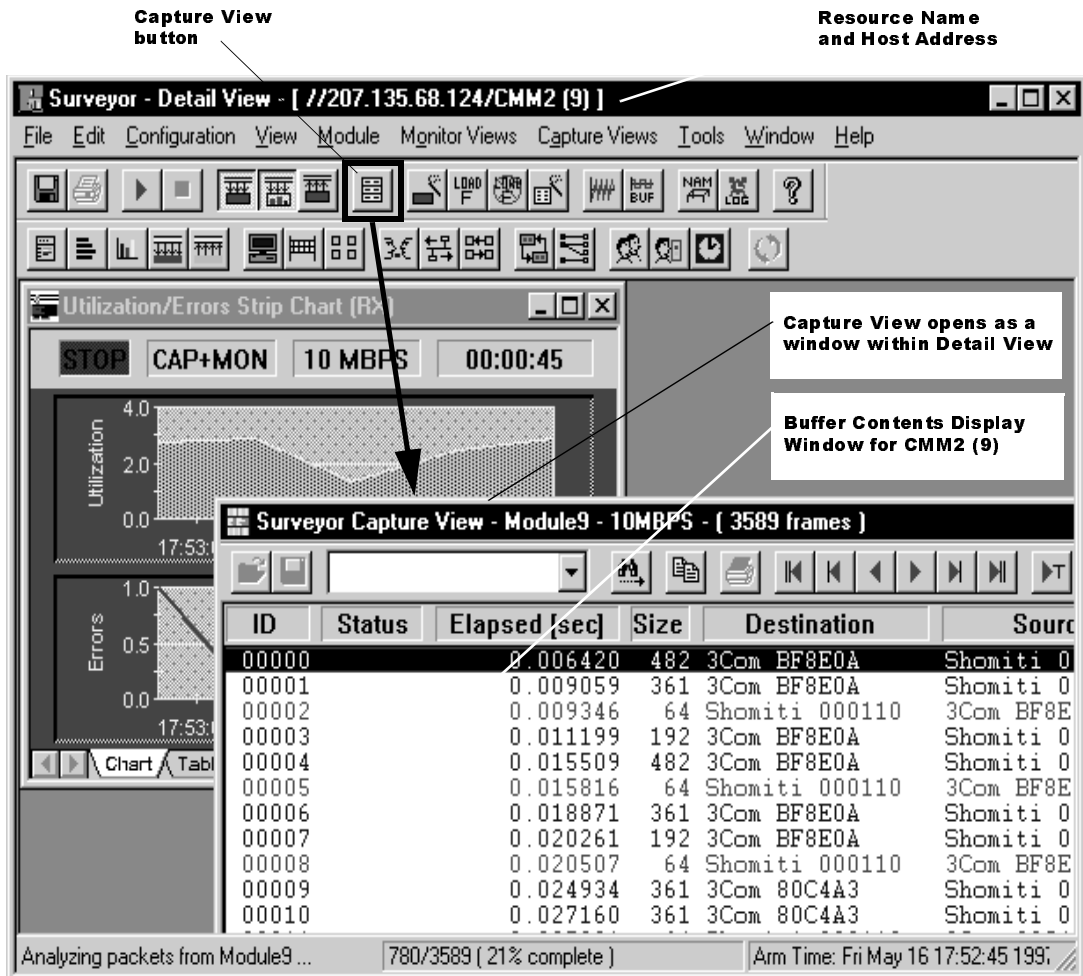



Figure 7. Capture View of Buffer Contents

You can also access Capture View from Summary View to view a Capture file. From Summary View, click the  button in the Surveyor toolbar. Figure 8 shows Capture View when accessed from Summary View. The contents of the Capture file are displayed in the Capture View window. Note that Capture View is displayed in a separate window.

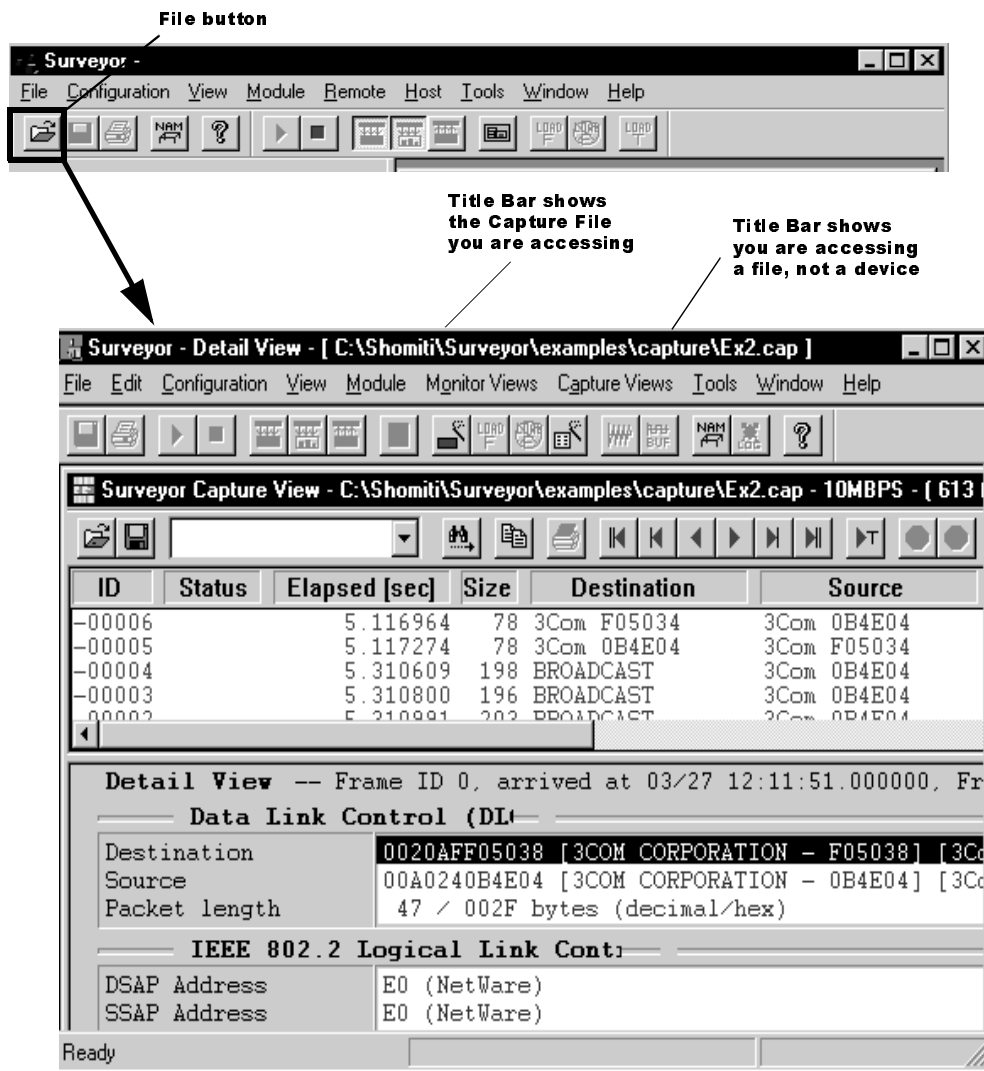








Figure 8. Display Capture View for a Capture File

You'll notice that many of the same functions can be performed from the different windows. This design allows you to perform all the tasks you might expect to do from any one of the major windows without having to switch to a different window.

Because of Surveyor's flexibility, you can open many different windows and subwindows within the program. To avoid confusion, it is recommended that you clean up windows you are not using.

Be sure to browse the Hints and Tips sections in the on-line Help system. There is a "Hints and Tips" section for all major functional areas within the product. Over time, you'll find the ways that you like to use the product the best. We encourage you to contact us and let us know so we can include these tips in the help system and pass these tips on to other customers and to user groups.

Here are ten tips to help you use the Surveyor interface:

- Click on a resource in the Resource Browser to select that resource.
- Press the  button to bring up Detail View for a resource. You can also bring up Detail View by double-clicking with the left mouse button on the active monitor view displayed within Summary View.
- Press the  button from Detail View to bring up the **Capture Filter** window. Use this window to create/edit capture filters.
- Press the  button from Detail View to bring up the **Display Filter** window. Use this window to create/edit display filters.
- Once a resource is stopped and you have captured data, press the  button in Detail View to bring up Capture View for analyzing packets and full protocol decode.
- Press the  button from Summary View to open a previously saved capture file and bring up Capture View.
- Use the buttons in the Data Views toolbar to open many views of the same resource within Detail View.
- Double-click on an alarm editor in the Alarm Browser to create an alarm group.
- Once the alarm group is created, drag and drop a resource from the Resource Browser onto an alarm group to assign the alarm group to that resource.
- If you have the Packet Blaster plug-in, use the  in Detail View to bring up the **Transmit Specification** dialog box to create data streams for transmit.

Buttons and Toolbars

Surveyor Toolbar



Open button

Opens a file, typically a capture file (.CAP). A dialog box displays showing all files with extension .CAP in the current directory. From the Summary Viewer, selecting a capture file to open will bring up Capture View.



Save button

Saves the current contents of the capture buffer to a file. A dialog box displays to select the file name and directory.



Print button

Prints the contents of the current view.



Name Table button

Brings up the **Name Table** dialog box for editing the current name table, saving a name table to a file, or loading a name table from a file.



Help button

Displays the help contents.

Module Toolbar (Summary View)



Start button

Starts a module. The module captures or transmits packets, depending on whether the mode is set to transmit or capture.



Stop button

Stops a module. The module ceases to capture packets or transmit packets.



Capture Mode button

Places the currently selected resource in capture mode. This button is gray if the resource is currently active (started).



Monitor Mode button

Activates the monitor functions for the currently selected resource. If the resource does not support monitoring functions, the resource is put into capture mode. This button is gray if the resource is currently active (started).



Transmit Mode button

Places the currently selected resource in transmit mode.



Detail View button

Brings up Detail View for the currently active resource.



Load Filter button

Brings up a dialog box to select a capture filter (.CFD extension). If a capture filter is opened, that filter is applied to the currently selected resource. This button is gray if the resource is currently active (started).



Unload Filter button

If a filter is loaded for the currently selected module, the filter is disabled. This button has no function if the currently selected resource is in transmit or monitor only mode. This button is gray if the resource is currently active (started).



Transmit button

Brings up a dialog box to select a transmit specification (.TSP extension) or a capture file (.CAP extension) for transmit. This button has no function if the currently selected resource is in capture or monitor mode. This button is gray if the resource is currently active (started).

Detail View Toolbar



Save button

Saves the current contents of the capture buffer to a file. A dialog box displays, allowing you to select the file name and directory.



Print button

Prints the contents of the current view.



Start button

Starts a module. The module captures or transmits packets, depending on the whether the mode is set to transmit or capture.



Stop button

Stops a module. The module ceases to capture packets or transmit packets.



Capture Mode button

Places the currently selected resource in capture mode. This button is gray if the resource is currently active (started).



Monitor Mode button

Activates the monitor functions for the currently selected resource. If the resource does not support monitoring functions, the resource is put into capture mode. This button is gray if the resource is currently active (started).



Transmit Mode button

Places the currently selected resource in transmit mode. This button is gray if the resource is currently active (started).



Capture View button

Selects Capture View mode for viewing captured information. You can see protocol decodes in this view. Capture View has its own toolbar to allow you to select other view of captured information.



Capture Filter button

Display the **Capture Filter** window. The window displays a previously opened filter or the default filter.



Load Filter button

Brings up a dialog box to select a capture filter (.CFD extension). If a capture filter is opened, that filter is applied to the currently selected resource. This button is gray if the resource is currently active (started).



Unload Filter button

If a filter is loaded for the currently selected module, the filter is disabled. This button has no function if the currently selected resource is in transmit or monitor only mode. This button is gray if the resource is currently active (started).



Display Filter button

Display the **Display Filter** window. The window displays a previously opened filter or the default filter.



Transmit Specification button

Brings up the **Transmit Specification** dialog box to define/load a transmit specification.



Transmit from Buffer button

Brings up a the dialog box to select a capture file and then load the capture file to the module for transmission.



Name Table button

Brings up the **Name Table** dialog box for editing the current name table or saving/loading a name table to/from a file.



Alarm List and Log button

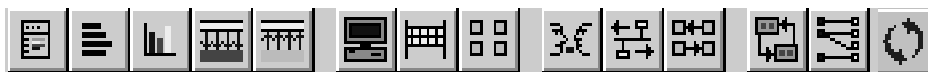
Brings up a table showing all alarm groups assigned to this resource. It lists alarm groups by name and identifies the type of alarm group, MAC, Token Ring, or Network.



Help button

Displays the help contents. Prints the contents of the current view.

Data Views Toolbar



(Expert only buttons)



MAC Statistics View button

Brings up MAC Statistics View for graphically viewing packet and error counters. This view also contains module and capture buffer status information. The view displays appropriate error counters depending on the mode, capture or transmit.



Frame Size Distribution View button

Selects Frame Size Distribution View for viewing the distribution of frame sizes.



Protocol Distribution View button

Selects Protocol Distribution View for viewing a chart of the distribution of major protocols. Control buttons in this view allow you to customize the way you view the protocol distribution.



Utilization/Error View button (Rx)

Brings up a strip chart that plots utilization and number of errors over time. The table for this view contains packet counters and error counters for receive.



Utilization/Error View button (Tx)

Brings up a strip chart that plots utilization and number of errors over time. The table for this view contains packet counters and error counters for transmit.



Host Table View button

Selects Host Table View for viewing information. You can see MAC stations and their associated traffic in this view.



Network Layer Host Table View button

Selects Network Layer Host Table View for viewing information. You can see network (IP/IPX) stations and their associated traffic in this view.



Application Layer Host Table View button

Selects Application Layer Host Table View for viewing information. You can see application stations and their associated traffic in this view.



Host Matrix View button

Selects Host Matrix View for viewing information. You can see all conversations between MAC stations in this view.



Network Layer Matrix View button

Selects Network Layer Matrix View for viewing information. You can see all network layer conversations and their associated traffic in this view.



Application Layer Matrix View button

Selects Application Layer Matrix View for viewing information. You can see all application conversations and their associated traffic in this view.



VLAN View button

Brings up VLAN view for viewing network traffic on virtual LANs. Cisco's ISL protocol is the only VLAN currently recognized.



Address Mapping View button

Brings up Address Mapping View for viewing associations between MAC station names and addresses and network station names and addresses.



Refresh button

Update the information in all open views.



Duplicate Address Button (Expert only)

Brings up a table showing all duplicate IP and IPX addresses. The duplicate network and MAC addresses associated each duplicate are displayed.



Expert View Button (Expert only)

Brings up a table showing all expert symptoms detected. There are two views of the expert information. The Analysis tab shows all expert symptoms detected. The Overview tab shows the total number of expert symptoms detected in each expert category.



Application Response Time Button (Expert only)

Brings up a table showing the applications detected and their minimum, maximum, and average response times. The number of connections for each application is also displayed.

Capture Filter Toolbar



Create Filter button

Creates a new filter. The default filter appears in the **Filter** window.



Open Filter button

Opens a filter. A dialog box displays to select the file. Capture filters are designated with an extension of .CFD files and display filters with an extension of .DFD.



Save Filter button

Saves the current contents of the **Filter** window to a file. A dialog box displays to specify the file name and directory. Capture filters are saved as .CFD files and display filters as .DFD files.



Print button

Prints the current contents of the **Filter** window.



Cut button

Cut the selected State or ELSE IF statement. The button does not work if other types of statements are selected.



Add button

Adds a new level if an ELSE statement or ROOT statement is selected. Adds a new ELSE if statement if a State or an IF statement is selected.



Show/Hide Detail button

Shows or hides the details of the current filter. Details are the number of filters used per state (maximum = 8) and the types of frames being captured for each IF or ELSE IF statement.



Load Filter button

Load the contents of the **Filter** window to the currently active module.



Disable Filter button

Disable the current capture filter. Subsequent starting of the module will capture all packets (use default filter).



Help button
Displays the help contents.

Display Filter Toolbar



Create Filter button
Creates a new filter. The default filter appears in the **Filter** window.



Open Filter button
Opens a filter. A dialog box displays to select the file. Capture filters are designated with an extension of .CFD files and display filters with an extension of .DFD.



Save Filter button
Saves the current contents of the **Filter** window to a file. A dialog box displays to specify the file name and directory. Capture filters are saved as .CFD files and display filters as .DFD files.



Print button
Prints the current contents of the **Filter** window.



Cut button
Cut the selected State or ELSE IF statement. The button does not work if other types of statements are selected.



Add button
Adds a new level if an ELSE statement or ROOT statement is selected. Adds a new ELSE if statement if a State or an IF statement is selected.



Show/Hide Detail button
Shows or hides the details of the current filter. Details are the number of filters used per state (maximum = 8) and the types of frames being captured for each IF or ELSE IF statement.



Turn ON Filter button
Use the contents of the **Filter** window as the display filter for all views. When viewing the capture buffer contents or a capture file in Capture View, all packets are filtered before display.



Turn OFF Filter button

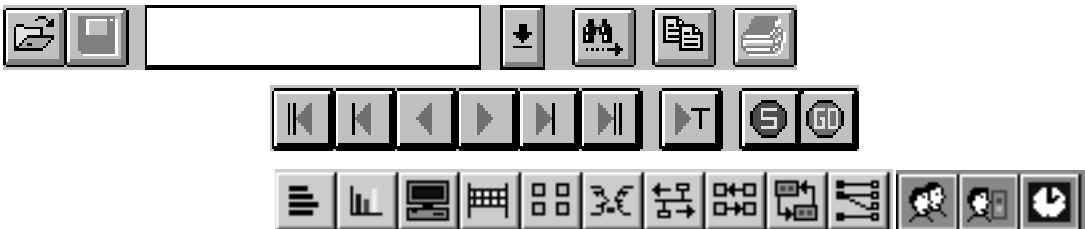
Disables the current contents of the **Filter** window as a filter for viewing. When viewing the capture buffer contents or a capture file in Capture View, all packets are displayed.



Help button

Displays the help contents.

Capture View Toolbar



Open File button

Opens a capture file (.CAP). A dialog box will display showing the current directory with all files with extension .CAP.



Save File button

Saves the current contents of this view to a file.



Search Box

Use the box to specify an ASCII text string for which to search. Once the string is entered, press the search button to the right of the search box.



Search button

Start search of the capture file contents for an ASCII text string. Specify the string in the search box to the left. The first instance of the string is found starting from the current position in the capture file.



Copy button

Copies the current contents of the **Summary** pane for pasting into other documents. A window displays with the text converted to ASCII format. Use the window to select the text you want and copy it to the clip board.



Print button

Print the currently selected line in the **Summary** pane.



Stop Load button

Capture files are loaded to Capture View as a background process. Pressing this button stops the background process. Press the Resume Load button to the right to resume the process.



Resume Load button

Capture files are loaded to Capture View as a background process. Pressing this button resumes the background process.



Go To Trigger button

Pressing this button moves you to the line in the capture file that was set as the trigger position. If no trigger position is set, this button moves you to the first captured frame.



Navigation buttons

Navigation buttons move you through the capture file. There are keys to go to the beginning and the end of the file, page up, page down, previous line, and next line.

Other buttons for views are the same as those in the **Data Views** toolbar.



Frame Size Distribution View button

Selects Frame Size Distribution View for viewing the distribution of frame sizes.



Protocol Distribution View button

Selects Protocol Distribution View for viewing a chart of the distribution of major protocols. Control buttons in this view allow you to customize the way you view the protocol distribution.



Host Table View button

Selects Host Table View for viewing captured information. You can see MAC stations and their traffic in this view.



Network Layer Host Table View button

Selects Network Layer Host Table View for viewing captured information. You can see network (IP/IPX) stations sorted according to the traffic variable you select in this view.



Application Layer Host Table View button
Selects Application Layer Table Host View for viewing captured information. You can see application stations sorted according to their names in this view.



Host Matrix View button
Selects Host Matrix View for viewing captured information. You can see all conversations between MAC stations in this view.



Network Layer Matrix View button
Selects Network Layer Matrix View for viewing captured information. You can see all network conversations for IP and IPX traffic in this view.



Application Layer Matrix View button
Selects Application Layer Matrix View for viewing captured information. You can see all application conversations in this view.



VLAN View button
Brings up VLAN view for viewing network traffic on virtual LANs. Cisco's ISL protocol is the only VLAN recognized.



Address Mapping View button
Brings up Address Mapping View for viewing associations between MAC station names and addresses and network station names and addresses.



Duplicate Address Button (Expert only)
Brings up a table showing all duplicate IP and IPX addresses. The duplicate network and MAC addresses associated each duplicate are displayed.



Expert View Button (Expert only)
Brings up a table showing all expert symptoms detected. There are two views of the expert information. The Analysis tab shows all expert symptoms detected. The Overview tab shows the total number of expert symptoms detected in each expert category.



Application Response Time Button (Expert only)
Brings up a table showing the applications detected and their minimum, maximum, and average response times. The number of connections for each application is also displayed.

File Formats

The following file formats are supported in Surveyor:

.CAP Extension – Capture Files

Capture files contain packets collected from the network. Capture file format is compliant with RFC 1761, referred to as “Snoop” format. However, capture files include extensions that expand the information provided by snoop format.

.NAM Extension – Name Table Files

Name table files contain equivalencies between symbolic names and hexadecimal names. The name table file format is identical to .ini file format. The default `hosts.nam` file contains names associated with well-known hexadecimal representations. For example, `BROADCAST=C000FFFFFFFF`.

.CFD Extension – Capture Filters

Capture filter files contain a set of instructions internal to Surveyor that tells the software to save only a subset of the all the information on the network.

.DFD Extension – View Filters

View filters files contain a set of instructions internal to Surveyor that tells the software to display only a subset of previously captured data. View filters are essentially the same as capture filters, except that they use capture files (.CAP files) as input rather than data being captured from the network.

.TSP Extension – Transmit Specifications

Transmit specifications contain a set of instructions internal to Surveyor that will generate packets. You can create transmit specifications and generate traffic if you have the Packet Blaster plug-in.

Providing a Name Table to Surveyor

A default name table file, `hosts.nam`, is included with the software. Surveyor boots using this default name table. If you wish to change the start up default name table, you must edit the `Surveyor.ini` file by following these instructions:

1. Locate the `Surveyor.ini` file in your Windows95 or WindowsNT directory.
2. Open the `Surveyor.ini` file with your text editor software.
3. Search for this line, `NameTable=C:\Shomiti\Surveyor\hosts.nam`.
4. Delete the `hosts.nam` text on that line.
5. Replace text with your default name table file. It should have the `.nam` extension.
6. Save the `Surveyor.ini` file, exit your editor and start Surveyor application.

Address and symbolic name associations can be discovered by Surveyor. This table can be saved as a file with the `.nam` extension and used as the default name table. Refer to Chapter 12 for more information on the name table.

*Note: The default name table can always be changed to another within the software by clicking on the **NAM** (Name Table button) and click **Open**. Find the name table file you want and Click **OK**.*

4 Configuring Surveyor

Configuring the Interface

In Surveyor, you can control the appearance of windows, the primary monitor view, the appearance of tables and charts, and the colors of decode displays. The following sections describe how to set up the interface to best meet your needs.

Customizing Views and Windows

The Surveyor windows interface is extremely flexible. It takes advantage of the features of Windows 95/NT to allow you to customize your interface.

Multiple windows can be opened within both Summary View and Detail View. These sub-windows can be minimized, maximized, expanded, reduced, and tiled within the area of the Summary or Detail View. You can open as many windows as you have resources in Summary View. You can have all available views of a single resource in Detail View. You can have many views windows open within Detail View, one for each resource.

Docking Windows

Summary View opens when Surveyor is started. The **Summary View** window is composed of Summary View area and three docking windows. The docking windows are:

- Alarm Browser
- Resource Browser
- Message View

You can size the docking windows by moving (click the left mouse and hold) the borders separating the windows. You can move the borders all the way to the edge of the **Summary View** window, thus hiding the docking windows. You can also completely close a docking window. If you close a docking window, use the options from the **View** menu to get the windows back.

You can extract any docking window from the **Summary View** window and make it a stand-alone window. If you turn off docking using the right mouse functions, the window will not dock again when it is moved back over the **Summary View** window, allowing you to cascade windows. You can also “float” a docking window within the main window. In effect, you can create your own customized view of all the windows available within the **Summary View** window.

Docking windows are a standard Windows 95/NT feature. Refer to the Windows documentation for a complete description of docking windows.

Setting the Monitoring View for a Module

One monitoring view is available for each module in Summary View. The first tab in the Summary View for a module displays the view selected.

1. In Summary View, choose **Module** from the **Configuration** menu.
2. Choose **Monitor View Preferences**.
3. Click the radio button in the **Monitor View Preferences** tab for the view you want. Only one view is allowed.
4. Click the **OK** button.

Configuring Chart Views

Protocol distribution view and frame size distribution view can be customized using buttons within the chart. The type of information in some chart views can be customized using the procedures below.

Charts graph the “top ten” stations or conversations based on a byte count. The count is the absolute percentage of the number of bytes out for stations, or the absolute number of bytes passed between stations for conversations. The count therefore provides a view of the stations or conversations with the most traffic, which is what users typically want to view. You can, however, create a “top ten” chart for any field that Surveyor supports. You can also reverse the sort order to create a “bottom ten” chart for any field that Surveyor supports.

1. In Detail View, make sure the view you want to customize is the currently active window.
2. Choose **Table** from the tab at the bottom of the view.
3. The data view appears as a table. Click on the column you want to use to create a “top ten” list. Note that the information in the table sorts in descending order for the column you selected. If the column you want is not there, see “Customizing Table Views” for information on how to insert a column into the table.

4. Click on the column again if you want to reverse the sort. This creates a view of the “bottom ten” stations or conversations.
5. Choose **Chart** from the tab at the bottom of the view to return to chart view.

Table Views

The type of information in some table views can be customized. You can add or subtract columns from the table.

1. In Detail View, make sure the view you want to customize is the currently active window.
2. Choose **View Options...** from the **Monitor Views** or **Capture Views** menu. If the **View Options...** selection is gray, no customization can be performed for this table.
3. Click the radio button for each column you want to display in the table.
4. Click the **OK** button.

Protocol Color Coding

Surveyor provides a real-time protocol decode called Packet Summary View and protocol decodes in Capture View. To use these displays more effectively, you may want to set the colors used for packet display. For example, you might want to display all transport layer packets in red and all other in black if you are looking only for protocol decode information in the transport layer.

To set up or change color coding for protocol decode, do the following:

1. Choose **System Settings...** from the **Configuration** menu. Select the **Protocol Color Coding** tab.
2. Click on a protocol layer.
3. Using the color buttons, set the foreground and background color display for the selected protocol.
4. Repeat as required for other protocol layers.
5. Make sure that the **Use Color Coding** box is checked.
6. Click the **OK** button.

Use the **Default All** button to return all color settings to their default values. Use the **Set Default** button to reset the default to the colors currently displayed.

Setting Protocol Summary Information in Capture View

When using Capture View, you can control the display of summary data for packet decoding. To use the summary display more effectively, you may want to view only the information for certain protocol layers in the Summary field. For example, you might want to display all information in the transport layer only. You may also want to include or exclude expert symptom information for each packet.

To set up or change layers to view for protocol decode, do the following:

1. Choose **Capture View Options** → **Display** from the **Configuration** menu.
2. Select the **Display Detail Protocol Summary** check box. If this box is not selected, all protocols are listed for the packet with no detail information.
3. Select the **Display Expert Symptoms** check box if you wish to include expert symptom information in the Summary field.
4. Select a protocol layer from the pull down menu.
5. Click the **OK** button.

Setting Start of Elapsed Time in Capture View

When using Capture View, you can control the display of summary data for packet decoding. To use these displays more effectively, you may want to set “time-zero” at a specific frame number rather than at the beginning of capture. For example, you might want to start elapsed time stamps at frame 5,000 rather than when the module is started.

To change the starting point for elapsed time, do the following:

1. Choose **Capture Display Options** → **Display** from the **Configuration** menu.
2. In the **Elapsed Time Set Mark Option** portion of the **Display Options** dialog box, select **Frame ID nnn's Arrival Time**. Set the frame ID number in the box. The default option is **Module Arm Time**, which starts time zero at the time the module is started.
3. Click the **OK** button.

Module Settings

Module settings configure options for the capture and monitor functions of devices. To configure modules, select **Module Settings...** from the **Configuration** menu. Tabs appear that apply to the currently active device type; a tab will only appear if this option can be set for the current device type. Hardware devices can have properties set according to the table below:

Table 6. Hardware Device Properties

<i>Hardware Device</i>	<i>Buffer Size</i>	<i>Packet Slice</i>	<i>Capture Buffer</i>	<i>Full Duplex</i>	<i>Expert Mode</i>	<i>Expert Symptoms</i>	<i>Expert Thresholds</i>
CMM1	NO	NO	YES	NO	YES	YES	YES
CMM2 or Explorer	NO	YES	YES	YES	YES	YES	YES
NDIS	YES	YES	YES	NO	YES	YES	YES

The Shomiti Voyager probe does not have any module settings. The **Module** choice will be grayed out on the **Configuration** menu for Voyager.

Default values for Module Settings:

Buffer Size	512K
Packet Slicing Size, Capture	Full packet length
Packet Slicing Size, Monitor	Full packet length (for CMM), 128 bytes (for NDIS)
Enable Full Buffer Auto Save	Not selected
Allow Full Duplex Mode	Not selected
Enable Expert Analysis Mode	Selected (must have the Expert plug-in installed)
Expert Symptoms	All symptoms enabled
Expert Threshold	Each threshold has its own default value

Buffer Size

NDIS modules require that a capture buffer size be set. The buffer size is the amount of system memory that will be used to save captured data. Buffer sizes can be set between 64K and 16M in multiples of two. Century Media Modules have a hardware buffer and do not require system memory for captured data. The default buffer size is 512K.

Packet Slice

CMM2 and NDIS support slicing packets. Packet slicing means that a subset of the entire packet is saved in the capture buffer. You can save the first 32 bytes (Mac layer), the first 64 bytes (Network layer), the first 128 bytes (Application layer) or the full length of the packet.

Packet slicing can be set separately for monitor and capture. For monitor, packet slicing can improve performance when monitoring the entire packet contents is not required. For capture, packet slicing can save space in the capture buffer for more packets when analysis of the entire contents of each packet is not required.

For CMM Modules, the default is no packet slicing (full packet length). For NDIS modules, the default setting is no packet slicing for capture, 128-byte packet slice for monitor.

Capture Buffer


All local devices support a save-to-disk function for the capture buffer. Check the **Enable Full Buffer Auto Save** box to enable the save-to-disk feature. When using the save-to-disk feature, capture is stopped when the buffer is full and the contents are written to disk. Capture is restarted as soon as the data is written to the file. When the capture buffers fills again, the new contents are appended to the file. If you start a new capture, the file is overwritten. If capture is stopped before the capture buffer contents are full, the buffer contents are not automatically written to disk; you must manually save the file to disk.

***CAUTION:** Save-to-disk is available for local modules only. If you intend to use this feature make sure the local host has the disk space required to store the data you want to save to disk. You can limit the size of the file by entering a value in the **Max File Size** field and prevent continuous capture from using all your disk space.*

Modes

Select the **Modes** tab from the **Configuration → Module → Settings...** to set the modes for a module.

Full-Duplex Mode

CMM2 modules can be enabled to function in full-duplex mode. CMM2 modules appear in the Resource Browser with the following icon:  CMM2. If full-duplex is enabled, both the capture and the transmit mode buttons may be set at the same time. The capture buffer memory within the CMM2 is allocated to both transmit and capture functions, one-half the memory allocated to each. Check or uncheck the box to enable or disable full duplex mode. The tab for is context sensitive and is only visible if the device is a CMM2. Select the **CMM2** tab from the **Configuration → Module → Settings...** menu to enable full-duplex mode for CMM2. The default is full-duplex not enabled, which means the CMM2 will only function in half-duplex mode.

Expert Analysis Mode

Expert Views and Alarms can be disabled. If disabled, no Expert Views or Alarms will display in Surveyor software.

Uncheck the **Enable Expert Analysis Mode** box to disable Expert Views and Alarms. The default is to enable Expert Analysis. If you do not have the Expert plug-in module, you will not be able to enable Expert Analysis Mode.

Expert Symptoms

Select the **Expert Symptoms** tab to set which expert symptoms will be recorded and counted in Surveyor's expert views. Use the check boxes to enable/disable any expert symptom. If Expert Analysis Mode is disabled, this tab will not appear in the **Configuration → Module → Settings...** menu. No symptoms are counted if Expert Analysis mode is disabled.

The default is to have all symptoms recognized and counted. If the MAC Layer or Network Layer symptoms are disabled, then all expert symptoms for the protocol layer are disabled.

The setting for TCP/IP Retransmissions enables the Non Responsive Stations expert symptom.

Expert Thresholds

Many expert symptoms have a threshold. When the threshold is exceeded, the event is recorded and counted in Surveyor's expert views. You can set these thresholds higher or lower from the **Expert Thresholds** tab.

Select the **Expert Thresholds** tab from the **Configuration → Module → Settings...** menu to set thresholds for recording and counting expert symptoms. If values exceed the levels set in this dialog box for an expert symptom, the expert symptom will be counted on the **Expert Overview** tab and recorded in the **Expert Analysis** tab of Expert View.

If Expert Analysis mode is disabled, this tab will not appear in the **Configuration → Module → Settings...** menu. No symptoms are counted if Expert Analysis mode is disabled. Thresholds cannot be set for an expert symptom if that symptom is disabled in the **Expert Symptoms** tab. If an expert symptom is disabled, it will be grayed in the **Expert Thresholds** tab.

Default thresholds for expert symptoms are shown below:

Utilization (%)	40
Bcast/Mcast (Pkts/Sec)	400
Errors (Pkts/Sec)	400
MST Topology Change (Pkts/Sec)	5
TCP/IP SYN Attack (Pkts/Sec)	100
TCP/IP Frozen Window (in Sec)	5
TCP/IP Long Ack (in MilliSec)	200
Non-Responsive Station (TCP Retrans)	3
BOOTP Requests (Pkts/Sec)	10
ARP Broadcast (Pkts/Sec)	10

System Settings

System settings establish general timing, file, and port information for the Surveyor system.

Configuring Ports to Scan

Surveyor must search the ports on the local system to find Century Media Modules. Sometimes this creates a problem with certain devices already on the system. Use this function to restrict the ports which are scanned. The dialog box for configuring ports to scan comes up on Surveyor start-up; ports to scan is typically configured at start-up, but can be changed from surveyor at any time.

You can use Surveyor to set the ports on the PC to scan at any time. To set up or change port scanning, do the following

1. Choose **System Settings...** from the **Configuration** menu. Select the **Scanning Ports** tab.
2. A dialog box appears showing the ports within the local system. Check the box of only those ports you want Surveyor to scan for a Century Media Module.
3. Click the **OK** button.

Configuring Remote Communications

The remote server protocol (RSP) is used to control the interface for connecting with remote systems. You configure the options that effect connection time outs, encryption of control packets, and auto-discovery of resources.

To configure the timers, select **System Settings...** from the **Configuration** menu. Select the **Remote Communications** tab.

Encrypt RSP Packets check box Select **encryption** if there is a need for security in the network when transferring packets between the remote resource and the local system. This is only necessary if high level of security is required on your network for the access of devices.

No Autodiscovery check box Select this box to prevent auto-discovery of remote resources. If selected, you will only be able to access remote resources by manual discovery of resources using the **Connect** option from the **Host** menu. This box can be selected when working with only local resources to eliminate viewing all resources in the Resource Browser. The auto-discovery of resources may take some time, especially in a large network.

RSP Time Out value Specifies in seconds how long the protocol waits before dropping a connection when the remote resource is not responding. The value must be between 1 and 30 seconds.

The default settings are as follows:

Encrypt RSP Packets check box Not selected

No Autodiscovery check box Not selected

RSP Time Out Value 10 seconds

Setting Update Timers

Timers control how often counters, tables, and displays are updated. There are two types of timers, display timers and polling timers. Polling timers control how often data is updated from remote systems. Display timers control how often displays of data are updated in the Surveyor software. All timer values are in seconds.

To configure the timers, select **System Settings...** from the **Configuration** menu. Select the **Timers** tab.

Polling Timers

MAC Layer Counters	Sets the interval for polling devices for MAC layer counters.
Network Layer Counters	Sets the interval for polling devices for network layer counters.
Host Table	Sets the interval for polling devices for MAC layer host table information.
Conversation Matrix	Sets the interval for polling devices for information on MAC, network, and application layer conversations.
Expert Data	Sets the interval for polling devices for expert data.
Remote Name Table	Sets the polling interval for refreshing the local copy of the name table for a remote resource.

Display Timers

Monitoring View, Local	Sets the time between refreshing counters in displays of counter data for resources in the local PC. This display timer is available for strip charts only.
Monitoring View, Remote	Sets the time between refreshing counters in displays of counter data for resources in remote hosts.

The values for polling timers must be between 1 and 214783647 seconds. The values for the display timers must be between 1 and 214783647 seconds. The display timers must be a multiple of the polling timers.

The default settings, in seconds, are as follows:

MAC Layer Counters	3
Network Layer Counters	5
Host Table	7
Conversation Matrix	10
Expert Data	15

Remote Name Table	300
Monitoring View, Local	1
Monitoring View, Remote	3

Configuring Counter Logging

Counter log files contain snapshots of Surveyor counter information. All MAC layer statistics can be recorded in the log file.

To configure counter logging, select **Log File Settings...** from the **Configuration** menu.

To enable counter logging, check the **Enable Logging** field. Set the time interval for capturing counter information in the **Time Interval** field. Set the number of rows (line entries) in the log file in the **Log File Maximum Rows** field. For example, setting **Log File Maximum Rows** to 4,000 and **Time Interval** to 5 will record the counter information 4,000 times, once every 5 seconds.

Keep the **Keep History Log** box selected to create history files of counter information. The history file is written when all lines in the log file are full. When a history file is created, the module log file is erased and new counter information is recorded starting with the first line of the file. History files are named by date and time. The format for the name of history files is:

```
mmddhhmm.ss
```

```
mm(month) dd(day) hh(hour) mm(minute) ss(second)
```

The minimum time between creation of unique history files is one second. If you disable the creation of history files and the log file for the module is full, a new log entry causes the module log file to be erased and no history of counters is saved.

The default settings are as follows:

Enable Logging	Not selected
Time Interval	5 seconds
Log File Maximum Rows	4,000
Keep History Log	Selected

Configuring Expert Logging

Expert log files contain entries of Surveyor expert events. All expert symptoms discovered by Surveyor are recorded in the log file. Entries in the expert log file are in ASCII text format.

To configure expert logging, select **View Options...** from the **View** menu. **You must have the Expert View analysis table active to configure the log file.**

To enable expert logging, check the **Log Entries to File** box. Specify the name of the log file in the **File Name** field. Log files are given a `.log` extension if no log extension is specified. Leave the **Clean Contents When Rearm** box checked to clear the log file of old entries when a capture is restarted.

No history files are created for the expert log file. When the log file fills with entries, additional entries will begin to overwrite entries in the file. Select the maximum size of the log file in the **Maximum Log File Size (MB)** field.

The default settings are as follows:

Log Entries to File	Selected
File Name	... \Shomiti \Surveyor \Log \Expert .txt
Clean Contents When Rearm	Selected
Maximum Log File Size (MB)	10

Configuring Alarms

Alarms can be configured to generate events such as e-mail messages, pages, or logging messages to a log file. E-mail recipients, pager recipients, and log file names are global parameters that you set. All alarms are automatically sent to one set of e-mail addresses and one log file.

The alarm E-mail feature works only with Microsoft Mail Exchange.

To configure alarm actions, select **Alarms** from the **Configuration** menu and then select either **E-Mail Settings**, **Pager Settings**, or **Log File Settings** from the submenu.

E-mail Settings	The set of e-mail addresses that will receive mail if an alarm triggers an event with the alarm action set to e-mail . When you click on the Add Recipients button in the menu you can set up e-mail addresses using Microsoft Mail's address book.
Pager Settings	The pager number that will receive a page if an alarm triggers an event with the alarm action set to pager . The other settings for the pager depend on the type of pager. For pager settings, you must set the delay to at least 3 seconds.
Log File Settings	The name of the log file that will have an entry if an alarm triggers an event with the alarm action set to log .

Configuring Century 12-Taps

A Century 12-Tap can be attached to the local system or be available as a remote resource on the network. Typically a Century 12-Tap will be used in the wiring closet with an Explorer and accessed as a remote resource. However, Century 12-Taps can be attached to the local system and accessed through a COM port on the PC. See “Setting the COM Port for Century 12-Tap” for information on configuring Century 12-Tap to talk to a local PC.

Century 12-Taps are devices that work in conjunction with an Explorer to monitor multiple network segments. When the Century 12-Tap is connected properly with an Explorer, its icon will be visible in the resource browser. If you cannot see the Century 12-Tap icon, refer to the Explorer and Century 12-Tap hardware documentation for more information on connecting Century 12-Taps and Explorers to the network.

Although the Century 12-Tap shows as a resource to the Surveyor software, it does not directly perform monitoring and other analysis functions. Century 12-Tap acts as a switching device for Explorer (or Century Media Modules), so one Explorer can be used to view many different LAN segments, one-at-a-time.

The Surveyor software can be used to control which LAN segment is selected by the Century 12-Tap. To set the LAN segment:

1. Double-click on the **Century 12-Tap** icon in the resource browser.
2. A list box appears showing the twelve port-pairs on the Century 12-Tap, numbered 1 to 12. You must know which LAN segments are connected to the port-pairs on the Century 12-Tap. Use the radio buttons to select the LAN segment you wish to monitor with Explorer. Only one LAN segment can be selected.
3. Use the **Bypass** check boxes to set any network segments that you want to restrict from being used with Explorer. Any segment with the **Bypass** box checked cannot be set as the LAN segment for Explorer.
4. Click the **OK** button.

Setting the COM Port for Century 12-Tap

The Century 12-Tap can be controlled from a PC running Surveyor software. The Surveyor software can be used to control which LAN segment is selected by the Century 12-Tap. The Century 12-Tap is often connected through an Explorer and viewed in the Resource Browser as a remote device. However, the Century 12-Tap can be connected to a COM port on the PC and controlled as a local resource from Surveyor. In this configuration, the COM port used to connect Century 12-Tap to the PC must be configured in Surveyor software.

To configure the COM port, select **System Settings...** from the **Configuration** menu. Select the **Century 12-Tap Local COM Port** tab. Set the COM port value to the COM port where the Century 12-Tap is connected to the PC. Just one port can be selected.


The Century 12-Tap is connected to the PC using a standard 9-pin serial cable.

Settings for Explorer and Voyager

You can use Surveyor to control Explorer. You must have “super-user” privileges to reset or update Explorer devices or change Voyager port settings

Resetting Explorer

The Explorer device can be reset from Surveyor software. To reset Explorer do the following:

1. Login to Surveyor with “super-user” privileges.
2. Click on the Explorer icon  in the Resource Browser.
3. Choose **Description** from the **Host** menu.
4. Click the **Reset Explorer/Image Upgrade** button.
5. Check the **Warm Boot** radio button under **Reset Options**. Leave all other fields blank or unmarked.
6. Click the **OK** button.

When you reset Explorer, you will lose the connection. Use the **Connect** option from the **Remote** menu to reconnect with Explorer.

Updating Explorer


You can update the software or change address information for an Explorer from Surveyor.

Before you can reset Explorer with a new image, you must place the new image on a server that runs TFTP protocol. Download the new software from Shomiti's Web site, <http://www.shomiti.com>. Go to the software updates section of the Web site to find the new Explorer image. Place the software on the server that runs the TFTP protocol.

Before you can update Explorer address information automatically, you must have a server that contains the new address information and runs the BOOTP protocol.

Use the following procedure to update Explorer.

1. Login to Surveyor with “super-user” privileges.

2. Click on the **Explorer**  icon in the Resource Browser.
3. Choose **Description** from the **Host** menu.
4. Set the new IP Address, IP Gateway Address, and Subnet Mask for Explorer. If no address update is needed, or you are updating the address from a BOOTP server, skip this step.
5. Click the **Reset Explorer/Image Upgrade** button.
6. Check the **Enable BOOTP** box if you are updating addresses from a BOOTP server.
7. Check the **Image Upgrade (TFTP)** box if you are updating addresses from a TFTP server.
8. Enter the IP address of a server that runs BOOTP and/or TFTP protocols in the **IP Boot Server** field.
9. If you are updating the Explorer image, set the path name to the software image file in the **Boot Image Filename** field.
10. Check the **Warm Boot** radio button under **Reset Options**.
11. Click the **OK** button.

