ClearSight Analyzer 7.0.7

User Guide



Document Version 1.00

IMPORTANT – READ CAREFULLY
END USER SOFTWARE LICENSE AGREEMENT (“Agreement”)

This Agreement is legally binding between you and ClearSight Networks, Inc. (“ClearSight”) and concerns your use of the ClearSight Software Product (“Software”) you are about to install on this computer. For purposes of this Agreement, the words “you” and “your” shall apply equally to the individual end user and his/her organization. Unless your organization has a separate written end user software license agreement relating to the Software, the following terms shall at all times and govern your use of the Software.

License Grant

ClearSight grants to you a license to use one copy of the Software on one computer. The word “use” means storing, loading, installing, executing or displaying the Software. You may not modify the Software or disable any licensing or control features of the Software. If the Software is licensed for “concurrent use”, you may install the Software on a shared server, but you may not allow more than the maximum number of authorized users to Use the Software concurrently. By entering into this Agreement, you represent to ClearSight that you are of legal age to do so.

Ownership

This Software is exclusively owned and copyrighted by ClearSight or its third party suppliers. Your license to use the Software confers no title or ownership in the Software nor is a sale of any rights in the Software. ClearSight's third party suppliers may individually protect their rights in the event of any violation of this Agreement.

Copies and Adaptations

You may make copies or adaptations of this Software only for archival purposes or when copying or adaptation is an essential step in the authorized Use of the Software. You must reproduce all copyright notices in/on the original Software on all copies or adaptations. You may not copy the Software onto any internal or external bulletin board or similar system. You may not copy any written materials or documentation without ClearSight's prior written permission.

No disassembly, decompilation, or decryption allowed, permitted or authorized.

You are licensed to use the Software's machine executable object code only. You may not disassemble or decompile the Software or any portion thereof in any manner whatsoever. You may not decrypt the Software unless decryption is a necessary part of the operation of the Software. If you have any knowledge of any other party's attempted disassembly, decompilation, or decryption of the Software, you agree promptly to provide ClearSight with all information you may possess regarding such activity.

Legal Use Only

You are expressly prohibited from any illegal use of this Software or from any use that promotes any illegal activity It is your sole responsibility to understand and obey all local, state, provincial, and/or federal laws that may apply to your use of this Software. ClearSight expressly disclaims any responsibility and liability for any wrongful or unlawful acts you may commit while using this Software. You agree to indemnify ClearSight for all claims, actions, legal fees, and/or court costs that may be brought against ClearSight as a result of your illegal use of this Software.

Transfer

Your license to use this Software will automatically terminate upon any legal transfer of this license to any other entity. Upon transfer, you must deliver the Software, including any copies and related documentation, to the transferee. The transferee must accept these License Terms as a condition to the transfer.

Termination

ClearSight may terminate your license immediately upon notice for failure to comply with any of these License Terms. Upon termination, you must immediately destroy the Software, together with all copies, adaptations and merged portions in any form.

Export Requirements

You may not export or re-export the Software or any copy or adaptation in violation of any applicable laws or regulations.

U.S. Government Restricted Rights

The Software and documentation have been developed entirely at private expense and are provided as “Commercial Computer Software” or “restricted computer software”. They are delivered and licensed as “commercial computer software” as defined in DFARS 252.227-7013 (Oct 1988), DFARS 252.211-7015 (May 1991) or DFARS 252.227-7014 (Jun 1995), as a “commercial item” as defined in FAR 2.101 (a), or as “Restricted computer software” as defined in FAR 52.227-19 (Jun 1987) (or any equivalent agency regulation or contract clause), whichever is applicable. U.S. Government users have only those rights provided for such Software and Documentation by the applicable FAR or DFARS clause or by this ClearSight standard software agreement for the product. This software was developed strictly through private funding.

Third Party Software

Any third-party software provided to you by ClearSight is provided for your convenience. It is not licensed to you under this license agreement and is not subject to any warranties contained herein. Your use of any such third-party software is governed by the third-party license agreement provided to you with such software.

ClearSight SOFTWARE WARRANTY STATEMENT

1. ClearSight SOFTWARE IS PROVIDED TO YOU “AS IS” WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, WHETHER ORAL OR WRITTEN, EXPRESS OR IMPLIED. ClearSight SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, ERROR FREE OR UNINTERUPPTED OPERATION, OR FITNESS FOR A PARTICULAR PURPOSE

2. ClearSight WARRANTS THAT ALL SOFTWARE WILL BE DELIVERED ON MEDIA THAT IS FREE FROM DEFECTS IN MATERIAL AND WORKMANSHIP, WHEN PROPERLY INSTALLED AND USED. IF ClearSight RECEIVES NOTICE OF ANY SUCH DEFECTS DURING THE FIRST THIRTY DAYS AFTER PURCHASE, ClearSight WILL REPLACE THE DEFECTIVE MEDIA AT NO CHARGE.

3. THE REMEDIES LISTED IN THIS WARRANTY STATEMENT ARE YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM YOU MAY MAKE UNDER THIS AGREEMENT. ClearSight'S LIABILITY FOR ANY LOSSES AND DAMAGES TO YOUR ORGANIZATION RESULTING FROM ANY CAUSE WHATSOEVER INCLUDING ClearSight'S NEGLIGENCE, ALLEGED DAMAGED OR DEFECTIVE GOODS, IRRESPECTIVE OF WHETHER SUCH DEFECTS ARE DISCOVERABLE OR LATENT, SHALL IN NO EVENT EXCEED THE UNIT LICENSE PRICE OF THE PARTICULAR SOFTWARE PRODUCT FOR WHICH LOSSES OR DAMAGES ARE CLAIMED, OR, AT THE ELECTION OF ClearSight, THE REPAIR OR REPLACEMENT OF DEFECTIVE OR DAMAGED GOODS. IN NO EVENT WHATSOEVER, INCLUDING THE CASE OF A CLAIM OF NEGLIGENCE, WILL ClearSight BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT), OR OTHER DAMAGES, WHETHER BASED IN CONTRACT, TORT, OR OTHERWISE.

THIS AGREEMENT IS HEREBY DEEMED TO HAVE BEEN ENTERED INTO BY THE PARTIES IN THE STATE OF CALIFORNIA, USA, AND SHALL BE GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA, USA.

Warning

Some parts of this product use Application Content Viewers in order to display the nature of the monitored network application. As these viewers are designed to display application data in the same way that the end user's viewer would, they are also potentially subject to all of the same theoretical vulnerabilities of the viewing application. As such, there is a potential risk that viewing application content infected by a virus may in turn infect the analyzer device. Although we have gone through extensive measures to prevent such a circumstance, the nature of the content viewer's goal of displaying an end user's experience makes this a theoretic possibility. Please take alternate measures to identify and prevent virus transmission on your analyzer device in order to prevent unintentional virus transmission.

Third Party Software Acknowledgement and Copyright Notices

ClearSight Networks, Inc. acknowledges the use of various third-party software products that are either used in the development of the ClearSight products, incorporated within the ClearSight products, or distributed with the Clearsight products. Detailed descriptions of the licenses involved can be found at:

http://www.clearsightnet.com/eula/third_party/CSA.html

Trademarks

Wireshark is a registered trademark of Gerald Combs.

The following trademarks are the property of ClearSight Networks:

ClearSight Networks™ VQFactor™ VRFactor™

Document Revision History

Revision	Location	Description
1.00 (10/23/09)		Initial Release

Contents

About This Guide 17
About Standalone and Distributed Features 18
Audience of this Guide 18
How this Guide is Organized 18
Conventions Used in this Guide 21
Indicators Used in this Guide 22
Customer Service 23
Contacting Technical Support 23
Other Departments 24

Chapter 1 Installing ClearSight 25
ClearSight System Requirements 25
Before Installing ClearSight 34
Installing ClearSight Analyzer Standalone 34
Installing on Windows XP 34
Installing on Windows Vista 36
Installing ClearSight Distributed 38
Installing on Windows XP 38
Installing on Windows Vista 40
Licensing ClearSight Standalone 44
Using the Trial Version to Request a License 44