***CAUTION:** You must use the **Warm Boot** option for Explorer to load the new image from the network. The **Cold Boot** option will not update the image.*

When you reset Explorer, you will lose the connection. Use the **Connect** option from the **Remote** menu to reconnect with Explorer.


When Explorer is restarted, the new software image is written to non-volatile memory in the Explorer and becomes the new executable image.


Use the **Cold Boot** option to force Explorer to run its self-tests to verify the unit is operating properly, but not as part of the update procedure.

Setting the Voyager Ports for Explorer

Surveyor supports a new multi-port RMON/RMON2 probe available from Shomiti called Voyager.

If the Explorer device is connected to a Voyager probe, you can set the port-pair mirrored to Explorer. At least one analyzer port on the Explorer must be connected to one Tap Port on Voyager; both analyzer ports may be connected to Voyager Tap Ports A and B. Setting the port-pair changes the segments connected to Voyager which are mirrored to Explorer through its Tap ports. To set or change the Voyager port-pair, do the following:

1. Login to Surveyor with "super-user" privileges.
2. Click on the Explorer  icon in the Resource Browser.

3. Click on the Multi Port Tap icon  in the Resource Browser. If Explorer is not connected properly to Voyager, this icon will not appear.
4. Select the port-pair from the menu. Only those port-pairs present on the Voyager hardware device will display. Ports are selected in pairs even if only one Voyager port is connected to a network segment or if only one Tap port is connected to Explorer.
5. Click the **OK** button.

This procedure does the same thing as pressing the ADVANCE button on the Voyager device until the desired port-pair is mirrored to the Tap ports.

Port numbers not physically present on Voyager will be gray. A selectable port-pair does not indicate that a link has been established from either Voyager port to a network segment, or whether the port-pair is in full-duplex or half-duplex mode. Refer to your *Voyager User's Guide* for information on making the proper connections to Explorer other information on setting up Voyager.

Advanced Configuration

SURVEYOR.INI File

The SURVEYOR.INI file contains Surveyor's configuration settings. You can save different sets of configuration information in different `.ini` files if you want to run the product with different configurations. Surveyor always looks for the file named SURVEYOR.INI in the `\Windows` directory and will use that file for its configuration. If no SURVEYOR.INI file is found in the directory, Surveyor will build another SURVEYOR.INI file based on the factory default configuration settings.

Different sets of configuration information can be especially useful for display and update timers. The first eight parameters of the SURVEYOR.INI file are the configuration values for the various display timers.

```
Counter Timer Value=3
```

```
Network Counter Timer Value=5
```

```
Host Timer Value=7
```

```
Matrix Timer value=10
```

```
Expert Timer Value=15
```

```
Remote Name Table Timer Value=300
```

```
Display Timer Value=3
```

```
Local Display Timer Value=1
```

For information on other SURVEYOR.INI settings, contact Shomiti Customer Support. It not recommended that you alter the SURVEYOR.INI file directly.

Customizing Expert Diagnostic Information

The `Expertmsg.ini` file contains Surveyor's diagnostic information. You can change the diagnostic information if you want. Surveyor always looks for the file named `Expertmsg.ini` in the Surveyor installation directory and will use that file for its diagnostic information. If no `Expertmsg.ini` file is found in the directory, Surveyor will not provide diagnostic information.

Changing the diagnostic information may be a useful way to customize Surveyor for your environment. For example, if you have a known problem area to check when certain conditions occur you can include this information directly in the diagnostic information.

Assigning Names to Protocols (Monitor)

Surveyor assigns names to protocols that have been detected, providing users with an easy way to view what protocols have been discovered on the network. In most cases, protocol names are well known; they are defined by the protocol's creator, or defined by a standards organization. However, you may want explicit information about a protocol that does not have a well known name or is counted in Surveyor monitor screens as a "TCP OTHER" or "UDP OTHER" protocol.

Surveyor includes a MONITOR.INI file to assign names to protocols. Entries in the MONITOR.INI file allow you to:

- Rename the protocols that are currently being detected. For protocols that use TCP or UDP as their transport protocol, the protocol can be assigned a name to override its default name.
- Extend the list of protocols that are monitored by Surveyor. You can extend the monitoring of protocols that use TCP or UDP as their transport protocol.

See the next section on how Surveyor assigns protocol names to learn how Surveyor names protocol by default. Understanding how Surveyor assigns names to protocols by default is important for understanding how protocol names can be altered and how protocols can be added using MONITOR.INI.

The assigning of protocol names does not effect protocol decode. See Assigning TCP or UDP Ports to Protocol Parsers for information on assigning protocol parsers to specific ports.

The MONITOR.INI file is located in your Windows 95/NT installation directory. Examples of usage are included in the file.

MONITOR.INI Format

MONITOR.INI contains two sections, TCP and UPD. Each section may have zero or more entries beginning with the keyword "mapping". Each "mapping" entry is following by an equal sign and a three variables:

mapping= <port num>,<short name>,<long name>

<port num> is a two-byte value that appears in a port fields of a TCP or UPD packet header. It identifies the protocol, by port number, to be included as a discrete protocol in Surveyor's monitor views.

<short name> is an alpha numeric string that is be between 1 and 12 characters This string is used as the name for the protocol in Surveyor's monitor tables.

<long name> is an alpha numeric string that should be between 1 and 50 characters. This string is used as the name of the protocol where Surveyor displays a long name.

The structure of the MONITOR.INI file is:

```
[TCP]
mapping=<port num>,<short name>,<long name>
.
.
mapping=<port num>,<short name>,<long name>
[UDP]
mapping=<port num>,<short name>,<long name>
.
.
mapping=<port num>,<short name>,<long name>
```

MONITOR.INI Examples

Example 1

Assume that you wish to rename TCP port 80 from HTTP to WWW for World Wide Web. The following entry would be made to the MONITOR.INI file in the TCP section:

```
[TCP]
mapping=80,WWW,World Wide Web
```

Example 2

Assume that a company is using a proprietary protocol named “Company X Protocol” that uses UDP port 921. By default this protocol would appear with the generic name “UDP WKP 921” in the monitor tables. Making the following entry to the MONITOR.INI file UDP section would give the protocol a name with more meaning:

```
[UDP]
mapping=921,CXP,Company X Protocol
```

Example 3

By default Surveyor/Explorer report X Windows network traffic with a single entry in the Protocol Distribution table even though X Windows could use non-WKP TCP ports in the range 6000 to 6063. For example, if 100 X Windows packets detected on port 6000 and 200 were detected on port 6029, the Protocol Distribution table would report that 300 hundred XWIN packets were detected. If the network manager wanted the Protocol

Distribution table to report the number of packet seen on each of the 64 X Window ports, the MONITOR.INI would need the following 64 entries:

```
[TCP]
mapping=6000,XWIN6000,X Windows on port 6000
mapping=6001,XWIN6001,X Windows on port 6001
.
.
mapping=6063, XWIN6063,X Windows on port 6063
```

Example 4

Assume that a company installed a audio/video application on its network named Video Audio Network Communicator. Assume that the application uses TCP port 2900. By default, packets on this port are attributed to the "TCP OTHERS" entry in the Protocol Distribution table along with other TCP non-WKP packets. To count and display the TCP port 2900 reported individually, the following entry needs to be made to the MONITOR.INI file:

```
[TCP]
mapping=2900,VIDEO,Video Audio Network Communicator
```

How Surveyor Assigns Protocol Names

Surveyor (and Explorer) explicitly monitor a predefined set of protocols/applications that use TCP or UDP as their transport layer. However, some of the TCP or UCP ports monitored are not given a well-known name. Also, some TCP and UDP ports are not explicitly monitored, and information about these remaining protocols are collected as though they were a single entity, one for TCP and one for UDP.

Surveyor monitors two port ranges, which are called Well Known Ports (WKP) and non-Well Known Ports (non-WKP). In summary, there are four different ways TCP/UDP ports are assigned names by Surveyor. They are:

- WKP that have been assigned a specific default name (i.e. HTTP, DNS, FTP, ...)
- WKP that use a generic name (i.e. TCP WKP 29, UDP PORT 64, ...)
- Non-WKP that have been assigned a specific default name (i.e. NFS, LOTUS NOTES, RADIUS, ...)
- Non-WKP that have not been assigned a name (TCP OTHER or UDP OTHER)

By changing the MONITOR.INI file, you can change names of generic names of WKPs and assign names to non-WKPs that are not assigned names by default.

Monitoring Well-Known Ports

Surveyor monitors all protocols that fall in the WKP (Well Known Port) range, ports with a value between 0 and 1023. If Surveyor/Explorer detects a TCP or UDP with a

port in the WKP range, information will be maintained on that port (total bytes, total packet, conversation, etc.).

Some of the ports have been assigned a name that is typically associated with the port value. For example, TCP port 80 is assigned the name HTTP. This name is used to represent that port when information about the port is displayed in the monitor tables of Surveyor.

Other WKPs are not assigned a default name. If these ports are detected, their name takes the generic form: "TCP WKP <port num>" or "UDP WKP: <port num>" where <port num> is the WKP value. For example, the TCP port 29 is not assigned a default name so if this port is detected the name used to represent the port would be: "TCP WKP 29".

Monitoring Non Well-Known Ports

Surveyor also collects information about a subset of ports that fall outside of the WKP range, port numbers greater than 1023. These ports are called non-WKP. Some of these ports are monitored by Surveyor since applications associated with them are widely accepted. The non-WKP ports that Surveyor monitors and their associated port values are listed below:

Table 7. Default Names for Non-WKP TCP Ports

<i>Name</i>	<i>TCP port values</i>
LOTUS NOTES	1352
TNS (Sybase)	1521
RSP	1704
TDS (Oracle)	2048
NFS	2049
CC:MAIL	3264
XWIN	6000-6063

Table 8. Default Names for Non-WKP UDP Ports

<i>Name</i>	<i>UDP port values</i>
RADIUS	1645
RSP	1704
RADIUS	1812
HSRP	1985
NFS	2049

Table 8. Default Names for Non-WKP UDP Ports

RTP	5004
RTCP	5005

Surveyor treats all other non-WKP as a single entity given a single generic name. The name for TCP non-WKP ports is "TCP OTHER". The name for UDP non-WKP ports is "UDP OTHER". For example, if 900 occurrences of the TCP port 11964 was detected and 200 occurrences of the TCP port 10564, there would be a single name to identify these 1100 occurrences of the TCP non-WKPs called "TCP OTHER".

Assigning TCP or UDP Ports to Protocol Parsers

Use the ANALYSIS.INI file to assign any built-in Surveyor parser to a TCP or UDP port. This is useful when a network is running a protocol/application over a TCP or UDP port that is not using the default port. The assignment of a proper parser allows Surveyor to properly decode and analyze the packets associated with the TCP or UDP port. The assigning of parsers does not effect how the information is displayed in Surveyor's monitor views. See Assigning Protocol Names for information on assigning names for monitor views.

The ANALYSIS.INI file is located in your Windows 95/NT installation directory. Examples of usage are included in the file.

ANALYSIS.INI Format

The ANALYSIS.INI file has two sections, TCP and UDP. A section contain one or more entries with the following format:

mapping=<port num>,<ip addr>,<parser name>,<name>

<port num>	is any valid 2 byte value that represents a TCP or UDP port value. It identifies the protocol, by port number, to be parsed in Surveyor's decode views.
<ip addr>	is a valid IP address in dotted decimal notation. This field can have a asterisk '*' to represent all IP addresses.
<parser name>	is the name of a valid Surveyor built-in parser. See Parser Names for a list of parsers.
<name>	is a name that will used to identify the mapping.

Example 1

Assume that the network administrator configured Oracle's TNS protocol to use TCP port 1029. This port value is different from the default value for TNS, which is 1521.

The entry in the ANALYSIS.INI would be:

```
[TCP]
mapping=1029,*,TNS,Oracle TNS
```

“Oracle TNS” is the string that will be used in Surveyor’s displays to identify this decode.

Example 2

Assume that the network administrator configured Sybase’s TDS protocol to use TCP port 11964. This value is different from the value for TDS which is 2048. Furthermore suppose the network administrator only wants to decode TCP port 11964 when associated with IP address 192.168.1.98. The entry in the ANALYSIS.INI file would be:

```
[TCP]
mapping=11964,192.168.1.98,TDS,Sybase TDS
```

Example 3

Assume that a two real-time application have been installed on a network that both use RTP (Real-Time Transport Protocol). Assume that one if the applications use UDP port 10564 and the other used 11964. Both of the UDP ports differ from the default the port of 5004. The entries in the ANALYSIS.INI file would be:

```
[UDP]
mapping=10564,*,RTP,RTP APPLICATION 1
mapping=11964,*,RTP,RTP APPLICATION 2
```

Parser Names

The tables in Appendix E contain the Parser Names that are built into Surveyor. Each parser is responsible for decoding a specific protocol. Parser Names are as similar as possible to protocol names. Parser Names must be entered exactly as shown in the tables to correctly reference the built-in parser.

5 Resources and Modes

Surveyor can gather statistical information and view network data from a variety of hardware sources. The types of information you receive from a resource depends on the hardware.

Surveyor's auto-discovery feature automatically scans the network for available resources, or you can enter the IP address of any host you can reach through a TCP/IP connection. Surveyor remembers the name of the most recent connection made so you can quickly reconnect to the host.

Surveyor provides a single window through which you can access all local and remote resources available in the network called the Resource Browser.

Resource Browser

The Resource Browser is a single window through which you can access all local and remote resources available in the network. The **Resource Browser** window works much the same as Microsoft Windows Explorer, allowing you to see hosts and their associated resources in a hierarchical relationship. "Branches" can be expanded or collapsed via point and click, so you can quickly customize your view of available resources.

Remote systems containing resources are listed by IP address unless there is a Surveyor name table on the system. If an entry exists in the name table for the IP address of the resource, the symbolic name in the name table is used to represent the resource. Resources within remote systems are listed by module type and module number. The module number is assigned by the software from the base address of the module, which is set by jumpers during hardware installation. For NDIS modules, the modules are numbered by the order in which they are discovered within the local or remote host. It is possible to have two different modules with the same name if they are within different hosts.

The Resource Browser opens as a docking window when Surveyor is started and can be moved to its own window outside the main window.

Double-click on a resource to display a default view of the resource in Summary View. If a remote resource is protected, you are asked for a user name and password. Drag and drop resources onto alarms in the Alarm Browser to activate an alarm for a resource.

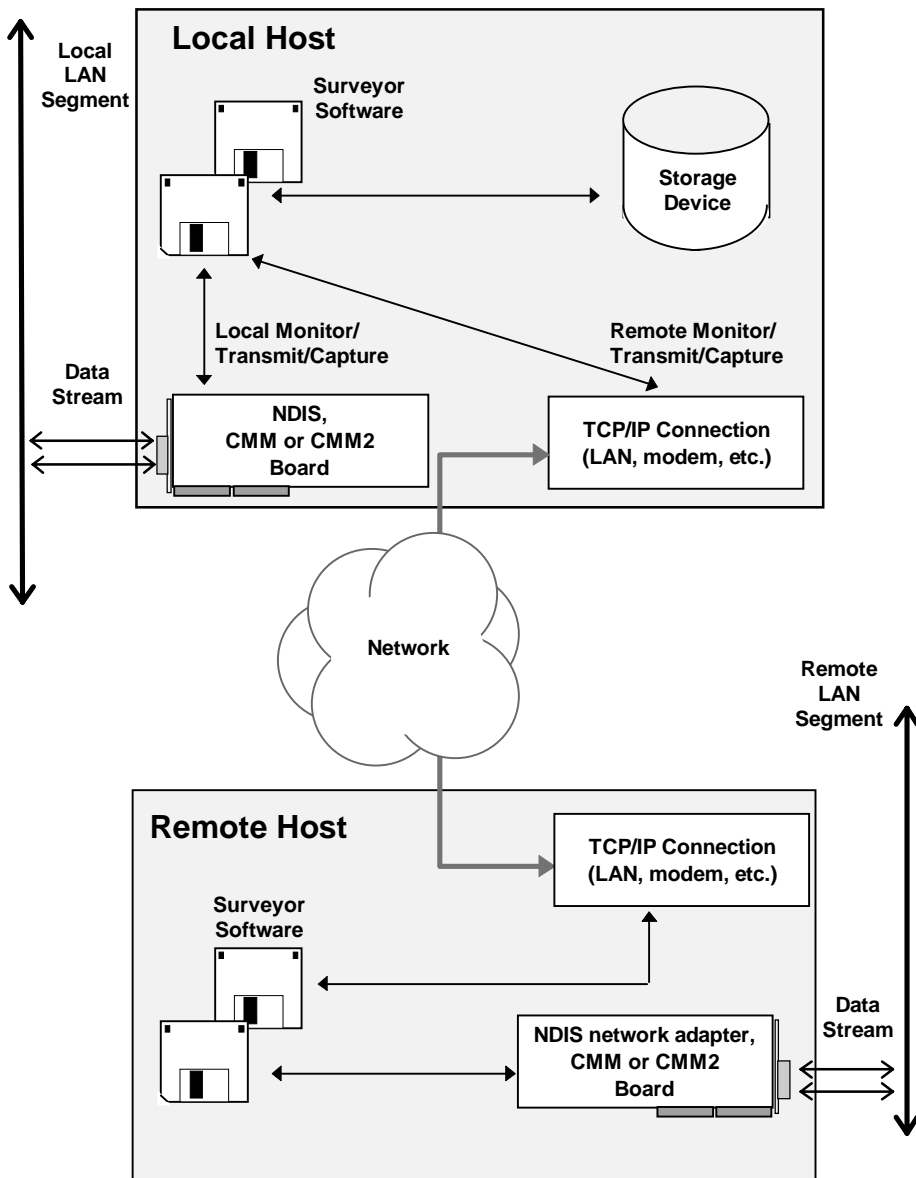
Remote vs. Local Resources

Local resources are those within the local PC running Surveyor. Remote resources are all other resources that can be reached through a TCP/IP connection. When running Surveyor from the PC, you have complete access and privileges to any resource in the PC. You can access remote resources and establish accounts for your local resources if you have the Remote plug-in software available from Shomiti. Both the local and the remote resource must have the plug-in for remote access to function.

Access to remote resources are controlled from the PC which contains the resource. For example, if your PC contains two CMM2 cards, accounts, privileges, and passwords for the CMM2 cards are established at your PC. Remote users must have access to a valid account to use the CMM2 in your PC.

The remote resource can be located in any host which can be accessed via a TCP/IP connection. You'll need to know the IP address of the remote host to log in to the remote resource. If the remote resource can be auto-discovered by Surveyor, the IP address or the name associated with the IP address of the host will display in the Resource Browser. Typically, resources on the same LAN segment can be auto-discovered.

See the figure on the following page for a diagram of how local and remote resources are accessed by Surveyor.

**Figure 9. Remote Host Connections**

Resource Protection

You are in control of local resources within a PC. Use the functions on the **Host** menu to add and delete users for a resource, change passwords and protections, or view the users currently logged in. There is a guest account for users with no account. The guest user can be given all privileges to effectively disable resource protection.

Note that there is no password protection for starting Surveyor on the local system. If you can start Surveyor from a system, you automatically have complete access to all local resources (called super-user privileges).

To access a remote resource, you must have an account and password set up on the remote system containing the resource or use the guest account.

Privileges for remote users can be set to:

Monitor Only	Allows a remote user to use the local device to monitor network activity only. You can access real-time monitor views on an armed (started) module, but cannot start/stop a module or define/load a filter.
Capture/Monitor	Allows a remote user to use the local device to monitor activity or capture network data. You can perform all Monitor Only functions plus capture data and perform full seven-layer decode on the packets. You can start/stop a module, define/load a filter and edit the contents of packets.
Full	Allows a remote user to use the local device to monitor activity, capture network data, or transmit network data. You can perform all Capture/Monitor functions plus all traffic generation capabilities available through the Packet Blaster plug-in module.
Super User	Allows a remote user the ability to transmit, capture, or monitor, plus set up, delete, and change accounts for the local PC. You have Full Access plus the ability to configure a deployed Explorer, change the access table, and unlock any locked module. Be careful when granting super-user privileges to remote users. This gives remote users complete control of your local resource.

Modes

Modes are applied to resources. Each resource can be in a different mode. There are five modes available with Surveyor, as follows:

Monitor	Provides real-time views and decodes of packets received by a device.
Capture	Allows packets received by a device to be stored in a buffer for analysis.
Capture + Monitor	Provides both real-time monitoring views and the ability to store packets for later analysis.
Transmit	Allows the transmission of packets from a device. You must have the Packet Blaster plug-in from Shomiti to use Transmit mode.
Capture + Transmit	Allows simultaneous capture and transmit from the same module (CMM2 modules only).

Both the monitor and capture functions look at the same bit stream being received by a device. The difference between these modes is how the bit stream is stored and viewed. Because each class of device has different capabilities for storing and viewing the bit stream, you must understand the capabilities of the device you are using to completely understand what is possible in each mode.

If you have the Packet Blaster plug-in, you can use any device in transmit mode.

CMM2	The current version of the Century Media Module fully supports all modes and all counters in Surveyor and supports the all monitor and capture functions at full line rate. The default mode for CMM2 is Capture + Monitor. In Capture + Transmit mode the buffer is split in two, half used for capture and half used for transmit.
CMM1	The earlier version of the Century Media Module can be used in all modes; however, only MAC frame and error counters are supported for monitoring. The default mode for CMM1 is Capture + Monitor.
NDIS	<p>Surveyor NDIS supports up to four Ethernet adapters. The first Ethernet adapter found during system initialization is seen by Surveyor software as module #1, the second as module #2, and so on.</p> <p>Ethernet adapters can be used to capture, transmit, or monitor, but have performance constraints. The effective rate at which an NDIS module can capture or monitor is</p>

limited because it must perform these functions in software rather than hardware. An NDIS adapter is often used in Monitor only mode to improve performance, since NDIS adapters cannot capture at full line rate. When using an NDIS adapter, check the **Information** tab to see information about what counters are supported. Each manufacturer supports a different set of counters. The default mode for NDIS adapters is Capture + Monitor.

Explorer

The Explorer is a protocol analysis tool that contains its own processor and two CMM2 modules. The Explorer modules fully supports all modes and all counters in Surveyor. The CMM2 modules are synchronized so you can analyze a full-duplex network segment from a single view. When viewing an Explorer resource in the Resource Browser, you will see three “devices”: one for the first CMM2 card, one for the second CMM2 card, and one for the two cards synchronized as a set. The default mode for modules in Explorer is Capture + Monitor.

Voyager

The Voyager is a multi-port RMON/RMON2 probe. Surveyor can display the RMON statistics collected by Voyager (version 1.1 and higher). Icons appear under the Voyager resource in the Resource Browser to select the port or port-pair to monitor. Monitor port-pairs when connected to full-duplex links. Monitor statistics display as for any other resource. The only mode for Voyager is Monitor.

Note: Voyager can mirror data from its probe ports to Explorer. You can control the Voyager ports that are mirrored from Surveyor through the Explorer device. A special Multi Port Tap icon appears under the Explorer resource in the Resource Browser to control which ports of Voyager are mirrored to Explorer. See the chapter “Customizing Surveyor” for more information on port selection.

Portable Surveyor

Portable Surveyor supports a single PCI CardBus card in a portable computer host. Because it is designed as a portable system, Portable Surveyor will rarely be seen as a remote resource.

Portable Surveyor can be used to capture, transmit, or monitor. It supports all the same standard Ethernet

counters as CMM1 or CMM2. The default mode for Portable Surveyor is Capture + Monitor.

Portable Surveyor has some performance constraints, although the device can capture at close to full line rate. See you Shomiti representative for more information on the performance characteristics of Portable Surveyor.

Century 12-Tap

Taps are fault-tolerant wiring devices that provide connections for Explorers or Century Media Modules. The tap shows as a “resource” to the Surveyor software, but is only used to select a LAN segment for monitoring and LAN analysis functions.

See Appendix A for more information on the implementation of Surveyor and a summary of all hardware differences.

Synchronized Resources

Synchronized resources are multiple hardware devices that have been connected so that they use the same clock timer. Synchronized devices display in the Resource Browser as a unique resource. For example, the two CMM2 boards in a full-duplex Explorer are synchronized. The Resource Browser shows three resources available within the Explorer; the first CMM2 module, the second CMM2 module, and the synchronized configuration of both CMM2 modules together. Synchronized resources are recognized by the synchronized resource icon in the Resource Browser.

Synchronizing resources allows single actions to start a resource pair. All statistics and all data about stations and conversations will appear as one resource to Surveyor, so you can perform all capture, transmit, and monitoring functions on a full-duplex network segment. Synchronized resources can also monitor two half-duplex segments. Synchronized CMM2 modules within an Explorer are typically used with a Century Tap or a Century 12-Tap to provide a connection to full-duplex network segment(s). The Century 12-Tap provides a convenient, software-controlled means to switch between segments. Contact customer support for more information on Explorer, Century Tap, and Century 12-Tap products.

Two CMM2 cards within the same PC can be synchronized. This requires a special cable between the two cards to synchronize their clocks. Call customer support for information on how to synchronize and use two CMM2 cards with a PC.

Hints and Tips for Resources

The following are a collection of hints and tips you may find useful when using resources or the Resource Browser:

- To connect to a remote host, choose **Connect...** from the **Remote** menu and enter the host IP address.
- To set up or change accounts, choose **Access Privileges...** from the **Host** menu.
- To see remote users logged on to your local resources, choose **Current Users...** from the **Host** menu.
- When using CMM1 or CMM2 modules, be sure you set the module port and speed before using the resource.
- Use the **Refresh** button in dialog boxes to update the list of users accounts currently established. Remote users with super-user privileges may have created a new account since the dialog box was initially displayed.
- Surveyor “remembers” hosts that you have connected to from the **Connect...** option of the **Host** menu. If you log in to a host and quit Surveyor, you’ll automatically get the **Connect New Host** dialog box when you restart the program. Click **OK** to log in to the last host you connected to, or press **Cancel** to abort the auto-discovery process.
- To prevent others from using a local resource, use **Lock** from the **Module** menu.
- Setting the mode to transmit disables monitor and capture unless your are using a CMM2 module in full-duplex mode. Setting the mode to monitor and/or capture disables transmit.
- Monitor mode can be set in addition to capture if the resource supports monitoring functions. If the resource does not support monitoring functions, the **Monitor** button is disabled.
- Use CMM2 modules for full-duplex capture and transmit.
- For options to be display under the **Host** menu, you must select the local host name in the Resource Browser. Selecting a resource within the local host, the options in the **Host** menu are unavailable.
- Use the **Description...** option from the **Host** menu to find out information about the host. Information includes host type, IP address, and the Surveyor software version. The host name must be highlighted in the Resource Browser to get a description.
- If you suspect that a remote resource is not responding, go to Summary View and look at the Resource Browser. If the host for the remote resource is not there, the connection has been lost with the remote host and the resource is not available. Red Xs appearing over a host in the Resource Browser indicate that the host is disconnected.

- To see which capture filter or transmit specification is associated with a particular resource, choose **Active TSP and Capture Filter** from the **Module** menu.

6 Views

There are numerous ways to view data from Surveyor. This section describes the primary windows you use to view data, and the actual data views you can see within each window. The primary windows for viewing information are:

Summary View	From Summary View you can see one view of many different resources. Viewing options include configurable charts and tables.
Detail View	From Detail View you can see many different views simultaneously of a single resource.
Capture View	From Capture View you can see many different views of previously captured data. Although the data is “static”, the presentation of the data is the same for data views.

The data views that can be seen within each primary window are described independently. Although you may be viewing data for different purposes from each primary view, the way the information is presented in a data view is virtually identical no matter which primary view you are using.

The table on the following page shows which data views are supported from each primary window.

Table 9. Data Views Supported in Primary Windows

Y = Data View Supported N = Data View Not Supported	Summary View	Detail View	Capture View (Static Data)
MAC Statistics	Y	Y	N
Utilization/Errors Strip Chart	Y	Y	N
Frame Distribution	Y	Y	Y
Protocol Distribution	Y	Y	Y
Host Table	Y	Y	Y
Network Layer Host Table	Y	Y	Y
Application Layer Host Table	Y	Y	Y
Host Matrix	Y	Y	Y
Network Layer Matrix	Y	Y	Y
Application Layer Matrix	Y	Y	Y
VLANs	Y	Y	Y
Address Map	Y	Y	Y
Duplicate Address (Expert plug-in only)	Y	Y	Y
Expert (Expert plug-in only)	Y	Y	Y
Application Response Time (Expert plug-in only)	Y	Y	Y
Packet Summary (real-time protocol decode)	Y	Y	N
Capture View (protocol decode)	N	Y	Y

Summary View

Summary View is Surveyor's global monitoring tool for network data. You can view real-time data from any local resource or any resource you can connect to on the network. You can filter the data before viewing by applying a capture filter.

Each resource is viewed through its own window within Summary View. You can open windows for as many resources as you wish. Furthermore, each resource window can be displayed in six different views.

There are six tabs available for different views within Summary View:

Monitor	Monitoring View. Refer to the list below for the choices. The selected view will show on the tab.
Rx	Receive counters. A list of MAC counters for receive and receive error counters.
Tx	Transmit counters. A list of MAC counters for transmit and transmit error counters.
Alarms	Shows the alarm tables applied to this resource.
Alarm Log	Log of all real-time alarm events that have occurred for this resource.
Description	Provides a brief description of the board, board address, and supported counters.

To change the Summary View for a resource, click the appropriate tab at the bottom of the resource window. The figure on the following page shows Summary View with windows open for multiple resources.

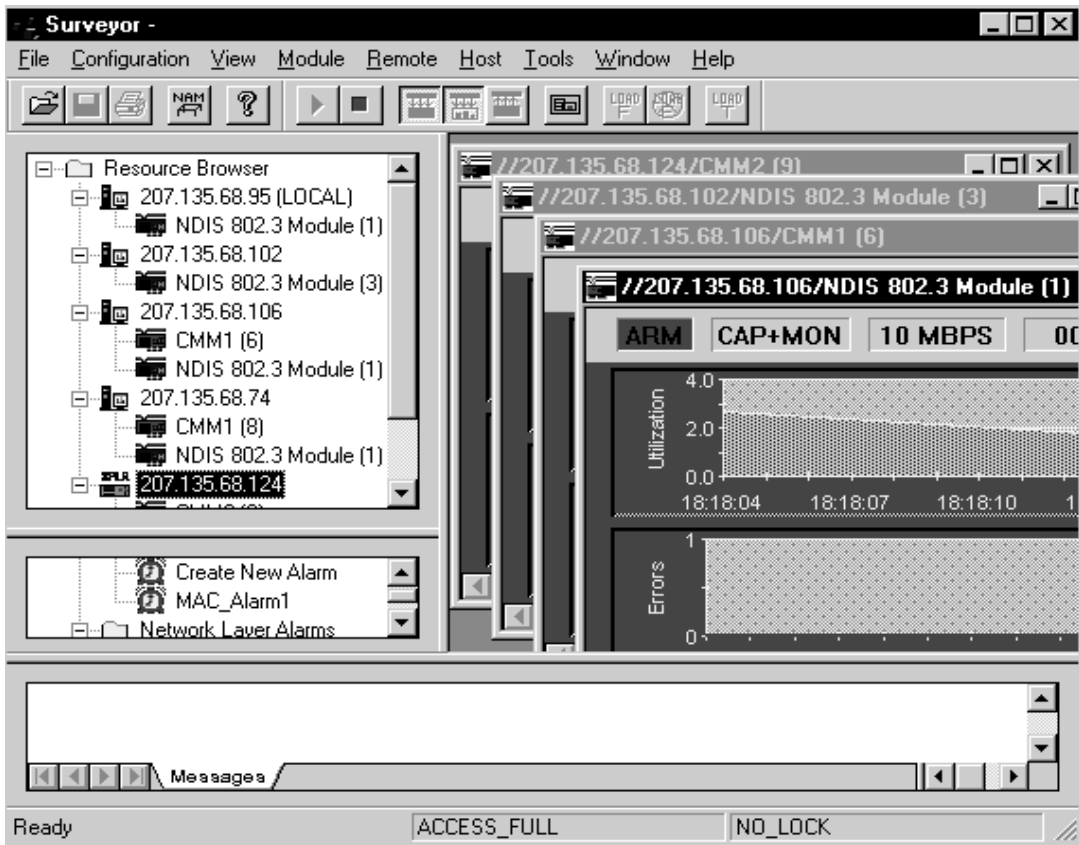


Figure 10. Summary View Window


Using the tabs, you can get a single monitoring view, see transmit or receive counters, view alarms set and alarms triggered for this resource, or get a description of the resource (counters supported, etc.). The first tab contains the monitoring view which can be configured to display any of the views listed on the following page.

Multiple monitoring views are available from within Summary View. Each view can display as a table or a chart, with the exception of Address Map View or Expert Views which only display as tables. Remember that in Summary View you set one of these views which will apply to all resources.

The monitoring views are listed below.

- Utilization/Error
- Frame Size Distribution
- Protocol Distribution
- Host Table
- Network Layer Host Table
- Application Layer Host Table
- Host Matrix
- Network Layer Matrix
- Application Layer Matrix
- VLAN
- Address Map
- Packet Summary
- MAC Statistics
- Expert
- Application Response Time
- Duplicate Address

You can change the monitoring view for Summary View by choosing **Monitor View Preferences** from the **Module** option in the **Configuration** menu. The view you select applies to what you see in the first tab. You can have a different single monitoring view for each resource.

In Summary View, you get one monitoring view of many different resources. Go to the Detail View to get many different views of a single resource or to perform detailed analysis functions on captured data. Double-click on the view for the resource or press the  button to go to Detail View.

Detail View

Detail View is the tool for performing detailed analysis of network data. You can view real-time data from the resource for which you have opened Detail View or you can view and analyze data stored in the capture buffer. You can filter the data before viewing by applying a display filter.

The Detail View allows multiple views for a single resource module and also allows the Capture View to be opened for that same module. By contrast, Surveyor's Summary

View allows one monitoring view for multiple resource modules and the Capture View cannot be opened.

You can have as many windows with data views as are available in Detail View. The initial data view you get of a resource is the view set in the **Configuration** menu for Summary View. Many of the table or chart views within Detail View can be customized.

Files or buffers, such as a capture file or capture buffer, are considered resources just like physical devices that are available from the Resource Browser. If you open a file from Summary View, a **Detail View** window will open for that resource. Viewing static resources such as files or buffers will change the options available from the toolbars and menus and the data views will appear somewhat different. Surveyor is designed so that you'll only be able to perform the functions that make sense for that resource.

For example, if you open the capture buffer, it automatically puts you into Capture View. Buttons for capture, transmit, and monitor are grayed out on the **Detail View** toolbar, since these functions make no sense for a file. If you select another view of the information in the file, it will appear in a table with a gray background indicating its a view of a static resource.

Detail View can display multiple views of information. Press the button on the **Data Views** toolbar for the view you wish to be displayed in Detail View. Packet Summary View is available from the **Monitor Views** menu. MAC Statistics and Utilization/Error views show counter information. For these views, the displays depends on the mode of the resource, capture or transmit.

The Data View buttons are as follows:



MAC Statistics (Rx)



MAC Statistics (Tx)



Frame Size Distribution



Protocol Distribution



Utilization/Error View (Rx)












Utilization/Error View (Tx)



Host Table




Network Layer Host Table

	Application Layer Host Table
	Host Matrix
	Network Layer Matrix
	Application Layer Matrix
	VLANs
	Address Map
	Duplicate Address
	Expert
	Application Response Time

Using Monitor + Capture Mode in Detail View

In Detail View for a resource, you can have both Monitor and Capture views of data. The use of these two modes together allows you to monitor traffic at the same time as you look at the contents of previously captured data. However, some of ways you can look at the capture or monitor data are the same. For example, you can view a host table for the monitor data and also view a host table for the contents of the capture buffer. Since the tables are formatted the same, which data are you looking at?


Surveyor provides some visual distinctions between capture and monitor views. For table information of the capture buffer data, all data in the table is grayed. For monitor data, the column and row titles are gray, but the data in the table is white. The title bar for a monitor view will say “Monitor View” and the title bar for a capture view will say “Capture View.”

If you start a resource and then stop it, you can look at the capture buffer contents using the  button to bring up Capture View. If you restart the resource (start a different capture operation), you will begin refilling the contents of the capture buffer and incrementing counters for monitor views. However, the previous views that you have of the capture buffer are still open windows within Detail View. In other words, the “view” and decode of previous information is still available, even though the capture buffer itself is refilling with new information. If you do not need this previous view of captured information, it is recommended that you close the **Capture View** window and all associated capture view windows. You can, of course, save this information to a file. Closing unused windows may avoid confusion when looking at similar monitor and

capture views. This will also help you distinguish between what is happening real-time and what was saved from the previous capture operation.

Capture View

Capture View is the tool for detailed analysis and editing of packets. You can view the data in the capture buffer or view previously captured information that has been saved to a file. You can filter the data before viewing by using a display filter. Capture View contains a Packet Editor for editing packets.

Click the  button on the Detail View toolbar to access Capture View. Use the green arrow buttons on the Capture View toolbar to move through the listed items. Capture View also opens automatically when you open a capture file (file with .CAP extension).

The initial Capture View display provides a protocol decode of all packets. Other views of captured information are available from the Capture View toolbar. Although similar to the Monitoring View toolbar buttons, the graphs and charts displayed by using the Capture View Toolbar Buttons display detail information about the packets decoded from the capture buffer only. Table data in these other views is grayed to indicate that it's a capture view, not a view of real-time data.

The initial **Capture View** window is divided into three parts or “panes.” Capture View shows a synopsis of all captured packets, provides a breakdown of the elements of the packet by protocol, and shows the hex and ASCII values for all characters in the packet. The three panes of the window can be sized any way you like. Click and drag the bars separating the panes to resize them. Use the F11 function key to zoom in on any of the three panes.

The Summary Pane, top, shows a summary of all packets. You can change the Summary Pane of the Capture View window to display the fields you want. Select **Display** from the **Configuration → Capture View Options** menu. Choose the items you want displayed by from the dialog box. Choose the **Display Detail Protocol Summary** check box and select the level of protocol detail information you want to display. If this check box is not selected, a synopsis of all protocols used in the packet is displayed. You can also control where “time-zero” begins within the flow of packets using the **Elapsed Time Set Mark Option** from the Display Options dialog box.

Clicking on a packet selects it and displays its detailed protocol breakdown (decode) and its hex values in the remaining two panes of the window.

The detail pane, middle, shows the values of the protocol elements associated with each protocol. For example, for the Data Link Control the values for the source address, destination address, and packet length are shown. Single clicking on a value highlights the value in both the detail pane and the hex pane.

The hex pane, bottom, shows the hex and ASCII values for all the bytes in the packet. Single clicking on a value highlights the value in both the detail pane and the hex pane.

A unique color can be used to display packets of each different protocol layer. Set color coding or change color associations from the **Configuration** menu. Choose the **Protocol Color Coding** tab from the **System Settings** menu option. See “Appendix D” for a list of Surveyor’s default protocol color codes. You can also enable or disable Expert Analysis views from the **Configuration → Capture View Options** menu.

You can export packet decode information to another source. You can also print a range of frames in a capture file or in the capture buffer to a text file. Frames can be saved in a variety of formats. See “Export Utilities” in Chapter 12 for more information.

If you have special decoding or display needs for non-standard protocols, see the “Advanced Configuration” section in Chapter 4 for information on assigning protocol parsers and assigning names to protocols. (Note: Support for non-standard protocols has changed from previous releases. The older method is still supported, but it strongly suggested that you convert to the new method. The newer method provides a general solution that supports any TCP or UDP port.)

Packet Editor

The Packet Editor can be used to modify the contents of packets when in Capture View. The editor provides two views of packets, detail view and hex view. Edits can be made within either view. Double-click on a packet in the Summary Pane of Capture View to edit a packet.

The editor must be enabled for use. To enable the Packet Editor, check **Enable Packet Edit** from the **Configuration → Capture View Options** menu.

The following buttons are available within the Packet Editor:

Auto CRC	Causes the 4-byte CRC error check value to be automatically calculated and written to the frame. With this option selected, creating frames with a bad CRC is not possible.
Compute CRC	Inserts the correct CRC error check value for the frame. You can use this option to create frames with or without correct CRC error check values.
Set Size	Sets the size of the packet. The current size of the packet is displayed for reference. Packet sizes from 8 to 1518 bytes are allowed.
Decode	Takes the values entered in the Hex View window of the Packet Editor, decodes the packet, and displays the resulting decode in the Decode View window.
Undo	Undo the last editing action. Only one level of undo is supported.
OK	Save edits.
Cancel	Leave the editor without saving changes.

Editing in Decode View

Editing in decode view allows you to edit packets without remembering offsets. Click on a field and a dialog box pops up which shows the current value for the field and asks for a new value. The dialog box for each field is slightly different. Most dialog boxes display and allow you enter values in hexadecimal or decimal. Some contain a **Use little-endian bit** order check box if bit order swapping is required. Changes made in decode view are automatically reflected in hex view.


Editing in Hex View

Edits are made in hex view by placing the cursor at a location and overwriting the current values. You can also paste (Ctrl + V) the contents of the paste buffer into a location. Values are always overwritten starting at the current cursor location in hex view so offsets remain correct.

Press the **Decode** button to display edits made in hex view in the decode view. Note that changes to the decode view are not automatic. This provides the option of creating error packets that can't be decoded properly.

Data Views

MAC Statistics View (Rx)

From Detail View, click on the  button to open a window with MAC Statistics View for capture. From Summary View, set the view preferences to **MAC Statistics (Rx)** to see this view in the first tab.

MAC Statistics View for capture shows module activity and counters during capture. It provides a visual reference for what a resource is doing. Counters are incremented as the resource captures packets. This view also provides general information about the resource.

The MAC Statistics View in capture mode is shown in the figure on the following page.

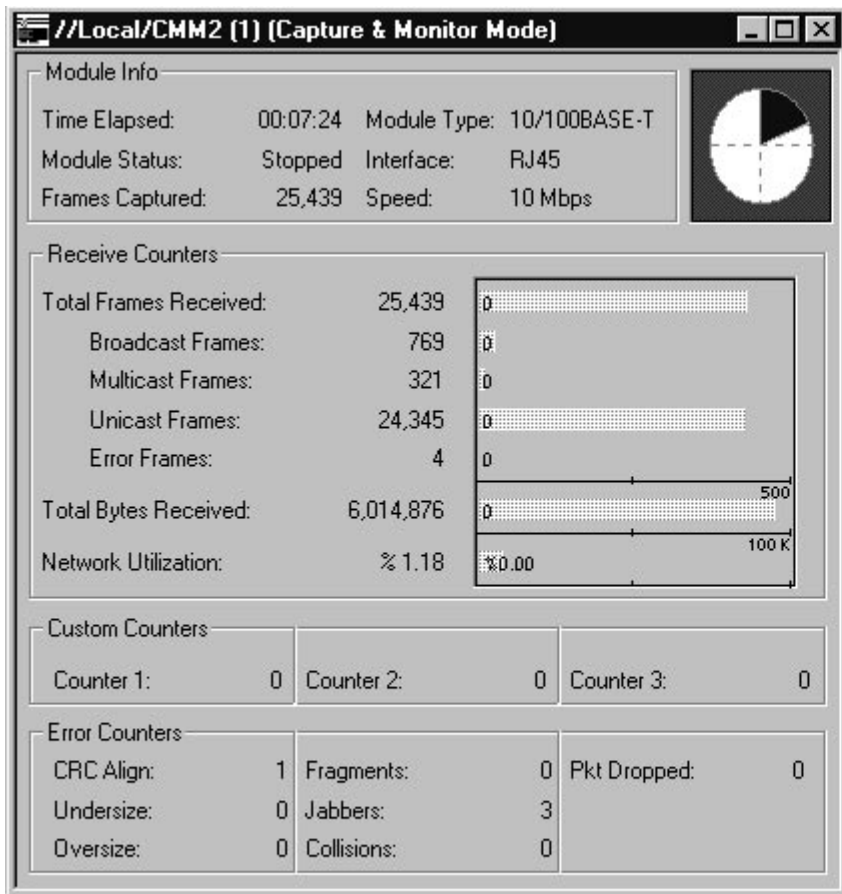



Figure 11. MAC Statistics View (Capture)

MAC Statistics View (Tx)

From Detail View, click on the  button to open a window with MAC Statistics View for transmit. From Summary View, set the view preferences to **MAC Statistics (Tx)** to see this view in the first tab.