Activating the Standard Version 45
Licensing ClearSight Distributed 47
Uninstalling ClearSight Standalone 49
Uninstalling ClearSight Distributed 50

Chapter 2 Connecting the ClearSight Analyzer to the Network . . . 51
Analyzer Placement Fundamentals 52
Inserting a Hub 53
Inserting a Tap 55
Using Port Mirroring 57
Connecting ClearSight Distributed Agents 59
Setting Up an Agent with Two Interface Cards 60
Example — Using Two Interface Cards 61
Summary 62

Chapter 3 Introducing the ClearSight Analyzer 63
ClearSight Features 64
New in CSA 7.0.7 65
Available Models 65
Basic Setup for ClearSight Standalone 66
Setting Up a User List on the Standalone Analyzer 66
Starting ClearSight Analyzer Standalone 71
ClearSight User Interface 72
ClearSight Toolbar 74
How to Use ClearSight 76
Real-Time Monitoring 78
Packet Capture 79
Postcapture Analysis 79

Chapter 4 Using ClearSight Distributed 83
The ClearSight Distributed System 83
About ClearSight Distributed Communications 86
Getting Started with ClearSight Distributed 86
Setting Up a User List on an Agent 87
Using the Agent Manager 91
Managing Distributed Agents in the Agent Manager 93
Adding Agents to the Agents List 93

Editing an Agent in the Agents List 96
Removing Agents from the Agents List 97
Connecting to Agents in the Agents List 97
Disconnecting a Connected Agent 98
Rebooting Agents in the Agents List 99
Updating the Software on an Agent 99
Starting and Stopping Capture 99
Saving an Agent's Capture Buffer to a Trace File 100
Using the Central Problem Manager 101
Fields in the Central Problem Manager 103
Configuring Agents to Report Problems 104
Copying Configuration Data 105
Other CSD-Specific Features 107
Secure Socket Layer (SSL) Option 107
Windows Security Manager Option 108

Chapter 5 Monitoring the Network with ClearSight 109
Working with Real-Time Monitor Displays 109
Choosing Which Applications to Display 110
Understanding and Navigating the ClearSight Workspace 112
About the Use of Color in ClearSight Displays 115
ClearSight Terminology 116
ClearSight's Model of the Network 117
ClearSight's Model and the OSI Model 118
Application Layer Monitoring 119
About Application Monitoring 119
Viewing Application Monitoring Detail Displays 120
Working with Application Monitoring Detail Displays 120
The Applications Pane 122
The Flows Pane 123
The Statistics Pane 126
Application Monitoring Detail Displays 131
Citrix Detail Display 132
DNS Detail Display 133
FTP Detail Display 134
Telnet Detail Display 136
HTTP Detail Display 138
POP Detail Display 140

SMTP Detail Display 142
MS SQL Detail Display 144
Oracle Detail Display 147
Exchange Detail Display 149
MSN Detail Display 150
VoIP Detail Displays 152
RTP Detail Display 159
RTSP Detail Display 161
IPTV Detail Display 162
Kerberos Detail Display 164
ISAKMP Detail Display 165
SMB Detail Display 166
Generic Detail Display 167
Network Layer Monitoring 168
Overview Tab (Network Layer) 169
Connections Tab (Network Layer) 170
Hosts Tab (Network Layer) 175
Charts Tab (Network Layer) 177
Multicast Tab (Network Layer) 178
Reserved IPv6 Multicast Addresses 179
Physical Layer Monitoring 180
Overview Tab (Physical Layer) 182
VLAN Tab (Physical Layer) 183
Subnet Tab (Physical Layer) 184
Nodes Tab (Physical Layer) 185
Charts Tab (Physical Layer) 186
Configuring the ClearSight Analyzer 188
Global Protocol Settings 189
Global Monitor Settings 190
Global Monitor Options 192
Application Layer Options 192
Network and Physical Layer Options 193
Global Protocol Forcing Options 195
Enable/Disable 195
Pattern 195
Start From and Skip Offset 196
Forced Protocol Type 196
Problem Thresholds 197