MAC Statistics View also shows module activity during transmit. It provides a visual reference for what the module is doing. The module identifier and the current mode are displayed in the window title bar. Counters are incremented as the module performs transmit functions.

The MAC Statistics View in transmit mode is shown in the figure on the following page.

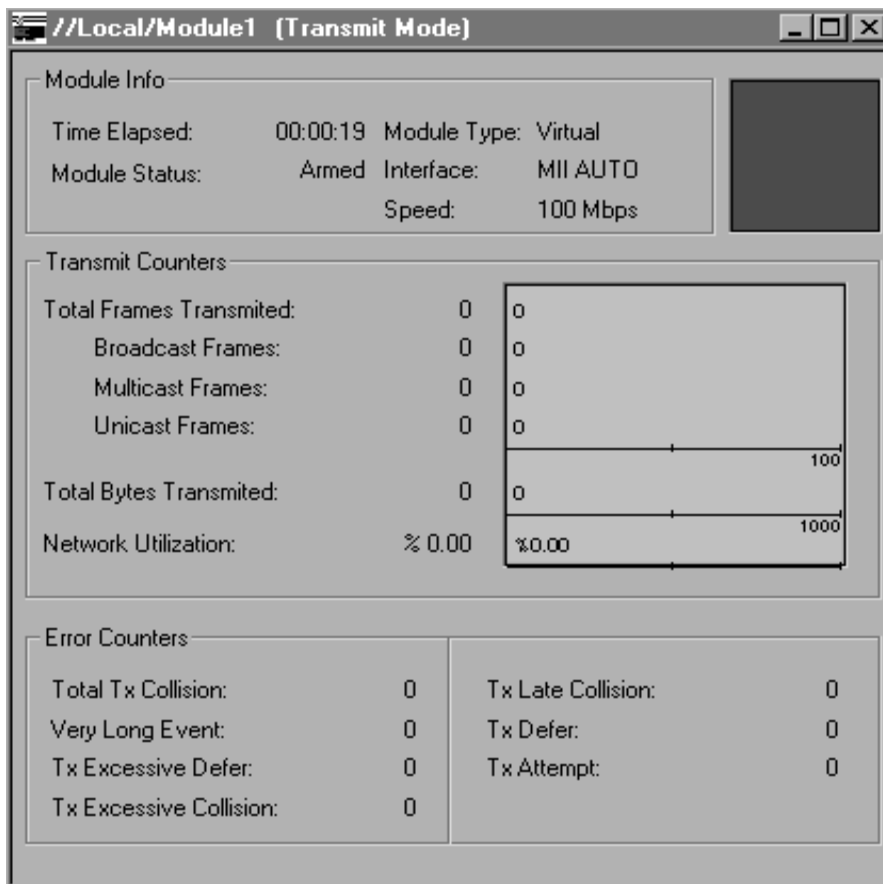



Figure 12. MAC Statistics View (Transmit)

Frame Size Distribution View

Frame Size Distribution View is available as a chart or a table. The chart can be toggled between a pie chart and a bar graph.


From Detail View, click on the  button to open a window with Frame Size Distribution View. From Summary View, set the view preferences to **Frame Size Distribution** to see this view in the first tab.

For both the chart and the table, each range of frame sizes is expressed as a percentage of the total number of frames counted.

Table 10. Table Columns for Frame Size Distribution View

<i>Table Column</i>	<i>Description</i>
Frame Size (Bytes)	Size of captured frames, in bytes
No. of Frames	Number of captured frames that are of this frame size
Percentage	Percentage of all captured frames that are of this frame size

Protocol Distribution View

From Detail View, click on the  button to open a window with Protocol Distribution View. From Summary View, set the view preferences to **Protocol Distribution** to see this view in the first tab.

Protocol Distribution View is available as a chart or a table. Protocol Distribution View shows the distribution of major network protocol types.

Chart

Protocol distribution as a chart can be viewed in many different ways, depending on the buttons selected in the view. The buttons are described below:

Protocol Buttons	Selects the types of protocol distribution you want to see. There are four protocol buttons that change the protocols you are viewing in the graph:
NET	Shows percentages of all packets by network layer protocol type, such as IP and IPX.
IP	Shows percentages of other protocols used within IP packets only.
IPX	Shows percentages of other protocols used within IPX packets only.
All	Shows percentages of all packets by application.

The NET and ALL buttons shows percentage breakdowns for all packets. The IP and IPX buttons show the percentages of only those packets that can be identified as containing IP or IPX information respectively.

Frame/Byte Buttons

Selects to view the distribution by byte count or frame count, or can be used to select distribution relative to network capacity. There are three buttons that control how the protocols are counted when displayed in the graph:

- Frm** Counts by frame and displays percentages relative to the total number of frames counted.
- Abs Bts** Counts by byte and displays percentages compared to the total network capacity.
- Rel Bts** Counts by byte and displays percentages relative to the total number of bytes counted.

Display Buttons

Controls the display of information. There are three buttons that control the display only:

- BAR** Display distributions as a bar graph.
- PIE** Display distributions as a pie chart.
- II** Pause the display. When pressed again, counters resume real-time update.

Table



Protocol Distribution View as a table shows frame and byte counts by protocol.

Table 11. Table Columns for Protocol Distribution View


<i>Table Column</i>	<i>Description</i>
Protocol Name	Name of a network protocol (i.e., ARP, IP, IPX, etc.)
Total Frames	Total number of captured frames that are associated with a particular protocol
Rel % Frames	Percentage of all frames captured that are associated with a particular protocol
Total Bytes	Total number of captured bytes that are associated with a particular protocol
Rel % Bytes	Percentage of all bytes captured that are associated with a protocol
Abs % Bytes	Percentage of network capacity (measured in bytes) that are associated with a protocol

Utilization/Error View

Utilization/Error View is a simple strip chart that plots points for network utilization over time. The scale for network utilization changes on-the-fly when a new peak percentage is reached. The time scale also scales automatically as the resource is monitored over time. The graph has an optional watermark showing the highest utilization point. The errors plotted on the graph are the total number of CRC and Alignment errors.

From Summary View, set the view preferences to **Utilization/Error** to see this view in the first tab. From Detail View, click on the **Capture**  button or the **Transmit**  button to open a window with the **Utilization** strip chart. From Detail View, the **Utilization/Error** chart is presented with the tables of transmit or receive counters.

Host Table View

From Detail View, click on the  button to open a window with Host Table View. From Summary View, set the view preferences to **Host Table** to see this view in the first tab.

Host Table View is available as a chart showing the ten MAC stations with the most traffic or as table showing all MAC stations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station address and name are provided in the table or chart. If a Surveyor name table exists with an address-to-name entry for this station, the **Station Name** field will be the station name in the name table. If no entry in a Surveyor name table exists, the name of the **Station Name** field will be the vendor identifier followed by the last 6 bytes of the station address.

Chart

Host Table View as a chart shows only ten MAC stations. The ten stations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the “top ten” stations based on a different station information field.

Table


Host Table View as a table shows network activity from the view of MAC stations. The table lists statistics for all stations found. The table can be customized to include other columns of information, or to delete columns you don't want to see. Table columns listed in italics are the default Host Table View columns.

Press the right mouse on any table entry to create a quick filter using the selected MAC station. See Chapter 7 for information on quick filters.

Table 12. Table Columns for Host Table View

Table Column	Description
MAC Station Name	Name of the MAC station
MAC Station Address	MAC station address
Frames In	Number of frames received by the MAC station
Rel % Frames In	Percentage of frames received by this MAC station relative to the total number of frames
Frames Out	Number of frames sent by the MAC station
Rel % Frames Out	Percentage of frames sent by this MAC station relative to the total number of frames
Bytes In	Number of bytes received by the MAC station
Rel % Bytes In	Percentage of bytes received by this MAC station relative to the total number of bytes
Abs % Bytes In	Percentage of bytes received by this MAC station relative to the total network capacity (measured in bytes)
Avg. Size In	Average number of bytes contained within frames received by the MAC station
Bytes Out	Number of bytes sent by the MAC station
Rel % Bytes Out	Percentage of bytes sent by this MAC station relative to the total number of bytes
Abs % Bytes Out	Percentage of bytes sent by this MAC station relative to the total network capacity (measured in bytes)
Errors Out	Number of transmittal errors generated by the MAC station
Broadcast Out	Number of broadcast frames generated by the MAC station
Multicast Out	Number of multicast frames generated by the MAC station

Network Layer Host Table View

From Detail View, click on the  button to open a window with Network Layer Host Table View. From Summary View, set the view preferences to **Network Layer Host Table** to see this view in the first tab.

Network Layer Host Table View is available as a chart showing the ten network stations with the most traffic or as a table showing all network stations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station address and name are provided in the table or chart. The name and address will be the same if Surveyor does not have a name table with an address-to-name correspondence for this station.

Chart

Network Layer Host Table View as a chart shows only ten network stations. The ten stations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the “top ten” stations based on a different station information field.

Table


Network Layer Host Table View as a table shows network activity from the view of network stations. The table lists statistics for all stations found. The table can be customized to include other columns of information. Table columns listed in italics are the default Network Layer Host Table View columns.

Press the right mouse on any table entry to create a quick filter using the selected network layer host. See Chapter 7 for information on quick filters.

Table 13. Table Columns for Network Layer Host Table View

Table Column	Description
Network Station Name	Name of the network station
Network Station Address	Network layer address
VLAN Id	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time.
Frames In	Number of frames received by the network station
Rel % Frames In	Percentage of frames received by this network station relative to the total number of frames
Frames Out	Number of frames sent by the network station
Rel % Frames Out	Percentage of frames sent by this network station relative to the total number of frames
Bytes In	Number of bytes received by the network station
Rel % Bytes In	Percentage of bytes sent by this network station relative to the total number of bytes
Abs % Bytes In	Percentage of bytes received by this network station relative to the total network capacity (measured in bytes)
Avg. Size In	Average number of bytes contained within frames received by the network station
Bytes Out	Number of bytes sent by the network station
Rel % Bytes Out	Percentage of bytes sent by this network station relative to the total number of bytes
Abs % Bytes Out	Percentage of bytes sent by this network station relative to the total network capacity (measured in bytes)
Avg. Size Out	Average number of bytes in the frames sent by the network station
Non-Unicast Out	Number of non-unicast frames generated by the network station

Application Layer Host Table View

From Detail View, click on the  button to open a window with Application Layer Host Table View. From Summary View, set the view preferences to **Application Layer Host Table** to see this view in the first tab.

Application Layer Host Table View is available as a chart showing the ten network stations with the most traffic or as a table showing all network stations.

The network station address and name are provided in the table or chart. The name and address will be the same if Surveyor does not have a name table with an address-to-name correspondence for this station.

Chart

Application Layer Host Table View as a chart shows only ten applications over network stations. The ten stations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the “top ten” stations based on a different station information field.

Table


Application Layer Host Table View as a table shows network activity from the view of application protocols running on network stations. The table lists all application protocols found on each network station. Each network station may have many application protocols in use. The table lists statistics of all applications within the stations found. The table can be customized to include other columns of information. Table columns listed in *italics* are the default Application Layer Host Table View columns.

Press the right mouse on any table entry to create a quick filter using the selected application layer host. See Chapter 7 for information on quick filters.

Table 14. Table Columns for Application Layer Host Table View

Table Column	Description
Network Station Name	Name of the network station
Network Station Address	Address of a network station in IP address format
VLAN Id	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time.
Application	Name of the application protocol
Frames In	Number of frames received by the network station for this application
Rel % Frames In	Percentage of frames received by this network station for this application relative to the total number of frames
Frames Out	Number of frames sent by the network station for this application
Rel % Frames Out	Percentage of frames sent by this network station for this application relative to the total number of frames
Bytes In	Number of bytes received by the network station for this application
Rel % Bytes In	Percentage of bytes received by this network station for this application relative to the total number of bytes
Abs % Bytes In	Percentage of bytes relative to the total network capacity (measured in bytes) received by this network station for this application
Avg. Size In	Average number of bytes contained within frames received by the network station for this application
Bytes Out	Number of bytes sent by the network station for this application
Rel % Bytes Out	Percentage of bytes sent by this network station for this application relative to the total number of bytes
Abs % Bytes Out	Percentage of bytes sent by this network station for this application relative to the total network capacity (measured in bytes)
Average Size Out	Average number of bytes contained in frames sent by the network station for this application
Non-Unicast Out	Number of non-unicast frames generated by the network station for this application

Host Matrix View

From Detail View, click on the  button to open a window with Host Matrix View. From Summary View, set the view preferences to **Host Matrix** to see this view in the first tab.

Host Matrix View is available as a chart showing the ten MAC conversations with the most traffic or as a table showing all MAC conversations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station addresses and names are provided in the table or chart. If a Surveyor name table exists with an address-to-name entry for this station, the **Station Name** field will be the station name in the name table. If no entry in a Surveyor name table exists, the name of the **Station Name** field will be the vendor name followed by the last 6 bytes of the station address.

Chart

Host Matrix View as a chart shows only ten MAC conversations. The ten conversations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the “top ten” conversations based on a different information field.

Table


Host Matrix View as a table shows network activity from the view of MAC station pairs. The table lists statistics for all pairs found. The table can be customized to include other columns of information. Table columns listed in italics are the default Host Matrix View columns.

Press the right mouse on any table entry to create a quick filter using the selected MAC layer conversation. See Chapter 7 for information on quick filters.

Table 15. Table Columns for Host Matrix View

Table Column	Description
MAC Station Name 1	Name of a MAC station
MAC Station Address 1	MAC station address
MAC Station Name 2	Name of a second MAC station
MAC Station Address 2	Address of a second MAC station
Frames 1→2	Number of frames sent from MAC Station 1 to MAC Station 2
Frames 2→1	Number of frames sent from MAC Station 2 to MAC Station 1
Frames 1↔2	Number of frames sent in either direction between MAC Station 1 and MAC Station 2
Rel % Frames 1↔2	Percentage of frames sent in either direction between MAC Station 1 and MAC Station 2 relative to the total number of frames
Bytes 1→2	Number of bytes sent from MAC Station 1 to MAC Station 2
Average size 1→2	Average size of the frames sent from MAC Station 1 to MAC Station 2
Bytes 2→1	Number of bytes sent from MAC Station 2 to MAC Station 1
Average Size 2→1	Average size of the frames sent from MAC Station 2 to MAC Station 1
Bytes 1↔2	Number of bytes sent in either direction between MAC Station 1 and MAC Station 2
Rel % Bytes 1↔2	Percentage of bytes sent in either direction between MAC Station 1 and MAC Station 2 relative to the total number of bytes
Abs % Bytes 1↔2	Percentage of bytes sent in either direction between MAC Station 1 and MAC Station 2 relative to the total MAC capacity (measured in bytes)
Average Size 1↔2	Average size of the frames sent in either direction between MAC Station 2 and MAC Station 1

Network Layer Matrix View

From Detail View, click on the  button to open a window with Network Layer Matrix View. From Summary View, set the view preferences to **Network Layer Matrix** to see this view in the first tab.

Network Layer Matrix View is available as a chart showing the ten network conversations with the most traffic or as a table showing all network conversations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station addresses and names in the conversation are provided in the table or chart. The name and address are the same if Surveyor does not have a name table with address-to-name correspondences.

Chart

Network Layer Matrix View as a chart shows only ten network conversations. The ten conversations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the “top ten” conversations based on a different information field.

Table


Network Layer Matrix View as a table shows network activity from the view of network station pairs. The table lists statistics for all pairs found. The table can be customized to include other columns of information. Table columns listed in italics are the default Network Layer Matrix View columns.

Press the right mouse on any table entry to create a quick filter using the selected network layer conversation. See Chapter 7 for information on quick filters.

Table 16. Table Columns for Network Layer Matrix View

Table Column	Description
Net Station Name 1	Name of a network station
Net Station Address 1	Network layer address of a network station
Net Station Name 2	Network layer address of a second network station
Net Station Address 2	Address of a second network station in IP address format
VLAN Id	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time.
Frames 1→2	Number of frames sent from Network Station 1 to Network Station 2
Frames 2→1	Number of frames sent from Network Station 2 to Network Station 1
Frames 1↔2	Number of frames sent in either direction between Network Station 1 and Network Station 2
Rel % Frames 1↔2	Percentage of frames sent in either direction between Network Station 1 and Network Station 2 relative to the total number of frames
Bytes 1→2	Number of bytes sent from Network Station 1 to Network Station 2
Average size 1→2	Average size of the frames sent from Network Station 1 to Network Station 2
Bytes 2→1	Number of bytes sent from Network Station 2 to Network Station 1
Average Size 2→1	Average size of the frames sent from Network Station 2 to Network Station 1
Bytes 1↔2	Number of bytes sent in either direction between Network Station 1 and Network Station 2
Rel % Bytes 1↔2	Percentage of bytes sent in either direction between Network Station 1 and Network Station 2 relative to the total number of bytes
Abs % Bytes 1↔2	Percentage of bytes sent in either direction between Network Station 1 and Network Station 2 relative to the total network capacity (measured in bytes)
Average Size 1↔2	Average size of the frames sent in either direction between Network Station 2 and Network Station 1

Application Layer Matrix View

From Detail View, click on the  button to open a window with Application Layer Matrix View. From Summary View, set the view preferences to **Application Layer Matrix** to see this view in the first tab.

Application Layer Matrix View is available as a chart showing the top ten application conversations or as a table showing all application conversations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station addresses and names in the conversation are provided in the table or chart. The name and address are the same if Surveyor does not have a name table with address-to-name correspondences.

Chart

Application Layer Matrix View as a chart shows only ten applications over network conversations. The ten conversations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the “top ten” conversations based on a different information field.

Table

Application Layer Matrix View as a table shows network activity from the view of applications over network station pairs. The table lists statistics for applications within all station pairs found. The table can be customized to include other columns of information. Table columns listed in *italics* are the Application Layer Matrix View default columns.

Press the right mouse on any table entry to create a quick filter using the selected network layer conversation. See Chapter 7 for information on quick filters.


Table 17. Table Columns for Application Layer Matrix View

<i>Table Column</i>	<i>Description</i>
<i>Net Station Name 1</i>	Name of a network station
<i>Net Station Address 1</i>	Network layer address of a network station
<i>Net Station Name 2</i>	Network layer address of a second network station
<i>Net Station Address 2</i>	Address of a second network station in IP address format
<i>Application</i>	Name of the application running over the network station pair

Table 17. Table Columns for Application Layer Matrix View

VLAN Id	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time. Click on the VLAN ID to see a network station or network conversation view of that VLAN.
Frames 1→2	Number of frames sent from Network Station 1 to Network Station 2 for this application
Frames 2→1	Number of frames sent from Network Station 2 to Network Station 1 for this application
Frames 1↔2	Number of frames sent in either direction between Network Station 1 and Network Station 2 for this application
Rel % Frames 1↔2	Percentage of frames sent in either direction between Network Station 1 and Network Station 2 for this application relative to the total number of frames
Bytes 1→2	Number of bytes sent from Network Station 1 to Network Station 2 for this application
Average size 1→2	Average size of the frames (in bytes) sent from Network Station 1 to Network Station 2 for this application
Bytes 2→1	Number of bytes sent from Network Station 2 to Network Station 1 for this application
Average Size 2→1	Average size of the frames (in bytes) sent from Network Station 2 to Network Station 1 for this application
Bytes 1↔2	Number of bytes sent in either direction between Network Station 1 and Network Station 2 for this application
Rel % Bytes 1↔2	Percentage of bytes sent in either direction between Network Station 1 and Network Station 2 for this application relative to the total number of bytes
Abs % Bytes 1↔2	Percentage of bytes sent in either direction between Network Station 1 and Network Station 2 for this application relative to the total network capacity (measured in bytes)
Average Size 1↔2	Average size (in bytes) of the frames sent in either direction between Network Station 1 and Network Station 2 for this application

VLAN View

From Detail View, click on the  button to open a window with VLAN View. From Summary View, set the view preferences to **VLAN** to see this view in the first tab.

VLAN View is available as table showing statistics or as a chart showing the ten virtual LANs with the most traffic. Click on the tab at the bottom of the window to select **Table** or **Chart**. The only virtual LAN protocol recognized at this time is Cisco's ISL protocol.

Chart

VLAN View as a chart shows only ten VLANs. The ten VLANs displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the "top ten" VLANs based on a different information field.


Table

VLAN View as a table shows network activity from the view of virtual LAN traffic. The table lists statistics for all VLANs found. The table can be customized to include other columns of information. You can click on any VLAN Id and see a Network Layer Host Table View or a Network Conversation Matrix View for that VLAN. Table columns listed in *italics* are the default VLAN View columns.

Table 18. Table Columns for VLAN View

<i>Table Column</i>	<i>Description</i>
<i>VLAN Id</i>	Number (in decimal) of the virtual LAN. Click on the VLAN ID to see network layer and application layer host and matrix tables of that VLAN.
<i>Frames</i>	Total frames captured that are associated with a VLAN
<i>Rel % Frames</i>	Percentage of all frames captured that are associated with a VLAN
<i>Bytes</i>	Total bytes captured that are associated with a VLAN
<i>Rel % Bytes</i>	Percentage of all bytes captured that are associated with a VLAN
<i>Abs % Bytes</i>	Percentage of the total network capacity in bytes that are associated with a VLAN
<i>Total Bytes</i>	Total bytes captured

Address Map View

From Detail View, click on the  button to open a window with Address Map View. From Summary View, set the view preferences to **Address Map View** to see this view in the first tab.

Address Map View is available as table showing all associations between MAC station names and addresses and network station names and addresses. Address Map View is not available as a chart. Use this table if you need to determine what MAC stations are associated with what network stations.

Table 19. Table Columns for Address Map View


<i>Table Column</i>	<i>Description</i>
MAC Station Name	Name of the MAC station
MAC Station Address	MAC station address
Network Station Name	Name of the network station
Network Station Address	Network layer address of the network station

Packet Summary View

Packet Summary View shows a real-time protocol decode. Packets received are decoded and the result of the decode is displayed. The packets scroll up the screen as they are decoded. A unique color can be used to display packets of each different protocol layer.

From Summary View, set the view preferences to **Packet Summary** to see this view in the first tab. From Detail View, select **Packet Summary** from the **Monitor View** menu to open a window with the Packet Summary View.

Duplicate Address View (Expert only)

From Detail View, click on the  button to open a window with Duplicate Address View. You can also see this view from Summary View. To see Duplicate Address View, set the view preferences to Duplicate Address View to this view in the first tab.


Duplicate Address View is available as table showing all duplicate network addresses. MAC station names and addresses and network station names and addresses. Duplicate Address View is not available as a chart. Use this table if you need to determine what stations may have duplicate addresses.

If you are monitoring a remote device, you must open one of the host tables for that remote device for new duplicate addresses to show in Duplicate Address View.

Table 20. Table Columns for Duplicate Address View

Table Column	Description
Network Station Name	Name of the network station
Network Station Address	Network layer address of the network station (duplicate)
MAC Station Name	Name of the MAC station
MAC Station Address	Address of the MAC station
VLAN ID	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time. Click on the VLAN ID to see a network station or network conversation view of that VLAN.

Expert View (Expert only)

From Detail View, click on the  button to open a window with Expert View. From Summary View, set the view preferences to Expert View to see this view in the first tab.

Two tables are available in Expert View, an Overview Table and an Analysis Table. Click on the tabs at the bottom of the window to switch tables. Expert view is not available as a chart.

Analysis Table

The analysis table shows each expert symptom found by Surveyor's expert software. When Surveyor finds an event that could indicate a network problem, the event is logged in the table. Frame ID (Capture View only), source address, destination address, VLAN ID, and the time stamp are provided for each entry in the table. Each table entry also shows a summary that provides more information about the symptom. Double-click on any table entry to view complete expert information about the symptom, including suggestions for correcting the problem.

The time stamps displayed in the Analysis table are based on the Windows system clock. For Capture View, frames are processed for inclusion in the table in batches of 100, so it is possible for two frames to have exactly the same time stamp. The order in which symptoms are displayed is always the same order in which they were encountered in the capture file or buffer.

Note: The time stamps when viewing a capture file in the Analysis table will contain the current system time and date, not the time and date when the information was captured. Also, the time stamp field in the Analysis table

increments from the time the device was last started for Explorer and Voyager devices. The time stamp values are not accurate for these devices.

Table 21. Table Columns for Expert View, Analysis Table

Table Column	Description
Expert Symptom	Symptom discovered by Surveyor's expert analyzer
Timestamp	Timestamp in the frame that caused the expert symptom
Expert Summary	More detailed information about the symptom. Double click on the row to see full information and suggested actions.
Frame ID	Frame number in the capture buffer or file that caused the expert symptom. Frame ID displays only when viewing the expert information from Capture View.
Address1	Source address in the frame that caused the expert symptom
Address2	Destination address in the frame that caused the expert symptom
VLAN ID	Number (in decimal) of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time. Click on the VLAN ID to see a network station or network conversation view of that VLAN.

Overview Table

The overview table shows a count of all expert symptoms found, displayed by category. The categories for the expert events give you a general picture of the types of expert events that are being discovered.

Table 22. Table Columns for Expert View, Overview Table

Table Column	Description
Expert Category	Category of symptom discovered by Surveyor
Value	Number of symptoms discovered in each category

The Overview Table counters are listed below.

ICMP All Errors	<u>Duplicate Network Address</u>
ICMP Destination Unreachable	MST Topology Change
ICMP Redirect	SAP Broadcasts
BOOTP Requests	OSPF Broadcasts
ARP Broadcasts	RIP Broadcasts
<u>NFS Retransmissions</u>	ISL Illegal VLAN ID
TCP/IP SYN Packets	ISL BPDU/CDP Packets
TCP/IP RST Packets	<u>IP Time to Live Expiring</u>
<u>TCP/IP Retransmissions</u>	<u>IP Checksum Errors</u>
<u>TCP/IP Zero Window</u>	<u>Illegal Network Source Address</u>
<u>TCP/IP Long Acks</u>	Illegal MAC Source Address
<u>TCP/IP Frozen Window</u>	Total MAC Stations
Network Overhead	Broadcast/Multicast Storm
<u>Non Responsive Stations</u>	Physical Errors
	<u>HSRP Errors</u>

More detail is provided for the counters that are underlined in the Overview Table tab. Click on any underlined counter to bring up a table listing the source address, destination address, count, and VLAN ID for all errors of this type. The detail table allows you to see immediately which stations are responsible for generating the most occurrences for a particular symptom.

Note: When viewing the statistics for a host pair from a remote resource, you must have the Application Layer Matrix View table open for that resource to see the statistics.


Table 23. Table Columns for Detail of Expert Overview Counters

Table Column	Description
Station Name 1	Name of the station.
Station Name 2	Name of the other station in the conversation. This field only has a value for symptoms that involve conversations.
Value	Number of times the symptom has occurred for this address or address pair.

Table 23. Table Columns for Detail of Expert Overview Counters

VLAN ID	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time. Click on the VLAN ID to see a network station or network conversation view of that VLAN.
----------------	---

Application Response Time View (Expert only)


From Detail View, click on the  button to open a window with Application Response Time View. From Summary View, set the view preferences to Application Response Time View to see this view in the first tab.

Application Response Time View is available as table showing connection time and connection number information about application protocols. Application response time view is not available as a chart. Use this table if you want to find out which applications are responding very slowly in the network.

Table 24. Table Columns for Application Response Time View

Table Column	Description
Protocol	Name of the application protocol discovered
Minimum Time	Shortest time taken for the application to make a connection
Maximum Time	Longest time taken for the application to make a connection
Average Time	Average time taken for the application to make a connection
Connections	Number of connections processed for this application

Hints and Tips for Using Views

- When viewing a table, single click on columns to sort the table data. Click on a column header to list rows in descending order of the values for that column. Click again on a column header and rows will be sorted this time in ascending order. Click on another column header and rows will be sorted by the values in that column. Every click on a column header toggles the sort between ascending and descending order for that column.
- A **Pause** button is available on some charts and tables. Click the  button to freeze the display. Click the button again to resume display update.
- The fields shown in some tables can be customized. Choose **View Options...** from the **View** menu in Detail View to change the columns that display for a table.

- There are many view windows you can open. You may want to keep the number of open windows to a reasonable level to avoid confusion and conserve system resources.
- The Summary View allows only one type of monitoring view per resource. Go to Detail View to see multiple views per resource simultaneously.
- In charts, hold down both the right and left mouse button and move the mouse to rotate the 3D graphic view.
- Double-click with the left mouse button on the view displayed within Summary View to bring up the Detail View for that resource.
- Use **Print** from the **File** menu to print the graph or chart in the currently selected window.
- Cells within a table or an entire table can be exported to an Excel™ spreadsheet. Go to the table view and select the **Export** option from the **File** menu to export the entire table. Information is saved in CSV format which can be opened from Excel.
- Double-click on the MAC Statistics View in Detail View to bring up Capture View.
- Data in a chart will be sorted by the last sorted column in the corresponding table.
- Click the right mouse on a table entry in Host Table, Network Table, Application Table, Host Matrix, Network Matrix, or Application Matrix view to bring up a menu for creating a quick filter. You'll get a choice of creating a capture or display filter unless you are in Capture View. In Capture View, you can only create a display filter. When you make a choice from the menu, the quick filter dialog box opens with the address(es) from the table entry in the address fields for creating a filter.
- In Capture View, press the F11 key to zoom in on any of the three panes in the window. Press F11 again to restore the view to all three panes.
- To see which capture filter or transmit specification is associated with a particular resource, choose **Active TSP** and **Capture Filter** from the **Module** menu.
- You can directly access statistics about a particular host associated with an expert event. From the Expert Overview table, click on any of the counters underlined in blue to see the symptoms broken down by host or conversation. You can then click on the host for more in-depth statistics.

7 Capture and Display Filters

Filters are extremely flexible. They allow you to filter and count data in just about any way you can imagine. We have provided example filters to give you an idea of the types of filters that can be created. In most instances you'll want to filter and capture only a subset of all network data. The same holds true for viewing data. In many cases you'll want to filter and view only a subset of the captured data.

To create Surveyor filters you use a graphical scripting language. You'll find it intuitive and easy to use if you have experience doing simple programming or experience working with "meta-languages." After you become familiar with this graphical scripting language, you'll have a powerful tool for getting exactly the data you want.

In capture filters, you construct statements that select and/or count incoming data. In view filters, you construct statements that select and/or count data to be displayed in Capture View. Each statement is composed of conditions (for example, `destination address = JSMITH`) and actions to take if the condition is satisfied (for example, capture the packet).

Capture and Display filters appear in their own windows. The windows show all the filter statements and the structure of the filter. The **Filter** window interface leads you through the process of creating filters. Dialog boxes are used to create the statements. You do not need to memorize specific syntax.

Convenient buttons are available to save, create, open, load, and unload Capture and Display filters. You can also add/delete statements from the toolbar or from the menus. When you add or modify a statement, its associated dialog box is displayed.



All changes and additions to the filter are made from dialog boxes. Dialog boxes appear when you double-click on the statements shown in the window; keystrokes and the right mouse button are context sensitive within the **Filter** window. You can write and attach a description to a Capture or Display Filter you save for later use.

Display filters allow you to view a subset of the data you have already captured. They can be used to refine your view of captured information. For example, you might choose to capture all packets sent/received by a specific IP network station. Later, you might decide you want to look at the data for specific types of packets that are flowing through the station. A display filter allows you to view this subset of captured data.


This section describes both Capture and Display Filters; there are only minor differences. Differences are clearly noted in the text.

Activating Capture and Display Filters

Display and capture filters are activated in different ways. Also, some options for capture filters are not used in display filters.

A display filter is active when it appears in the Filter window and the  button is pressed on Filter toolbar. The default for the display filter is ON; the display filter is active unless you press the  button. If you close the Filter window, the display filter is no longer active.

You can keep the display filter ON at all times; if you make changes, the next time you view data in Capture View the new filter will be used immediately. If you already have a Capture View window open for the capture file, select the **Refresh...** option from the **File** menu in Capture View to refresh the view using the new filter. There is only one display filter that applies for all view windows.

The capture filter must be loaded to the hardware module. It is not active until you press the  button on the Filter toolbar. It remains active for that module until you unload the filter. Since capture filters are associated with a hardware module, different capture filters can be loaded to different modules.

Some options available in capture filters make no sense for display and are therefore not supported:

- **Actions** -- Display filters do not use custom counters. The actions “capture” and “trigger” used with capture filters are replaced by the action “display.”
- **ROOT statement** -- Display filters do not have a global setting for Counter 1 as custom counters are not supported. The buffer trigger position is not supported for display filters.

Filter Parts and Structure

The capture or display filter consists of labels and a series of statements that define actions. The actions result in the subset of data that is captured or displayed by Surveyor. The statements and labels have an order, structure, and syntax. You always start and stay in `State0` until an action takes you to a different state.

Structure

Capture and display filters have the following structure:

```
ROOT statement      The root statement for capture filters
                    contains settings for global variables
                    ((Counter 1 and post trigger buffer
                    position)). The root statement for display
                    filters contains no variables.)

STATE0 identifier   Label for GoTo actions
                    IF statement (Specify conditions and
                    actions)
                    ELSE IF statement (optional - same structure
                    as IF statement)
                    other ELSE IF statements
                    ELSE statement (if no conditions satisfied,
                    take these actions)

STATE1 identifier   Label for GoTo actions)
                    IF statement (Specify conditions and
                    actions)
                    ELSE IF statement (optional - same structure
                    as IF statement)
                    other ELSE IF statements
                    ELSE statement (if no conditions satisfied,
                    take these actions)

.                  .                  ..
.                  .                  ..
.                  .                  .

STATE7 identifier   Label for GoTo actions)
                    IF statement (Specify conditions and
                    actions)
                    ELSE IF statement (optional - same structure
                    as IF statement)
                    other ELSE IF statements
                    ELSE statement (if no conditions satisfied,
                    take these actions)
```

Frame Types

Four types of frames can be collected and displayed. Capture-and display frame types are set in any IF or ELSE IF statement.

Frame types are:

Good Frames	Frames that have no errors.
CRC Error Frames	All frames that contain CRC or Alignment errors (this will include runt frames).
Runt Frames	All runt frames. All runt frames are also considered CRC errors.
Other Frames	All other types of frames. For example, an oversize frame.

States

States are similar to labels (addresses) for a set of statements. States allow multiple sets of statements in a filter. You can specify up to 8 states. You always start and stay in State0 until an action takes you to a different state.

In most instances, you will only need only one or two states in a filter. Here is example filter showing three states:

```
STATE0
IF (DA=Santosh) GoTo State1
ELSE IF (DA=Yancy) GoTo State2
ELSE GoTo CurrentState

STATE1
IF (DA_IP_Filter1) Counter1; Capture; GoTo CurrentState
ELSE GoTo State0

STATE2
IF (DA_IP_Filter2) Counter2; Capture; GoTo CurrentState
ELSE GoTo State0
```

States are selected in the action portion of dialog boxes for statements. "Current state" means stay in the state number that contains the statement. When you select a state other than the current state, a GoTo phrase will display as part of the statement in the **Filter** window. The GoTo state always displays for the ELSE statement, even if its the current state.

Statements

To create statements, you use the dialog boxes to create a condition and to specify actions to be taken if the condition is satisfied. Once a condition is true, the next condition is not examined. For the next frame you remain in the current state or go to a different state, depending on the `GoTo` action specified in the statement. If no condition is met, the actions in the `ELSE` statement are taken.

Below is a synopsis of the logic sequence for statements:

IF statement	IF (these conditions are satisfied) THEN (take these actions, go to State n)
ELSE IF statement	ELSE IF (these conditions are satisfied) THEN (take these actions, go to State n)
ELSE IF statement	ELSE IF (these conditions are satisfied) THEN (take these actions, go to State n)
ELSE statement	ELSE (take these actions, go to State n)

Filter Elements

In Advanced mode, filter elements are the primary building blocks of a filter combination. A filter element contains the patterns for creating the logical conditions that will be used as a test against incoming frames.

Filter elements are always assigned a name and that name is referenced in the filter combination. Filter element templates are provided which can be used as is, or you can define your own filter elements. Typically you will define your own filter elements based on the templates provided. See “Standard Filter Elements” in Appendix B for the filter elements supplied with Survevor.

Most filter elements have a defined offset and pattern within a frame. However, some elements have no specific offset and length, such as `MatchAll`. Some template filter elements have predefined values, such as `DA_BROADCAST (FFFFFFFFFFFFFF)`.

The filter elements you create will usually have a specific hexadecimal or decimal value assigned to them as well. For example, assume you want to filter the IP destination address for the value `206.250.221.1`. You could select the `DA_EV2_IP` template filter element and then create a filter element specific to your needs. The new filter element can be used to create the filter combinations you require for filtering frames.

Any specific value you create for filter elements can have “don’t care” values. For example, assume you’re only looking for `FF34` in the first two bytes of the MAC destination address. You could specify the values in your filter as `FF34XXXXXX`, where `X` indicates you don’t care about the values in the last three offsets. Note that for IP

addresses using decimal values you can only use X characters for complete sub-addresses. For example, 128.XXX.2.2 is allowed, but 128.12X.2.2 is not allowed.

Actions

Actions are set in the action portion of the dialog box for IF and ELSE IF statements. Actions are all that can be set in an ELSE statement.

Actions available for capture filters are:

Capture	Capture the frame.
Trigger	Capture the frame and mark it as a trigger. In view mode, a trigger frame is numbered as frame zero and marked with the name TRIGGER .
Increment Counter	Increment the custom counter. Counter 1, Counter 2, Counter 3, or any combination of the custom counters can be incremented.
GoTo State	<p>Go to a state. The state can be the current state or any other state defined in the capture filter. The state is like a label or routine name in a program. It's there so it can be referenced by a GoTo action.</p> <p>If Trigger is selected as an action, Capture is automatically selected as well. The only function of Trigger is to mark a frame to specify the post trigger buffer position.</p>

Actions available for display filters are:

Display	is the only action available in statements for display filters.
GoTo State	Go to a state. The state can be the current state or any other state defined in the display filter. The state is like a label or routine name in a program. It's there so it can be referenced by a GoTo action.

Filter Dialog Boxes

Dialog boxes appear so you can construct ROOT, ELSE, ELSE IF, or IF statements. Double-clicking on a statement displays its dialog box.

Root Dialog Box

The dialog box for the **ROOT** statement allows you to set the condition of Counter 1 in filter combinations, and set the post trigger buffer position. No **ROOT** dialog box appears for display filters.

Counter 1	The condition value of Counter 1 for testing conditions can be set. For example, if the custom counter is set to 10 in the ROOT statement, and Counter 1 is used as part of a condition, the condition will be satisfied when the counter reaches 10.
Post Trigger Buffer Position	This defines what percentage of the buffer used to store frames once data capture is triggered. For example, assume the post trigger buffer position is set to 50% for a module with 4MB of memory. After the module is triggered, frames will be captured until 2MB of the module memory is full.

IF and ELSE IF Dialog Box

The dialog boxes for an **ELSE IF** or **IF** statement are identical. The dialog boxes for the **IF** or **ELSE IF** statements have two modes, Quick and Advanced. Select the mode by clicking on the appropriate tab at the top of the box. Quick mode allows you to create a simple filter using station addresses. Advanced mode allows you to filter on any element or offset within the packet and to create logical combinations of these elements.

The dialog box is divided into two parts, **Condition** and **Action**. The condition part of the dialog box is for setting filter combinations and, if necessary, changing the type of frames to be filtered. The action part of the dialog box is for setting actions and setting the next state to execute. It consists of check boxes to select the actions you want. The actions are only taken if the conditions set in the combination filter are satisfied. A pull-down box selects where to go once actions are complete. **Current State** results in remaining in the current state.

The frame type check boxes allow you to select the types of frames you want to capture with this **IF** statement. For example, if you want to capture only good frames, leave the **Good Frames** box checked and deselect all other frame types. If you want to capture only error frames, leave all frame types selected with the exception of the **Good Frames** box.

ELSE Dialog Box

The dialog box for the **ELSE** statement is identical to the action part of the dialog box for the **IF** statement. You can specify actions for the **ELSE** statement but no conditions. The **ELSE** statement actions are taken when no conditions for previous statements are satisfied.

Filter Modes

Use one of two modes to build filters, Quick or Advanced. Quick mode allows you to do simple filtering on station addresses (MAC, IP, or IPX). Advanced mode allows you create more complex filters using user-defined filter elements and logical operators. Advanced mode provides an interface for setting up user-defined filter elements.

User-defined elements allow precise control over the information captured or displayed. Surveyor includes templates to aid in the creation of filter elements, and includes some ready-to-use elements (for example, capture a broadcast packet).

The tabs at the top of the dialog box for an IF or ELSE IF statement select the mode for the current statement. A statement is created using either Quick or Advanced mode.

If you create a statement in one mode and then change the mode, once you click on the **OK** button in the dialog box the new mode applies. Information entered using the other mode for this statement is lost.

You can have a statement that uses Advanced mode and another statement that uses Quick mode within the same state.

Quick Mode

Quick mode provides a way to set up simple filters using station addresses, network addresses and protocols. Quick mode is one of two modes available for setting up IF and ELSE IF statements in filters. To enter Quick mode, open an IF or ELSE IF statement and, if necessary, click on the **Quick** tab.

The dialog box for Quick mode has two parts: condition and action. You set conditions for the filter in Quick mode by filling out a row in the dialog box. Each row consists of a protocol selection, two station addresses, and a direction indicator. Four sets of conditions (hence four rows) can be set in Quick mode.

The protocol is selected from the pull-down box. Station addresses can be entered directly or by selecting the **Station** field and then double-clicking on an address in the name table. The direction indicator allows you to select a direction between stations. Check boxes allow to enable or disable the current row. You can filter for packets going from Station1 to Station2 (->), Station2 to Station1 (<-), or gather packets in either direction (<->). Put an X in the row to disable the row as a condition in the filter.

You can also use wildcards when specifying addresses to capture data on more than one station. An "X" used as a character for an address string means that any value will be accepted for that position; for example, 343F4AXXXXXX.

In Quick mode, you make extensive use of the current name table. If you are just starting with Surveyor, you will probably want to build a name table with the names

and addresses of stations on your network. If you have a name table for your network, be sure to load the name table so names are available in the window.

Actions are the same for all statements regardless of the mode.

The conditions defined in each row in Quick mode have an implied OR operator. If you want more flexibility with AND, OR, or NOT operators, use Advanced mode.

Creating Condition Lines

Four condition lines can be set for an IF statement in Quick mode. Select a protocol, a frame type, and a direction for each line from the pull-down boxes. A station address that corresponds to the protocol can be entered in the **Station 1** or **Station 2** fields. Both fields may contain an address. Set up only the lines required for your filter.

Protocols	MAC, IP, or IPX.
-----------	------------------

Frame Types	All, EV2 (EthernetII), SNAP, 8022 (IEEE 802.2), 8023 (IEEE 802.3) (Frame type applies to IP-layer addresses only)
--------------------	--

Directions

Station 1 is Source Address, Station 2 is Destination Address

Station 2 is Source Address, Station 1 is Destination Address

Station 1 is either Source or Destination Address

Station 2 is either Source or Destination Address

If no value is entered for a **Station** field, all stations are captured. For example, if you set an address for Station 1, no address for Station 2, and set the direction to -> all packets having Station 1 as the Source Address are captured, regardless of the Destination Address.

If the station address is not the same type as the protocol selected an error message appears. For example, if you set the protocol to **IPX**, you are not allowed to insert a MAC address on that condition line. Only the frame types used with the selected protocol are allowed. For example, if the protocol is set to **IP** you can only select **EV2** or **SNAP**. If the protocol is set to **MAC**, the frame type is set to **All** and no options are available.

Condition lines can be enabled or disabled for the statement. Make sure that the condition line has the **Enable** check box selected to enable the condition line.

An OR operation is implied between condition lines. For example, assume you set up two condition lines. If the conditions of either line are satisfied, the condition is satisfied.

Name Table Window

The **Name Table** window shows all name and address associations, including the protocol and the frame type. The name and address associations displayed are those in the currently active name table. Load the correct name table before accessing the **IF Statement** dialog box to make sure names are available. Double-clicking on a name table entry will load that name into the currently-selected **Station Address** field.

Advanced Mode

Advanced mode provides a way to set up any type of filter required. Advanced mode is one of two modes available for setting up IF and ELSE IF statements in filters. To enter Advanced mode, open an IF or ELSE IF statement and, if necessary, click on the **Advanced** tab.