Problem Actions 197
Decode 197
VoIP E-model 198
VoIP Codec 198
Report Settings 198
History Report Database Settings 199
WEP Key 199
The Address Book Tab 199
The Filter Tab 199
Changing Window Styles 200

Chapter 6 Capturing Data with ClearSight 201
About Capture 201
The Capture Workspace 202
The Statistics Tab 205
The Settings Tab 206
Selecting a Filter 207
Setting the Buffer Size 208
Specifying the Buffer Full Action 208
Setting the Slice Size 209
Setting the Auto Save Parameters 209
Setting the Capture Options 210
The Trigger Tab 213
Setting the Post-Trigger Settings 214
Setting Time-Based Triggers 214
Setting Filter-Based Triggers 214
Setting an Alarm-Based Trigger 214
Observing the Capture in Progress 216

Chapter 7 Postcapture Analysis 217
About Postcapture Analysis 217
Working with Postcapture Analysis Displays 218
Smart Navigation between the ClearSight and Decode Tabs 221
Smart Navigation from the ClearSight Tab 222
Smart Navigation from the Decode Tab 224
Using Automatic Filters in the Postcapture Displays 226
Working with the Decode Tab 226
Panes in the Decode Tab 228

The Summary Pane 228
The Detail Pane 230
The Hex Pane 232
Searching for Frames in the Decode Tab 232
Decoding Ethernet OAM Frames 233
Decoding 3G-324M Frames 235
Configuration Options for the Decode Tab 237
Decode General Options 237
Trace File Open Behavior 238
Trace Files 239
Options 240
Problem Generation 240
Timer Simulation Settings 241
Decode Settings 242
Ladder View 243
Network Connections 243
Applications 243
Decode Display Options 244
Options 245
Summary Optional Fields 245
Protocol Colors 246
Protocol Font 246
Decode Protocol Forcing Options 247
Enable/Disable 248
Pattern 248
Start From and Skip Offset 248
Forced Protocol Type 248
LWAPP 248
EtherOAM 249
WiMax 249
Decode IPSec Options 249
ESP General Settings 251
ESP Parameter Sets 251
Working with Trace Files 251

Chapter 8 Multi-Segment Analysis 253

About Multi-Segment Analysis 253
Creating Merged Trace Files 254
Viewing Combined VoIP Flows 257

Working with the Ladder View 258
Viewing Other Combined Flows 259
Working with the Ladder View 260
Using Auto-Combine Filters 261
Using the Multi-Tiered Tab 264
Using the NAT Tab 265
Combining Flows Manually 266
Real-Time Multi-Segment Monitoring 267

Chapter 9 Using Filters 269
About Filters 269
Automatic Filters vs. Defined Filters 269
Using Filters in Real-time or During Post Analysis 270
Packet-Based Filters vs. Flow-Based Filters 271
Using Automatic Filters 272
Automatic Capture Filters 272
Automatic Display Filters 273
Using Defined Filters 274
Setting Application Layer Filters 277
Setting DNS Filters 278
Setting FTP Filters 280
Setting HTTP Filters 282
Setting POP Filters 284
Setting SMTP Filters 286
Setting MSN Filters 288
Setting Voice-H.323 Filters 289
Setting Voice-SIP Filters 291
Setting Voice-Skinny Filters 293
Setting Voice-MGCP Filters 294
Setting Voice-Megaco Filters 296
Setting ISAKMP Filters 297
Setting Kerberos Filters 298
Setting RTSP Filters 300
Setting IPTV Filters 302
Setting SMB Filters 303
Setting Flow Filters 304
Setting Pattern Filters 305

Setting IP Subnet Filters 307
Setting Protocol Filters 308
Setting Parent Protocol Filters 308
Setting IP Filters 309
Setting TCP Filters 311
Setting UDP Filters 313
Setting MAC Address Filters 314
Setting Physical Layer Filters 315
The Filter List 317

Chapter 10 Working with Alerts 319
About Alerts 320
Working with the Alert Display 320
Issues Tab Information in the Alert Display 322
Problems Tab Information in the Alert Display 323
Defining Severities and Actions 324
Defining Severities 324
Defining Actions 325
Configuring Email Actions 326
Configuring Pager Actions 328
Configuring Script Actions 330
Configuring SNMP Actions 332
Viewing the Action List 333
Setting Thresholds for Problem Reporting 334
Setting DNS Thresholds 335
Setting FTP Thresholds 336
Setting Telnet Thresholds 339
Setting Citrix Thresholds 339
Setting HTTP Thresholds 340
Setting POP Thresholds 341
Setting SMTP Thresholds 343
Setting MSN Thresholds 344
Setting H.323 Thresholds 345
Setting SIP Thresholds 347
Setting Skinny Thresholds 348
Setting MGCP Thresholds 349
Setting Megaco Thresholds 350
Setting RTP Thresholds 351

Setting RTSP Thresholds 353
Setting IPTV Thresholds 355
Setting ISAKMP Thresholds 356
Setting Kerberos Thresholds 356
Setting SMB Thresholds 357
Setting IP Thresholds 358
Setting IPv6 Thresholds 360
Setting DLC Thresholds 361

Chapter 11 Using the Address Book 363
About the Address Book 363
Working with the Address Book 364
Enabling Automatic Address Book Entries 365

Chapter 12 Using Reports 367
About Reports 367
Generating Reports in Windows XP 369
The Report Workspace 369
Using Application Reports 372
DNS Reports 373
FTP Reports 374
Telnet Reports 374
HTTP Reports 375
POP Reports 376
SMTP Reports 377
MS SQL Server Reports 377
Oracle SQL Server Reports 378
VoIP Reports 380
IPTV Quality Reports 382
Kerberos Reports 382
ISAKMP Reports 382
Exchange Reports 383
MSN Reports 383
SMB Reports 384
RTSP Reports 384
Using Network Reports 386
Network Overview Reports 386

Connections Reports 386
IP Matrix Reports 386
IP Hosts Reports 387
Application Distribution Reports 387
IP Protocol Distribution Reports 387
IP Response Time Distribution Reports 387
Using DLC Reports 388
DLC Overview Reports 388
Nodes Reports 388
VLAN Reports 388
Utilization Distribution Reports 388
Creating a User-Defined Report 389
Using the History Reporter 391
Controlling the Accumulation of Data 392
Creating a History Report 394
Trending Charts 396
Creating a VoIP Call Log 397
Using the Call Browser 398

Chapter 13 Using the Packet Generator 399
The Packet Generator Option 399
ClearSight Packet Generator Features 400
Using the Packet Generator 401
The Statistics Table 402
Traffic Graphs 403
Traffic Control Buttons 403
The Send Packet Dialog Box 404
Type 404
Size 405
Traffic 406
Option 406
Header Edit 406
Hex Values 408
Saving a Profile 408
The Send Buffer Dialog Box 409
Option 410
Traffic 411
Replace Connection 411

Saving a Profile 412
The Profile List 413

Chapter 14 Linking to ClearSight Apex 415
What Apex Provides 415
Where to Find the Links 416

Chapter 15 Sending Error Reports to ClearSight Networks 419
Basic Operation of the Error Reporting Feature 419

Appendix A Configuring Special Network Cards 423
Configuring the Gigabit-XD Ethernet Card 423
Mode Options 424
Physical Connection Options 425
Configuring the 10-Gigabit Ethernet Card 426
Mode Options 427
Capture Mode Options 427

Index 429

About This Guide

This guide describes how to install, connect, and operate the ClearSight® Analyzer software. The ClearSight Analyzer software monitors and analyzes your network, providing information that lets you:

- Manage IP-based flows for popular applications using the ClearSight Analyzer's intuitive application monitoring interface.
- Monitor Service Level Agreements to ensure that you receive the bandwidth you pay for.
- Detect and resolve network problems in real time using the ClearSight Analyzer's powerful alert detection capabilities.
- Generate a wide variety of reports that assist you in planning for the future of your network.
- Perform traditional network protocol analysis.