The dialog box for Advanced mode has two parts, **Condition** and **Action**. Conditions are set in Advanced mode by creating filter combinations in the **Condition** box near the top of the window. The filter combinations are built by selecting a combination of filter elements, operators, and custom counters.

You build the filter combination by double-clicking on filters elements and single clicking on operators (**AND**, **OR**, and **NOT**) or **Counter 1**. Illegal combinations are not allowed by the dialog box. For example, you can't specify an AND and an OR operator right next to each other or filter elements right next to each other. Example filter combinations are shown below:

```
DA_BROADCAST AND NOT DA_IP  
DA=Santosh AND (Counter1>=10)  
NOT DA=Santosh OR PktTypeArp
```

In Advanced mode, you may make use of the current name table. Be sure to load a name table so names are available when you click on the **Names...** button.

Actions are same for all statements regardless of the mode.

Creating Filter Elements

The **Offset** and **Pattern** fields define the "masks" that comprise a filter element. The offset defines the position within the packet to start comparing the packet contents with the values in the pattern. If a match occurs, then this portion of the condition is satisfied.

The pattern can be specified as a decimal or a hexadecimal value. The **Dec** and **Hex** buttons to the right of each **Pattern** field determine if the pattern is in decimal or hexadecimal. An X in any position within the pattern indicates that this is a “don’t care” position and that any value will create a match.

The **Name** field shows the name of the filter element. Enter a unique name for the filter element in this field. Once you create a filter element and click on the **Add** button, the name will appear in the **Filter Information** window to the left.

Creating Filter Combinations

The **Filter Combination** field shows the syntax for the condition. You double-click on filters elements and single-click on operators and they appear in the **Filter Combination** field.

If the operation you perform makes no sense to create a Filter Combination, the operation is not allowed. For example, an OR operator makes no sense after an AND operator. As another example, inserting a filter element immediately after another filter element makes no sense and the operation is not allowed.

Press the **AND**, **OR**, or **NOT** buttons to add operators to the filter combination. The operator displays in the **Filter Combination** field. The addition of operators is context sensitive; you cannot add an operator where it makes no logical sense. For example, you cannot add an AND operator immediately after an OR operator. Press the **Clear** button to erase the contents of the **Filter Combination** field.

Counter 1 is a special key that adds a filter element for testing the value of Counter 1. The most common use of Counter 1 is to set it to a particular value and then begin capture once this value is reached. The initial value for Counter 1 is set in the **ROOT** statement in a capture filters.

Filter Examples

Filter examples are supplied with Surveyor. To see examples, open a capture filter file (**FILTER** subdirectory, **.CFD** extension) or a display filter file (**FILTER** subdirectory, **.DFD** extension) from the **Filter** window. From the **Module** menu, select **Filter Description** to access a description of any filter. To find more examples, look in the `..\Surveyor\examples\capture` directory.

Filter Example, Quick Mode

The **Capture Filter** window on the following page shows the capture filter **DA_SA1.CFD**. This filter captures all packets going to and coming from a MAC station. Separate counts are made of the packets sent and the packets received.

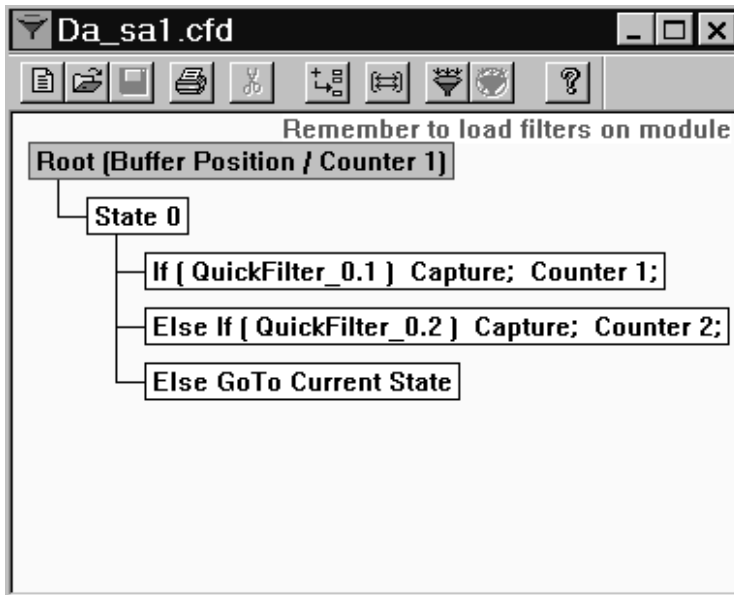


Figure 13. Capture Filter Window and Capture Filter Definition Example

Packets are tested first by the IF statement in State 0. If the packet contains the MAC address specified in the dialog box as a destination address, the packet is captured, Counter 1 is incremented, and the flow continues. Packets are then tested by the ELSE IF statement. If the packet contains the MAC address specified in the dialog box as a source address, the packet is captured, Counter 2 is incremented, and the flow continues. If the packet does not contain the MAC address, the packet is not captured and the next packet is filtered. The following figure shows the dialog box for the IF statement.

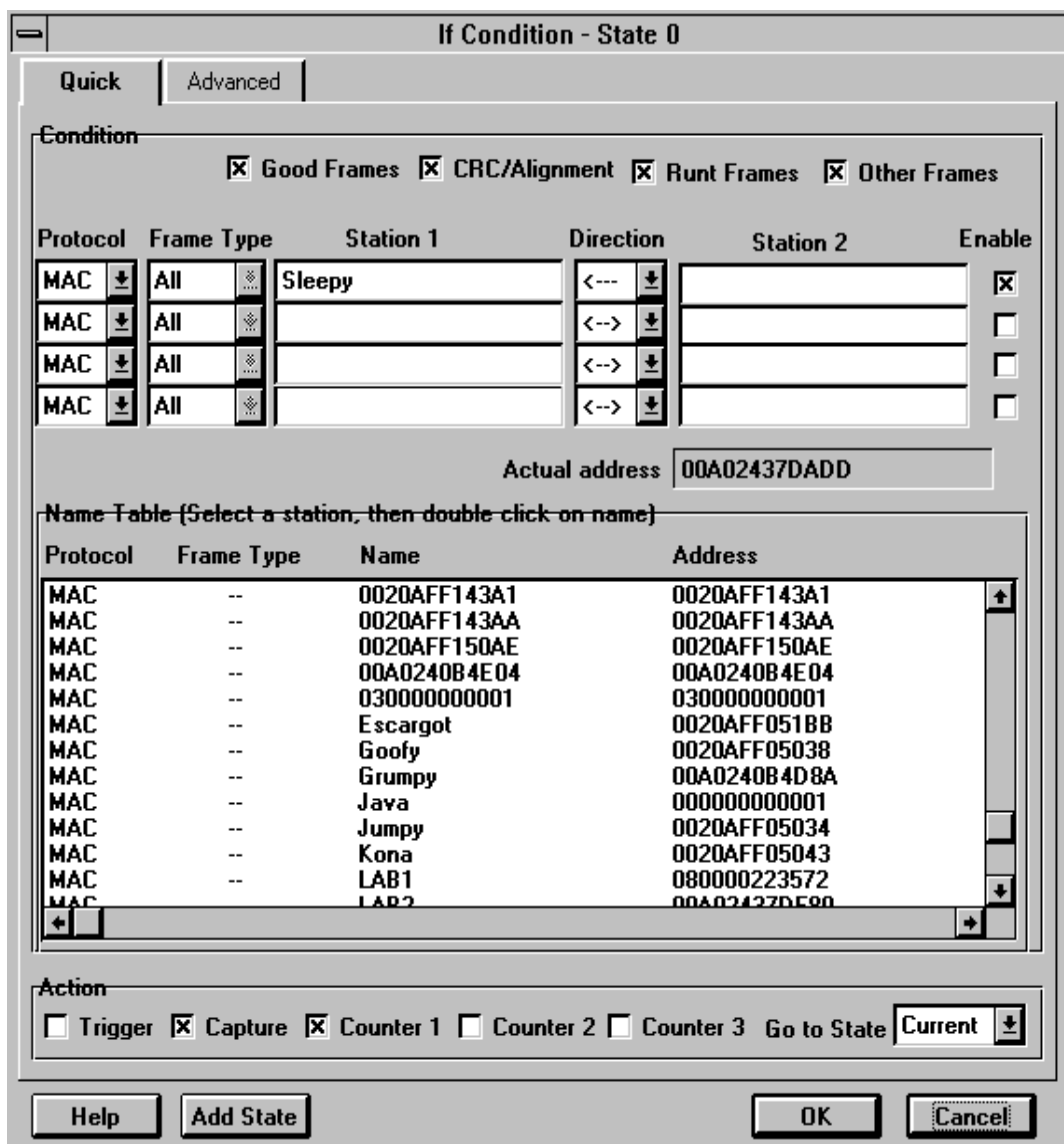


Figure 14. Example IF statement Dialog Box, Quick Mode

In the example, when Sleepy is the Destination Address, capture the packet and increment Counter 1. When Sleepy is NOT the Destination Address, execute the ELSE statement (the next statement in the filter).

Filter Example, Advanced Mode

The **Capture Filter** window below shows the capture filter `EXAM1.CFD`. This filter starts collecting all packets when the first broadcast packet is encountered.

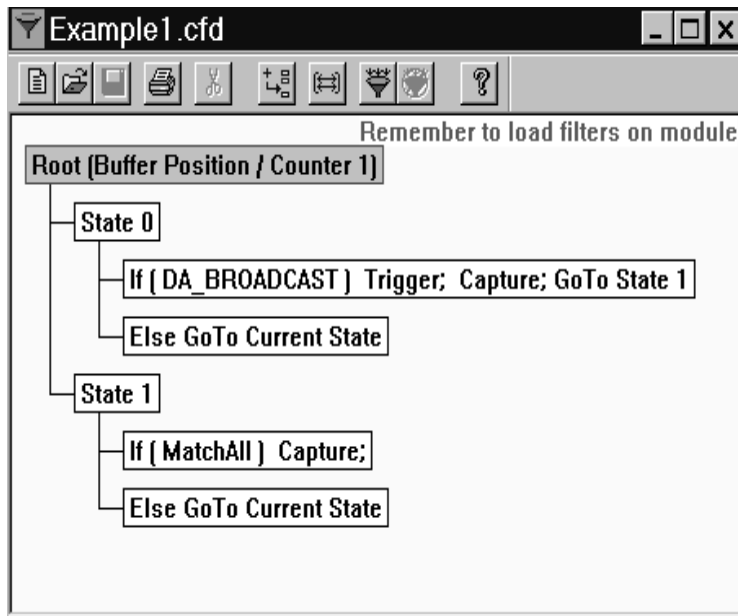


Figure 15. Advanced Mode, Capture Filter Definition

Packets are tested first by the `IF` statement in `State0`. If the packet matches the broadcast mask (`FFFFFFFFFFFF` in the first six bytes) in the **IF Statement** dialog box, the packet is captured and the flow continues with `State1`. If the packet does not contain the Broadcast address, the packet is not captured and the next packet is filtered.

`State1` is executed after the first broadcast packet is encountered. The `IF` statement in `State1` indicates that any packet should be captured. The flow for testing packets remains in `State1` until the capture process is stopped.

The figure below shows the dialog box for the `IF` statement.

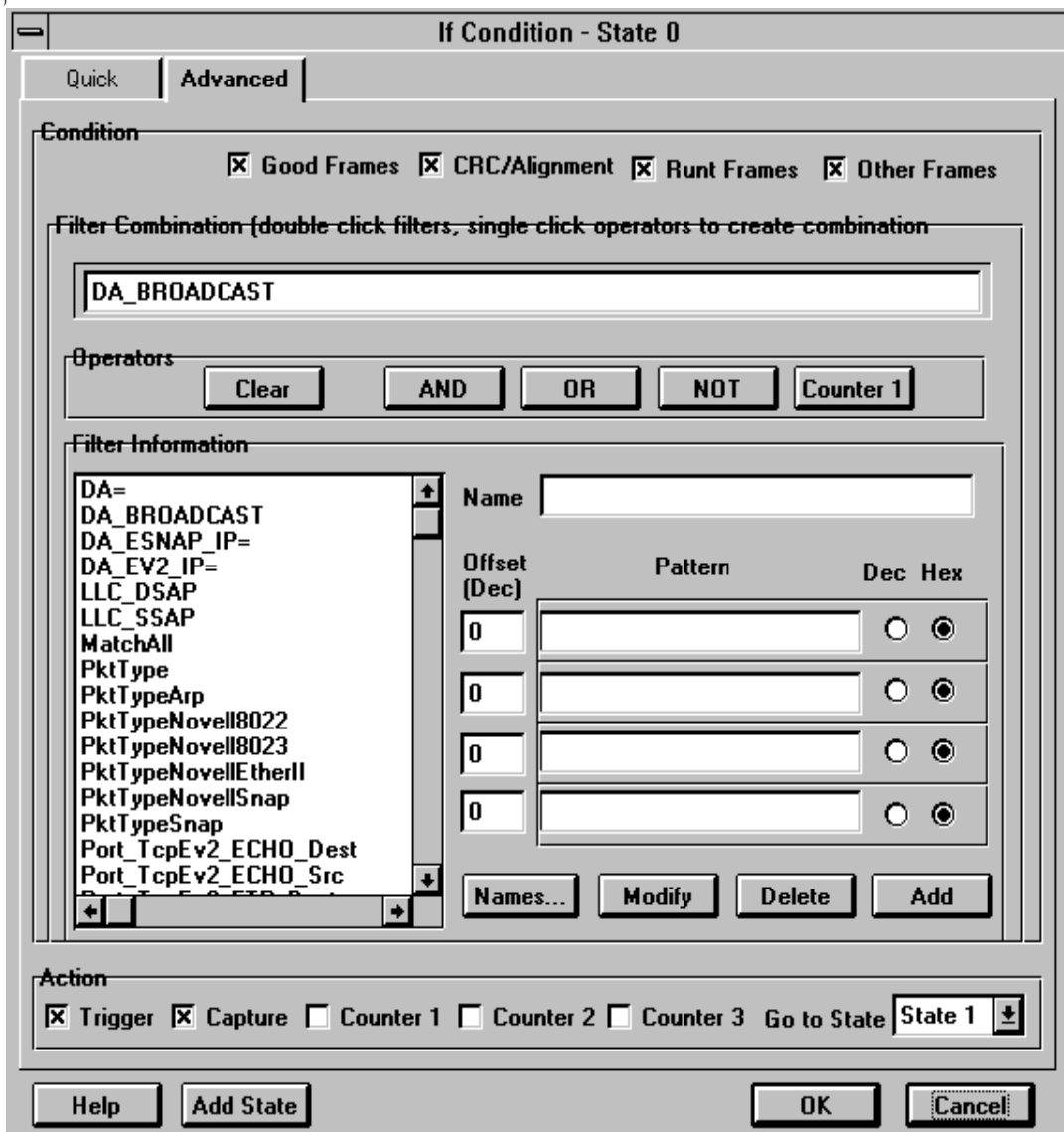



Figure 16. Example IF statement Dialog Box, Advance Mode


In the example, when DA_BROADCAST is matched, capture the packet and set the trigger position. When DA_BROADCAST is NOT matched, execute the ELSE statement (the next statement in the filter).

Rules of the Capture or Display Filter

- The maximum number of filter elements allowed in a state is 8. Filter elements that are reused in different statements do not count against the maximum.
- Counter 1 is the only custom counter that can be used as an element to create a filter element combination.
- There is always at least one IF and one ELSE statement per state. ELSE IF statements are optional.
- The Post Trigger Buffer Position must be greater than zero and less than 100.
- There is always one and only one ROOT statement; you can't delete the ROOT statement.
- In the capture filter, setting trigger will always set capture.

Hints and Tips for Using Filters

- Remember to load the Capture filter to the module before you start capture.
- To edit a statement in the **Display Filter** or **Capture Filter** window, double-click on the statement.
- Use the  button to add states or statements to the **Display Filter** or **Capture Filter** window.
- If you want to look at captured data in many different ways, use display filters rather than capture filters. Capture large blocks of unfiltered data and look at different subsets of the data by using a variety of display filters.
- Use quick mode for capturing or displaying station-to-station or router-to-router activity.
- Always attach a description to a filter you are saving with the **Filter Description** option in the **Filters** menu.
- Remember to leave the **Display Filter Description** window open when using display filters. When the window is closed the filter is no longer active.
- Use the right mouse button to learn about the options available for any statement in a filter. You can immediately see what options are possible depending on where you are in the filter.
- Each bidirectional Quick filter line uses two, filter elements; a single directional Quick filter line uses one filter element.
- If you have already captured data and then create a display filter, the filter is not automatically applied. Use the **Refresh** option from the **File** menu to apply the display filter to the captured data.

- You can use the  button on the Filters toolbar or close the **Display Filter Description** window to turn a display filter off and show the entire contents of the capture buffer or capture file.
- To see which capture filter is associated with the current resource, choose **Active TSP and Capture Filter** from the **Module** menu.

8 Transmit Specification

The Packet Blaster plug-in allows you to generate packets and send them onto a network. This can be used to force the network to respond to known or suspected problem conditions or loads. Transmitted data can answer “What If?” questions about the network or particular network resources.


To transmit data, you first set up a Transmit Specification. After the Transmit Specification is loaded to a module, click on the **Start** button to begin transmit. You can also transmit a previously captured data file (capture file).

You can transmit the contents of a capture file. Data previously collected in the capture file can be loaded to a module and sent to the network.

Using a Century Media Module, you can transmit packets at full network speed or faster. This allows you to set up high traffic conditions and see how the network performs. Surveyor can also transmit a variety of user-defined packet contents to see their effect on the network.

With multiple modules, transmitted data can be captured by another Century Media Module. You can use the capture and view features in the Surveyor System Manager software to analyze the results, all from the same PC.

Transmit Specifications

An example **Transmit Specification** dialog box is shown in the figure on page 8-3. For additional views of this dialog box, see the Transmit Specification examples at the end of this chapter. To bring up the **Transmit Specification** dialog box, press the  button from the **Detail View** toolbar.

Transmit Specification Dialog Box

Transmit Specifications are defined in a dialog box. The **Transmit Specification** dialog box contains:

- A **Defined Streams** list box (top) for viewing defined streams.
- Radio buttons and fields for defining a stream (middle)
- Buttons for adding, modifying, or deleting streams, editing data
- Transmission status information
- Buttons for loading the module, opening/saving the specifications, and adding streams using templates and Magic PacketsTM

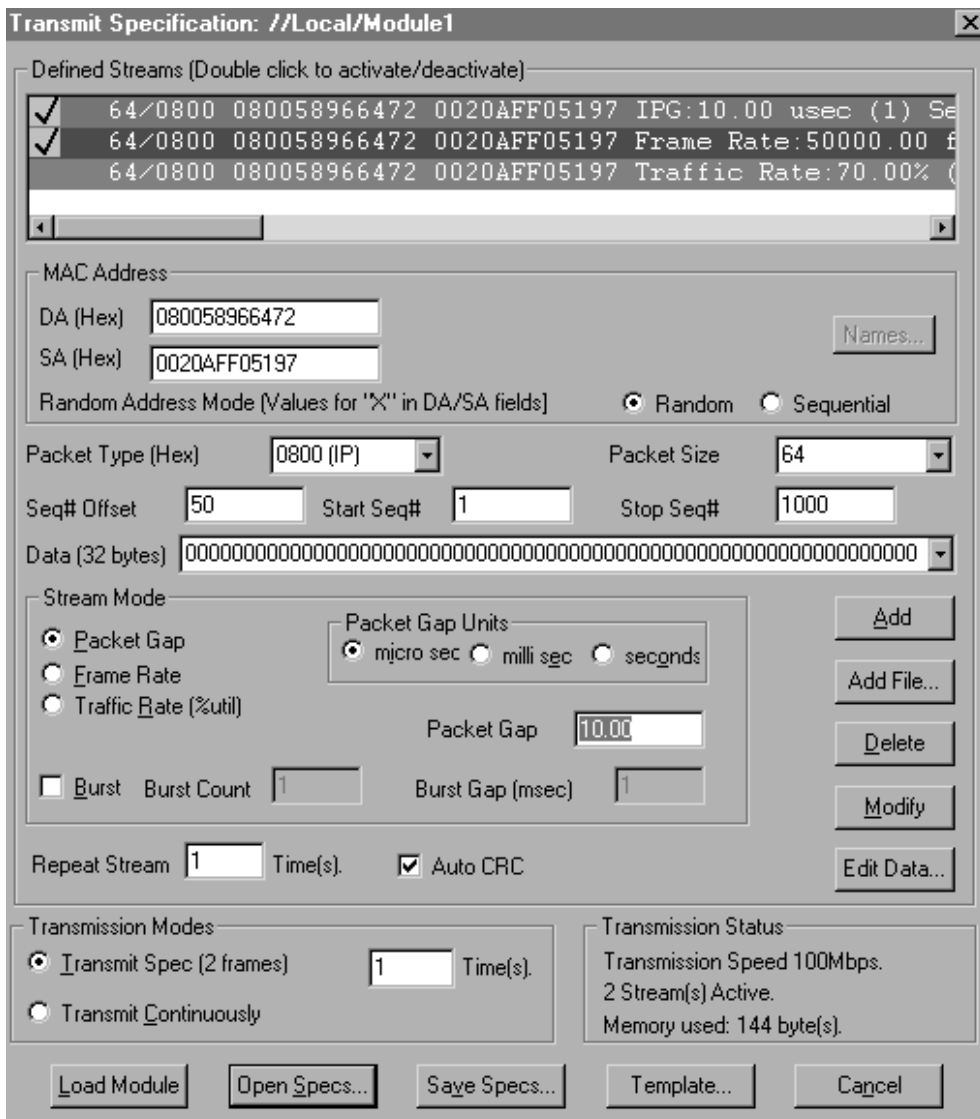


Figure 17. Transmit Specification Dialog Box

Defined Streams List Box

A defined stream is a specification for transmitting frames from a module. Multiple streams can be defined for a Transmit Specification. Define a stream using the options available from the dialog box and click on the **Add** button. You can also add a capture file as a defined stream using the **Add File...** button. The added stream appears in the

Defined Streams list box. Streams are transmitted by the module in the order in which they are defined.

A defined stream may be activated or deactivated by double-clicking on the stream. An activated stream has a check mark next to it in the **Defined Streams** list box and is highlighted with the Windows highlight color; a deactivated stream has no check mark and displays in the Windows inactive color. Only activated streams are loaded to the module when you click on the **Load Module** button. Before loading a module, make sure you have activated the streams you want.

Figure 17 shows a synopsis of all streams defined for the Transmit Specification. In the example, three streams are defined and only two are activated. The stream highlighted in the highlight color set for Windows 95 is the currently selected stream. Streams highlighted in the inactive color set for Windows 95 are inactive. The settings for the currently selected stream show in the fields of the dialog box below the **Defined Streams** list box.

If you modify the values in the current stream and click on **Add**, a new stream is added as the stream after the currently selected stream in the **Defined Streams** list box. If you modify the values in the current stream and click on **Modify**, the definition of the current stream is changed.

Radio Buttons and Fields for Defining a Stream

Specify the contents and the size of the stream using the **DA**, **SA**, **Packet Type**, **Packet Size**, and **Data** fields. **DA** and **SA** values can be retrieved from the currently active name table using the **Names...** button. Random or sequential address generation is supported by selecting the appropriate radio buttons and using **X** values in the **DA** or **SA** field.

Sequence numbers (**Start Seq#** and **Stop Seq#**) are used to number the packets; packet numbering may be useful at the receiving end. When viewing packets at the receiving end, the default location for the two-byte sequence number is 32H and 33H. This value can be set in the **Seq# Offset** field.

Set the stream mode using the radio buttons and the **Burst** check box. The stream mode defines the rate at which packets are transmitted from a module and whether bursts of packets with a different rate will be transmitted within the stream.

Set the **Repeat Streams** field to repeat the stream more than one time. This setting specifies the number of times to repeat one complete stream – not how many times to repeat transmission of the entire specification, nor the number of bursts within the stream. The **Auto CRC** check box specifies if a valid CRC will be automatically generated for the stream.

Stream Buttons

The **Add**, **Add File...**, **Modify**, **Delete**, and **Edit Data...** buttons perform functions for a single stream.

Add	Adds a new stream after the currently selected stream in the Defined Streams window. The values displayed in the fields of the Transmit Specification window are used as the values for the new stream.
Add File...	Adds a new stream defined by capture file (.CAP file) in the Defined Streams window. A dialog box appears asking for the name of the capture file. The first packet in the capture file is the defined stream. All subsequent packets in the capture file are ignored.
Modify	Changes the definition of the current stream. The values displayed in the fields of the Transmit Specification window overwrite the values of the currently selected stream.
Delete	Deletes the currently selected stream.
Edit Data...	Brings up the packet editor. You can use the packet editor to modify the currently selected stream.

Transmission Mode and Status Controls

The **Transmission Mode** radio buttons control how many times all streams are transmitted once they are loaded to the module. You can transmit the entire specification *n* times or continuously. The transmission mode is not part of the **Transmit Specification** when saving to a file.

The **Transmission Status** section provides information about the number of activated streams, speed of transmission, and the amount of module memory used by active streams.

Transmit Specification Control Buttons

The **Load Module**, **Open Specs**, and **Save Specs** buttons perform functions on a complete **Transmit Specification**. Be sure to use the **Load Module** button to load the specification to the module before you begin transmission. The **Template** button allows you to use predefined data as a starting point for new stream. It also lets you create Magic Packets™. The buttons are:

Load Module	Loads the current resource with the currently defined Transmit Specification. Be sure to use the Load Module button to load the specification to the resource before you begin transmission.
Open Specs...	Opens a previously saved Transmit Specification. A dialog box appears to specify the name and location of the Transmit Specification.
Save Specs...	Saves the currently defined Transmit Specification to a file. A dialog box appears to specify the name and location of the Transmit Specification.
Template...	Shows menus that list the currently defined templates for packets. Selecting a template places the values of the template in the fields of the Transmit Specification dialog box. You can then change the values of the fields in the Transmit Specification dialog box or use the Edit Data... button to create exactly the packet you wish.
Cancel	Exit the Transmit Specification dialog box. Make sure you have added/modified all streams, saved new Transmit Specifications, and loaded the resource before pressing Cancel.

Repeating Frames

There are three ways to repeat frames when transmitting:

Check the Bursts box	Repeats frames of a stream with a specific timing set between the frames. The special timing is set in the Burst Gap field, the number of repetitions in the Burst Count field.
Repeat Streams	Repeats the stream <i>n</i> times. The gap between frames is set by the Stream Mode as a packet gap, frame rate, or traffic rate.
Set the Transmission Mode	You can set the module to loop through the entire Transmit Specification <i>n</i> number of times. Streams are repeated in the specification from first to last until you stop the module or all streams are transmitted <i>n</i> times.

WARNING: *Repeating frames using the transmission mode feature is a function implemented in software for NDIS or CMM! modules; there is a time gap of about 50ms between each transmission of the entire specification. Use **Repeat Frames 'n' Times** or **Bursts** where timing issues are critical when sending frames for these devices.*

Ways of repeating frames can be used together. For example, assume the following two streams are defined:

```
Stream 1; packet gap=100msec, burst count=4, burst gap=4msec,  
repeat frame 2 times  
Stream 2; packet gap=200msec, no burst
```

The example results in the following:

```
Transmit Stream 1  
Wait 100msec  
Transmit Stream 1  
Wait 100msec  
Transmit Stream 1  
Wait 100msec  
Transmit Stream 1  
Wait 104msec  
Transmit Stream 1  
Wait 100msec  
Transmit Stream 1  
Wait 100msec  
Transmit Stream 1  
Wait 100msec  
Transmit Stream 1  
Wait 104msec  
Transmit Stream 2  
Wait 200msec
```

If the transmission mode is set to continuous, the entire sequence above is repeated until the module is stopped.

The **Repeat Stream** field sets how many times to repeat the current stream. For example, if the **Repeat Stream** field is set to a value of 8, the current stream would be sent 8 times before the next stream in the Transmit Specification is sent.

Stream Modes

An interpacket gap for a frame can be set in three different ways; Packet Gap, Frame Rate and Traffic Rate. The stream mode defines the rate at which packets are transmitted from a module. The modes are:

Packet Gap	The rate is set as an interval of time between packets. The interval can be set in seconds, milliseconds, or microseconds.
Frame Rate	The rate is set in number of frames per second.
Traffic Rate	The rate is set as a percentage of the maximum speed (10Mbps or 100Mbps) for the module.

Using Century Media Modules, if you want to transmit at faster than line rate, set the gap to 0.88 microseconds for 100Mbps or 3.2 microseconds for 10Mbps.

Bursts

Bursts cause a stream to be transmitted again and again. Check the **Bursts** box to send a burst of packets with the stream. Set **Burst Count** to the number of times to send the frame. An interval (packet gap) can be set between bursts in the **Burst Gap** field.

The following example shows how bursts and burst timing work. Assume three streams are defined as follows:

```
Stream 1; Packet Gap=100msec., No burst
Stream 2; Packet Gap=20msec, Burst Count=3, Burst Gap=4msec
Stream 3; Packet Gap=5msec., No burst
```

The example results in the following:

```
Transmit Stream 1
Wait 100msec
Transmit Stream 2
Wait 20msec
Transmit Stream 2
Wait 20msec
Transmit Stream 2
Wait 24msec
Transmit Stream 3
Wait 5msec
```

Transmission Mode

You can either transmit the specification continuously or transmit it n times.

Select **Transmit Continuously** to transmit activated streams in a loop until the module is stopped.

Select **Transmit Spec (N frames)** to transmit activated streams a specific number of times. The number of streams does not necessarily equate to the number of frames transmitted.

WARNING: The transmission mode should always be set prior to loading the module. The transmission mode is not saved as part of the Transmit Specification. Unless you set the transmission mode, you may inadvertently flood the network with packets.

The **Transmission Status** area of the dialog box provides status information about the transmission. The fields indicate the speed of the currently active module, the number of streams that are active, and the total memory in the buffer required to transmit the specification. The total memory increments as you add/change streams, giving you an instant reflection of how much data you are transmitting. A warning message is shown if you exceed the transmit buffer size.

Specifying Transmit Data

Data fields for the Transmit Specification can be modified in two ways: by using the Packet Editor or by changing the data fields shown in the **Transmit Specification** dialog box. If you are inserting a new stream, you can use a template as the starting point for packet data. The insertion of a new packet into the **Defined Streams** list box will appear below the currently highlighted packet stream.

Packet Editor

The packet editor can be used to modify the contents of a stream data. The editor provides two views of packets, a decoded view and a hex view. Edits can be made within either view. Select the **Edit Data** button to bring up the editor.

The following buttons are available within the packet editor:

Compute CRC	Inserts the correct CRC error check value for the frame. You can use this option to create frames with or without correct CRC error check values.
Decode	Takes the values entered in the Hex View window of the packet editor, decodes the packet, and displays the resulting decode in the Decode View window.
Undo	Undo the last editing action. Only one level of undo is supported.

OK	Save edits.
Cancel	Leave the editor without saving changes.

Editing in Decode View

Editing in decode view allows you to edit packets without remembering offsets. Click on a field and a dialog box pops up which shows the current value for the field and asks for a new value. The dialog boxes for each field is slightly different. Most dialog boxes display and allow you enter values in hexadecimal or decimal. Some contain a **Use little-endian bit order** check box if bit order swapping is required. Changes made in decode view are automatically reflected in hex view.

Editing in Hex View

Edits are made in Hex view by placing the cursor at a location and overwriting the current values. You can also paste (Ctrl + V) the contents of the paste buffer into a location. Values are always overwritten starting at the current cursor location in hex view so offsets remain correct.

Press the **Decode** button to display edits made in hex view in the decode view. Note that changes to the decode view are not automatic. This provides the option of creating error packets that can't be decoded properly.

NOTE: NDIS modules cannot transmit without a valid CRC.

Changing Fields Directly in the Dialog Box

The values of various fields in the currently selected stream are shown in the Transmit Specification fields below the **Defined Stream** list box. You can change the stream data by editing these fields directly.

DA and SA Fields

The **DA** and **SA** fields define the MAC layer destination address and MAC layer source address for the stream. Note that the MAC address values appear in the stream synopsis in the **Defined Streams** list box.

Use an X in any offset of the **DA** or **SA** fields to indicate "wild card" addresses. Surveyor will generate packets with different values in that offset. For example, set the **DA** field to 432FFFFFFX. When transmitting packets, values will be generated either sequentially or randomly and sent for the last 2 positions of the DA.

The values for the wild cards can be random or sequential, as defined by the **Random Access Mode** buttons below the **DA** and **SA** fields.

Click on the **Names** button to see the currently active name table. You can set the DA or SA from the name table and they will appear in the **DA** or **SA** fields in the **Transmit Specification** window. The name appears to the right of the DA or SA address if the name table contains a symbolic name for the address.

Packet Type

Sets the packet type for the current stream. Use the pull-down box to see available options. In the example stream, the packet is an IP packet. This field can also be used to enter the packet length for IEEE802.2 or SNAP frames.

Packet Size

Sets the packet size. Use the pull-down box to view common sizes. The size must be from 8 to 15,000 bytes.

Data Field

Specifies the data to be sent as part of the packet. Use the pull-down box to see commonly used values. Any hexadecimal values can be entered in the **Data** field and sent with the packet. Up to the first 32 bytes of data can be specified in this field. The entire data within the packet can be edited using the Packet Editor.

Sequence Numbers

Sets a starting number and ending numbers for packets transmitted, and also sets the offset within the frame where the sequence number will be stored. You cannot store the sequence number in the first 12 offsets of the frame. Also, you should take care not to store the sequence number in any part of the packet that contains other information that will be used by the network or by the receiving station.

Auto CRC Check Box

Setting the check box also affects the contents of the stream. If checked, a correct CRC value is automatically generated for the packet. If unchecked, bad CRC packets can be generated using CMM1 or CMM2 modules. NDIS modules cannot generate bad CRC packets.

Using Templates

If you are inserting a new stream, you can use a template as the starting point for packet data. To select a template, click on the **Template...** button at the bottom of the **Transmit Specification** dialog box. Nested menus appear to select a template.

Templates insert the required values for commonly known packet types in the data for the stream. For example, if you select the template for IPX, the value 0x8137 is inserted in the **Packet Type** field.

You can create and insert your own templates into the menus. You can also insert Magic Packets™ using the **Template...** menu.

Transmitting Capture Files

You can transmit the contents of a capture file as one of the streams in the Transmit Specification. Place a capture file as a stream into the **Defined Streams** list box using the **Add File...** button.

The entire contents of the capture file is transmitted with timestamps intact. As with any other stream, you can repeat transmission of the file by using the **Repeat Stream** field. All other fields do not apply when the stream is defined by a capture file.

Transmit Specification Examples

Transmit Specification examples are supplied with Surveyor. Open a transmit specification file (\transmit subdirectory, .TSP extension) from the **Transmit Specification** dialog box to see examples.

Two Transmit Specification examples are provided. The file names correspond to the example files in the software.

Packet Gaps Example	This example shows a stream from Sample_3.tsp that uses packet gaps.
----------------------------	--

Bursts Example	This example shows a stream from Sample_1.tsp that uses bursts.
-----------------------	---

To find more examples, look in the ..\Surveyor\examples\transmit directory.

Transmit Specification Example, Packet Gaps

A Transmit Specification example in its dialog box is shown below. The dialog box only shows the values for one stream of Sample_3.tsp. Multiple streams are defined in the specification.

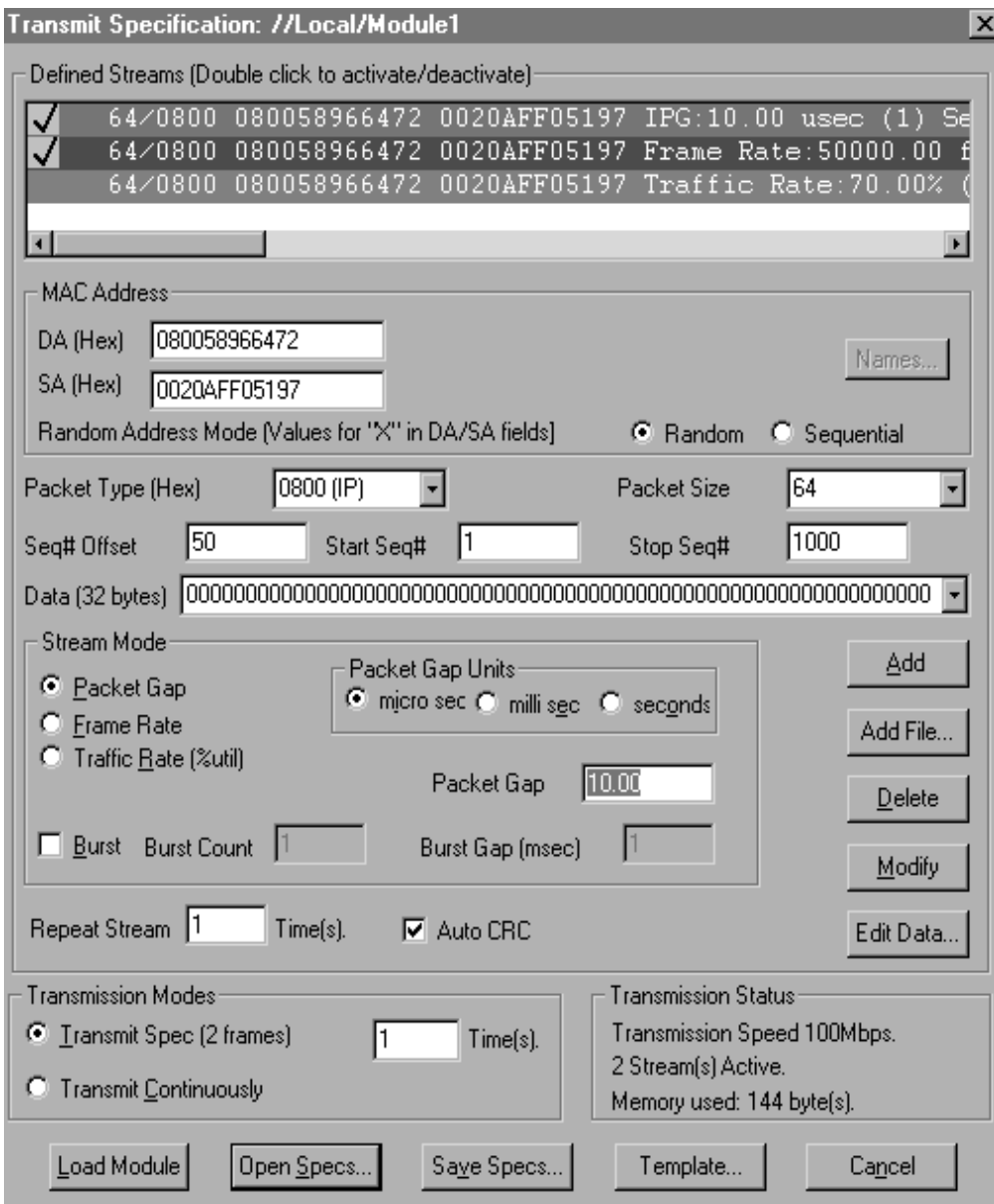


Figure 18. Transmit Specification Dialog Box, Packet Gaps

Transmit Specification Example, Bursts

A **Transmit Specification** dialog box is shown below. The dialog box only shows values for one stream of `Sample_1.tsp`. Multiple streams are defined in the specification.

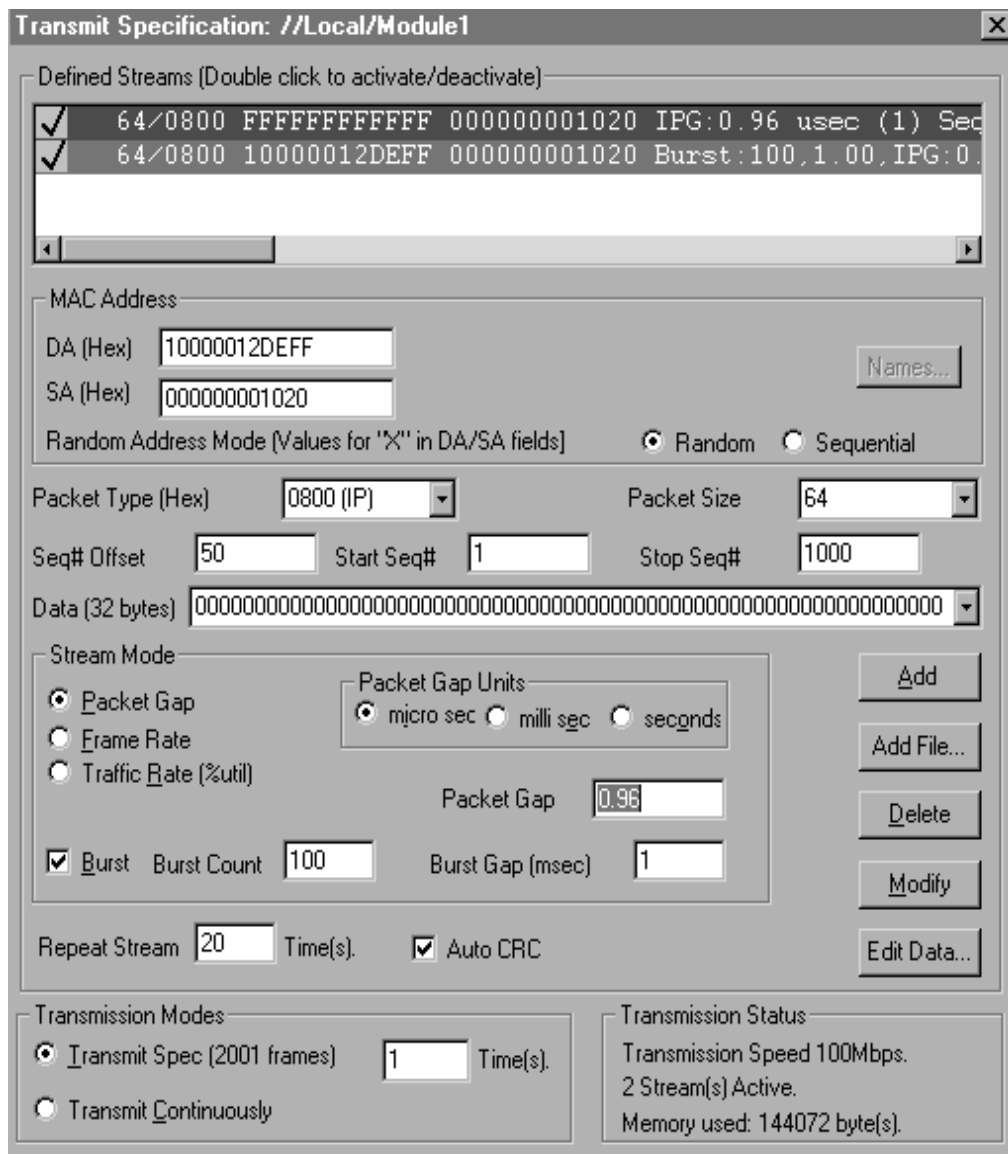


Figure 19. Transmit Specification Dialog Box, Bursts

Hints and Tips for a Transmit Specification

- Take care with what you transmit. Surveyor can transmit packets at more than 100% of network bandwidth. It is possible to flood the network and cripple performance.
- Make sure that the streams you want are activated before you load the specification to the module.
- Always set the transmission mode before loading the specification to a module. Unless you do, you may inadvertently flood the network with packets. The transmission mode is not saved as part of the specification, so it should be checked before each module load.
- Transmitted packets can be sent to another module. Use sequence numbers to aid in analyzing the packets at the receiving end.
- Using bursts is the easiest way to simulate high traffic conditions.
- Always save your defined specification. The Transmit Specification can only be saved using the dialog box.
- An NDIS module cannot transmit bad physical layer error packets, such as bad CRC packets, runt packets, oversized packets, packets with less than minimum packet size, and so on. Use CMM1 or CMM2 modules to generate these error packets.
- TSP files created using Surveyor can be used with the Century Tool Kit under Windows 95 for network component testing, switches, bridges, or other store-and-forward network devices.
- To see which transmit specification is associated with a particular resource, choose **Active TSP and Capture Filter** from the **Module** menu.

9 Alarms (Alarm Browser)

Surveyor's alarms facility enables you to create alarms to automatically monitor network resources. Access to Surveyor's alarms facility is through the **Alarm Browser** docking window located in Surveyor's main window. The **Alarm Browser** window features a hierarchical directory comprising folder, file and application icons that can be manipulated using point-and-click mouse commands.

Alarms are created using an Alarms Editor. The **Alarms Editor** window contains an alarm table. Each alarm within the alarm table contains default threshold values, notification settings, a sampling interval value, and an **Enable/Disable** click box. After editing and enabling a desired set of alarms, you assign a unique name to the alarm group.

Alarm groups are applied to network resources by dragging the resource's icon from the **Resource Browser** window to the alarm group. The network resource icon appears in the Alarm Browser directory under the alarm group upon which it was dropped. Starting the resource will automatically activate the use of the alarm group for that resource. You must have Monitor or Capture mode set for a resource to have alarms trigger and have alarm actions occur.

Multiple resources can be dragged and dropped onto a single alarm group. Resources can be applied to multiple alarm groups.

Actions resulting from alarms are varied and extremely flexible because they are assigned to each individual alarm. When an alarm threshold is exceeded, an audible beep sounds on the host, and an alarm message appears in the **Message** window. Individual alarms can also be configured to log alarms to a log file, contact individuals by e-mail, dial pager numbers, restart the resource, auto save data, or stop the resource and save data.

Alarm Browser

The Alarm Browser enables you to create/modify and use alarm groups to monitor local and remote network resources. The **Alarm Browser** window, through which you access and use all of the alarm browser components, appears in the Surveyor startup window.

Surveyor's alarm browser appears and operates much like the graphical user interface used by Microsoft Windows 95 Explorer. Alarm browser's hierarchical directory structure features folder, file, and application icons that you manipulate using point-and-click mouse commands. Additionally, the Alarm Browser interface provides convenient check boxes that enable you to quickly expand or collapse portions of the Alarm Browser directory. This is useful if you create numerous alarm groups or if you assign alarm groups to many network resources.

The Alarm Browser contains five folders, Expert Alarms, Application Response Time Alarms, Ethernet MAC Layer Alarms, Token Ring Alarms, and Network Layer Alarms. Expert Alarms and Application Response Time Alarms are only available if you have the Expert plug-in. Each folder contains an alarms editor. These editors are used to select, modify, and create alarm groups.

Multiple resources can be dragged and dropped onto a single alarm group. When an alarm is triggered for a resource, the resource flashes in the **Alarm Browser** window. To stop an alarm group from monitoring a network resource, use the mouse to select the resource and press the **Delete** key.

Alarm Editors

There are five Alarm Editors. The Expert Alarm Editor and Application Response Time Alarm Editor are only available if you have the Expert plug-in.


Expert Alarm

Allows you to modify and enable any of the 35 alarm types contained in Surveyor's **Expert** alarm table. Alarms test for discrete conditions at different protocol layers, such as NFS retransmissions at the application layer, overload utilization percentages at the MAC layer, or TCP/IP SYN packets at the transport layer. See the chapter on the Expert System for a description of the expert alarms.

Application Response Time

Allows you to modify and enable any of 8 alarm types contained in Surveyor's **Application Response Time** alarm table. Alarms test for application response times related to application protocols such as SMTP, HTTP, or NFS.

Ethernet MAC Layer Alarm	Allows you to modify and enable any of 21 alarm types contained in Surveyor's Ethernet MAC Layer alarm table. Alarms test for conditions related to Ethernet conditions such as utilization rate, packet size, errors, and frame types.
Token Ring Alarm	Allows you to modify and enable any of 29 alarm types contained in Surveyor's Token Ring alarm table. Alarms test for conditions related to Token Ring conditions such as utilization rate, packet size, errors, and frame types.
Network Layer Alarm	Allows you to modify and enable any of the 65 alarm types contained in Surveyor's Network Layer alarm table. Alarms test for conditions related to Network Layer conditions such as IP/IPX/ARP packet or octet

Click on the appropriate  icon to display the alarm table you want. Each alarm can be used with the default values provided by Surveyor, or you can modify them with the alarms editor to precisely meet your resource monitoring needs.

Alarm Groups

You can create an unlimited number of alarm groups. When you create an alarm group, the alarm table editor asks you to name the new alarm group. Surveyor will save the alarm group file in the appropriate folder.

All the “enabled” rows in the table comprise an alarm group. Alarm groups are named and then associated with resources.

Alarms and Alarm Events

The entire table of alarms you can set is shown in each alarm editor. Each line in the table is called an alarm or alarm row. You can enable as many alarms as you want in the table.

If a threshold is exceeded for any enabled alarm row within an alarm table, an alarm event occurs. The event is reported according to the value configured in the **Action** field for the alarm row in the table.

Thresholds and Alarms

Alarm thresholds are set by specifying the values in the **Sample Type**, **Rising Value**, **Falling Value**, and **Interval** fields for each alarm row in the alarm table. The numbers or percentages set for rising and falling values are referred to as thresholds. The key to creating a meaningful alarm is to specify these values so you get alerted to the exact network conditions you want to analyze.

The sample type can be set to either **Delta** or **Absolute**. The setting for the **Sample Type** field determines how Surveyor will use the threshold values set in the **Rising Value** and **Falling Value** fields.

An absolute sample means that if the **Rising Value** is exceeded an alarm event occurs. If a value is specified for the **Falling Value**, an alarm event occurs when the counter resets to zero.

A delta sample type means that if a difference between samples increases (rising) or decreases (falling) over time more than the specified threshold, an alarm event occurs. The **Interval** field sets the time period between samples. Samples are actually taken at least twice as often as the interval to allow the detection of threshold crossings that span the sample boundary. For example, if the delta sample is taken twice per interval, the sum of the latest two samples are compared to the threshold.

For most cases, the default Sample Type of Delta is more useful. One exception is the MAC Layer Alarm for Utilization. Because utilization is expressed in the **Rising Value** field as a percentage, the absolute sample type is more useful to catch utilization that exceeds a certain percentage from a baseline of zero network traffic.

Alarm Actions

Each line in an alarm table has a unique set of actions associated with it that will occur if the alarm is triggered. You always get at least two actions when an alarm is triggered – an audible alarm and a message in the **Message** window. You can have one of seven actions associated with the alarm:

Message	records the message in the Message window in the Surveyor main window and sounds the audible alarm. No other actions occur if this setting is selected.
E-mail	sends the message to pre-configured e-mail addresses. Your e-mail application does not need to be running for alarms to generate e-mail messages.
Pager	sends alarms to pre-configured pager numbers.
Log	records alarms in a pre-configured log file.

Stop&Save	stops the module when the alarm occurs.
Restart	resets all counters and begins capture from the point where the alarm occurred.
Auto Save	automatically saves data in the capture buffer at the time the event occurs.

When sending E-mail or making a call to a pager, multiple addresses/numbers can be configured from the **Configuration** menu. Setting the addresses/numbers for alarm actions is a global setting. All alarms reported by Surveyor will go to the same set of E-mail addresses/Pager numbers. For example, you cannot send some alarms to one set of e-mail addresses and some alarms to another set of e-mail addresses.

When storing the alarm in a log file, only one log file can be configured. However, you can change the name of the log file at any time and future alarms will be written to the new file.

If the alarm causes the resource to stop, Surveyor saves the capture buffer data to a file. The name automatically assigned to this file is based on the date and time of the alarm event.

If the alarm restarts the resource, all counters are set to zero and the resource begins capture. This allows you to collect data and count it after a particular event has occurred.

Expert Alarms

During transmit or receive, expert symptoms are logged as they occur. You can test for certain thresholds for these conditions by setting alarms using the Expert Alarms Editor. See the chapter on the Expert system for more information about the expert alarms listed below.

Expert Alarms are only available if you have the Expert plug-in. The table on the following page lists all Expert Alarms.

Table 25. Expert Alarms**APPLICATION LAYER**

ICMP All Errors
ICMP Destination Unreachable
ICMP Redirect
Excessive BOOTP
Excessive ARP
NFS Retransmissions

TRANSPORT LAYER

TCP/IP SYN Attack
TCP/IP RST Packets
TCP/IP Retransmissions
TCP/IP Zero Window

DATA LINK LAYER, ETHERNET

Overload Utilization Percentage
Overload Frame Rate
Illegal MAC Source Address
Total MAC Stations
New MAC Stations
Excessive Broadcasts
Excessive Multicasts
Excessive Collisions


NETWORK LAYER

Duplicate Network Address
Unstable MST
SAP Broadcasts
OSPF Broadcasts
RIP Broadcasts
Total Router Broadcasts
ISL Illegal VLAN ID
ISL BPDU/CDP Packets
IP Time to Live Expiring
Illegal Network Source Address

DATA LINK LAYER, TOKEN RING

Overload Utilization Percentage
Overload Frame Rate
Illegal MAC Source Address
Total MAC Stations
New MAC Stations
Excessive Broadcasts
Excessive Multicasts

Alarm List and Log

From Detail View, click on the  button to open a window with alarm list and log.
From Summary View, click on the **Alarms** tab.

Alarm view is a table showing all alarm groups assigned to this resource. It lists alarm groups by name and identifies the type of alarm group, MAC, Token Ring, or Network.

Hints and Tips for Alarms

- Once an alarm group is created, drag and drop a resource from the Resource Browser onto an alarm group to assign the alarm group to that resource.
- You can drag and drop multiple resources to one alarm group. You can also drag and drop one resource to many alarm groups.
- Remember that alarm groups are assigned to resources, not individual alarms within an alarm group. If you only want a single alarm, create an alarm group with only one alarm enabled.
- Click, hold, and drag a column border to resize columns in the alarm table.
- To set more than one alarm of the same type, click on the type you want to duplicate and press the Insert key. A new alarm row appears below the current row. Fill out the settings in the new row.
- To set one alarm that has multiple actions, click on the Alarm Type you want to duplicate and press the Insert key. A new alarm row appears below the current row. Change the **Actions** field of the new row to the additional action you want. For example, you could have one alarm of type Packets with the action set to E-mail and one alarm of type Packets with the alarm type set to Pager. Note that if the alarm rows are identical except for the action, you will get two messages in the message window for the alarm, since a message is always posted when any alarm is triggered.
- You can copy values in one alarm row to another. Click on the Alarm Type in the alarm row you want to copy. The row highlights; press **Ctrl + C** to copy. Click on the Alarm Type in the alarm row where you want to place the copied values and press **Ctrl + V**.

Alarm Examples

Three examples are provided for alarms and alarm groupings. Each provides a picture of an alarm table and a description of what will occur when specific alarm rows are enabled in an alarm table.

Alarm Example, Utilization

Variable	Sample Type	Rising Value	Falling Value	Severity	Actions	Interval	Enabled
Utilization	Absolute	50		Information	Message	5	<input checked="" type="checkbox"/>

Figure 20. Alarm Example, Utilization

This simple example shows an alarm group consisting of one MAC Layer alarm for Utilization. This alarm samples network traffic at five-second intervals. When the absolute, rising value of 50 (percent utilization) is exceeded, Surveyor issues an audible alarm and displays a message in Surveyor's message window.

Alarm Example, MAC Errors

Variable	Sample Type	Rising Value	Falling Value	Severity	Actions	Interval	Enabled
Errors	Delta	250		Warning	E-Mail	5	<input checked="" type="checkbox"/>
	Delta	50		Information	Message	5	<input checked="" type="checkbox"/>
Undersize Frames	Delta	10		Information	Message	5	<input checked="" type="checkbox"/>
Oversize Frames	Delta	10		Information	Message	5	<input checked="" type="checkbox"/>
CRC/Alignment	Delta	10		Information	Message	5	<input checked="" type="checkbox"/>
Fragments	Delta	10		Information	Message	5	<input checked="" type="checkbox"/>

Figure 21. Alarm Example, MAC Errors

This example shows an alarm group consisting of six MAC Layer alarms: Errors (two alarms), Undersize Frames, Oversize Frames, CRC/Alignment, and Fragments. Each of these alarm counters are checked at five-second intervals. When an alarm threshold for any of these five alarms is exceeded, Surveyor issues an audible alarm and displays a message in Surveyor's message window.

Assume that overall error rate is of particular interest in this example. The Severity setting instructs Surveyor to include a "Warning!" statement with all alarm messages when the error rate is greater than 250. The Actions setting instructs Surveyor to send an e-mail message whenever the rising value (threshold) for the overall error rate exceeds 250.

Alarm Example, Frame Size

Variable	Sample Type	Rising Value	Falling Value	Severity	Actions	Interval	Enabled
Oversize Frames	Delta	100		Information	Log File	5	<input checked="" type="checkbox"/>
512-1023 Bytes Fra	Delta	5000		Information	Log File	5	<input checked="" type="checkbox"/>
1024-1518 Bytes Fr	Delta	5000		Information	Log File	5	<input checked="" type="checkbox"/>

Figure 22. Alarm Example, Frame Size

This example shows an alarm group consisting of three MAC Layer alarms: Oversize Frames, 512-1028 Byte Frames, and 1024-1518 Byte Frames. Each of these alarms samples network traffic at five-second intervals. When an alarm threshold for any of these three alarms is exceeded, Surveyor issues an audible alarm and displays a message in Surveyor's **Message** window. In addition, the alarms will be logged to the Log file specified.

10 Expert System

Expert Overview

Automatic diagnostic analysis, expert data views, application response times, and expert alarms are referred to collectively as Surveyor's Expert Features. Expert Features are available in Surveyor menus and toolbars if you have installed the Surveyor Expert plug-in module.

Expert Views

The new expert views can present expert information on capture files, a capture buffer, or in real-time monitoring mode. The following Expert views are available from the **Data Views** or **Capture View** toolbar:

- **Expert View**
When you click on Expert View, two types of expert tables are available – Expert Overview and Expert Analysis. Expert Overview is a statistics table presenting counters for each of the Expert Symptoms. Expert Analysis lists each specific symptom.
- **Application Response Time View**
The Application Response Time view depicts performance information for specific applications. For each supported application the Application Response Time View will present the Application, Minimum Response Time (Min Time), Maximum Response Time (Max Time), Average Response Times (Avg Time), and the Number of Connections (Connections) processed to derive these times.
- **Duplicate Network Address View**
The Duplicate Network Address view depicts each duplicate network (IP/IPX) address detected and its associated MAC layer bindings.

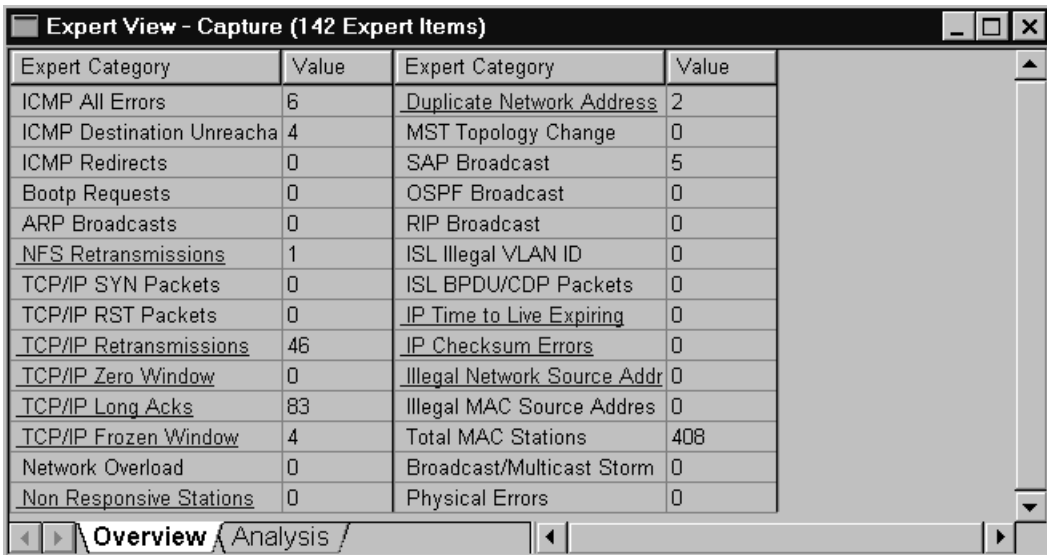
See Chapter 6, "Views" for more information on Expert Views.

Expert Symptoms and Diagnosis

Expert logic internal to Surveyor reports significant symptoms of potential network problems as well as helpful diagnostic information related to the symptom. These events are determined by Surveyor's expert logic. No configuration is required to use the expert logic; however, some of the default thresholds for expert events may be changed.

Expert Overview Table

When Surveyor finds an event that could indicate a network problem, the event is logged in the Expert Analysis table, and the appropriate counters are incremented in the Expert Overview table. An example Expert Overview table is shown below.



Expert Category	Value	Expert Category	Value
ICMP All Errors	6	<u>Duplicate Network Address</u>	2
ICMP Destination Unreacha	4	MST Topology Change	0
ICMP Redirects	0	SAP Broadcast	5
Bootp Requests	0	OSPF Broadcast	0
ARP Broadcasts	0	RIP Broadcast	0
<u>NFS Retransmissions</u>	1	ISL Illegal VLAN ID	0
TCP/IP SYN Packets	0	ISL BPDU/CDP Packets	0
TCP/IP RST Packets	0	<u>IP Time to Live Expiring</u>	0
<u>TCP/IP Retransmissions</u>	46	<u>IP Checksum Errors</u>	0
<u>TCP/IP Zero Window</u>	0	<u>Illegal Network Source Addr</u>	0
<u>TCP/IP Long Acks</u>	83	Illegal MAC Source Address	0
<u>TCP/IP Frozen Window</u>	4	Total MAC Stations	408
Network Overload	0	Broadcast/Multicast Storm	0
<u>Non Responsive Stations</u>	0	Physical Errors	0

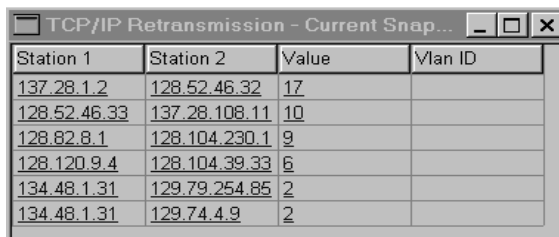
Overview / Analysis /

Figure 23. Expert Overview Table Example

Click on the counters underlined in blue in the display to pop-up the Expert Overview Detail table. This table shows more detailed information about the specific events in a symptom category, such as symptom counts by station address.

Only the last 2,001 occurrences of an expert symptom are listed in the Expert Detail table.

An example of the Expert Overview Detail table is shown below, after clicking on the TCP/IP Retransmissions counter:



Station 1	Station 2	Value	Vlan ID
137.28.1.2	128.52.46.32	17	
128.52.46.33	137.28.108.11	10	
128.82.8.1	128.104.230.1	9	
128.120.9.4	128.104.39.33	6	
134.48.1.31	129.79.254.85	2	
134.48.1.31	129.74.4.9	2	

Figure 24. Expert Overview Detail Table Example

You can select any row in the table to find out statistics about the host or hosts. The Expert Overview Host Summary appears, showing types and counts of all expert symptoms found for this host(s), packet and octet counts, plus the associated MAC Address for the host(s).

The following example shows the Expert Overview Host Summary screen after clicking on the first row of the Expert Overview Detail table for TCP/IP Transmissions. Other symptoms discovered for this host pair are listed. In the example, the screen shows 24 TCP/IP Long Acks for this host pair as well as 17 TCP/IP Transmissions.

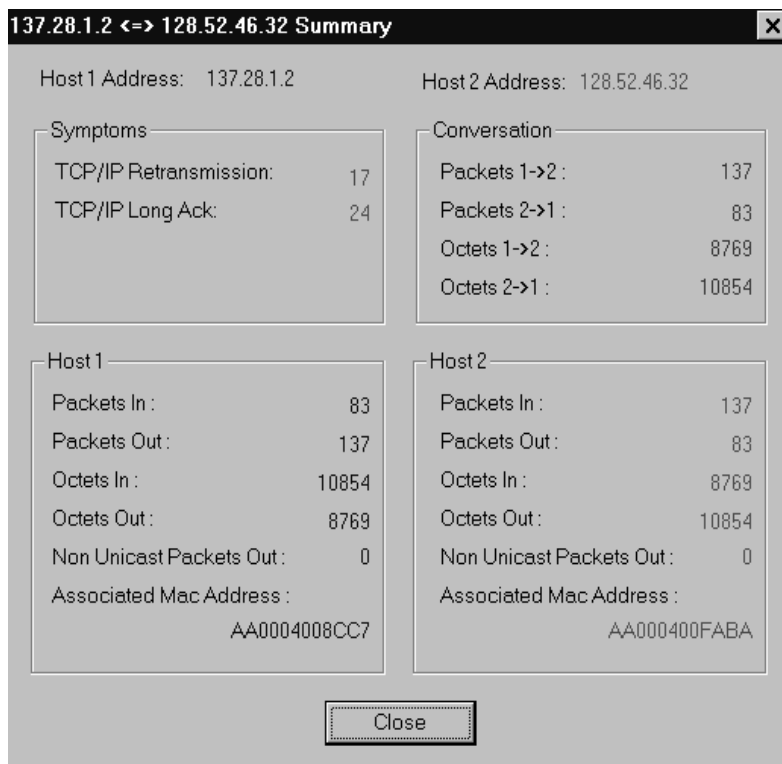


Figure 25. Expert Overview Host Summary Example

Expert Analysis Table

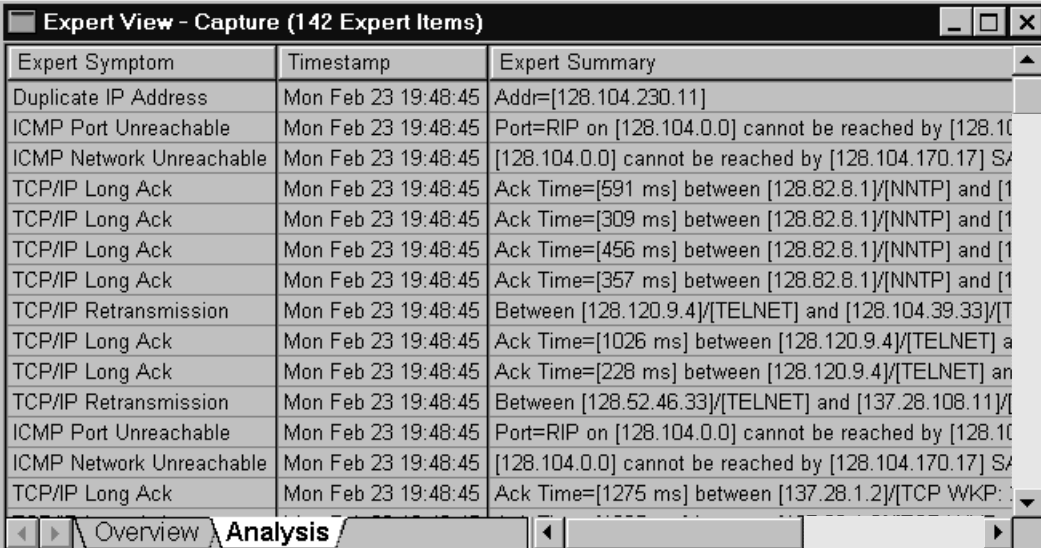
Frame ID (Capture View only), source address, destination address, VLAN ID, and the timestamp are provided for each entry in the Expert Analysis Table. Each table entry also shows a summary that provides more information about the symptom. The Expert Analysis Table contains the last 2,001 symptoms detected for the module.

The following is a list of the general categories of symptoms discovered by Shomiti's expert logic:

- Application Layer: NFS Retransmission, All ICMP Errors, Excessive BOOTP, Excessive ARP
- Transport Layer: TCP/IP Retransmission, TCP/IP Zero Window, TCP/IP Frozen Window, TCP/IP Long Ack, TCP/IP SYN Attack
- Network Layer: Duplicate IP or IPX Address, IP TTL Expiring, IP Illegal Source Address, ISL Illegal VLAN ID, Unstable MST

- MAC Layer: Illegal MAC Source Address, Broadcast/Multicast Storms, Physical Errors

The figure below shows an example of an Expert Analysis Table.



Expert Symptom	Timestamp	Expert Summary
Duplicate IP Address	Mon Feb 23 19:48:45	Addr=[128.104.230.11]
ICMP Port Unreachable	Mon Feb 23 19:48:45	Port=RIP on [128.104.0.0] cannot be reached by [128.104.170.17] SA
ICMP Network Unreachable	Mon Feb 23 19:48:45	[128.104.0.0] cannot be reached by [128.104.170.17] SA
TCP/IP Long Ack	Mon Feb 23 19:48:45	Ack Time=[591 ms] between [128.82.8.1]/[NNTP] and [128.104.170.17]
TCP/IP Long Ack	Mon Feb 23 19:48:45	Ack Time=[309 ms] between [128.82.8.1]/[NNTP] and [128.104.170.17]
TCP/IP Long Ack	Mon Feb 23 19:48:45	Ack Time=[456 ms] between [128.82.8.1]/[NNTP] and [128.104.170.17]
TCP/IP Retransmission	Mon Feb 23 19:48:45	Ack Time=[357 ms] between [128.82.8.1]/[NNTP] and [128.104.170.17]
TCP/IP Long Ack	Mon Feb 23 19:48:45	Between [128.120.9.4]/[TELNET] and [128.104.39.33]/[TELNET]
TCP/IP Long Ack	Mon Feb 23 19:48:45	Ack Time=[1026 ms] between [128.120.9.4]/[TELNET] and [128.104.39.33]/[TELNET]
TCP/IP Long Ack	Mon Feb 23 19:48:45	Ack Time=[228 ms] between [128.120.9.4]/[TELNET] and [128.104.39.33]/[TELNET]
TCP/IP Retransmission	Mon Feb 23 19:48:45	Between [128.52.46.33]/[TELNET] and [137.28.108.11]/[TELNET]
ICMP Port Unreachable	Mon Feb 23 19:48:45	Port=RIP on [128.104.0.0] cannot be reached by [128.104.170.17] SA
ICMP Network Unreachable	Mon Feb 23 19:48:45	[128.104.0.0] cannot be reached by [128.104.170.17] SA
TCP/IP Long Ack	Mon Feb 23 19:48:45	Ack Time=[1275 ms] between [137.28.1.2]/[TCP WKP] and [128.104.170.17]

Figure 26. Expert Analysis Table Example

From Expert Analysis Table you can double-click on any symptom to display an Expert Message. Contents of the **Expert Diagnosis** window include:

- Information on the selected Expert Symptom from the Expert Analysis table
- Possible Causes
- Recommended Actions

The figure below shows an example of the **Expert Diagnosis** window.

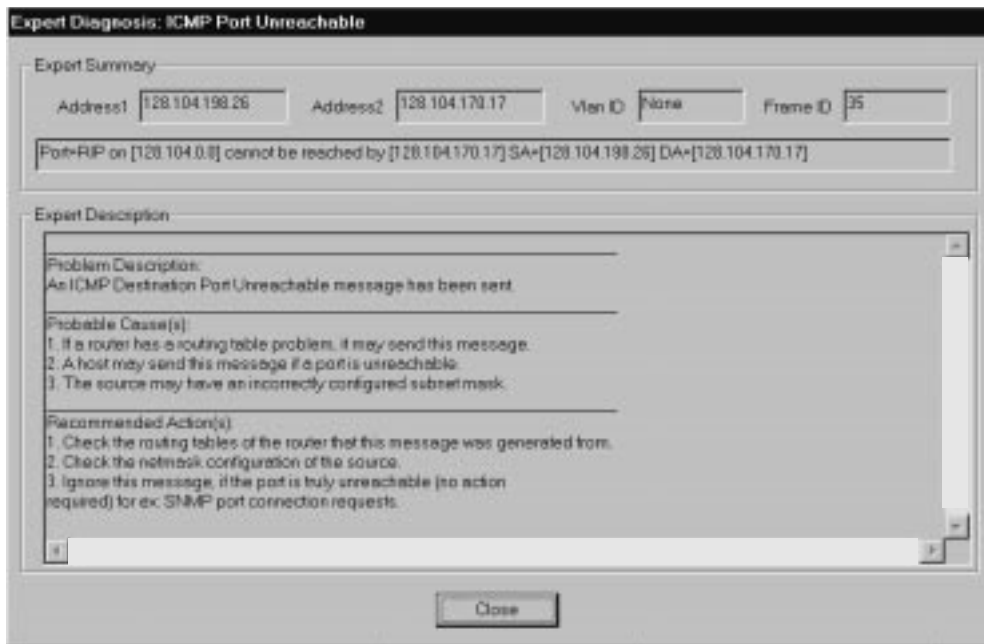


Figure 27. Expert Diagnosis Example

Expert Alarms

Expert Alarms allows you to set thresholds related to Expert Symptoms. Alarms can be configured to perform an action such as a page or e-mail, as with all other Surveyor alarms. Alarms test for thresholds at different protocol layers, such as the number of NFS retransmissions at the application layer or a specific overload utilization percentage at the MAC layer.

Some network problems are not single events, but are indicated by certain thresholds or counters being exceeded. To catch these type of problems, use Expert Alarms. Many event counters are available from the Expert Alarm Table that can be used to flag network conditions that are not single events, such as excessive multicast broadcasts.

Customizing Expert Diagnostic Information

Surveyor provides diagnostic information that is general to all networks. However, you can customize the diagnostic information to your environment.

As you use any diagnostic system you may find that certain error events occur regularly and or that events have a unique meaning in your environment. Custom solutions may apply to fixing the problems that are indicated by expert symptoms. By customizing the diagnostic information, you build an “information base” that applies to your particular environment. When the same problems occur, the custom information displays as well as standard information, providing the diagnostician with the benefit of previous experience related to your particular network.

The `Expertmsg.ini` file contains Surveyor’s diagnostic information. This file can be changed using a text editor, thus giving you a way to add information. Rules for adding information to `Expertmsg.ini` are included at the beginning of the file. Either possible causes or recommended actions can be added, or any other special technical note.

Surveyor always looks for the file named `Expertmsg.ini` in the Surveyor installation directory and will use that file for its diagnostic information. If no `Expertmsg.ini` file is found in the directory, Surveyor will not provide diagnostic information.

Application Response Time

The response time for various applications is measured in milliseconds (ms). A threshold can be set in the Application Response Time Alarms for all supported applications. Supported applications are:

- DNS
- FTP
- Gopher
- HTTP
- NFS
- NNTP
- POP
- SMTP
- TELNET

Application Layer

Excessive ARP

Counter

The Excessive ARP counter increments when a change in the number of ARP requests per second exceeds a threshold. The default threshold is a delta of 10 ARP requests per second; however, this value can be changed from the Expert Thresholds tab in the **Configuration** → **Module** → **Settings...** menu. A count of all Excessive ARP events displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Excessive ARP events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the rate of change for ARP requests. For example:

Rate of change of ARP Requests=20

Expert Diagnosis

Problem Description:

The expert threshold for ARP Broadcasts requests has been exceeded for this segment, resulting in an Excessive ARP symptom.

Probable Cause(s):

1. The network is overloaded.
 2. Variations in application traffic patterns.
 3. Heavy Internet usage.
 4. Too many new TCP/IP connections.
-

Recommended Action(s):

1. Load balance your network.
2. If you see repeated overloads and maybe too many retransmissions, your router or switch may need upgrading.
3. Your network may have just come up after a power down; if so, ignore this problem.
4. If it is due to higher Internet usage, then ignore this message.

Excessive BOOTP

Counter

The Excessive BOOTP counter increments when a change in the number of Bootp/Dhcp requests per second exceeds a threshold. The default threshold is a delta of 10 Bootp/Dhcp requests per second; however, this value can be changed from the Expert Thresholds tab in the **Configuration** → **Module** → **Settings...** menu. A count of all Excessive BOOTP events displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Excessive BOOTP events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the rate of change for Bootp/Dhcp requests. For example:

Rate of change of Bootp/Dhcp Requests=25

Expert Diagnosis

Problem Description:

The expert threshold for number of BOOTP/DHCP requests has been exceeded for this segment.

Probable Cause(s):

1. The network has many devices that are being reset.
2. The DHCP server has many requests from floating clients.

Recommended Action(s):

1. Load balance your network.
2. Add more DHCP servers.
3. Your network may have just come up after a power down; if so, ignore this problem.

ICMP All Errors

Counter

ICMP All Errors is a counter of all ICMP symptoms. A count of all ICMP symptoms displays in the **Overview** tab of Expert View. This counter can also be set in Expert Alarms to set a threshold for all ICMP errors.

The following types of ICMP errors are counted:

- **Destination Unreachable**
Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed [D/F Set], Source Route Failed, Destination Network Unknown, Destination Host Unknown, Destination Network Access Denied, Destination Host Access Denied, Network Unreachable for TOS, Host Unreachable for TOS, Destination Unreachable (catches all other Destination Unreachable Errors)
- **Source Quench**
- **Redirect**
Network Redirect, Host Redirect, Network Redirect for TOS, Host Redirect for TOS, ICMP Redirect (catches all other Redirect errors)
- **Time Exceeded**
ICMP Time Exceeded, Time To Live Exceeded, Fragment Reassembly Time Exceeded
- **Parameter Problem**
Bad IP Header, Required IP Option Missing, ICMP Parameter Problem (catches all other Parameter errors)

ICMP Bad IP Header

Counter

ICMP Bad IP Header events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Bad IP Header events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. Examples are:

```
Sent by Destination Host [206.250.228.69] to  
[206.250.228.11]. Bad Octet at 14. SA=[206.250.228.11]  
DA=[206.250.228.69]
```

```
Sent by Gateway [206.250.228.61] to [206.250.228.11] when  
forwarding to Destination [206.250.228.69]. Bad Octet at  
14. SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Parameter Problem (IP header is bad) message has been sent.

Probable Cause(s):

1. A host/router may send this message if the IP header parameters have problems that prevents it from processing the packet.
2. A host/router may have a bad network stack or a bad interface card.
3. There may be incorrect arguments in IP options.

Recommended Action(s):

1. Check the **ICMP Pointer** field to see the octet in the IP header where the error was detected.
2. Verify that the source that sent this IP header has a good network interface card.
3. Check if the network stack on the source that sent the bad IP header parameters is working properly.

ICMP Destination Host Access Denied

Counter

ICMP Destination Host Access Denied events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Destination Host Access Denied events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11]
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Host Administratively Prohibited message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if the destination host does not have proper access.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source and/or the router.
3. Ignore this message, if the host is truly prohibited (no action required).

ICMP Destination Host Unknown

Counter

ICMP Destination Host Unknown events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Destination Host Unknown events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11]  
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Host Unknown message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if it does not know the destination host.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source and/or the router.
3. Ignore this message, if the host is truly unknown (no action required).

ICMP Destination Network Access Denied

Counter

ICMP Destination Network Access Denied events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Destination Network Access Denied events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11]  
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Network Administratively Prohibited message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if the network does not have proper access.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source and/or the router.
3. Ignore this message, if the network is truly prohibited (no action required).

ICMP Destination Network Unknown

Counter

ICMP Destination Network Unknown events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Destination Network Unknown events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11]  
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Network Unknown message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if it does not know the destination network.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source and/or the router.
3. Ignore this message, if the network is truly unknown (no action required).

ICMP Destination Unreachable

ICMP Destination Unreachable is a counter of all ICMP destination unreachable errors over a period of time per segment. A count of all destination unreachable ICMP symptoms displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms for all destination unreachable ICMP errors.

The following types of destination unreachable ICMP errors are counted:

Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed [D/F Set], Source Route Failed, Destination Network Unknown, Destination Host Unknown, Destination Network Access Denied, Destination Host Access Denied, Network Unreachable for TOS, Host Unreachable for TOS, Destination Unreachable (catches all other Destination Unreachable Errors)

Expert Symptom

ICMP Destination Unreachable is also an expert symptom, and has its own expert diagnosis. However, this expert symptom reflects only those destination unreachable conditions which cannot be assigned to one of the other destination unreachable symptoms defined above.

ICMP Destination Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11]  
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Unreachable message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a destination is unreachable.
3. If the packet needs to be fragmented and yet the don't fragment flag is set the host/router will send this message.
4. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the destination is truly unreachable (no action required).

ICMP Fragment Reassembly Time Exceeded

Counter

ICMP Fragment Reassembly Time Exceeded events are counted in the All ICMP Errors counter. A count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Fragment Reassembly Time Exceeded events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Sent by Destination Host [206.250.228.69] to  
[206.250.228.11]. SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Fragment Reassembly Time Exceeded message has been sent.

Probable Cause(s):

1. A host may send this message if it cannot reassemble the fragments (due to missing fragments) on time.
2. There may be a lot of missing IP fragments (possibly due to NFS traffic or network overload).
3. If the routing tables are incorrect on the source.

Recommended Action(s):

1. Check the routing tables of the source.
2. Check the netmask configuration of the source.
3. Check if there are missing IP fragments.
4. May need to upgrade the host that sent this message.

ICMP Fragmentation Needed [D/F set]

Counter

ICMP Fragmentation Needed [D/F set] events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Fragmentation Needed [D/F set] events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
MTU of next Hop=2 to reach [206.250.228.69]. Cannot be
reached by [206.250.228.11] as D/F Set. SA=[206.250.228.11]
DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination (Fragmentation needed, but, D/F set) Unreachable message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. If the packet needs to be fragmented and yet the don't fragment flag is set the host/router will send this message.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the D/F is meant to be set (no action required).

ICMP Host Redirect

Counter

ICMP Host Redirect events are counted in the ICMP Redirect Errors counter and the ICMP All Errors counter. A count of ICMP redirect errors and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP redirect errors or for all ICMP errors.

Expert Symptom

ICMP Host Redirect events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] from  
[206.250.228.11] SA=[206.250.228.11]DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Host Redirect message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the redirect message is valid (no action required).

ICMP Host Redirect for TOS

Counter

ICMP Host Redirect for TOS events are counted in the ICMP Redirect Errors counter and the ICMP All Errors counter. A count of ICMP redirect errors and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP redirect errors or for all ICMP errors.

Expert Symptom

ICMP Host Redirect for TOS events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] and
TOS 22 from [206.250.228.11] SA=[206.250.228.11]
DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Redirect for TOS and Host message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the redirect message is valid (no action required).

ICMP Host Unreachable

Counter

ICMP Host Unreachable events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Host Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11]  
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Host Unreachable message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a destination host is unreachable.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the host is truly unreachable (no action required).

ICMP Host Unreachable for TOS

Counter

ICMP Host Unreachable for TOS events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Host Unreachable for TOS events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
TOS=22 service on [206.250.228.69] unavailable for  
[206.250.228.11] SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Host is Unreachable for TOS message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a destination host is unreachable for the type of service requested.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the host is truly unreachable for TOS (no action required).

ICMP Network Redirect

Counter

ICMP Network Redirect events are counted in the ICMP Redirect Errors counter and the ICMP All Errors counter. A count of ICMP redirect errors and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP redirect errors or for all ICMP errors.

Expert Symptom

ICMP Network Redirect events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] from  
[206.250.228.11] SA=[206.250.228.11]DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Network Redirect message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the redirect message is valid (no action required).

ICMP Network Redirect for TOS

Counter

ICMP Network Redirect for TOS events are counted in the ICMP Redirect Errors counter and the ICMP All Errors counter. A count of ICMP redirect errors and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP redirect errors or for all ICMP errors.

Expert Symptom

ICMP Network Redirect for TOS events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] and
TOS 22 from [206.250.228.11] SA=[206.250.228.11]
DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Redirect for TOS and Network message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the redirect message is valid (no action required).

ICMP Network Unreachable

Counter

ICMP Network Unreachable events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Network Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11]  
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Network Unreachable message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a destination host is unreachable.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the host is truly unreachable (no action required).

ICMP Parameter Problem

Counter

ICMP Parameter Problem events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Parameter Problem events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Bad IP Header sent from [206.250.228.11] to  
[206.250.228.69]. SA=[206.250.228.11] DA=[206.250.228.69]
```

This Expert Symptom will be used to identify a parameter problem only if the problem cannot be identified as a Bad IP Header or as a Missing IP Option.

Expert Diagnosis

Problem Description:

An ICMP Parameter Problem message has been sent.

Probable Cause(s):

1. A host/router may send this message if the IP header parameters have problems that prevents it from processing the packet.
2. A host/router may have a bad network stack or a bad interface card.
3. There may be incorrect arguments in IP options.

Recommended Action(s):

1. Check the **ICMP Pointer** field to see the octet in the IP header where the error was detected.
2. Verify that the source that sent this IP header has a good network interface card.
3. Check if the network stack on the source that sent the bad IP header parameters is working properly.

ICMP Port Unreachable

Counter

ICMP Port Unreachable events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Port Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Port=22 on [206.250.228.69] cannot be reached by  
[206.250.228.11] SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Port Unreachable message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a port is unreachable.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the port is truly unreachable (no action required) for example, SNMP port connection requests.

ICMP Protocol Unreachable

Counter

ICMP Protocol Unreachable events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Protocol Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Protocol=IP on [206.250.228.69] cannot be reached by  
[206.250.228.11] SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Protocol Unreachable message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a protocol is unreachable.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the protocol is truly unreachable (no action required).

ICMP Redirect

Counter

ICMP Redirect is a counter of all ICMP redirect errors over a period of time per segment. A count of all redirect ICMP symptoms displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

The following types of ICMP redirect errors are counted:

Network Redirect, Host Redirect, Network Redirect for TOS, Host Redirect for TOS, ICMP Redirect (catches all other Redirect errors)

Expert Symptom

ICMP Redirect is also an expert symptom, and has its own expert diagnosis. However, this expert symptom reflects only those redirect conditions which cannot be assigned to one of the other redirect symptoms defined above.

ICMP Redirect events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] from  
[206.250.228.11] SA=[206.250.228.11]DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Redirect message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message, if the redirect message is valid (no action required).

ICMP Required IP Option Missing

Counter

ICMP Required IP Option Missing events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Required IP Option Missing events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Bad IP Header sent from [206.250.228.11] to  
[206.250.228.69]. SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Parameter Problem (IP Options required, but, missing) message has been sent.

Probable Cause(s):

1. A host/router may send this message if the IP header parameters have problems that prevents it from processing the packet.
2. A host/router may have a bad network stack or a bad interface card.
3. There may be incorrect arguments in IP options.

Recommended Action(s):

1. Check the **ICMP Pointer** field to see the octet in the IP header where the error was detected.
2. Verify that the source that sent this IP header has a good network interface card.
3. Check if the network stack on the source that sent the bad IP header parameters is working properly.