NOTE: This guide refers to the ClearSight Analyzer software as "ClearSight" for short.

About Standalone and Distributed Features

This manual describes ClearSight Analyzer in both its standalone and distributed configurations. With some isolated exceptions noted in the manual, the features available in ClearSight Analyzer's standalone configuration are the same as those available in a connected ClearSight Distributed Agent. The major difference is that when working with a connected ClearSight Distributed Agent, you enter commands and view ClearSight displays from the Agent Viewer instead of on the local PC.

Chapter 4, Using ClearSight Distributed describes the ClearSight Distributed system in detail, including information on how to connect to Agents from the Agent Viewer, set up system wide alert reporting, and so on. The rest of the chapters in this manual describe how to use ClearSight's features to monitor and analyze the network once connected to a Distributed Agent.

NOTE: CSD is not supported in CSA version 7.0.7.

Audience of this Guide

This guide assumes that you are familiar with basic networking concepts and are ready for a tool that can help you manage and troubleshoot your network without having to hunt through screens of hexadecimal code. ClearSight is simple enough for the beginning network troubleshooter, yet sophisticated and powerful enough for the most advanced network administrators.

How this Guide is Organized

Chapter 1, Installing ClearSight	Describes how to install the ClearSight Analyzer software on a PC that meets the minimum system requirements.

Chapter 2, Connecting the ClearSight Analyzer to the Network	Discusses how to connect ClearSight to the network in a way that maximizes the effectiveness of your network monitoring and analysis.
Chapter 3, Introducing the ClearSight Analyzer	Introduces the ClearSight Analyzer, describes its capabilities, and shows how it can help you troubleshoot your network.
Chapter 4, Using ClearSight Distributed	Describes the Distributed version of ClearSight Analyzer. ClearSight Distributed lets you connect to remote ClearSight Agents from a central ClearSight Agent Viewer. This way, you can receive comprehensive monitoring and analysis of a distributed network environment from a central Agent Viewer.
Chapter 5, Monitoring the Network with ClearSight	Describes how to work with ClearSight's real-time network monitoring displays to understand and troubleshoot your network. Includes discussions of ClearSight's model of the network as well as application monitoring in general.
Chapter 6, Capturing Data with ClearSight	Describes how to use ClearSight to capture data from the network. Includes capture configuration options and displays.
Chapter 7, Postcapture Analysis	Describes how to use ClearSight's powerful postcapture analysis capabilities to interpret, understand, and troubleshoot network data.
Chapter 8, Multi-Segment Analysis	Describes how to use ClearSight's multi-segment analysis capabilities, including discussions of how to merge trace files, and how to create and interpret combined flows.

Chapter 9, Using Filters	Describes how to use ClearSight's filtering capabilities, including discussions of automatic vs. defined filters, capture vs. display filters, and packet-based vs. flow-based filters.
Chapter 10, Working with Alerts	Describes how to work with ClearSight's Alerts Log, including how to define severities, associate actions with severities, and set thresholds for problem detection.
Chapter 11, Using the Address Book	Describes how to use ClearSight's Address Book feature to assign meaningful names to be used in ClearSight's Decode tab in place of IP addresses.
Chapter 12, Using Reports	Describes how to use ClearSight's Reports feature to view different types of reports for different types of network data.
Chapter 13, Using the Packet Generator	Describes how to use ClearSight's integrated packet generator.
Chapter 14, Linking to ClearSight Apex	Describes how to link to the ClearSight Apex product for access to an expert knowledge base.
Chapter 15, Sending Error Reports to ClearSight Networks	Describes how to error reports to ClearSight Networks in the event of a crash.
Appendix A, Configuring Special Network Cards	Describes how to connect the optional 10/100 Full Duplex Ethernet and Gigabit Ethernet adapters to the network, as well as how to set special configuration options for just these adapters.

Conventions Used in this Guide

The following notational conventions are used in this guide.