ICMP Source Quench

Counter

ICMP Source Quench events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Source Quench events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. Examples are:

```
Sent by Destination Host [206.250.228.69] to  
[206.250.228.11]. SA=[206.250.228.11] DA=[206.250.228.69]  
Sent by Gateway Host [206.250.228.61] to [206.250.228.11]  
when forwarding to Destination [206.250.228.69].  
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Source Quench message has been sent.

Probable Cause(s):

1. If a router has a buffer space problem, it may send this message.
2. A host may send this message if it can't keep up with processing of packets and is reaching its limits.
3. The network may be overloaded.

Recommended Action(s):

1. Check the routing table buffer statistics and upgrade the router if problem persists.
2. If the message is from a host, you may need to upgrade it's resources.
3. Increase the bandwidth of your network to reduce network overload.
4. Ignore this message, if it is infrequent as the problem will rectify itself.

ICMP Source Route Failed

Counter

ICMP Source Route Failed events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Source Route Failed events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11]  
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Destination Unreachable (Source Route Failed) message has been sent.

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if it cannot route the packet.
3. The source may have an incorrectly configured subnet mask.

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.

ICMP Time Exceeded

Counter

ICMP Time Exceeded events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Time Exceeded events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Sent by Gateway [206.250.228.61] to [206.250.228.11] when
forwarding to Destination [206.250.228.69]
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Time Exceeded message has been sent.

Probable Cause(s):

1. A router may send this message if it encounters an IP packet with a TTL value of 0.
2. The source may have an incorrectly configured subnet mask, causing longer hops.
3. If the routing tables are incorrect on the source.
4. A host may send this message if it cannot reassemble the fragments (due to missing fragments) on time.

Recommended Action(s):

1. Check the routing tables of the source.
2. Check the netmask configuration of the source.
3. Check if there are missing IP fragments.
4. May need to upgrade your router or host.

ICMP Time to Live Exceeded

Counter

ICMP Time to Live Exceeded events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** tab of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Time to Live Exceeded events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the IP addresses involved. For example:

```
Sent by Gateway [206.250.228.61] to [206.250.228.11] when
forwarding to Destination [206.250.228.69]
SA=[206.250.228.11] DA=[206.250.228.69]
```

Expert Diagnosis

Problem Description:

An ICMP Time To Live Exceeded message has been sent.

Probable Cause(s):

1. A router may send this message if it encounters an IP packet with a TTL value of 0.
2. The source may have an incorrectly configured subnet mask, causing longer hops.
3. If the routing tables are incorrect on the source.

Recommended Action(s):

1. Check the routing tables of the source.
2. Check the netmask configuration of the source.

NFS Retransmissions

Counter

NFS Retransmissions is a counter of all NFS Retransmissions over a period of time per segment. A count of all NFS Retransmissions displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

NFS Retransmission events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the addresses of the client and server involved. For example:

```
Client [206.250.228.69] retransmitting to Server  
[206.250.228.14]
```

Expert Diagnosis

Problem Description:

There is a retransmission of an NFS request packet as the RPC identifier for this connection has been reused.

Probable Cause(s):

1. An NFS data maybe transmitted over several fragmented IP packets. If any of the IP fragments are missing, it will result in a retransmission.
2. The network is overloaded.
3. The path to the receiving station has long delays.
4. There may be an overloaded switch or router.

Recommended Action(s):

1. Check if there are any missing IP fragments.
2. If you see repeated delays and too many retransmissions, your router or switch may need upgrading.

Transport Layer

Non Responsive Station

Counter

Non Responsive Station is a counter of all non-responsive stations over a period of time per segment. A non-responsive station is defined as successive TCP/IP retransmissions over the same connection that are greater than a threshold value. The default threshold is 3 successive retransmissions; however, this value can be changed from the **Expert Thresholds** tab in the **Configuration** → **Module** → **Settings...** menu. A count of all non-responsive stations displays in the **Overview** tab of Expert View. A threshold for the number of Non Responsive Station events can be set in Expert Alarms.

Expert Symptom

Non Responsive Station events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides the IP address of the non-responsive station. For example:

```
Station [206.250.228.11] not responding
```

Expert Diagnosis

Problem Description:

The successive retransmissions expert threshold has been exceeded, resulting in a Non Responsive Station symptom.

Probable Cause(s):

1. The ACK sent by the receiver was lost.
2. The network is overloaded.
3. The path to the receiving station has long delays.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may be an overloaded switch or router.

Recommended Action(s):

1. Load balance your network.
2. If you see repeated delays and too many retransmissions, then your router or switch may need upgrading.

TCP/IP Frozen Window

Counter

The TCP/IP Window Frozen counter increments when the TCP/IP window is frozen for greater than a threshold value, measured in seconds. The default threshold is a frozen window of 5 seconds; however, this value can be changed from the **Expert Thresholds** tab in the **Configuration → Module → Settings...** menu. A count of all TCP/IP Window Frozen events displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

TCP/IP Window Frozen events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the frozen window size, duration, and the well-known ports(WKP) involved, including the port number and the IP address. For example:

```
Frozen at 29909 for [19 ms] between [206.250.228.69]/[TCP/
IP WKP:1988] and [206.250.228.11]/[SMTP]
```

A frozen window event is defined as the TCP/IP window size remaining the same for all packets over a 5 second period for one connection in one direction. If only one packet is detected over the 5 second interval, this is also logged as a TCP/IP frozen window event. Events of this type can indicate when a problem with the TCP/IP connection or excessive network traffic.

Expert Diagnosis

Problem Description:

A TCP/IP packet has the window size stuck for longer than 5 seconds. If the window size is less than the maximum, then the flow of data is restricted as the sender will not exceed the receiver's window size.

Probable Cause(s):

1. The receiver is overloaded.
2. The receiver has run out of buffer space.
3. There may be a problem with the receiver's TCP/IP stack.
4. There may too many connections to the receiver causing reduced buffer space.

Recommended Action(s):

1. Upgrade the receiver's CPU and or Memory.
2. Reduce the number of connections to the receiver.
3. Increase the network bandwidth.

TCP/IP Long Ack

Counter

The TCP/IP Long Ack counter increments when the TCP/IP acknowledgment for a connection is not seen for greater than a threshold value, measured in milliseconds. The default threshold is no acknowledgment for 200 milliseconds; however, this value can be changed from the **Expert Thresholds** tab in the **Configuration** → **Module** → **Settings...** menu. A count of all TCP/IP Long Ack events displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

TCP/IP Long Acks are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the acknowledgment time and the well-known ports(WKP) involved, including the port number and the IP address. For example:

```
Ack Time= [300 ms] between [206.250.228.69]/[TCP/IP  
WKP:1988] and [206.250.228.11]/[SMTP]
```

The time required to acknowledge a TCP/IP packet is calculated for every packet. When a value exceeds 200ms, the event is logged as an Expert Symptom.

Expert Diagnosis

Problem Description:

A TCP/IP ACK (Acknowledgment) has taken longer than 200 msec to arrive to the sender.

Probable Cause(s):

1. The receiver which generated the ACK was very busy.
2. The network is overloaded.
3. The path to the sender from the receiver has long delays.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may be an overloaded switch or router in the path.

Recommended Action(s):

1. Load balance your network.
2. If you see repeated delays and long acknowledgments, your receiver may need upgrading.

TCP/IP Retransmissions

Counter

TCP/IP Retransmissions is a counter of all TCP/IP Retransmissions over a period of time per segment. This variable counts the number of retransmitted packets to measure excessive retransmission in TCP/IP. A count of all TCP/IP Retransmissions displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Retransmissions are determined by sweeping the capture data periodically to catch connections that retransmitted within an interval.

Expert Symptom

TCP/IP Retransmissions are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the well-known ports(WKP) involved, including the port number and the IP address. For example:

```
Between [206.250.228.69]/[TCP/IP WKP:1988] and  
[206.250.228.11]/[TCP/IP WKP:197]
```

Expert Diagnosis

Problem Description:

A TCP/IP packet has been retransmitted as the sequence number is being repeated. There was no ACK (acknowledgment) from the receiver, causing the sender to retransmit the packet.

Probable Cause(s):

1. An ACK sent by the receiver was lost.
2. The network is overloaded.
3. The path to the receiving station has long delays.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may be an overloaded switch or router.

Recommended Action(s):

1. Load balance your network.
2. If you see repeated delays and too many retransmissions, your router or switch may need upgrading.

TCP/IP RST Packets

Counter

TCP/IP RST Packets is a counter of all TCP/IP RST Packets over a period of time per segment. This variable counts the number of RST responses to monitor resets in TCP/IP. A count of all TCP/IP RST packets displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

TCP/IP SYN Attack

Counter

The TCP/IP SYN Attack counter increments when a change in the number of SYN requests per second exceeds a threshold. The default threshold is a delta of 100 SYN requests per second; however, this value can be changed from the Expert Thresholds tab in the **Configuration** → **Module** → **Settings...** menu. A count of all TCP/IP SYN Attack events displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

TCP/IP SYN Attack events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the rate of change for SYN requests. For example:

Rate of change of TCP/IP SYNs=150

Expert Diagnosis

Problem Description:

The threshold for the number of SYN connections on the segment has been exceeded. There may be a SYN attack.

Probable Cause(s):

1. An intruder is trying to break into your network.
 2. The network is heavily overloaded.
 3. Your Web server is under attack.
 4. There may be a problem with the receiver's TCP/IP stack.
 5. There may be an overloaded switch or router.
-

Recommended Action(s):

1. Load balance your network.
2. If you see all the SYNs going to the same station, you may be under attack.
3. If you see too many SYN requests coming from unknown IP addresses, you need to use a firewall or some other means of authentication.

TCP/IP Zero Window

Counter

TCP/IP Zero Window is a counter of all TCP/IP Zero Window events over a period of time per segment. A count of all TCP/IP Zero Window events displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

All TCP/IP zero window events are also counted as frozen window events.

Expert Symptom

TCP/IP Zero Window events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the time, location, and the well-known ports(WKP) involved, including the port number and the IP address. For example:

```
Stuck at 0 for [14 ms] between [206.250.228.69]/[TCP/IP  
WKP:1988] and [206.250.228.11]/[SMTP]
```

The TCP window size is examined for every packet to check against a window size of zero. If the window size remains zero for 5 seconds for one connection in one direction, the event is logged. If only one packet with a zero window size is detected over the 5 second interval, this is also logged as a TCP/IP zero window event. Events of this type indicate when a receiver's buffer is full which can indicate problems with the network.

Expert Diagnosis

Problem Description:

A TCP/IP packet has zero window size for longer than 5 secs. The receiver is shutting down communication and will accept no more data from the other end.

Probable Cause(s):


1. The receiver is overloaded.
2. The receiver has run out of buffer space.
3. The non-responsive receiver intends the sender to close the connection.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may too many connections to the receiver causing reduced buffer space.

Recommended Action(s):

1. Upgrade the receiver's CPU and or Memory.
2. Reduce the number of connections to the receiver.
3. Increase the bandwidth of your network.

Network Layer

Duplicate Network Address

A separate table showing duplicate network addresses is available. Press the  button on the Data View or Capture View toolbar to see this table.

Counter

Duplicate Network Address is a counter of all duplicate network addresses over a period of time per segment. A count of all duplicate network addresses displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms for all duplicate network Addresses.

Expert Symptom

Duplicate network addresses are automatically logged as either “Duplicate IP Address” or “Duplicate IPX Address” expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the duplicate IP or IPX address. For example:

Addr=[206.250.228.67]

Expert Diagnosis

Problem Description:

This network address has multiple MAC station address association. This is a serious problem if the associated MAC stations are not routers.

Probable Cause(s):

1. An existing network address has been assigned to a new machine without verification.
2. An old (discarded) machine using this address has been re-introduced into the network.

Recommended Action(s):

Change the network address of one or more hosts so that there are no duplicates.

HSRP Coup

Counter

HSRP Coup events are counted in the HSRP Errors counter, which displays in the Overview tab of Expert View. A Coup message indicates that the router wishes to become active. A threshold can be set in Expert Alarms for HSRP Coup/Resign packets, which includes both Resign and Coup HSRP messages.

Expert Symptom

HSRP Coup events are automatically logged as expert symptoms. The Symptom Summary field in the Analysis Table provides the IP address of the router trying to become active. For example:

SA=[206.250.226.11] DA=[206.250.228.69]

Expert Diagnosis

Problem Description:

A Router has generated an HSRP Coup message.

Probable Cause(s):

1. The router wishes to become the active router.

Recommended Action(s):

1. Make sure that the router coming up is a stand by router.
2. Make sure there was a router Resign message (by Master router) before coup.

HSRP Errors

Counter

Some Hot Standby Routing Protocol (HRSP) packets are counted in the HSRP Errors counter, which displays in the Overview tab of Expert View. Both Coup and Resign packets are counted. Coup/Resign packets in the HRSP are used to activate/deactivate routers. A threshold can be set in Expert Alarms for HSRP Coup/Resign packets, which includes both Resign and Coup HSRP messages.

HSRP Resign

Counter

HSRP Resign events are counted in the HSRP Errors counter, which displays in the Overview tab of Expert View. A Resign message indicates that the router is requesting to become inactive. A threshold can be set in Expert Alarms for HSRP Coup/Resign packets, which includes both Resign and Coup HSRP messages.

Expert Symptom

HSRP Resign events are automatically logged as expert symptoms. The Symptom Summary field in the Analysis Table provides the IP address of the router trying to become inactive. For example:

SA=[206.250.226.11] DA=[206.250.228.69]

Expert Diagnosis

Problem Description:

A router has generated an HSRP Resign message.

Probable Cause(s):

1. The router no longer wishes to be the active router.

Recommended Action(s):

1. Make sure the router is going back to stand by mode.
2. Make sure you get a Coup message or Hello message from new router that has taken over.

Illegal Network Source Address

Counter

Illegal Network Source Address is a counter of all illegal network source addresses over a period of time per segment. A count of all illegal MAC source addresses displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Illegal network source addresses are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides the number of illegal address encountered. For example:

Number of illegal sources (since last)=[22]

This symptom can help catch malfunctioning routers or bad addresses generated due to collisions.

Expert Diagnosis

Problem Description:

A broadcast network address has appeared as a source address. This is problem associated with a bad host.

Probable Cause(s):

1. Someone is transmitting illegal frames using a traffic generator.
2. There may be a faulty adapter card/host.

Recommended Action(s):

Filter on the MAC address and determine the faulty card and replace it.

IP Checksum Errors

Counter

IP Checksum Errors is a counter of all incorrect IP checksums over a period of time per segment. A count of all IP Checksum Errors events displays in the Overview tab of Expert View.

Expert Symptom

IP Checksum Errors events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides the IP source and destination address for the checksum error. For example:

SA=[206.250.228.69] DA=[206.250.228.11]

Expert Diagnosis

Problem Description:

An IP packet has a checksum value that is in error. The packet may be discarded.

Probable Cause(s):

1. The station that sent this packet may have a faulty network stack.
2. The router that forwarded this packet may have a faulty stack.

Recommended Action(s):

1. Identify the station that sent this packet (source addresses).
2. Verify the network layer stack for this station. The station may need to be reset.

IP Time to Live Expiring

Counter

IP Time to Live Expiring is a counter of all expiring connections over a period of time per segment. A count of all IP Time to Live Expiring events displays in the Overview tab of Expert View. A threshold for this counter can be set in Expert Alarms to generate an alarm based on a specific number of expiring connections.

Expert Symptom

IP Time to Live Expiring events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the “time-to-live” (TTL) and the source and destination addresses. For example:

TTL=1 SA=[206.250.228.69] and DA=[206.250.228.11]

Expert Diagnosis

Problem Description:

An IP packet has a time to live value that is going to expire. The packet may be discarded.

Probable Cause(s):

1. The network is overloaded.
2. Router tables may be misconfigured.

Recommended Action(s):

1. Increase the network bandwidth.
2. Check your router configuration.

ISL BPDU/CDP Packets

Counter

ISL BPDU/CDP Packets is a counter of all Bridge Protocol Data Unit (BPDU) or Cisco Discovery Protocol (CDP) packets in an ISL frame over a period of time per segment. A count of BPDU/CDP packets displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms to generate an alarm based on a specific number of BPDU/CDP packets.

ISL Illegal VLAN ID

Counter

ISL Illegal VLAN ID is a counter of all ISL illegal VLAN IDs over a period of time per segment. A count of all ISL Illegal VLAN ID displays in the **Overview** Tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

ISL Illegal VLAN IDs are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides the number of the illegal VLAN ID. For example:

```
VLAN ID=[1036]
```

Expert Diagnosis

Problem Description:

The VLAN ID in the ISL protocol is illegal. The allowable range is from 1 to 1024.

Probable Cause(s):

1. An error made in the VLAN configuration for the Switch may have introduced an illegal VLAN ID.
2. A faulty Switch.

Recommended Action(s):

1. Reconfigure your Switch's VLAN configuration to use valid ID's.
2. Replace the faulty Switch.

Unstable MST

Counter

The Unstable MST counter increments when a change in the number of MST topology changes per second exceeds a threshold. The default threshold is a delta of 5 topology changes per second; however, this value can be changed from the Expert Thresholds tab in the **Configuration** → **Module** → **Settings...** menu. A count of all Unstable MST events displays in the Overview Tab of Expert View. A threshold for this counter can be set in Expert Alarms.

MST topology changes are topology changes required to support IEEE 802.1d (Minimum Spanning Tree). Excessive topology changes infer that the Minimum Spanning Tree (MST) is unstable.

Expert Symptom

Unstable MST events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the rate of change for the MST topology. For example:

Rate of change of Topology=10

Expert Diagnosis

Problem Description:

The threshold for the number of IEEE 802.1D packets with topology change bit has been exceeded for this segment. The Spanning tree may be unstable.

Probable Cause(s):

1. There may be too many configuration changes for the bridge or switch.
2. There may be a temporary loss of connectivity.

Recommended Action(s):

1. Identify the device causing this message and fix it.

OSPF Broadcasts

Counter

OSPF Broadcasts is a counter of all OSPF broadcasts over a period of time per segment. A count of all OSPF broadcasts displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

If OSPF broadcasts fall below a certain threshold, this may indicate that a OSPF router is not functioning properly.

Network Overload

Counter

Network Overload is a counter of instances where a threshold for the percentage change in network utilization is exceeded. Network utilization is compared to the utilization for the previous time segment. The default threshold is a 40% change in network utilization; however, this value can be changed from the Expert Thresholds tab in the **Configuration** → **Module** → **Settings...** menu. A count of all instances where the threshold is reached displays in the Overview tab of Expert View.

Expert Symptom

Network Overload events are automatically logged as expert symptoms. The Symptom Summary field in the Analysis Table provides information about the change in utilization. For example:

```
%Utilization=42
```

Expert Diagnosis

Problem Description:

The utilization expert threshold has been exceeded for this segment, resulting in a LAN Overload symptom.

Probable Cause(s):

1. The network is overloaded. Variations in application traffic patterns.
 2. Heavy Internet usage.
 3. Too many broadcast/multicast packets.
-

Recommended Action(s):

1. Load balance your network.
2. If you see repeated overloads and/or too many retransmissions, your router or switch may need upgrading.

RIP Broadcasts

Counter

RIP Broadcasts is a counter of all RIP broadcasts over a period of time per segment. A count of all RIP broadcasts displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

If RIP broadcasts fall below a certain threshold, this may indicate that a RIP router is not functioning properly.

SAP Broadcasts

Counter

SAP Broadcasts is a counter of all SAP broadcasts over a period of time per segment. A count of all SAP broadcasts displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

If SAP broadcasts fall below a certain threshold, this may indicate that a SAP router is not functioning properly.

Total Router Broadcasts

Counter

Total Router Broadcasts is a counter of all total router broadcasts over a period of time per segment. A threshold for this counter can be set in Expert Alarms for total router broadcasts.

If total router broadcasts go above a certain threshold, this may indicate that a router in the network is generating excessive broadcast messages.

MAC Layer

Broadcast/Multicast Storms

Counter

The Broadcast/Multicast Storms counter increments when a change in the number of total Broadcast/Multicast packets per second exceeds a threshold. Broadcast/Multicast Storms can be used to monitor extreme peaks in the number of broadcast and/or multicast messages. The default threshold is a delta of 400 broadcast/multicast events per second; however, this value can be changed from the Expert Thresholds tab in the **Configuration → Module → Settings...** menu. A count of all instances where the threshold is reached displays in the Overview tab of Expert View.

Expert Symptom

Broadcast/Multicast Storm events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the rate of change for broadcast and multicast packets. For example:

Rate of change of Bcast/Mcast Packets=500

Expert Diagnosis

Problem Description:

The broadcast storm expert threshold has been exceeded for this segment, resulting in a MAC Broadcast Storm symptom.

Probable Cause(s):

1. The network is overloaded.
2. Variations in application traffic patterns.
3. Heavy Internet usage.
4. Too many broadcast/multicast packets from the switch/bridge.

Recommended Action(s):

1. Load balance your network.
2. If you see repeated storms, your router or switch may need upgrading or reconfiguring.

Excessive Broadcasts

Counter

Excessive Broadcasts is a counter that can be used to monitor fluctuations in the number of broadcast messages over a period of time per segment. A delta threshold for this counter can be set in Expert Alarms to establish what is considered excessive broadcasts. An alarm event can also be generated based on an absolute number of multicasts over time.

The default is 400 broadcast packets per sec on a 100MB network.

Excessive Collisions

Counter

Excessive Collisions is a counter that can be used to monitor fluctuations in the number of collisions or the absolute number of collisions over a period of time per segment. A delta threshold for this counter can be set in Expert Alarms to establish what is considered excessive collisions. An alarm event can also be generated based on an absolute number of collisions over time.

The Excessive Collision counter is incremented by counting runt packets and by counting packets with CRC errors. The Excessive Collisions counter only applies to Ethernet networks.

Excessive Multicasts

Counter

Excessive Multicasts is a counter that can be used to monitor fluctuations in the number of multicast messages over a period of time per segment. A delta threshold for this counter can be set in Expert Alarms to establish what is considered excessive broadcasts. An alarm event can also be generated based on an absolute number of multicasts over time.

The default is 400 multicast packets per sec on a 100MB network.

Illegal MAC Source Address

Counter

Illegal MAC Source Address is a counter of all illegal MAC station source addresses over a period of time per segment. A count of all illegal MAC source addresses displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Illegal MAC source addresses are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides the number of illegal address encountered. For example:

Number of illegal sources (since last)=[22]

This symptom can help catch malfunctioning NIC cards or bad addresses generated due to collisions. Illegal MAC source addresses may be discovered on Ethernet or Token Ring networks.

Expert Diagnosis

Problem Description:

A broadcast Ethernet (or Token Ring) address has appeared as a source address. This is problem associated with a bad adapter card.

Probable Cause(s):

1. Someone is transmitting illegal frames using a traffic generator.
2. There may be a faulty adapter card.

Recommended Action(s):

Filter on the Network address and determine which host has the faulty card and replace it.

New MAC Stations

Counter

New MAC Stations is a counter of all the new MAC stations over a period of time per segment. A threshold for this counter can be set in Expert Alarms. The threshold for new MAC stations is typically set to 1 as an absolute value.

The new MAC station counter detects new MAC stations (nodes) on a LAN segment. After a segment is stabilized with a specific number of stations, this counter can indicate possible intruder stations.

Overload Frame Rate

Counter

Overload Frame Rate counts frames over a one-second time period. A threshold for the number of frame per second can be set in Expert Alarms.

Overload Frame Rate can help catch network overloads.

Values for the threshold can range from 1 to 148,800 frames/sec for a 100 MB network. The default is 37,200 frames/sec.

Overload Utilization Percentage

Counter

Overload Utilization Percentage counts bits over time and compares this value to the maximum utilization possible (bandwidth). A threshold for this percentage value can be set in Expert Alarms.

Overload utilization percentage can help catch network overloads.

The default for a 100MB network is 25% of maximum utilization.

Physical Errors

Counter

The Physical Errors counter increments when a change in the number of total MAC physical errors per second exceeds a threshold. Physical errors include CRC/alignment errors, dropped events, collisions, jabbers, oversize packets, undersize packets, and fragments. The default threshold is a delta of 400 physical error packets per second; however, this value can be changed from the Expert Thresholds tab in the **Configuration** → **Module** → **Settings...** menu. A count of all instances where the threshold is reached displays in the Overview tab of Expert View.

Expert Symptom

Physical Error events are automatically logged as expert symptoms. The **Symptom Summary** field in the Analysis Table provides information about the rate of change for total MAC physical errors. For example:

Rate of change of Errors=450

Expert Diagnosis

Problem Description:

The errors threshold has been exceeded for this segment, resulting in a MAC Physical Errors symptom.

Probable Cause(s):

1. The network is overloaded.
 2. A faulty hub/switch/router device.
 3. A hub may have been incorrectly used. For example, an uplink port may have been used as a data port.
 4. An end station may have a faulty network interface card.
-

Recommended Action(s):

1. Restart capture after setting up a filter to capture error packets (only).
2. Based on the capture results, isolate the device that is in error and fix the problem.

Total MAC Stations

Counter

Total MAC Stations is a counter of all the MAC stations over a period of time per segment. A count of all MAC stations displays in the **Overview** tab of Expert View. A threshold for this counter can be set in Expert Alarms. The MAC station counter helps detect excessive MAC stations (nodes) on a LAN segment. This helps indicate possible intruder stations as well as help the network manager limit and control the number of stations allowed on a segment.

Hints and Tips for Expert Features

- Double-click any symptom in the Analysis Table to view Diagnostic information.
- You can jump directly to the frame in Capture View that is associated with the expert symptom. Select (single-click) the expert symptom from the Analysis Table using the right mouse button. Select the **Go To Frame...** option. The frame associated with the expert symptom displays in Capture View.
- When looking at Expert View in Monitor only mode, no Frame ID displays for Expert Symptoms detected and you cannot examine a frame related to a symptom. If you need to look at specific frames related to Expert Symptoms, look at the frame information in the capture buffer or in a capture file.
- Expert Views can be disabled on a per module basis. Select **Module** → **Settings...** from the **Configuration** menu and choose the **Modes** Tab. Remove the check from the **Expert Views** box.
- Click, hold, and drag a column border to resize columns in any Expert View Table. Increasing the size of the **Symptom** column gives you a view of the complete name of the symptom.
- Click, hold, and drag a column border to remove columns in any Expert View Table. Double-click on the same column border to bring back the display of a column.
- Duplicate addresses appear both in the Duplicate Network Address Table and as a symptom in the Analysis Table of Expert View.
- You can directly access statistics about a particular host associated with an expert event. From the Expert Overview table, click on any of the counters underlined in blue to see the symptoms broken down by host or conversation. You can then click on the host for more in-depth statistics.
- Thresholds can be set for Expert Symptoms. Select **Module** → **Settings...** from the Configuration menu and choose the Expert Thresholds Tab. Change the threshold value for any of the listed symptoms.
- Expert Symptoms can be selectively disabled. Select **Module** → **Settings...** from the Configuration menu and choose the Expert Symptoms Tab. Remove the check from the Expert Symptoms you wish to disable.
- Expert Symptoms can be displayed in the Summary field of Capture View. From the Configuration menu, select **Capture View Options** → **Display** and select the **Display Expert Symptom** check box. Packets that trigger an expert symptom and have expert symptom information will display in reverse video.

Summary of Expert Counters and Symptoms

The table on the following page provides a summary of expert features by symptom/counter/application name. The meanings of the column headings are listed below.

Expert Symptom	Logged as an Expert Event and appears in the Analysis Tab of Expert View.
Counter in Expert View	Has a counter associated with it that displays in the Overview tab of Expert View.
Expert Alarm	Has an alarm you can set in the Expert Alarm editor.
Application Response Time Alarm	Has an alarm you can set in the Application Response Time Alarm editor.
Expert Threshold	A threshold can be set in the Expert Threshold tab from the from the Configuration → Module → Settings... menu.

Table 26. Summary of Expert Features

X = present

z = does not exist as a unique counter, but is counted in other categories

Counter, Symptom, or Application	Expert Symptom	Counter in Expert View	Expert Alarm	Application Response Time Alarm	Expert Threshold
Application Response Time				X (by application)	
Broadcast/ Multicast Storm	X	X			X
DNS Response Time				X	
Duplicate Network Address (also displays as a separate view)	X	X	X		
Excessive ARP	X	X	X		X
Excessive BOOTP	X	X	X		X
Excessive Broadcasts			X		
Excessive Collisions			X		
Excessive Multicasts			X		
FTP Response Time				X	
Gopher Response Time				X	
HSRP Coup	X	z	z		
HSRP Errors		X	X		
HSRP Resign	X	z	z		
HTTP Response Time				X	
ICMP All Errors		X	X		
ICMP Bad IP Header	X	z	z		

Table 26. Summary of Expert Features

X = present

z = does not exist as a unique counter, but is counted in other categories

<i>Counter, Symptom, or Application</i>	<i>Expert Symptom</i>	<i>Counter in Expert View</i>	<i>Expert Alarm</i>	<i>Application Response Time Alarm</i>	<i>Expert Threshold</i>
ICMP Destination Host Access Denied	X	z	z		
ICMP Destination Host Unknown	X	z	z		
ICMP Destination Network Access Denied	X	z	z		
ICMP Destination Network Unknown	X	z	z		
ICMP Destination Unreachable	X	X	X		
ICMP Fragment Reassembly Time Exceeded	X	z	z		
ICMP Fragmentation Needed [D/F set]	X	z	z		
ICMP Host Redirect	X	z	z		
ICMP Host Redirect for TOS	X	z	z		
ICMP Host Unreachable	X	z	z		
ICMP Host Unreachable for TOS	X	z	z		
ICMP Network Redirect	X	z	z		
ICMP Network Redirect for TOS	X	z	z		
ICMP Network Unreachable for TOS	X	z	z		
ICMP Parameter Problem	X	z	z		

Table 26. Summary of Expert Features

X = present

z = does not exist as a unique counter, but is counted in other categories

<i>Counter, Symptom, or Application</i>	<i>Expert Symptom</i>	<i>Counter in Expert View</i>	<i>Expert Alarm</i>	<i>Application Response Time Alarm</i>	<i>Expert Threshold</i>
ICMP Port Unreachable	X	z	z		
ICMP Protocol Unreachable	X	z	z		
ICMP Redirect	X	X	X		
ICMP Required IP Option Missing	X	z	z		
ICMP Source Quench	X	z	z		
ICMP Source Route Failed	X	z	z		
ICMP Time Exceeded	X	z	z		
ICMP Time to Live Exceeded	X	z	z		
Illegal MAC Source Address (Ethernet or Token Ring)	X	X	X		
Illegal Network Source Address	X	X	X		
IP Checksum Errors	X	X			
IP Time to Live Expiring	X	X	X		
ISL BPDU/CDP Packets		X	X		
ISL Illegal VLAN ID	X	X	X		
New MAC Stations			X		
Network Overload	X	X			X
NFS Response Time				X	
NFS Retransmissions	X	X	X		

Table 26. Summary of Expert Features

X = present

z = does not exist as a unique counter, but is counted in other categories

<i>Counter, Symptom, or Application</i>	<i>Expert Symptom</i>	<i>Counter in Expert View</i>	<i>Expert Alarm</i>	<i>Application Response Time Alarm</i>	<i>Expert Threshold</i>
NNTP Response Time				X	
Non Responsive Stations	X	X			X
OSPF Broadcasts		X	X		
Overload Frame Rate			X		
Overload Utilization Percentage			X		
Physical Errors	X	X			X
POP Response Time				X	
RIP Broadcasts		X	X		
SAP Broadcasts		X	X		
SMTP Response Time				X	
TCP/IP Long Ack	X	X			X
TCP/IP Retransmissions	X	X	X		
TCP/IP RST Packets		X	X		
TCP/IP SYN Attack	X	X	X		X
TCP/IP Window Frozen	X	X			X
TCP/IP Zero Window	X	X	X		
TELNET Response Time				X	
Total MAC Stations		X	X		
Total Router Broadcasts			X		
Unstable MST	X	X	X		X

11 Counters

Surveyor provides sophisticated counters to enable you to precisely monitor network activity. Surveyor features three types of counters at the MAC layer: Packet Counters, Custom Counters, and Error Counters. When the **MAC Statistics** window is in Capture mode, you can use all three types of counters. When the **MAC Statistics** window is in Transmit mode, custom counters are not relevant and do not appear in the **MAC Statistics** window.

Surveyor provides three types of MAC layer counters:

Packet Counters	Count the number and type of packets and bytes captured or transmitted by the Surveyor.
Custom Counters	User-defined counters that you can use to control data capture activities while the Surveyor is in capture mode.
Error Counters	Count the number of errors that occur while the Surveyor is capturing or transmitting data.
Expert Counters (Expert Only)	Count the number of Expert events discovered by Surveyor's expert logic.

Log files contain snapshots of Surveyor counter information. All byte, frame, and error counter values are recorded in the log file. Refer to the section on Logging for more information.

Packet Counters

Packet counters count the number of packets/bytes received or transmitted. Packet counters are viewed from the **MAC Statistics** window. The following packet counters are supported:

- Total Frames
- Broadcast Frames
- Multicast Frames
- Unicast Frames
- Error Frames
- Total Bytes Received

A breakdown of the total number of error frames is provided by the error counters.

Custom Counters

Custom counters are user-defined counters established in capture filters. When a certain condition in the filter is satisfied, counter 1, 2, or 3 can be incremented as a result of one of the actions taken by the capture filter. Custom counters are available in capture mode only.

Custom counters are incremented in the MAC Statistics view as packets are captured. By setting counters, you can visually see in the MAC Statistics view how many frames of a certain type have been captured.

Error Counters

Individual error counters do not necessarily add up to the total number of error frames. Single errors may be counted as two or three different types. For example a runt frame is also counted as a CRC error. Alignment errors are also counted as CRC errors. An RXERR is a physical layer error and will not show up in the total error count.

The following table contains an alphabetical list, with descriptions, of Surveyor's Ethernet error counters.

Table 27. Alphabetical List and Descriptions of Ethernet Error Counters

Collision	A counter that shows the best estimate of the total number of collisions (packets arriving at exactly the same time) on this Ethernet segment. Transmit collisions are not counted.
CRC/Align Error	A counter that shows the total number of packets received that had a length between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets (FCS/CRC Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Drop Events	A counter that shows the total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition was detected.
Fragments	A counter showing the total number of packets received that were less than 64 octets and had either an FCS/CRC error or an Alignment Error.
Jabbers	A counter that shows the total number of packets that were received that were longer than 1518 octets and had either an FCS/CRC error or an Alignment Error.
Oversize	A counter showing the total number of packets received that were longer than the 1518 octets and were otherwise well formed (good FCS).
Total Tx Collision	A counter showing the total number of collisions that have occurred when attempting to transmit.
Tx Attempt	A counter of the number of transmission attempts that have failed.
Tx Defer	A counter that shows the number of times the transmitter had transmit data available and was ready to transmit but had to defer transmission due to sensing other traffic.
Tx Excessive Collision	A counter that shows the number of times packets collided 16 times without successful transmission.
Tx Excessive Defer	A counter that shows the number of times the transmitter had to defer for greater than 3,036 byte times.

Table 27. Alphabetical List and Descriptions of Ethernet Error Counters

Tx Late Collision	A counter that shows the number of collisions that occur greater than 512 bit times after a transmission has started.
Undersize	A counter showing the total number of packets received that were less than 64 octets in length and were otherwise well-formed (good FCS).
Very Long Event	A counter that shows the number of times the transmitter is active for greater than a maximum event length. The maximum event length is 4ms to 7ms for 10Mbps network speeds and 0.4 to 0.75ms for 100Mbps network speeds.

The following table contains an alphabetical list, with descriptions, of Surveyor's Token Ring error counters.

Table 28 Alphabetical List and Descriptions of Token Ring Error Counters

Abort Delimiter	A counter that records events where a reporting Ring Station encounters recoverable internal errors, forcing it to transmit an Abort Delimiter frame.
AC Error	A counter that records events where the reporting Ring Station's nearest active upstream neighbor could not set the address recognized bits or frame copied bits in the newly transmitted frame after copying the bits on the last frame received.
Burst Error	A counter that records events where the reporting Ring Station encounters signal transition or signal error on the Token Ring physical medium
Frame Copy	A counter that records when a reporting Ring Station copies a frame containing the Ring Station's own (duplicate) address.
Frequency	A counter that records events where the reporting Ring Station attempts to receive a frame containing an improper ring-clock frequency.
Internal Error	A counter that records events where the reporting Ring Station encounters a recoverable internal error.
Line Error	A counter that records events where the reporting Ring Station's checksum process detects an error in a received data frame or token that the Ring Station transmitted.
Lost Frame	A counter that records events where a reporting Ring Station generates a frame to a specific address and does not receive the returned frame.
Token Error	A counter that records events where the Token Ring Active Monitor does not detect a ring token.

Expert Counters

Expert counters are only used if you have Surveyor's Expert plug-in. Expert counters count the number of Export events discovered by Surveyor's expert logic. Some counters are used in the Expert Alarm editor and some display in the Overview Table of Expert View. See the *Expert Systems* chapter for more information on expert counters.

The following table contains an alphabetical list, with descriptions, of Surveyor's expert counters.

Table 29. Alphabetical List and Descriptions of Expert Counters

Broadcast/Multicast Storms	A counter of all Broadcast/Multicast Storm events. The event occurs when a change in the number of total Broadcast/Multicast packets per second exceeds a threshold.
Duplicate Network Address	A counter of all duplicate network addresses over a period of time per segment.
Excessive ARP	A counter of all Excessive ARP events. The event occurs when a change in the number of ARP requests per second exceeds a threshold.
Excessive BOOTP	A counter of Excessive BOOTP events. The event occurs when a change in the number of Boot/Dhcp requests per second exceeds a threshold over a period of time per segment.
Excessive Broadcasts	A counter of the number of broadcast messages over a period of time per segment.
Excessive Collisions	A counter of the absolute number of collisions over a period of time per segment.
Excessive Multicasts	A counter of the number of multicast messages over a period of time per segment.
ICMP All Errors	A counter of all ICMP symptoms. This includes all destination unreachable errors, redirect errors, source quench, time-out errors, and parameter problems.

Table 29. Alphabetical List and Descriptions of Expert Counters

ICMP Destination Unreachable	A counter of all ICMP destination unreachable errors over a period of time per segment. Unreachable errors include Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed [D/F Set], Source Route Failed, Destination Network Unknown, Destination Host Unknown, Destination Network Access Denied, Destination Host Access Denied, Network Unreachable for TOS, and Host Unreachable for TOS.
ICMP Redirect	A counter of all ICMP redirect errors over a period of time per segment. Redirect errors include Network Redirect, Host Redirect, Network Redirect for TOS, and Host Redirect for TOS.
Illegal MAC Station Address	A counter of all illegal MAC station source addresses over a period of time per segment.
Illegal Network Source Address	A counter of all illegal network source addresses over a period of time per segment.
IP Checksum Errors	A counter of all incorrect IP checksums over a period of time per segment
IP Time to Live Expiring	A counter of all expiring connections over a period of time per segment.
ISL BPDU/CDP Packets	A counter of all Bridge Protocol Data Unit (BPDU) or Cisco Discovery Protocol (CDP) packets over a period of time per segment.
ISL Illegal VLAN ID	A counter of all ISL illegal VLAN IDs over a period of time per segment.
Network Overload	A counter of all instances where a threshold for the percentage change in network utilization is exceeded.
New MAC Stations	A counter of all the new MAC stations over a period of time per segment.
NFS Retransmissions	A counter of all NFS Retransmissions over a period of time per segment.
Non Responsive Stations	A counter of all Non Responsive Station events. A non-responsive station is defined as successive TCP/IP retransmissions over the same connection that are greater than a threshold value.
OSPF Broadcasts	A counter of all OSPF broadcasts over a period of time per segment.

Table 29. Alphabetical List and Descriptions of Expert Counters

Overload Frame Rate	A counter of frames over a one-second time period.
Overload Utilization Percentage	Counts bits over time and compares this value to the maximum utilization possible (bandwidth).
Physical Errors	A counter of all Physical Error events. The event occurs when a change in the number of total MAC physical errors per second exceeds a threshold.
RIP Broadcasts	A counter of all RIP broadcasts over a period of time per segment.
SAP Broadcasts	A counter of all SAP broadcasts over a period of time per segment.
TCP/IP Frozen Window	A counter of all TCP/IP Frozen Window events over a period of time per segment.
TCP/IP Long Acks	A counter of all TCP/IP Long Ack events over a period of time per segment.
TCP/IP Retransmissions	A counter of all TCP/IP Retransmissions over a period of time per segment.
TCP/IP RST Packets	A counter of all TCP/IP RST Packets over a period of time per segment.
TCP/IP SYN Attack	A counter of all TCP/IP SYN Attack events. The event occurs when a change in the number of SYN requests per second exceeds a threshold.
TCP/IP Zero Window	A counter of all TCP/IP Zero Window events over a period of time per segment.
Total MAC Stations	A counter of all the new MAC stations over a period of time per segment.
Total Router Broadcasts	A counter of all total router broadcasts over a period of time per segment.
Unstable MST	A counter of all excessive MST topology events. The event occurs when a change in the number of MST topology changes per second exceeds a threshold.

Counter Log File Overview

Counter log files contain snapshots of Surveyor counter information. All byte, frame, and error counter values are recorded in the log file. The time interval for capturing snapshots, the number of snapshots in the log file, and the creation of history files are set in the **System Settings** option of the **Configuration** menu.

For Surveyor, log files are maintained by module. A log file and a set of history files are created in a unique directory for each Century Media Module and each Ethernet Adapter. The directory for the module log is named

`..\Surveyor\log\local\module_n`. The module log file is named `module_n.csv` where `n` is the number of the module. The log directory structure starts from the installation directory for Surveyor.

For Surveyor in NDIS mode, log files are maintained by the Ethernet adapter (NDIS) running the Surveyor software. The directory for the NDIS log is named

`..\Surveyor\log\local\NDIS_n` and the NDIS log file is named `NDIS_n.csv` where `n` is the number of the adapter the NDIS driver detected.

The log files are text files in CSV format, a format easily imported into spreadsheet applications such as Microsoft Excel. Each line entry in the log file will create a separate row in the spreadsheet. Column titles for all counters are provided in the CSV text file. A template file for viewing counter information as graphs is provided. The template file works with Microsoft Excel™ Version 5.0 or greater.

See “Configuring Counter Logging” in the “Customizing Surveyor” chapter.

Log Directory Structure

The following is the directory structure for log files. The root directory is the installation directory for Surveyor, usually `c:\Surveyor`.

```
(root)\log\local\module_1 (directory for module 1)
  module_1.csv (log file for module 1)
  \history (history directory for module 1)
    mmdhmm.ss (first history file for module 1)
    mmdhmm.ss (second history file for module 1)
    mmdhmm.ss (third history file for module 1)
(root)\log\local\module_2 (directory for module 1)
  module_2.csv (log file for module 2)
  \history (history directory for module 2)
    mmdhmm.ss (first history file for module 2)
    mmdhmm.ss (second history file for module 2)
    mmdhmm.ss (third history file for module 2)
(root)\log\local\module_n (directory for module n)
  module_n.csv (log file for module n)
  \history (history directory for module n)
    mmdhmm.ss (first history file for module n)
    mmdhmm.ss (second history file for module n)
    mmdhmm.ss (third history file for module n)
(root)\log\local\NDIS_1 (directory for Ethernet Adaptor 1)
  NDIS_1.csv (log file for NDIS adapter)
  \history (history directory for NDIS adapter)
    mmdhmm.ss (first history file)
    mmdhmm.ss (second history file)
    mmdhmm.ss (third history file)
(root)\log\local\NDIS_n (directory for Ethernet Adaptor 'n')
  NDIS_n.csv (log file for NDIS adapter)
  \history (history directory for NDIS adapter)
    mmdhmm.ss (first history file)
    mmdhmm.ss (second history file)
    mmdhmm.ss (third history file)
```

12 Utilities

Surveyor includes the following utilities to enhance your ability to manage your Ethernet, Fast Ethernet, or Token Ring network:

Name Table Utility	Provides associations between symbolic names and network addresses.
NIS-to-Name-Table Utility	Converts an NIS name table on a UNIX system to Surveyor format.
Sniffer Translator Utility	Enables Surveyor and Sniffer systems to exchange captured data.
Get Version Information Utility	Provides information about Century Media Modules installed in your PC.
Identify-a-Module Utility	Verifies that the correct module is connected to the correct network or network segment.
Logging Utilities	Provides logging of counter, expert, and alarm information.
Export Utilities	Provides various means to export Surveyor data to different formats.

Name Table Utility

A name table provides associations between easy-to-remember symbolic names (Mickey) and hard-to-remember network addresses (0x78AB00004235).

Surveyor and Explorer learn names automatically by viewing the network portion of DNS, SAP, and NetBOIS packets. A default name table is supplied by Surveyor containing well-known name-to-address associations. You can change the default name table. A conversion utility (**NIS-to-Name-Table** utility) is available to convert existing name tables into the name table format used by Surveyor.

The name table contains three columns: Protocol, Name, Address. The 1st column contains the name of the Protocol that the address is associated. The 2nd contains a

name in the form of a character string that represents the address. The 3rd column contains the numeric address. Names can be associated with MAC, IP, IPX, or SNA addresses in a name table.

The Name Table dialog box initially displays the default name table. You can manually add, modify, or delete name table entries. You can also change the active name table so that Surveyor will use a different name table file. You can create many name tables, but only one table is active at a time.

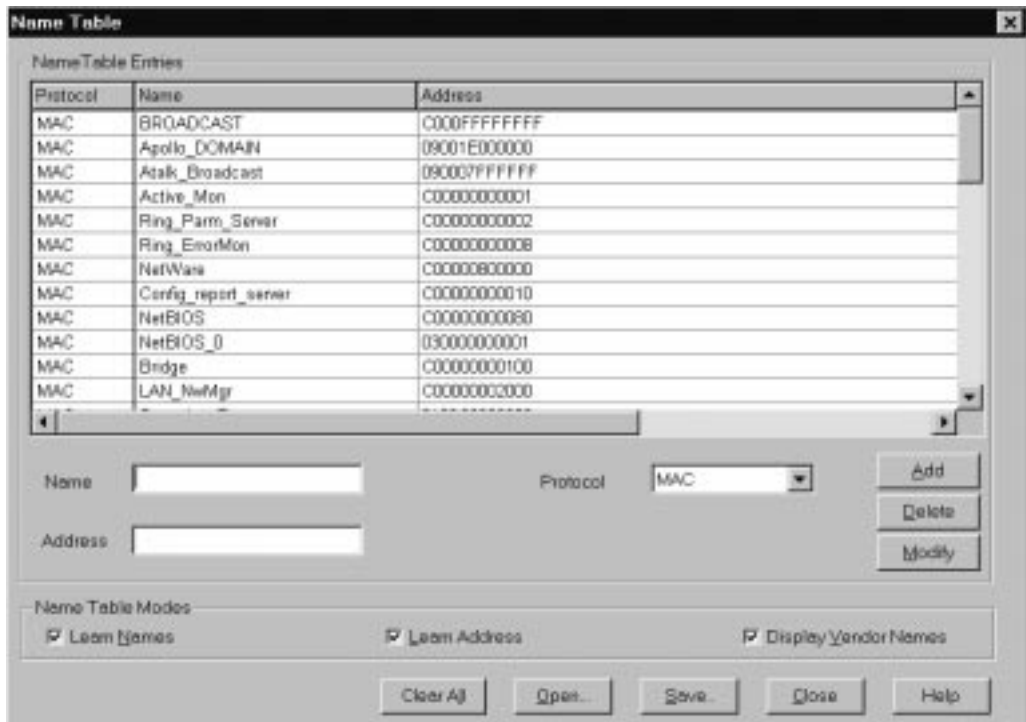


Figure 28. Example Name Table Dialog Box

You can also let Surveyor learn names and addresses automatically from the network for MAC, IP, IPX, or SNA protocols. You can have Surveyor record all new addresses in the name table, or only those that have a corresponding symbolic name. Surveyor can capture name-address associations in real-time monitoring mode as well as capture mode. New names are added to the name table in monitor mode as they are discovered in the data stream. You must save any changes to the currently active name table in a name table file or changes will be lost when you exit Surveyor.

To learn all addresses, select the **Learn Addresses** check box in the Name Table dialog box. Surveyor will enter all new addresses. If no symbolic name is associated with an address, the address is repeated in the name column for that entry in the name table.

To learn only addresses that have corresponding symbolic names, make sure the **Learn Names** check box is selected and the **Learn Addresses** check box is NOT selected in the Name Table dialog box. Surveyor will only add an item to the name table when it discovers a character string associated with an address from a DNS, SAP, or NetBOIS packet.

You can display the ASCII characters for well-known vendor names in the MAC address. Check the **Display Vendor Names** box to display vendor names. Vendor names will be displayed in the monitoring and capture views as well as in the name table.

Name table data is presented as a table which can be sorted by clicking the column headers. Click and drag on column dividers to size columns.

For remote resources, Surveyor uses names learned from remote as well as local resources when displaying capture or monitor views. A local copy of the remote name table is updated at a specified time interval. The time interval for refreshing the remote name table is set in the **Configuration** menu of Surveyor. If there are duplicate names between remote and local resources, local names take precedence and the name table will display the local name only.

The active name table can be loaded from a file. Loading the name table from a file will overwrite all existing entries in memory. Keep this in mind when using the network to learn names; until names are saved to a file, they can be lost if you exit Surveyor or overwrite the name table contents.

Entries in the currently active name table appear in a **Name Table** area that is within the dialog boxes for appropriate filter statements. The **Name Table** window shows all name and address associations, including the protocol and the frame type. Before starting to write a capture or display filter, make sure the name table you want is the currently active name table (loaded into memory). This ensures that the proper symbolic names are available.

To use the same name table information for all systems running Surveyor, you can set up a common default name table. All Surveyor users can configure the path and name of the default name table, which can be the same file stored on a server. See “Providing a Name Table to Surveyor” in Chapter 3 for more information.

Name table entries are limited to 1,024 entries.

Building a Name Table From the Network

The following provides a general outline of how to build a name table for the names in your network.

1. Run Surveyor in monitor mode. Do not use any filters. The **Learn Names** check box must be selected in the **Name Table** dialog box; if you also select the **Learn Addresses** option, Surveyor places any addresses it sees on the network into the name table as they are discovered in the data stream.
2. If you have names you want to associate with addresses learned from the network, edit the name table using the **Name Table** dialog box. This step can also be performed after the name table is saved.
3. Save the name table to a file. You must save the name table before you exit Surveyor or new name table data will be lost. If you save the name table data to the default name table, `hosts.nam`, the new name table data will be loaded automatically whenever you restart Surveyor. If you save the name table to a new file, use the `.nam` file extension for easy reference.

NIS-to-Name-Table Conversion Utility

The `NIS2NAM.SH` utility converts an NIS name table on a UNIX system to the name table format used by Surveyor. It provides a method of creating a Surveyor name table with addresses and associated symbolic names without having to re-enter information.

`NIS2NAM.SH` is installed in the `..\Shomiti\Surveyor\scripts` directory. It is a UNIX shell script, designed to run under a Bourne shell. To use the conversion utility, copy the `NIS2NAM.SH` file to a UNIX system as a text file. The UNIX system must have NIS running for the utility to produce the new name table for use with Surveyor.

To execute the command on the UNIX system, type:

```
NIS2NAM <output-name-table>
```

`<output-name-table>` is the name you select for the new Surveyor name table. The UNIX system is searched for the NIS name table. If no NIS name table exists, the utility returns an error message. Once the new name table is created, copy it as a text file to the `..\Shomiti\Surveyor` directory on your Windows system running Surveyor.

NOTE: *The name table automatically loaded by Surveyor is `hosts.nam`. If you use another name for your converted name table, you will need to load the name table before performing other Surveyor functions.*

The default name table loaded by Surveyor may be changed. Change the Name Table= parameter in the surveyor.ini file to set a new default name table file.

Sniffer™ Translator Utility

Translators convert captured data back and forth between Surveyor capture file format (.cap files) and Sniffer uncompressed trace format (.enc or .trc files). Capture files are stored in 'Snoop' format, compliant with RFC 1761. Capture files include extensions that provide additional information fields not found in RFC 1761. Start a translator by selecting one of the following from the **Tools** menu.

Snoop to Sniffer™	Converts Surveyor capture files to uncompressed trace files that can be viewed with the Sniffer.
Sniffer™ to Snoop	Converts uncompressed trace files (.enc or .trc format) to Surveyor capture files.

Get Version Information Utility

From Summary View, click on the **Description** tab for a resource. The following information displays:

- Base address for the module
- Revision level
- Module type
- Serial number for the module board
- Capture memory size
- Counters supported

Module Identification Utility (CMM Only)

You may want to verify that the correct Century Media Module is connected to the correct network or network segment. If you have multiple modules in a system, you can identify which is which. An LED next to the interface connections for the board will blink for the selected module.

1. From the Summary View, make sure that the resource you want to check is the currently active resource.

2. From the **Module** menu, choose **Identify**.
3. Look at the back of the system where modules are connected to the network. The LED for the selected module will blink.

Logging Utilities

Surveyor creates log files of counter, expert, and alarm information. Log file size, log file name, and disabling or enabling log files can be configured in Surveyor. To configure log files, see the “Configuring Surveyor” chapter.

To access counter log files, see the section called “Counter Log File Overview” in the “Counters” chapter. For information on exporting counter log file information to an Excel spreadsheet, see the section called “Export Counter Log Files to Excel” in the following section.


Export Utilities

Data from Surveyor can be exported to other formats. Use the procedures below to export packet information, counter data, graphs, and tables to other formats. Packet decodes can be exported to a text format. Tables or counter log files can be exported to CSV format. Graphics can be exported as bitmaps.

Exporting Packets

You can export packet decode information to another source. However, this cannot be done directly from the Capture View window. You must copy the data to an intermediate window.

To export packet decode information, do the following:

1. Set the summary pane of the Capture View window to display the protocol decode information you want to export. For example, packets numbered -0004 through 0013.
2. Select a packet within the window.
3. Press the  button. A window displays containing the protocol decode data that was visible in the summary pane of the Capture View window.
4. Select the data you want from the window and press Ctrl + C.
5. Switch to the application where you want to store the packet information.
6. Press Ctrl + V.
7. Click on a Surveyor window to return to Surveyor.

If you select a portion of the current packet within the detail decode of the packet, the entire decode for this single packet is moved to the copy window for export.

Exporting Tables to CSV Format or Graphs to a Bitmap

You can export tables to CSV format (Excel) or charts to BMP format (bitmapped graphic). When saving a chart to a bitmap, it is recommended that the display settings for your monitor be greater than 256 colors to create an image with accurate colors.

1. Select the view you want to export. Press one of view buttons on the Data Views or the Capture View toolbar. If you already have the desired view window open, click the window to make it the currently selected view.
2. Click the Table tab to export to CSV format or click the Chart tab to export to a bitmap.
3. Choose **Export...** from the **File** menu.
4. Enter the file name in the **Save As** dialog box. Table views will automatically be saved in CSV format and the file is given an extension of .csv. Chart views will automatically be saved in BMP format and the file is given an extension of .bmp.
5. Click the **Save** button.

Exporting to Optimal CSV Format

Optimal Performance, from Optimal Networks Inc., is a tool for planning, deploying, and troubleshooting distributed applications on large enterprise networks. Surveyor exports data into a special .csv file format that can be easily read by the Optimal Performance product. When saving a chart to a bitmap, it is recommended that the display settings for your monitor be greater than 256 colors to create an image with accurate colors.

Perform the following steps to export data to Optimal Performance format:

1. Select Application Layer Matrix from the Monitor View or Capture View menus.
2. Select the Table tab to view the data in tabular format.
3. Choose **View Options** from the **View** menu. Using the check boxes, select six additional columns to display:

Station Address 1

Station Address 2

Frames 2 --> 1

Frames 1 --> 2

Bytes 1 --> 2

Bytes 2 --> 1

4. Choose **Export to Optimal Performance** from the **File** menu.

5. Enter the file name in the **Save As** dialog box. Table views will automatically be saved in Optimal CSV format and the file is given an extension of `.csv`.
6. Click the **Save** button.

Surveyor logs both a start and stop time to the `.csv` file. The start time is the time the table/chart window is first opened and the stop time is the last time the file is exported or saved to disk.

Exporting Counter Log Files to Excel

Use these steps to view the counter data in the log files as Excel™ 5.0 graphics. The Excel template, `charts.xlt`, is located in the `..Shomiti\Surveyor\examples` directory.

1. Start Excel 5.0 and open `charts.xlt`. You should see an empty worksheet called "Data Sheet". Worksheets are named using tabs at the bottom of the Excel rows and columns.
2. Open the log file. Remember to set the **Files of Type** field in the **Open** dialog box, to `.csv` or to All Files (`*.*`) so you can see the log file.
3. Select the entire worksheet. Move the mouse to the small button at the top left corner of the worksheet. Click the button to highlight everything on the worksheet.
4. Use **Copy** from the **Edit** menu or `Ctrl + C` to copy the contents of the worksheet into the Windows clipboard.
5. Switch to the previously opened **Charts** window. To change windows, pull down the Windows menu and click on **Charts**.
6. Click cell **A1** of **Data Sheet** in the **Charts** window, the cell in the top-left corner of the worksheet.
7. Use **Paste** from the **Edit** menu or `Ctrl + V` to paste the data into the worksheet named **Data Sheet**.
8. Select one of the names on the bottom tabs to see a graph. Twelve graphs and one spreadsheet showing computed data are available. Select a graph by clicking on one of the tabs at the bottom of the spreadsheet.

The rows of counter data displayed in a graph are the most current rows. For example, when displaying 500 rows of counter information, only the 500 most recently captured sets of counter information are used in the graph. Three types of graphs are available, each with four different row counts.

- Network Utilization (500, 1,000, 2,000, or 4,000 rows)
- Bytes (500, 1,000, 2,000, or 4,000 rows)
- Packets (500, 1,000, 2,000, or 4,000 rows)

Refer to Excel documentation for more information on using templates in Microsoft Excel.

A Implementation Profile

Buffers

Two types of buffers are essential to the execution of Surveyor's features:

Real-Time Buffer

A real-time buffer provides the transient data storage area for on-the-fly frame analysis which, in conjunction with MAC statistics and error counters, produces real-time LAN analysis and monitoring information. Data captured from the network is copied to this area after filtering. The data is immediately available for evaluation, and for streaming copy to disk, after which it is discarded from the buffer.

Capture/Transmit Buffer

A separate capture buffer provides a durable data store of LAN traffic filtered and captured in real-time, which is kept for later analysis or to be saved to disk. The same buffer is used as storage for packets to be transmitted when performing LAN component testing.

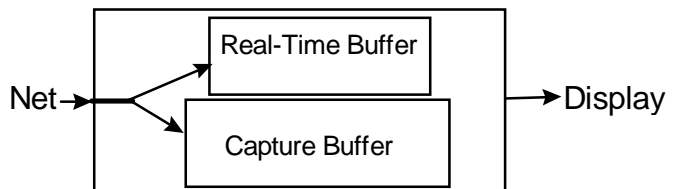


Figure 29. Surveyor and Interface

Surveyor supports CMM1, CMM2, and NDIS (10/100 Ethernet or Token Ring) LAN interfaces. Buffering is Implemented with these interfaces as follows. Cumulative system resource demands can limit

performance of any features which require system resources, as noted.

How Resources Use Buffers

Three primary device types use capture and real-time buffers:

NDIS

Surveyor NDIS supports up to four Ethernet adapters. The first Ethernet adapter found during system initialization is seen by Surveyor software as module #1, the second as module #2, and so on.

When Surveyor uses Ethernet adapter cards, both buffers are implemented in software, thus requiring system resources. To the extent that a system can keep up with traffic captured by an NDIS card, all LAN traffic will be copied to Surveyor and filtered, sliced if necessary, then routed to the capture buffer, real-time buffer, or both if desired. System resource demands increase with the complexity of analysis and monitoring configured, and very much by the number of NDIS interfaces Surveyor is controlling. All Surveyor real-time functions will be available, excluding any MAC error counters which are not implemented on the card.

CMM1

This is a high speed analyzer network interface card with on-board capture/transmit buffer and filtering. This, along with other hardware features, guarantees full line-speed capture and transmit for 10/100 Mbps Ethernets. Due to this on-board implementation, there is no demand for system resources, regardless of the number of cards being controlled. However, because CMM1 does not include a real-time buffer, the real-time functionality it provides is limited to network statistics and MAC error counters.

CMM2

Version 2 of Century Media Module adds an on-board real-time buffer and data slicing to provide full real-time functionality. Simultaneous data copies to the capture and real-time buffers are an option. Real-time functions introduce some system resource dependency: the need to copy periodic real-time monitor, analysis, and/or protocol decode updates to Surveyor, and optionally to copy the real-time buffer to disk. Using real-time functions on

multiple cards will increase resource demands, but much less than NDIS. All Surveyor features are supported on CMM2.

Voyager

Voyager is a multi-port RMON probe that gathers statistics. Data for all probe ports in the Voyager (version 1.1 and higher) device can be seen from Surveyor. Voyager can gather monitoring statistics at line rate and stores them in its local hardware.

For Voyager, Surveyor merely looks at the statistics passed from the probe; there is no use of a real-time or a capture buffer. Only those Surveyor real-time functions that can make use of the RMON statistics are available.

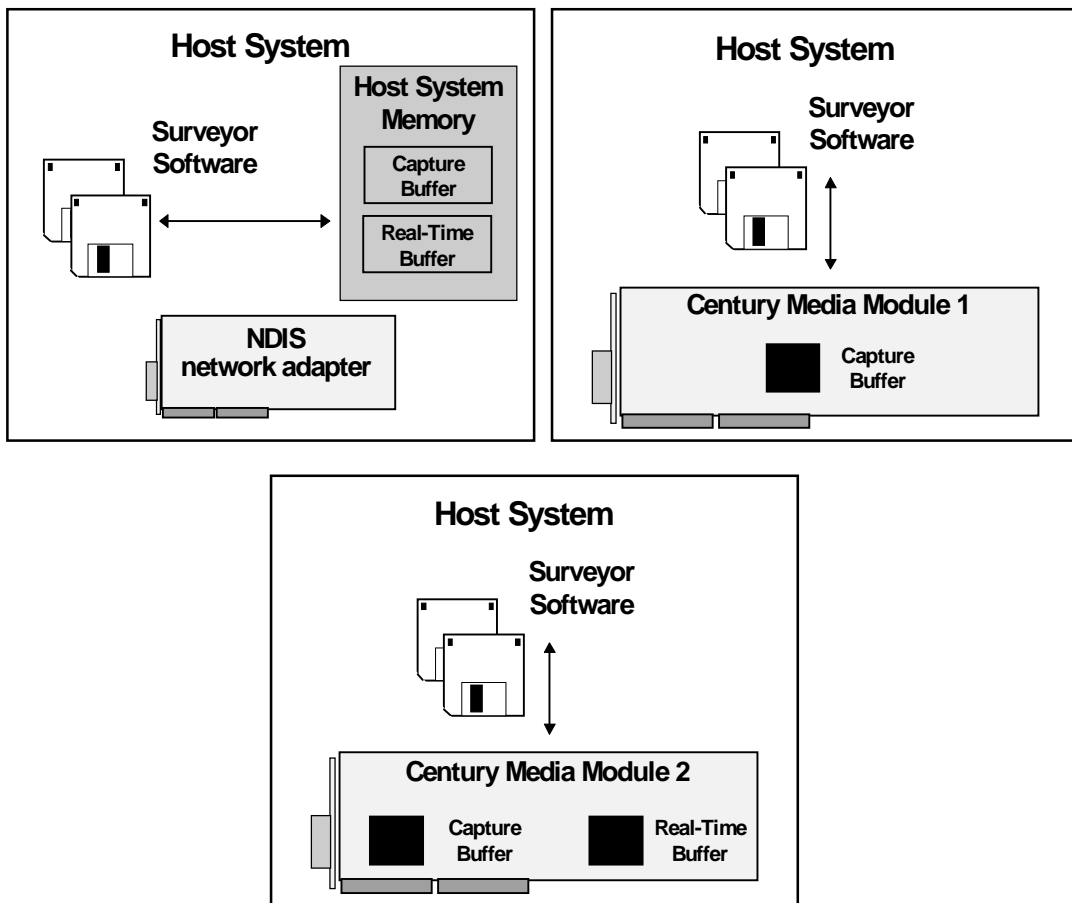


Figure 30. Surveyor Capture and Real-time Buffers

Hardware Dependencies

The tables that follow in this section list functions supported by Surveyor that have hardware dependencies.

Table 30. NDIS, CMM1 and CMM2 Real-Time Functions

<i>Real-Time Functions</i>	<i>NDIS</i>	<i>CMM1</i>	<i>CMM2</i>
Real-Time Buffer Size	64K	N/A	512K
Performance	10Mbps: 1-3Mbps 100Mbps: 1-5Mbps	N/A	10Mbps: 5-10Mbps 100Mbps: 5-20Mbps
Network Statistics	All but error rate	Utilization, error/s, packets/s, bytes/s	All
Packet Decode Summary	Yes	N/A	Yes
Alarm Thresholds	All except errors not passed by NDIS	Utilization, errors, packets, bytes, MAC error counters	All
One Screen Full-Duplex	No	No	Yes
Packet Slicing	Yes	No	Yes
Monitor Filter	Yes	N/A	Yes

Table 31. NDIS, CMM1 and CMM2 Capture Functions

<i>Capture Functions</i>	<i>NDIS</i>	<i>CMM1</i>	<i>CMM2</i>
Capture Buffer Size	64K-16M*	4M, 16M	4M,16M,32M,64M
Performance	10Mbps: 5-10Mbps 100Mbps: 5-15Mbps	Full Line Rate 10/100 Mbps	Full Line Rate 10 /100 Mbps
7-Layer Decode	Yes	Yes	Yes
One Screen Full-Duplex	No	No	Yes
Filter	Yes	Yes	Yes
Error Frame Capture	No	Yes	Yes
Post Capture Views	Yes	Yes	Yes
Frame Error Counter	adapter dependent	Yes	Yes

Table 32. NDIS, CMM1 and CMM2 Connectivity

Connectivity	NDIS	CMM1	CMM2
Media	10/100 Ethernet, 4/16 TR	10/100 Ethernet	10/100 Ethernet
Max Interfaces/System	4	8	16
On-Board Transceivers	10/100 Ethernet, 4/16 TR	10Mbps RJ45 10/100Mbps MII	10/100Mbps RJ45 10/100Mbps MII
Portability	Laptop	Dolch type portable	Shomiti Explorer
Remote Management	Yes	Yes	Yes
Max Interfaces/System	4	8	16

*Limited by available PC system memory. Smaller when running Windows NT.

Table 33. NDIS, CMM1 and CMM2 Transmit Functions

Transmit Functions	NDIS	CMM1	CMM2
Transmit Buffer	64K-16M*	4M, 16M	4M,16M,32M,64M
Performance	10Mbps: 5-10Mbps 100Mbps: 5-15Mbps	Full Line Rate 10 and 100 Mbps	Full Line Rate 10 and 100 Mbps
Intelligent Frame Edit	Yes	Yes	Yes
Transmit Frame Size	Protocol valid sizes	8 - 15,000 Bytes	8 - 15,000 Bytes
Transmit Captured Files & User-Generated Frames	Yes	Yes	Yes
Transmit Error Frames	No	Yes	Yes
Simultaneous Transmit and Receive	No	No	Yes

About NDIS Mode

Surveyor in NDIS mode uses an NDIS driver and interfaces to a variety of network adapters. All basic capture, transmit, and monitor functions are the same in NDIS mode. The unique capabilities in the software interface due to using an NDIS driver are described below:

Captured Packets

Since the NDIS interface filters out frames with errors, only “good” Ethernet frames are captured. In addition, Surveyor in NDIS mode captures both frames received by the Ethernet adapter as well as frames transmitted by the Ethernet adapter.

Capture Rate / Transmit Speed

Capture/transmit rates depend on the network adapter and the CPU. Typically, the rate will fall below the 100Mbps capability of Fast Ethernet.

Counters

The error counters supported through the NDIS interface are those counters supported by the network adapter. Some vendors do not support any error counters. Only supported error counters are incremented and shown within data views.

Transmit Specification

The minimum and maximum values for the **Packet Size** field are 64 and 1518 bytes. The radio button for setting the packet gap in microseconds is grayed. Packet gaps in microseconds are not supported.

Entering a zero in the **Packet Gap** field forces the shortest gap possible.

The **Interface** and **Interface Mode** options are grayed on the **Module** menu when an NDIS module is the currently selected module. The **Identify** option on the **Module** menu is grayed and does not function when the current module is an NDIS module.

NDIS Configuration Options

Set Capture Buffer and Packet Slicing Size

The capture buffer memory size can be set in increments that double from 64K to 16MB. To set the buffer size, select the **Buffer Size** tab from the **Configuration -> Module Settings** menu and click the radio button corresponding to the buffer size. Since the buffer uses virtual memory, the system is not required to have more physical memory than the buffer size (e.g., you can set the buffer size to 16MB on a machine with 8MB of memory).

B Standard Filter Elements

All filter elements and templates supplied with Surveyor are described below. Templates need to given a value and saved as a user-defined filter element before they can be used in a capture or display filter.

Table 34. Surveyor Filter Elements and Templates, Ethernet

<i>Filter Element</i>	<i>Description</i>	<i>Offset</i>	<i>Value</i>
CiscoISL	Filter element for collecting Cisco ISL frames.	0	01000C0000
DA=	Template for setting a destination address. Filters for addresses at the MAC level.	0	XXXXXXXXXXXX
DA_BROADCAST	Filter element to capture/display broadcast frames.	0	FFFFFFFFFFFF
DA_SNAP_IP=	Template for setting the IP destination address, when IP is embedded in an Ethernet SNAP frame.	14 39	AAAA03XXXXXX0800 255.255.255.1
DA_EV2_IP=	Template for setting the IP destination address when IP is embedded in a Ethernet Version II frame.	12 30	0800 255.255.255.1
ICMP	Filter element for collecting all PING activity.	12 23	0800 01
ICMP_Echo	Filter element for collecting all PING requests.	12 23 34	0800 01 08
ICMP_EchoReply	Filter element for collecting all PING replies.	12 23 34	0800 01 00

Table 34. Surveyor Filter Elements and Templates, Ethernet

<i>Filter Element</i>	<i>Description</i>	<i>Offset</i>	<i>Value</i>
LLC_DSAP	Template for setting the LLC destination address point.	14	XX
LLC_SSAP	Template for setting the LLC source address point, offset.	15	XX
MatchAll	Filter element to capture/display all frames.	N/A	None
Pkt Type	Template for setting the packet type.	12	XXXX
PktTypeEV2_AppleTalk	Filter element for collecting AppleTalk packet types embedded in Ethernet Version II frames.	12	809B
PktTypeEV2_ARP	Filter element for collecting ARP packet types embedded in Ethernet Version II frames.	12	0806
PktTypeEV2_IP	Filter element for collecting IP packet types embedded in Ethernet Version II frames.	12	0800
PktTypeEV2_IPX	Filter element for collecting IPX packet types embedded in Ethernet Version II frames.	12	8137
PktTypeNovell8022	Filter element for collecting Novell 802.2 packet types.	12	E0E003
PktTypeNovell8023	Filter element for collecting Novell 802.3 packet types.	12	XXXXFFFF
PktTypeSnap	Filter element for collecting SNAP frames.	14	AAAA03
PktTypeSnap_AppleTalk	Filter element for collecting AppleTalk packet types embedded in Ethernet SNAP frames.	14	AAAA03XXXXXXXX809B
PktTypeSnap_ARP	Filter element for collecting ARP packet types embedded in Ethernet SNAP frames.	14	AAAA03XXXXXXXX0806
PktTypeSnap_IP	Filter element for collecting IP packet types embedded in Ethernet SNAP frames.	14	AAAA03XXXXXXXX0800

Table 34. Surveyor Filter Elements and Templates, Ethernet

<i>Filter Element</i>	<i>Description</i>	<i>Offset</i>	<i>Value</i>
PktTypeSnap_IPX	Filter element for collecting IPX packet types embedded in Ethernet SNAP frames.	14	AAAA03XXXXXXXX8137
Port_TcpEv2_ECHO_Dest	Collect all frames with destination port ECHO when TCP is embedded in an Ethernet II frame.	12 23 36	0800 06 7
Port_TcpEv2_ECHO_Src	Collect all frames with source port ECHO when TCP is embedded in an Ethernet II frame.	12 23 34	0800 06 7
Port_TcpEv2_NNTP_Dest	Collect all frames with destination port NNTP when TCP is embedded in an Ethernet II frame.	12 23 36	0800 06 119
Port_TcpEv2_NNTP_Src	Collect all frames with source port NNTP when TCP is embedded in an Ethernet II frame.	12 23 34	0800 06 119
Port_TcpEv2_SMTP_Dest	Collect all frames with destination port SMTP when TCP is embedded in an Ethernet II frame.	12 23 36	0800 06 25
Port_TcpEv2_SMTP_Src	Collect all frames with source port SMTP when TCP is embedded in an Ethernet II frame.	12 23 34	0800 06 25
Port_TcpEv2_WWW-HTTP_Dest	Collect all frames with destination port WWW-HTTP when TCP is embedded in an Ethernet II frame.	12 23 36	0800 06 80
Port_TcpEv2_WWW-HTTP_Src	Collect all frames with source port WWW-HTTP when TCP is embedded in an Ethernet II frame.	12 23 34	0800 06 80
Port_UdpEv2_ECHO_Dest	Collect all frames with destination port ECHO when UDP is embedded in an Ethernet II frame.	12 23 36	0800 06 7

Table 34. Surveyor Filter Elements and Templates, Ethernet

<i>Filter Element</i>	<i>Description</i>	<i>Offset</i>	<i>Value</i>
Port_UdpEv2_ECHO_Src	Collect all frames with source port ECHO when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		34	7
Port_UdpEv2_FTP_Dest	Collect all frames with destination port FTP when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		36	21
Port_UdpEv2_FTP_Src	Collect all frames with source port FTP when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		34	21
Port_UdpEv2_NFS_Dest	Collect all frames with destination port NFS when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		36	2049
Port_UdpEv2_NFS_Src	Collect all frames with source port NFS when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		34	2049
Port_UdpEv2_RPC_Dest	Collect all frames with destination port RPC when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		36	111
Port_UdpEv2_RPC_Src	Collect all frames with source port RPC when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		34	111
Port_UdpEv2_SMTP_Dest	Collect all frames with destination port SMTP when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		36	25
Port_UdpEv2_SMTP_Src	Collect all frames with source port SMTP when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		34	25
Port_UdpEv2_SNMP_Dest	Collect all frames with destination port SNMP when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		36	161

Table 34. Surveyor Filter Elements and Templates, Ethernet

<i>Filter Element</i>	<i>Description</i>	<i>Offset</i>	<i>Value</i>
Port_UdpEv2_SNMP_Src	Collect all frames with source port SNMP when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		34	161
Port_UdpEv2_TELNET_Dest	Collect all frames with destination port TELNET when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		36	23
Port_UdpEv2_TELNET_Src	Collect all frames with source port TELNET when UDP is embedded in an Ethernet II frame.	12	0800
		23	06
		34	23
SA=	Template for setting a source address.	26	None
SA_ESNAP_IP	Template for setting the IP source address, when IP is embedded in an Ethernet SNAP frame.	14	AAAA030000000800
		35	255.255.255.1
SA_EV2_IP	Template for setting the IP source address when IP is embedded in a Ethernet Version II frame.	12	0800
		26	255.255.255.1

Table 35. Standard Filter Elements and Templates, Token Ring

Filter Element	Description	Offset	Value
TR_MAC_Active_Monitor_Present	Collect all Active Monitor Token Ring MAC frames.	117	0505
TR_MAC_Beacon	Collect all Beacon Token Ring MAC frames.	117	0202
TR_MAC_Change_Parameters	Collect all Change Parameters Token Ring MAC frames.	17	0C
TR_MAC_Claim-Token	Collect all "Claim Token" Token Ring MAC frames.	117	0303
TR_MAC_Duplicate_Address	Collect all Duplicate Address Token Ring MAC frames.	17	07
TR_MAC_Initialize_Ring_Station	Collect all Initialize Ring Station Token Ring MAC frames.	17	0D
TR_MAC_Lobe_Test	Collect all Lobe Test Token Ring MAC frames.	17	08
TR_MAC_Remove_Ring_Station	Collect all Remove Ring Station Token Ring MAC frames.	17	0B
TR_MAC_Report_Error	Collect all Report Error Token Ring MAC frames.	17	29
TR_MAC_Report_Monitor_Error	Collect all Report Monitor Error Token Ring MAC frames.	17	28
TR_MAC_Report_NAUM_Change	Collect all Report NAUM Change Token Ring MAC frames.	17	26
TR_MAC_Report_New_Active_Monitor	Collect all Report New Active Monitor Token Ring MAC frames.	17	25
TR_MAC_Poll_Error	Collect all Poll Error Token Ring MAC frames.	17	27
TR_MAC_Report_Ring_Station_Active	Collect all Report Ring Station Active Token Ring MAC frames.	17	22
TR_MAC_Report_Ring_Station_Attachments	Collect all Report Ring Station Attachments Token Ring MAC frames.	17	24
TR_MAC_Report_Ring_Station_State	Collect all Report Ring Station State Token Ring MAC frames.	17	23
TR_MAC_Report_Transmit_Forward	Collect all Report Transmit Forward Token Ring MAC frames.	17	2A
TR_MAC_Request_Initialization	Collect all Request Initialization Token Ring MAC frames.	17	20

Table 35. Standard Filter Elements and Templates, Token Ring

<i>Filter Element</i>	<i>Description</i>	<i>Offset</i>	<i>Value</i>
TR_MAC_Request_Ring_Station_Active	Collect all Request Ring Station Active Token Ring MAC frames.	17	0E
TR_MAC_Request_Ring_Station_Attachments	Collect all Request Ring Station Attachments Token Ring MAC frames.	17	10
TR_MAC_Request_Ring_Station_State	Collect all Request Ring Station State Token Ring MAC frames.	17	0F
TR_MAC_Response	Collect all Response Token Ring MAC frames.	17	00
TR_MAC_Ring_Purge	Collect all Ring Purge Token Ring MAC frames.	117	0404
TR_MAC_Standby_Monitor_Present	Collect all Standby Monitor Present Token Ring MAC frames.	117	0606
TR_MAC_Transmit_Forward	Collect all Transmit Forward Token Ring MAC frames.	17	09
TR_NON_MAC	Collect all non-MAC Token Ring frames.	1	40

C Keyboard Shortcuts

A list of all the keyboard shortcut is provided below:

Function Keys

Function keys perform different operations depending on the window they are used from.

Key	<i>Summary View</i>	<i>Detail View</i>
F1	Help	Help
F2	System Settings	Capture View Display Options
F3	Module Settings	Module Settings
F4	Module Monitor View Preferences	Create Display Filter
F5	Connect to Remote	Create Capture Filter
F6	Load Capture Filter	Load Capture Filter
F7	Open Capture File	Expert Summary View
F8	Save Capture	Save Capture
F9	Go to Detail View	Capture View
F10	Start/Stop	Start/Stop
F11	N/A	N/A
F12	N/A	N/A

From All Windows...

Alt + F4	Close Window
Ctrl + O	Open
Ctrl + S	Save

From Summary View...

Ctrl + T	Start Module
Ctrl + P	Stop Module
Ctrl + R	Go to Detail View

From Detail View...

Ctrl + T	Start Module
Ctrl + P	Stop Module

From Capture View Window...

Home	Select the first line
End	Select the last line
Page up	Scroll up one page
Page down	Scroll down one page
Up arrow	Select the preceding line
Down arrow	Select the next line
Right arrow	Move data in Summary pane one character to the right
Left arrow	Move data in Summary pane one character to the left

From the Capture Filter Window...

Ctrl + N	Bring up new default capture filter
Ctrl + P	Print capture filter
Home	Select the first statement
End	Select the last statement
Page up	Scroll up one page
Page down	Scroll down one page
Up arrow	Select the preceding statement
Down arrow	Select the next statement
Tab	Select next state
Shift + Tab	Select previous state
Plus	Expand state (Numeric pad only)

Asterisk (*)	Expand branch (Numeric pad only)
Minus (-)	Collapse branch (Numeric pad only)
Ctrl + Asterisk	Expand all branches (Numeric pad only)
Space	Bring up dialog box to edit statement
Double-click	Bring up dialog box to edit statement
Right mouse	List possible actions
Insert	<p>Add a statement or add a state.</p> <p>If a ROOT or ELSE statement is selected, add a state.</p> <p>If an IF statement is selected, add an ELSE IF statement before the ELSE statement.</p> <p>If an ELSE IF selected, add an ELSE IF statement after the currently selected statement.</p> <p>If a state is selected, add an IF statement; if an IF statement already exists for the state, add an ELSE IF statement.</p>
Delete	<p>Delete statement or state.</p> <p>If an ELSE IF selected, remove the statement.</p> <p>If a state is selected, remove the entire state.</p> <p>If any other statement is selected, Delete performs no action.</p>

D Protocol Information

A list of recommended references is provided below. Use these references to gather more information about protocols and network traffic analysis. For detailed information about any protocol we suggest you obtain the RFC (Request for Comment) for the protocol registered with ANSI (American National Standards Institute).

Protocol Reference Documentation

AppleTalk	Inside AppleTalk 2nd edition: Network Systems Development Apple Computer, Inc. by Gursharan S. Sidhu et al. Richard F. Andrews, Alan B. Oppenheimer.
ARP	RFC 826, An Ethernet address resolution protocol.
BGP	RFC 1267, BGP-3.
BootP	RFC 951, Bootstrap Protocol.
CTERM	Digital Terminal software Architecture, Network command Terminal, Version 1.4.
DAP	DECnet Digital Network Architecture - Data Access Protocol functional specifications, version 5.6.
DHCP	a)RFC 1541, Dynamic host configuration Protocol. b)RFC 1533, DHCP option and bootp vendor extensions. c)RFC 1340, Assigned numbers, (page 69- ARP parameters).
DNS	RFC 1035, Domain implementation and specifications.
EGP	RFC 904, Exterior Gateway Protocol formal specifications.
FOUND	Digital Terminal software Architecture, Foundation service specifications, Version 2.4.

FTP	RFC 959, File Transfer Protocol.
GGP	RFC 823, The DARPA internet gateway.
HTTP/1.1	Internet Draft:<Draft-ietf-http-v11-spec-00.txt>
IBM-NetBIOS	IBM LAN technical reference: IEEE 802.2 and NetBIOS application Program Interfaces, First Edition, December 1993.
ICMP	RFC 792, Internet Control Manager Protocol.
IEEE 802.1D	a)ISO/IEC 10038: 1993. b)ANSI/IEEE std 802.ID, 1993 edition.
IGMP	RFC 1112, Host extension for IP multicasting.
IGRP	Internetworking Technology Overview, Cisco Systems, Inc., 1993.
IP	RFC 791, Internet Protocol.
IPX	IPX Router specifications Ver 1.10.
IPX-RIP	IPX router specification, September 2, 1992 Revision A.
LPR	UNIX Network Programming by W.R.Stevens.
MIME	a) RFC 1341, MIME. b) RFC 822, Standard for the format of ARPA internet text messages.
MOP	DECnet Digital Network Architecture - Maintenance Operations functional specifications, version 3.0.0, September 1983.
MOUNT	RFC 1094, NFS Specifications.
NCP	RFC 1553, Compressing IPX header over WAN media (cpx).
NDS	Novell's Guide To Network LAN Analysis - 2nd edition (chapter 20).
NetWare	NetWare LAN Analysis. Laura Campbell, Novell Press, 1993.
NFS	RFC 1094, NFS specifications.
NICE	DECnet Digital Network Architecture - DNA Network Functional specifications, version 4.0.0, order No. AA-X437A-TK.
NLSP	IPX router specification part number 107-000029-001.
NNTP	RFC 977, Network News Transfer Protocol.
NSP	Digital Network Architecture, NSP, Functional Specifications, Phase IV, Version 4.0.1

NTP	RFC 958, Network Time Protocol.
OSPF	RFC 1583, OSPF Version 2.
Packet Burst Pro	Novell's Guide To Network LAN Analysis - 2nd edition (chapter 16).
PORT Mapper	RFC 1057, RPC specifications.
RARP	RFC 903, A reverse address resolution protocol.
RPC	UNIX Network Programming by W.R.Stevens.
rexec	UNIX Network Programming by W.R.Stevens.
RIP	RFC 1058, Routing Information Protocol.
rlogin	RFC 1282, BSD Rlogin.
RPC	RFC 1057, RPC specifications.
rsh	UNIX Network Programming by W.R.Stevens.
SAP	IPX router specification September 2, 1992 Revision A.
SMTP	RFC 821, Simple mail transfer protocol.
SNMP	RFC 1157, Simple network management protocol.
SPX	IPX Router specifications, Ver 1.10.
TCP	a) RFC 793 Transmission Control Protocol. b) DARPA Internet Program Protocol Specifications.
TCP/IP	Internetworking with TCP/IP, Volume 1. Douglas E. Comer, Prentice Hall, 1995.
Telnet	RFC 764, Telnet protocol specifications.
TFTP	RFC 1350, Trivial file transfer protocol.
UDP	RFC 768, User datagram Protocol.
X-Windows	RFC 1013, X-Windows Protocol.
Yellow Pages	Networking on the Sun Workstation, Sun Microsystems, Inc., Part NO:800-1324-03 rev B of 17 Feb 1986.

Protocol Display Colors

The table below lists the colors used to display protocols in Surveyor chart views.

Table 36 Colors Used to Display Protocols in Surveyor

<i>Protocol</i>	<i>Color</i>
IP	Orange Red
IPX	Dark Khaki
ARP	AQUA
RARP	Blue
NetBIOS	Green
DDP	Blanched Almond
AARP	Cornflower Blue
DRP	Cornsilk
Bootp	PURPLE
POP	Blue
FTP	Medium Turquoise
RIP	Papaya Whip
OSPF	Chocolate
SMTP	Yellow
XWindows	Tomato
HTTP	Red
Telnet	Cyan
DNS	Deep Pink
NFS	Dark Green
NNTP	DK_GREEN
NLSP	Dark Olive Green
NCP	GOLD
SAP	Maroon
SPX	Dark Orchid
SMB	Coral
MOP	Dark Sea Green
LAT	Dark Slate Blue
RSP	Gray50
ICMP	Magenta
SNMP	CRIMSON
GGP	Deep Sky Blue
EGP	Dodger Blue
IGRP	Firebrick
BGP	Floral White
NDS	Forest Green
Others	Gray75

E Parser Names

The Parser Names recognized by Surveyor are organized by protocol suite in the following tables. Parser Names must be spelled exactly as shown when used in the **Analysis.ini** file. See “Advanced Configuration” in the “Customizing Surveyor” chapter for information on using Parser Names.

Table 37. Parser Names, DLC Suite

<i>Parser Name</i>	<i>Protocol</i>
ETHERNETV2	Ethernet Version 2
IEEE8023	IEEE 802.3 (RAW)
IEEE8022	IEEE 802.2 (LLC - Logical Link Control)
IEEESNAP	IEEE Sub-Network Access Protocol
IEEE8025	IEEE 802.5 Token Ring (what about TR MAC and TR LLC)
FDDI	
LOOPBACK	IEEE 802.1d
IEEE8021P	IEEE 802.1p - Generic Attribute Registration Protocol (GARP)
IEEE8021Q	IEEE 802.1q - Virtual Bridged Local Area Networks Protocol

Table 38. Parser Names, Applications and Others

<i>Parser Name</i>	<i>Protocol</i>
CCMAIL	CC:Mail
NOTES	Lotus Notes
TDS	Sybase Tabular Data Stream
TNS	Oracle's Transparent Network Substrate Protocol
SMB	Server Message Block

Table 39. Parser Names, Apple Talk Suite

<i>Parser Name</i>	<i>Protocol Name</i>
AARP	AppleTalk Address Resolution Protocol
ADSP	AppleTalk Data Stream Protocol
AEP	AppleTalk Echo Protocol
AFP	AppleTalk Filing Protocol
ASP	AppleTalk Session Protocol
ATP	AppleTalk Transaction Protocol
AURP	AppleTalk Update-based Routing Protocol
DDP	Datagram Delivery Protocol
LAP	Link Access Protocol
NBP	Name Binding Protocol
PAP	Printer Access Protocol
RTMP	Routing Table Maintenance Protocol
ZIP	Zone Information Protocol

Table 40. Parser Names, Banyan Suite

<i>Parser Name</i>	<i>Protocol Name</i>
VARP	Vines Address Resolution Protocol
VFRP	Vines Fragmentation Protocol
VICP	Vines Internet Control Protocol
VIP	Vines Internet Protocol
VIPC	Vines Interprocess Communication Protocol
VNETRPC	Vines Network Remote Procedure Call
VRTP	Vines Routing Update Protocol
VSSP	Vines Sequenced Packet Protocol

Table 41. Parser Names, Cisco Suite

<i>Parser Name</i>	<i>Protocol Name</i>
CDP	Cisco Discovery Protocol
DISL	Dynamic Inter-Switch Protocol
HSRP	Hot Standby Router Protocol
ISL	Inter-Switch Link Protocol
VTPADVT	VLAN Trunk Protocol - Advertisement
VTPSTAT	VLAN Trunk Protocol - Status
IGRP	Interior Gateway Routing Protocol (see Internet Protocol suite)
EIGRP	Enhanced Interior Gateway Routing Protocol (see Internet Protocol suite)

Table 42. Parser Names, DECnet Suite

<i>Parser Name</i>	<i>Protocol Name</i>
CTERM	Network Command Terminal
DAP	Data Access Protocol
DRP	DECnet Routing Protocol
FOUND	Foundation Services
MOP	Maintenance Operation Protocol
NICE	Network Information and Command Exchange Protocol
NSP	Network Service Protocol

Table 43. Parser Names, Fujitsu Suite

<i>Parser Name</i>	<i>Protocol Name</i>
FNA	Fujitsu network Architecture
DAP	Local Network Flow Control

Table 44. Parser Names, IBM Suite

<i>Parser Name</i>	<i>Protocol Name</i>
3270	3270 Terminal
NETBEUI	NetBIOS Extended User Interface
SNA	Server Network Architecture
XID	

Table 45. Parser Names, Internet Suite

<i>Parser Name</i>	<i>Protocol Name</i>
ARP	Address Resolution Protocol
DVMRP	Distance Vector Multicast Routing Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
GGP	Gateway to Gateway Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
MOSPF	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
RARP	Reverse Address Resolution Protocol
RSVP	Resource Reservation Protocol
RTCP	Real Time Transport Control Protocol
RTP	Real Time Transport Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
FTP	File Transfer Protocol
GOPHER	Gopher
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IMAP	Internet Message Access Protocol
LDAP	Lightweight Directory Access Protocol
LPR	Printer (Need to added ProtoIDs support)
MIME	Multipurpose Internet Mail Extensions
MOUNT	NFS Mount
NBNAME	NetBIOS Name Service over IP

Table 45. Parser Names, Internet Suite

<i>Parser Name</i>	<i>Protocol Name</i>
NBDDATAGRAM	NetBIOS Datagram Service over IP
NBSESSION	NetBIOS Session Service over IP
NETCP	NetScout Control Protocol
NFS	Network File Server
NIS	Network Information Services
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
POP	Post Office Protocol
PORTMAP	Port Mapper
RADIUS	Remote Authentication Dial In User Service
REXEC	Remote Program Execution (FIX IN PROTOIDS and PDDTABLE)
RIP	Routing Information Protocol
RLOGIN	Remote Login
RSHELL	Remote Shell
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMPTRAP	Simple Network Management Protocol Trap
SUNRPC	Sun's Remote Procedure Call
TELNET	Remote Terminal Protocol
TFTP	Trivial File Transfer Protocol
XDMCP	X Display Manager Control Protocol
XWIN	X Windows

Table 46. Parser Names, Internet Next Generation Suite

<i>Parser Name</i>	<i>Protocol Name</i>
DNCPNG	Dynamic Host Configuration Protocol over IPng
ICMPNG	Internet Control Message Protocol over IPng
IDRPNG	Interdomain Routing Protocol over IPng
IPNG	Internet Protocol (Version 6) Next Generation
OSPFNG	Open Shortest Path First over IPng
RIPNG	Routing Information Protocol over IPng
RSVPNG	Resource Reservation Protocol over IPng

Table 47. Parser Names, Netware Suite

<i>Parser Name</i>	<i>Protocol Name</i>
IPX	Internet Packet Exchange
IPXBURST	IPX Packet Burst Mode
IPXDIAG	IPX Diagnostic Protocol
IPXNB	NetBIOS over IPX
IPXRIP	Routing Information Protocol over IPX
IPXWAN	Wide Area Network Protocol over IPX
NBCAST	Netware Broadcast Message Protocol
NCP	Netware Core Protocol
NDS	Netware Directory Services
NLSP	Netware Link State Protocol
NMPI	Name Management Protocol
SAP	Service Advertising Protocol
SERIAL	Serialization Protocol
SPX	Sequenced Packet Exchanged
SPX2	Sequenced Packet Exchanged Version 2 (use SPX)
WDOG	Netware Watch Dog Protocol

Table 48. Parser Names, PPP Suite

<i>Parser Name</i>	<i>Protocol Name</i>
PPPCAP	Challenge Handshake Authentication Protocol
PPPIPCP	IP Control Protocol
PPPIPCP	IPX Control Protocol
PPPLCP	Link Control Protocol
PPPNBFCP	NetBOIS Control Protocol

Table 49. Parser Names, XNS Suite

<i>Parser Name</i>	<i>Protocol Name</i>
IDP	Internetwork Datagram Protocol
PEP	Packet Exchange Protocol
SSP	Sequence Packet Protocol
XECHO	XNS Echo Protocol
XERROR	XNS Error Protocol
XRIP	XNS Routing Information Protocol

Glossary

.CAP extension	File extension for all capture files.
.CFD extension	File extension for all capture filters.
.DFD extension	File extension for all view filters.
.NAM extension	File extension for all name tables.
.TSP extension	File extension for all transmit specifications.
12-Tap	See “Century 12-Tap”
Abort Delimiter	A counter that records events where a reporting Ring Station encounters recoverable internal errors, forcing it to transmit an Abort Delimiter frame.
AC Error	A counter that records events where the reporting Ring Station’s nearest active upstream neighbor could not set the address recognized bits or frame copied bits in the newly transmitted frame after copying the bits on the last frame received.
Actions	Events that occur as the result of testing conditions within statements in a filter.
Activated Stream	A defined packet or set of packets that is included in a transmit specification. Activated streams are loaded to a module for transmission.
Address	A character or group of characters that identifies some other data source or destination.
Alarm	A message posted to Surveyor indicating a certain condition has occurred or a threshold has been reached.

Alarm Browser	A window used to list, select, and set alarms.
Alarm Falling Threshold	Falling threshold value to be compared to counter data. If the counter value or its delta value over time falls below the threshold, an alarm event is triggered.
Alarm Generation Type	Is this a rising, falling or “rising or falling” type of alarm. Used at the time of comparing the sampled value against a corresponding rising or falling threshold.
Alarm Interval	The interval, in seconds, over which data is sampled and compared.
Alarm Log	A list of all alarms triggered by incoming data to Surveyor.
Alarm Rising Threshold	Rising threshold value to be compared to counter data. If the counter value or its delta value over time raises above the threshold, an alarm event is triggered.
Alarm Sample Type	The type of the alarm, Delta or Absolute. Delta alarm types measure increases or decreases over time; absolute alarm types measure only the absolute value of a counter.
Alarm Setting	A set of conditions that when satisfied will cause Surveyor to record an entry in the alarm log.
Alarm Severity	Type of notification to be posted to the Message window upon alarm trigger. Valid types are informational, warning, and serious.
Alarm Value	The Alarm variable value from the last sample period.
Alignment Error Counter	A counter that shows the number of frames received or discarded with both framing errors and CRC errors.
Analysis Table	Table in Surveyor's Expert system that lists all expert symptoms discovered over time.
Application Response Time	The time required to establish a session with an application protocol, measured in milliseconds. Surveyor tracks average time, the shortest time, and the longest time required for connections to a protocol over the monitored network segment.
Base Address	The address of the Century Media Module or other resource within the PC system's low memory.
Burst	For transmission from Surveyor, a flood of frames sent at the maximum speed of the network.

Burst Error	A counter that records events where the reporting Ring Station encounters signal transition or signal error on the Token Ring physical medium
Burst Gap	For transmission from Surveyor, a pause between a set of packets sent at the maximum network speed and another set of packets sent at the maximum network speed.
Capture	The processing of receiving frames from the network and storing them in the Surveyor capture buffer.
Capture Buffer	The DRAM memory in Century Media Module (or system memory on a NDIS host) that stores packets captured from the network. The CMM2 buffer size can be 4MB, 16MB, 32MB, or 64MB depending on the Century Media Module model in use.
Capture File	File used to store frames captured from the network. A capture file must be given a name with an extension of .cap. Captured frames are not automatically stored in a file - the contents of the capture buffer must be saved using the Save or Save As options.
Capture Filter	A set of conditions that determine the frames to be captured and how the captured frames are counted. The capture filter consists of programming-like statements that set variables and specify conditions and actions for the capture of frames.
Capture Filter Window	A window for defining capture filters.
Capture Mode	The mode in which Surveyor receives network data and stores it in the Capture Buffer.
Capture View	A window for viewing and decoding network packets saved to a file or in the capture buffer.
Captured Frames	Frames stored within Surveyor's capture buffer.
Century Media Module 1	A hardware device available from Shomiti that allows the capture of network data at full line rate.
Century Media Module 2	A hardware device available from Shomiti that allows the capture of network data at full line rate and supports real-time monitoring functions.
Century 12-Tap	A fault-tolerant wiring device, available from Shomiti, that can be inserted into twelve, full-duplex or half-duplex, 10 or 100 Mbps Ethernet links. Century 12-Tap

	provides the ability to view up to twelve full-duplex segments from a single Surveyor installation.
(CMM1)	See "Century Media Module 1"
(CMM2)	See "Century Media Module 2"
CRC Errors	A counter that shows the number of frames received or discarded with Cyclical Redundancy Check (CRC) errors. The CRC error counter does not include framing errors.
DA	Destination address. MAC level station address of where a frame is sent.
Deactivated Stream	A defined packet or set of packets defined in a transmit specification but not currently active. Deactivated streams are NOT loaded to a module for transmission.
Defined Stream	In transmission mode, a sequence of bytes you specify for transmission on the network. Multiple streams can be defined for transmission.
Detail Pane	See Packet Detail Pane.
Detail View	The primary monitoring view for a single network resource. Multiple views of each resource can display in the Detail View.
Device	A single hardware device that provides data to Surveyor.
Display Filter Window	A window for defining display filters.
DRAM	Direct Random Access Memory.
Duplicate Network Address	An IP or IPX address that is discovered in packets that contain the same MAC address.
ELSE statement	The last statement for a level in a capture filter. If no combination of conditions in other statements for this level are met, the actions in the ELSE statement are taken.
ELSE IF statement	Statement in a capture or display filter. Always comes between an IF statement and an ELSE statement. Provides for the specification of additional conditions and actions for a state.
Expert Alarms	Messages posted to Surveyor indicating a certain condition has occurred or a threshold has been reached. Expert alarms are based on a set of counters related to

	Expert Symptoms or to other conditions that can signal a network problem.
Expert Diagnosis	Discussion of probable causes and possible solutions for Expert Symptoms detected by Surveyor.
Expert Symptom	A network condition that may indicate a network problem. Expert symptoms are detected by Surveyor's expert logic and logged in the Expert Analysis table.
Expert View	Surveyor data view showing expert symptoms and expert counters for a time period.
Explorer	A network troubleshooting and monitoring system available from Shomiti. Portable and rack mountable, Explorer is designed for field service and network operations personnel. Explorer can be accessed locally or remotely by Surveyor software and provides tools to diagnose, troubleshoot and monitor any full or half-duplex 10/100 Ethernet network.
Fast Ethernet	IEEE 802.3 compliant MII (Media Independent Interface) network. Capable of speeds up to 100 Mbps.
Frame	Sequence of contiguous bits bracketed by and including beginning and ending flag sequences. A recognizable sequence of bits within a data stream.
Frame Copy	A counter that records when a reporting Ring Station copies a frame containing the Ring Station's own (duplicate) address.
Frame Rate	The speed at which frames are received/transmitted on the network.
Frequency	A counter that records events where the reporting Ring Station attempts to receive a frame containing an improper ring-clock frequency.
Frozen Window	Condition where the TCP/IP window size remains the same for all packets over a time period.
Good Frames	Frames that pass all alignment and CRC checks are counted as good frames.
GoTo	In the Filter window, "GoTo" shows jumps to levels within the capture filter. Selecting a level other than the current level in the action portion of a statement dialog box creates a GoTo phrase in the Filter window. The object of the GoTo phrase is always a state in the filter.

Hex Pane	Portion of the Capture View window that displays the hex values of a packet stored in a capture file or capture buffer.
Host	A computer upon which a particular program or resource is located. In the context of Surveyor, the host is the computer upon which the Surveyor program is running.
IF Statement	First statement for a level in a filter. Specifies conditions and actions. Use the IF statement dialog box to create a condition filter comprised of filter elements and operators specify the actions to take if the condition filter is satisfied.
Internal Error	A counter that records events where the reporting Ring Station encounters a recoverable internal error.
Line Error	A counter that records events where the reporting Ring Station's checksum process detects an error in a received data frame or token that the Ring Station transmitted.
Link Speed	The maximum rate at which a device can transmit/ receive data on the network, typically described in bits/ second.
Local Host	A networked computer that is running the program or resource being described. In the context of Surveyor, a local host is the computer that is (1) running the Surveyor program under discussion and (2) located on a network where at least one other computer (remote host) is also running a copy of the Surveyor program.
Log Files	Files containing snapshots of Surveyor counter information.
Lost Frame	A counter that records events where a reporting Ring Station generates a frame to a specific address and does not receive the returned frame.
Message Window	A window that displays all alarm, log, and error messages received by Surveyor.
Mode of Operation	Defines the current relationship between Surveyor and a resource. Surveyor can transmit data from a resource (transmit), receive data from a resource (capture), view a resource (monitor), or view and receive data from a resource simultaneously (monitor + capture)

Module	A hardware device attached to the network that can be used by Surveyor software to perform LAN analysis and monitoring functions. Surveyor can use network interface cards and Century Media Modules as modules.
Module Speed	The rate at which Surveyor will capture/transmit packets on the network. The speed is either 10 or 100 Mbps.
Module Status	Indicates whether or not the module is actively capturing/transmitting frames. "Arm" indicates that the module is capturing/transmitting.
Module Type	Indicates the Century Media Module model. Currently, two models exist, CMM1 and CMM2.
Monitor	View activity on the network in real time.
Monitor and Capture Mode	Allows Surveyor to view and receive data from a resource simultaneously.
Monitor Mode	Allows Surveyor to view in real time the data coming to a resource.
Name Table	Table containing name and address associations for stations on the network. The address can be in the format of the MAC, IP, or IPX protocol.
NDIS	Network Driver Interface Specification.
Network	An interconnected group of nodes.
Network Adapter	Hardware board for connecting a station or node to an Ethernet LAN.
NIS	Name Information Service.
Overview Table	Table in Surveyor's Expert system that lists all counters for expert events discovered over time.
Packet	A sequence of digits including data and control signals that is switched as a composite whole. Data, control signals, and error control information are arranged in a specific format. For Surveyor, packet and frame are used interchangeably.
Packet Detail Pane	A portion of the Capture View window that displays the detailed breakdown of a packet that is stored in a capture file or capture buffer. Packets are broken down by protocol and field value within the protocol.

Packet Drop	A counter that shows the number of dropped packets when running in NDIS mode. This counter is always zero when using Century Media Modules and capturing packets at line rate.
Packet Editor	A dialog box available from Capture View for changing or creating packets.
Packet Gap	Time interval between packets. A packet gap can be specified when transmitting packets.
Packet Size	The size of a packet sent during transmission mode. Any packet size up to 15,000 bytes can be transmitted.
Packet Summary Pane	In Capture View, the top portion of the window that provides a summary view of all the captured packets.
Packet Summary View	Real-time protocol decode summary.
Packet Type	The type of packet sent in transmission mode. Packet types are IP, IPX, ARP, and AARP, or any other type specified by the user. It can also be the packet length field for 802.2 and SNAP frames.
Pause	Stop the continuous update of the data when viewing any resource.
Post Trigger Buffer Position	Percentage of the capture buffer used to store frames after the module is triggered.
Protocol	Set of rules, format, and timing governing the operation of functional units of a communications system.
Real-Time Buffer	Buffer used in Century Media Modules V2 to store data received from the network. This circular buffer is continuously updated and overwritten as information is received. The Real-Time buffer supports monitoring functions.
Remote Host	A remote, networked computer that is running the particular program or resource that is being described. In the context of Surveyor discussions, a remote host is a networked computer, other than the local Surveyor host, that is also running a copy of the Surveyor program.
Remote Server Protocol (RSP)	Remote Server Protocol is the Shomiti proprietary protocol based on TCP/IP to transfer data or commands for Surveyor between the local station and the remote host. You can encrypt packets passed back and forth

	between the local station and the remote host when using RSP to transfer data and commands.
Resource	Any source that provides data to Surveyor. This can be a Century Media Module, an Ethernet Adapter, multiple devices synchronized to provide a single data stream, or a data file.
Resource Browser	The resource browser is a single window through which you can access all local and remote resources available in the network.
Root Statement	The first statement in all capture filters. Specifies global variables and global values.
Runt Frame Counter	A counter that shows the number of short frames that have been received.
Rx Collision Counter	A counter that shows the number of collisions (packets arriving at exactly the same time) that have occurred. Transmit collisions are not counted.
Rx Overflow Counter	A counter that shows the number of times the receive FIFO queue overflowed for packets being received.
Rx Oversize Counter	A counter showing the number of frames received with greater than the 1518-byte maximum frame size.
RXERR Error Counter	A counter showing the number of times RXERR is asserted by the physical signaling portion of the media (100 Mbps).
SA Source address	MAC level station address of where a frame is coming from.
Short Rx Event Counter	A counter showing the number of frames received or discarded where the activity of receiving the frame took less than 74 bit times.
Start Sequence Number	A number assigned in the transmit specification that indicates where the transmission sequence starts. The number can be used at the receiving end to note the start of a sequence.
State	A symbolic label used as an address for a set of statements in a filter.
Stop Sequence Number	A number assigned in the transmit specification that indicates where the transmission sequence stops. The

	number can be used at the receiving end to note the end of a sequence.
Stream	A continuous sequence of data elements transmitted in a defined format.
Summary Pane	In Capture View, the top portion of the window that provides a summary of all the captured packets.
Summary View	The primary monitoring view for all network devices. One view of every device can display in the Summary View. This window has three docking windows; the Resource Browser window, the Alarm Browser window, the Summary View window, and the Message window.
Synchronized Resource	Multiple hardware devices logically joined to provide a single data source to Surveyor.
Token Error	A counter that records events where the Token Ring Active Monitor does not detect a token.
Total Tx Collision Counter	A counter showing the total number of collisions that have occurred when attempting to transmit.
Traffic	Transmitted and received frames or packets.
Traffic Rate	When transmitting from Surveyor, a percentage of the maximum capacity of the network to carry packets.
Transmit Mode	One of the modes for using Surveyor. In transmit mode, data streams loaded are transmitted on the network when the resource is started.
Transmit Specification	A definition of packets to be transmitted on the network by Surveyor.
Tx Attempt Counter	A counter of the number of transmission attempts that have failed.
Tx Defer Counter	A counter that shows the number of times the transmitter had transmit data available and was ready to transmit but had to defer transmission due to sensing other traffic.
Tx Excessive Collision Counter	A counter that shows the number of times packets collided 16 times without successful transmission.
Tx Excessive Defer Counter	A counter that shows the number of times the transmitter had to defer for greater than 3,036 byte times.

Tx Late Collision Counter	A counter that shows the number of collisions that occur greater than 512 bit times after a transmission has started.
View	Any one of many displays of network data provided by Surveyor.
Very Long Event Counter	A counter that shows the number of times the transmitter is active for greater than a maximum event length. The maximum event length is 4ms to 7ms for 10Mbps network speeds and 0.4 to 0.75ms for 100Mbps network speeds.
WKP	Abbreviation for well known port, a known port address on the network.
Zero Window	Condition where the TCP/IP window size remains zero for all packets over a time period

Index

Numerics

12-Tap (see, Century 12-Tap) 4-13

A

Abort Delimiter Counter 11-5

AC Error Counter 11-5

Access privileges 3-3

 super-user 3-3

activated 7-2

Activating capture filters 7-2

Activating display filters 7-2

Address Mapping View 6-29

Advanced mode 7-10

Alarm Browser 9-2

Alarm Browser window 9-2

Alarm editors 9-2

Alarm List 9-6

Alarm Log 9-6

Alarms 9-3

 absolute sample type 9-4

 actions 9-5

 E-mail 9-4

 Log 9-4

 Pager 9-4

 Restart 9-5

 Stop&Save 9-5

 alarm actions 4-12

 e-mail settings 4-12

 log file settings 4-12

 pager settings 4-12

 alarm actions overview 9-4

 alarm editor 9-3

 alarm groups 9-3, 9-6

 alarm thresholds 9-4

 delta sample type 9-4

 examples 9-7

 Frame Size 9-8

 MAC Errors 9-8

 Utilization 9-7

 Falling Value field 9-4

 hints and tips 9-7

 Interval field 9-4

 log file settings 4-12

 overview 9-1

 Packet Size example 9-7

 pager settings 4-12

 Rising Value field 9-4

 Sample Type field 9-4

 table of, 9-3

Alignment Error Counter 11-3

Analysis Table, Expert View 6-30

AND operator 7-10, 7-11

Application Layer Host Table View 6-19, 6-20

Application Layer Matrix View 6-23, 6-25, 6-26

Application Response Time Alarms 10-7

Application Response Time View 6-33

Auto CRC check box 8-4, 8-11

Auto-discovery 4-9

 default accounts 3-3

 remote resources 4-9, 5-2

Automatic diagnosis 10-1

B

- Base memory address 2-3
- bitmaps, exporting 12-7
- Bridge Protocol Data Unit (BPDU) 10-49
- Broadcast/Multicast Storms 10-54, 11-6
- Buffer size 4-5
- Burst Error Counter 11-5
- Burst timing 8-8
- Bursts 8-8
 - bursts example 8-8
 - example 8-8

C

- Capture + Monitor mode 5-5
- Capture + Transmit mode 5-5
- Capture buffer 4-6
 - Enable Full Buffer Auto Save box 4-6
 - Max File Size field 4-6
 - save-to-disk function 4-6
- Capture files
 - transmitting 8-12
- Capture filter
 - actions
 - Capture 7-6
 - Counter 7-6
 - Go To State 7-6
 - Trigger 7-6
 - filter definition example 7-14
- Capture filter rules 7-16
- Capture Filter toolbar 3-17
- Capture Filter window 7-12
- Capture mode 5-5
- capture name-address associations 12-2
- Capture View 6-8
 - buffer contents 3-8
 - capture file 3-9
 - data views supported 6-2
 - detail pane 6-8
 - hex pane 6-9
 - options 6-8
 - protocol decode
 - color coding 4-3
 - summary pane 6-8
 - toolbar 6-8
- Capture View toolbar 3-19
- Capture View window 6-8

- Capture/Transmit Buffer A-1
- Century 12-Tap 4-13, 5-7
 - configuring 4-13
 - setting the COM port 4-8, 4-13
- Century Media Module 1 (CMM1) 5-5
- Century Media Module 2 (CMM2) 5-5
- Chart views 4-2
 - configuring 4-2
 - creating a "bottom ten" chart 4-2
 - creating a "top ten" chart 4-2
- Cisco Discovery Protocol (CDP) 10-49
- CMM1 5-5, A-2
- CMM2 5-5, A-2
- Color coding protocols 4-3
- Condition lines 7-9
 - directions 7-9
 - frame types 7-9
 - protocols 7-9
- Configuring
 - alarm actions 4-12
 - counter logging 4-11
 - ports to scan 4-8
 - table views 4-3
- connection time, applications 6-33
- Counter log files 4-11
- Counter logging 4-11
 - create history files 4-11
 - enabling 4-11
 - example 4-11
- Counters 11-1
 - ARP Broadcasts 10-8
 - Broadcast/Multicast Storms 10-54
 - counter log file overview 11-5
 - Destination Unreachable 10-16
 - Duplicate Network Address 10-43
 - error counters
 - Ethernet, list of 11-3
 - Token Ring, list of 11-5
 - Excessive BOOTP 10-9
 - Excessive Broadcasts 10-55
 - Excessive Collisions 10-55
 - Excessive Multicasts 10-55
 - expert counters, list of 11-6
 - export Counter log file to Excel 12-8
 - history files 11-9
 - ICMP All Errors 10-10
 - ICMP Redirect 10-29
 - Illegal MAC Source Address 10-56

- Illegal Network Source Address 10-46
- IP Checksum Errors 10-47
- IP Time to Live Expiring 10-48
- ISL BPDUs/CDP Packets 10-49
- ISL Illegal VLAN ID 10-49
- MAC layer counters 11-1
 - Custom Counters 11-1
 - Error Counters 11-1
 - Packet Counters 11-1
- Network Overhead 10-52
- Network Overload 10-52
- NFS Retransmission 10-35
- Non Responsive Stations 10-36
- OSPF Broadcasts 10-51
- Overload Frame Rate 10-57
- Overload Utilization Percentage 10-57
- Physical Errors 10-58
- RIP Broadcasts 10-53
- SAP Broadcasts 10-53
- TCP/IP Long Ack 10-38
- TCP/IP Retransmissions 10-39
- TCP/IP RST Packets 10-40
- TCP/IP SYN Attack 10-41
- TCP/IP Window Frozen 10-37
- TCP/IP Zero Window 10-42
- total MACstations 10-59
- Total Router Broadcasts 10-53
- Unstable MST 10-50

- Counts, expert symptoms 10-2
- CSV format, exporting 12-7
- Custom counters 11-2
 - Counter#1 7-6, 7-10, 7-11
 - Counter#2 7-6
 - Counter#3 7-6

- Customer Support iv
- Customizing
 - chart views 4-2
 - views and windows 4-1

- Customizing Expert Diagnostic Information 10-7

D

Events

- ICMP Fragmentation Needed 10-18
- DA and SA fields 8-10
- DA field 8-4

- Data field 8-4

- Data views 6-1, 6-11

- Address Map View 6-29
 - Application Layer Host Table View 6-20
 - Application Layer Matrix View 6-26
 - Application Response Time View 6-33
 - Duplicate Address View 6-29
 - Expert View 6-30
 - Frame Size Distribution View 6-13
 - Host Matrix View 6-22
 - Host Table View 6-16
 - MAC Statistics View (Rx) 6-11
 - MAC Statistics View (Tx) 6-12
 - Network Layer Host Table View 6-17
 - Network Layer Matrix View 6-24
 - Packet Summary View 6-29
 - Protocol Distribution View 6-14
 - Utilization/Error view 6-16
 - VLAN View 6-28

- Data Views toolbar 3-15

- Defined Stream list box 8-10
 - changing fields 8-10

- Defined streams 8-3
 - buttons and fields 8-4
 - defining a stream 8-4
 - Using Templates 8-11

- Defined Streams list box 8-3, 8-4

- Detail button 3-7

- Detail View 3-6, 6-5
 - buttons 6-6
 - data views supported 6-2
 - Monitor + Capture mode 6-7

- Detail View toolbar 3-13

- Dhcp 10-9

- diagnostic information, customizing 10-7

- Display filter
 - actions

- GoTo State 7-6

- Display filter actions
 - display 7-6

- Display filter rules 7-16

- Display Filter toolbar 3-18

- display filter, activating 7-2

- Display timers 4-10

- allowable values 4-10

- Monitoring View, Local 4-10

- Display timers Monitoring View, remote 4-10

- display vendor names 12-3

Duplicate Address View 6-29
Duplicate Network Address 11-6
duplicate network addresses 10-43

E

Edit packets 8-9
 Decode View 6-11, 8-10
 Hex View 6-11, 8-10
Editing packets 6-10
Elements B-1
ELSE Dialog Box 7-7
ELSE IF dialog box 7-7
E-mail
 settings 4-12
Encryption 4-9
 Encrypt RSP Packets check box 4-9
Error counters 11-2, 11-6
Excessive ARP 10-8, 11-6
Excessive BOOTP 10-9, 11-6
Excessive Broadcasts 10-54, 10-55, 11-6
Excessive Collisions 10-55, 11-6
Excessive Multicasts 10-55, 11-6
Expert Alarm Table 10-6
Expert Alarms 10-6
Expert counters 11-6
Expert Events
 Broadcast/Multicast Storm 10-54
 Duplicate Network Address 10-43
 Excessive ARP 10-8
 Excessive BOOTP 10-9
 ICMP Bad IP Header 10-11
 ICMP Destination Host Access Denied 10-12
 ICMP Destination Host Unknown 10-13
 ICMP Destination Network Access Denied 10-14
 ICMP Destination Network Unknown 10-15
 ICMP Fragment Reassembly Time Exceeded 10-17
 ICMP Host Redirect 10-19
 ICMP Host Redirect for TOS 10-20
 ICMP Host Unreachable 10-21, 10-22
 ICMP Network Redirect 10-23
 ICMP Network Redirect for TOS 10-24
 ICMP Network Unreachable 10-25
 ICMP Parameter Problem 10-26
 ICMP Port Unreachable 10-27
 ICMP Protocol Unreachable 10-28
 ICMP Redirect 10-29
 ICMP Required IP Option Missing 10-30
 ICMP Source Quench 10-31
 ICMP Source Route Failed 10-32
 ICMP Time Exceeded 10-33
 ICMP Time to Live Exceeded 10-34
 Illegal MAC source addresses 10-56
 Illegal network source addresses 10-46
 IMCP Destination Unreachable 10-16
 IP Checksum Errors 10-47
 IP Time to Live Expiring 10-48
 ISL Illegal VLAN IDs 10-49
 Network Overload 10-52
 Non Responsive Station 10-36
 Physical Error 10-58
 TCP/IP Long Ack 10-38
 TCP/IP Retransmissions 10-39
 TCP/IP SYN Attack 10-41
 TCP/IP Window Frozen 10-37
 TCP/IP Zero Window 10-42
 Unstable MST 10-50
Expert log files 4-11
Expert logging 4-11
 enabling 4-12
Expert Overview 10-2
Expert Overview Detail Table 10-3
Expert Overview Host Summary screen 10-3
Expert Overview Table 10-61
Expert Overview table 10-1
Expert plug-in 2-2
Expert View 6-30
Expertmsg.ini 10-7
Explorer 4-14, 5-6
 Cold Boot option 4-15
 resetting 4-14
 updating 4-14
 Warm Boot option 4-15
Export counter log files to excel 12-8
Export utilities 12-6
Exporting Graphs 12-7
Exporting packets 12-6
Exporting tables 12-7
Exporting to Optimal CSV Format 12-7

F

Filter combinations 7-10
Filter elements 7-5

Filters

- actions 7-6
 - Advanced mode 7-10
 - Advanced mode example 7-14
 - combinations 7-11
 - creating 7-1
 - creating elements 7-10
 - dialog boxes 7-6
 - IF and ELSE IF 7-7
 - elements 7-5, B-1
 - examples 7-11
 - frame Types 7-4
 - hints and tips 7-16
 - masks 7-10
 - modes 7-8
 - Advanced mode 7-10
 - Quick mode 7-8
 - overview 7-1
 - Quick mode 7-8
 - rules 7-16
 - standard templates 7-5
 - statements 7-5
 - ELSE IF statement 7-5
 - ELSE statement 7-5
 - IF statement 7-5
 - states 7-4
 - structure described 7-3
 - templates B-1
- Frame Copy Counter 11-5
- Frame Size Distribution View 6-13
- Frame types 7-4
- Good Frames 7-4
 - Other Frames 7-4
 - Runt Frames 7-4
- Frequency Counter 11-5

G

- Get Version Information Utility 12-5

H

- Help System (on line) iv
- Hints and Tips 10-60
- History files 4-11
- Host Information, from Expert View 10-3
- Host Matrix View 6-21, 6-22

Host Table View 6-16

I

- ICMP All Errors 11-6
- ICMP Destination Unreachable 11-7
- ICMP Redirect 11-7
- ICMP Redirect Errors
 - Types of, 10-29
- IF and ELSE IF dialog box
 - Capture 7-6
 - Counter 7-6
 - Display 7-6
 - Go To State (display filter) 7-6
 - GoTo State 7-6
 - overview 7-7
 - Trigger 7-6
- IF dialog box 7-7
- IF statement
 - condition lines 7-9
- IF statement example
 - Advanced Mode 7-15
 - Quick mode 7-13
- Illegal MAC Source Addresses 10-56
- Illegal MAC Station Address 11-7
- Illegal Network Source Address 10-46, 11-7
- Installation 2-1
- Interface pop-up menu 3-3
- Internal Error Counter 11-5
- IP Checksum Errors 10-47, 11-7
- IP Time to Live Expiring 11-7
- ISL BPDU/CDP Packets 11-7
- ISL Illegal VLAN ID 11-7
- ISL Illegal VLAN IDs 10-49

K

- Keyboard shortcuts C-1

L

- Launching Surveyor 3-1
- learn addresses 12-3
- learn names 12-2
 - remote resources 12-3
- Line Error Counter 11-5
- Local resources 5-2

- Log file 4-12
 - directory structure 11-10
- Logging Utility 12-6
- Login accounts 3-3
- Login dialog box 3-2
- Lost Frame Counter 11-5

M

- MAC Statistics View (Rx) 6-11
- MAC Statistics View (Tx) 6-12
- MII Auto Negotiate 3-4
- MII Mode 3-4
- Modes 5-5
 - advanced 7-10
 - Capture 5-5
 - Capture + Monitor 5-5
 - Capture + Transmit 5-5
 - Monitor 5-5
 - stream 8-4
 - stream mode 8-7
 - Transmission 8-5
 - transmission 8-8
 - status controls 8-5
 - Transmit 5-5
- Module
 - buffer size 4-5
 - CMM1, CMM2 and NDIS settings 4-5
 - Detail View 6-5
 - identification 12-5
 - NDIS 5-5
 - default mode 5-6
 - numbering 5-1
 - setting buffer Size 4-5
 - supported counters 5-6
 - NDIS module numbering 5-5
 - selecting 3-3
 - selecting a port and speed 3-4
 - setting the monitoring view 4-2
 - settings 4-5
 - set-up 2-2
- Module Identification Utility 12-5
- Module menu 3-3, 3-4
- Module number 3-2
- Module ports 3-4
- Module Settings option 4-5
- Module toolbar (Summary View) 3-11
- Monitor + Capture mode 6-7

- Monitor views (see, data views) 6-11
- MST topology changes 10-50

N

- Name Table
 - change default name table 3-23
 - default name table 3-23
- Name table 5-1
 - building from the network 12-4
 - default 12-4
 - remote resources 12-3
 - save to a file 12-6
 - symbolic name vs. IP address 5-1
- Name Table Utility 12-1
- Name Table window 7-10
- name-to-address associations 12-1
- NDIS 5-5, A-2
- Network Layer Host Table View 6-17
 - station address 6-18
- Network Layer Matrix View 6-24
- Network Overload 11-7
- Network security (See, Encryption) 4-9
- New MAC Stations 11-7
- New MAC stations 10-57
- NFS Retransmissions 11-7
- NIS-to-Name-Table Conversion Utility 12-4
- Non Responsive Stations 10-36, 11-7
- NOT operator 7-10, 7-11

O

- Optimal CSV Format 12-7
- OR operator 7-10, 7-11
- OSPF Broadcasts 10-51, 11-7
- Overload Frame Rate 10-57, 11-8
- Overload Utilization Percentage 10-57, 11-8
- Overview Table, Expert View 6-31

P

- Packet Blaster plug-in 2-2, 5-5, 8-1
- Packet counters 11-2
- Packet Drop Counter 11-3
- Packet Editor 6-10
 - Auto CRC 6-10
 - Compute CRC 6-10

-
- Decode 6-10
 - editing in decode view 6-11
 - editing in Hex View 6-11
 - Set Size 6-10
 - Undo 6-10
 - Packet editor 8-9
 - Compute CRC button 8-9
 - Decode button 8-9
 - editing in Decode view 8-10
 - editing in Hex view 8-10
 - Undo button 8-9
 - Packet Size field 8-4, 8-11
 - Packet slicing 4-6
 - Packet Summary View 6-29, 6-30, 6-31, 6-32, 6-33
 - color coding 4-3
 - Packet Type 8-11
 - Packet Type field 8-4, 8-12
 - Packets
 - editing 6-10
 - Pager
 - settings 4-12
 - Physical Errors 11-8
 - Physical errors 10-58
 - Plug-ins
 - RAM requirements 2-2
 - Polling timers 4-10
 - allowable values 4-10
 - Conversation Matrix 4-10
 - Host Table 4-10
 - MAC layer counters 4-10
 - Network layer counters 4-10
 - Portable Surveyor 5-6
 - Ports 4-8
 - scanning 4-8
 - Scanning Ports tab 4-9
 - Post Trigger Buffer Position 7-7
 - Protocol Distribution View 6-14
 - Protocols
 - color coding 4-3
 - Default All button 4-3
 - Set Default button 4-3
 - list of supported protocols 1-3
 - reference documentation D-1
 - Q**
 - Quick mode 7-8
 - filter example 7-11
 - R**
 - Real-Time Buffer A-1
 - Refresh option 7-2
 - Remote communications
 - configuring 4-9
 - Remote plug-in 2-2, 3-1, 3-2, 5-2
 - Remote resources 5-2
 - auto-discovery 4-9, 5-2
 - Remote server protocol (see RSP) 4-9
 - Repeat Streams field 8-4
 - Repeating transmitted frames 8-6
 - Resource Browser 5-1
 - Resources 5-1
 - auto-discovery 4-9, 5-2
 - defined 6-6
 - disabling resource protection 5-4
 - privileges
 - Capture/Monitor 5-4
 - Full 5-4
 - monitor Only 5-4
 - Super User 5-4
 - protecting 5-4
 - remote vs. local 5-2
 - synchronization 5-7
 - RFC (request for comment) D-1
 - RIP Broadcasts 10-53, 11-8
 - ROOT dialog box
 - Counter#1 7-7
 - Post Trigger Buffer Position 7-7
 - Root dialog box 7-7
 - ROOT statement 7-3
 - Router Broadcasts 10-53
 - RSP 4-9
 - Time Out value 4-9
 - RST Responses 10-40
 - Runt Frame Counter 11-3
 - Rx Collision Counter 11-3
 - Rx Overflow Counter 11-3
 - Rx Oversize Counter 11-3

S

- SA field 8-4
- SAP Broadcasts 10-53, 11-8
- Scanning ports 3-2
- Scanning Ports tab 4-9
- Sequence numbers 8-4
- Sequence Numbers field 8-11
- Setting update timers 4-10
- Shomiti Customer Support iv
- Short Rx Event Counter 11-4
- Sniffer to Surveyor translation 12-5
- Sniffer Translator Utility 12-5
- Specifying transmit data 8-9
- Starting Surveyor 3-1
- State0 7-2
- STATE0 identifier 7-3
- Statements 7-5
- States 7-4
- Stream buttons 8-5
 - Add 8-5
 - Add File 8-5
 - Edit Data 8-5
 - Modify 8-5
- Stream contents 8-4
- Stream modes 8-7
 - Frame Rate 8-8
 - Packet Gap 8-8
 - Traffic Rate 8-8
- Stream size 8-4
- Streams
 - modes 8-7
 - modifying data 8-9
 - stream mode 8-4
- Summary View 6-2
 - Alarm Log tab 6-3
 - Alarms tab 6-3
 - changing views 6-3
 - data views supported 6-2
 - Description tab 6-3
 - getting one view of multiple resources 6-5
 - Monitor tab 6-3
 - monitoring views 6-5
 - orientation 3-5
 - Rx tab 6-3
 - selecting the monitoring view 6-5
 - setting the monitoring view 4-2
 - Tx tab 6-3
 - viewing multiple resources 6-3
 - window description 6-4
- Supported Applications Layer Applications
 - List of, 10-7
- Surveyor
 - accessing remote resources 2-3
 - configuring the interface 4-1
 - connectivity A-6
 - features overview 1-3
 - functions overview 1-2
 - installation 2-1
 - launching 3-1
 - navigation tips 3-5
 - starting 3-1
 - system requirements 2-1
 - CPU 2-1
 - disk Space 2-1
 - network adapters 2-1
 - RAM 2-1
 - system software 2-1
 - video display 2-1
 - system settings 4-8
 - tips for using the interface 3-10
 - uninstall previous versions 2-2
 - utilities 12-1
 - Get Version Information 12-1
 - Identify-a-Module 12-1
 - Logging 12-1
 - Name Table 12-1
 - NIS-to-Name-Table 12-1
 - Sniffer Translator 12-1
- Surveyor toolbar 3-11
- Surveyor.ini file 3-23
- Surveyor.nam 3-23
- Surveyor-to-Sniffer translation 12-5
- Synchronized resources 5-7
- System requirements 2-1
- System Settings dialog box 3-1
 - ports to scan 3-1

T

- Table views 4-3
- TCP/IP Frozen Window 11-8
- TCP/IP Long Ack 10-38
- TCP/IP Long Acks 11-8
- TCP/IP Retransmissions 11-8
- TCP/IP RST Packets 11-8

TCP/IP SYN Attack 10-41
TCP/IP SYN Packets 11-8
TCP/IP Window Frozen 10-37
TCP/IP Zero Window 11-8
Templates B-1
timestamp, Analysis Table 6-30
Token Error Counter 11-5
Toolbars
 Capture Filter toolbar 3-17
 Add button 3-17
 Create Filter button 3-17
 Cut button 3-17
 Disable Filter button 3-17
 Help button 3-18
 Load Filter button 3-17
 Open Filter button 3-17
 Print button 3-17
 Save Filter button 3-17
 Show/Hide Detail button 3-17
 Capture View toolbar 3-19
 Address Map View button 3-21
 Application Layer Host Table View button 3-21
 Application Layer Matrix View button 3-21
 Copy button 3-19
 Frame Size Distribution View button 3-20
 Go To Trigger button 3-20
 Host Matrix View button 3-21
 Host Table View button 3-20
 navigation buttons 3-20
 Network Layer Host Table View button 3-20
 Network Layer Matrix View button 3-21
 Open File button 3-19
 Print button 3-19
 Protocol Distribution View button 3-20
 Resume Load button 3-20
 Save File button 3-19
 Search Box 3-19
 Search button 3-19
 Stop Load button 3-20
 VLAN View button 3-21
 Data View toolbar
 Address Map View button 3-16
 Application Layer Host Table View button 3-16
 Application Layer Matrix View button 3-16
 Frame Size Distribution View button 3-15
 Host Matrix View button 3-16
 Host Table View Table button 3-15
 MAC Statistics View button 3-15
 Network Layer Host Table View button 3-15
 Network Layer Matrix View button 3-16
 Protocol Distribution View button 3-15
 Refresh button 3-16
 Utilization/Error View button (Rx) 3-15
 Utilization/Error View button (Tx) 3-15
 VLAN View button 3-16
 Data Views toolbar 3-15
 described 3-11
 Detail toolbar
 Save button 3-13
 Detail View toolbar 3-13
 Alarm List and Log button 3-14
 Capture Filter button 3-13
 Capture Mode button 3-13
 Capture View button 3-13
 Display Filter button 3-14
 Help button 3-14
 Load Filter button 3-14
 Monitor Mode button 3-13
 Name Table button 3-14
 Print button 3-13
 Start button 3-13
 Stop button 3-13
 Transmit from Buffer button 3-14
 Transmit Mode button 3-13
 Transmit Specification button 3-14
 Unload Filter button 3-14
 Display Filter toolbar 3-18
 Add button 3-18
 Create Filter button 3-18
 Cut button 3-18
 Help button 3-19
 Open Filter button 3-18
 Print button 3-18
 Save Filter button 3-18
 Show/Hide Detail button 3-18
 Turn OFF Filter button 3-19
 Turn ON Filter button 3-18
 Module toolbar

- Capture Mode button 3-12
 - Detail View button 3-12
 - Load Filter button 3-12
 - Monitor Mode button 3-12
 - Stop button 3-11
 - Transmit button 3-12
 - Transmit Mode button 3-12
 - Unload Filter button 3-12
 - Module toolbar (Summary View) 3-11
 - Surveyor Toolbar 3-11
 - Help button 3-11
 - Name Table button 3-11
 - Open File button 3-11
 - Print button 3-11
 - Save button 3-11
 - Surveyor toolbar
 - Start button 3-11
 - Total MAC Stations 11-8
 - Total MAC stations 10-59
 - Total Router Broadcasts 11-8
 - Total Tx Collision Counter 11-3
 - Transceivers 2-2, 3-4
 - Transmission
 - bursts 8-8
 - repeating frames 8-6
 - status 8-5, 8-9
 - transmitting capture files 8-12
 - Transmission mode
 - status controls 8-5
 - Transmission modes 8-5, 8-8
 - Transmit Continuously 8-8
 - Transmit Spec (N frames) 8-9
 - Transmission status 8-9
 - Transmit
 - repeat frames 8-6
 - Bursts 8-6
 - example 8-7
 - Repeat Streams 8-6
 - Transmission Mode 8-6
 - Transmit mode 5-5
 - Transmit Specification 8-1
 - control buttons 8-5
 - Cancel 8-6
 - Load Module 8-6
 - Open Specs 8-6
 - Save Specs 8-6
 - Template 8-6
 - dialog box 8-2
 - dialog box example 8-3
 - examples 8-12
 - Bursts 8-14
 - Packet Gaps 8-12
 - Hints and Tips 8-15
 - sequence numbers 8-4
 - Transmit Specification dialog box
 - Auto CRC Check Box 8-11
 - DA and SA fields 8-10
 - Data field 8-11
 - Packet Size 8-11
 - Packet Type 8-11
 - Sequence Numbers 8-11
 - specifying transmit data 8-9
 - transmission status 8-9
 - Transmitting capture files 8-12
 - Tx Attempt Counter 11-3
 - Tx Defer Counter 11-3
 - Tx Excessive Collision Counter 11-3
 - Tx Excessive Defer Counter 11-3
 - Tx Late Collision Counter 11-4
- ## U
- Unstable MST 10-50, 11-8
 - Update timers
 - polling and display 4-10
 - setting 4-10
 - User privileges 5-4
 - Capture/Monitor 5-4
 - Full 5-4
 - Monitor Only 5-4
 - Super User 5-4
 - Utilities
 - list of 12-1
 - Utilization/Error View 6-16
- ## V
- vendor names 12-3
 - Very Long Event Counter 11-4
 - Views 6-1, 6-8
 - configuring table views 4-3
 - customizing 4-1
 - Hints and Tips 6-33
 - VLAN View 6-28
 - Voyager 5-6

Setting ports 4-15

W

Windows

- customizing 4-1

- docking 4-1

- extracting docking windows 4-2

- resizing docking windows 4-1

X

X offsets (wildcard) 8-10