Bold face — Bold is used for the names of menus, buttons, and fields in the ClearSight user interface. For example:

Click the **Monitor** button in the ClearSight toolbar**.**

Italic — Italic font is used in two different ways:

- the first time a new term or concept is introduced,
- in cross references to headings or chapters. For example:

See *About Custom Conversion Rules* on *page 44*.

Bold italic — Bold italic font is used to indicate user-defined variables. For example:

Enter the date in ***yymmdd*** format.

> — A single right angle bracket is used to separate a series of choices in a menu. For example:

Select the **File > Save** command.

< > — Angle brackets indicate that the item enclosed within the brackets is the name of a key on the computer keyboard. For example:

The Windows keyboard shortcut is <CTRL - C>.

Indicators Used in this Guide

This guide uses the following indicators. You should read them carefully before proceeding.

WARNING: A warning is used to indicate information that you need to know to avoid causing damage to data files, program files, or hardware devices.

NOTE: A note is used to indicate important information about using the ClearSight Analyzer.

IMPORTANT: This indicator is used to bring general information to your attention.

TIP: A tip is used to indicate additional actions you can take.

Customer Service

Contact ClearSight Networks Customer Service department with product questions, licensing questions, or other issues using the information in Table i. The Customer Service department's hours of operation are from 8:00 AM to 5:00 PM Pacific Time, Monday through Friday.

Table i: Customer Service Contact Information

Telephone	800 825-7563 (U.S and Canada) 510 824-6000
Fax	510 824-6100
Email	support@clearsightnet.com
Web	http://www.clearsightnet.com
Mail	46401 Landing Parkway Fremont, CA 94538-6496

Contacting Technical Support

Technical support is available Monday through Friday between 06:00 and 18:00 Pacific Standard Time.

To obtain technical support for any ClearSight product, please contact our Technical Support Department using any of the following methods:

- Toll Free: 800 825-7563 (available in the U.S. and Canada)
- Phone: 510 824-6000
- Fax: 510 824-6100
- E-mail: support@clearsightnet.com
- Web: http://www.clearsightnet.com/support.jsp

In addition, the latest versions of application Help files, application notes, and software updates are available on our website at:

- http://www.clearsightnet.com

Other Departments

Table ii shows how to reach additional departments at ClearSight Networks.

Table ii: Additional ClearSight Networks Departments

Sales	sales@clearsightnet.com
Marketing	marketing@clearsightnet.com

Chapter 1

Installing ClearSight

This chapter covers the following major topics:

- *ClearSight System Requirements*
- *Before Installing ClearSight*
- *Installing ClearSight Analyzer Standalone*
- *Installing ClearSight Distributed*
- *Licensing ClearSight Standalone*
- *Licensing ClearSight Distributed*
- *Uninstalling ClearSight Standalone*
- *Uninstalling ClearSight Distributed*

ClearSight System Requirements

ClearSight is a powerful network analysis tool; it requires a powerful system for optimal performance. This section lists the minimum system requirements for:

- *ClearSight Standalone System Requirements*
- *ClearSight Agent Manager and Agent System Requirements*

- *ClearSight Agent Manager Only System Requirements*
- *ClearSight Distributed Agent Only System Requirements*

ClearSight Standalone System Requirements

Table 1-1 and Table 1-2 list the minimum system requirements for the ClearSight Analyzer.

Table 1-1: ClearSight Standalone Minimum System Requirements (Windows XP)

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with a CD drive for software installation.
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum (2 GHz recommended).
RAM	512 MB minimum (1 GB recommended)
Hard Disk Space	250 MB. In addition, you should have space to store saved trace files. Individual trace files can be as large as 1 GB, but it is not recommended to open a trace file larger than 256 MB.
Operating System	Microsoft Windows XP Home Edition with SP2. Disable the firewall. Microsoft Windows XP Professional with SP2. Disable the firewall.
Monitor	VGA color monitor with 1024x768 resolution and 256 colors.
Network Adapter	Network connection with NDIS-compliant network device driver.

Table 1-2: ClearSight Standalone Minimum System Requirements (Windows Vista)

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with audio output and a DVD-ROM drive for software installation.
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum (2 GHz recommended).
RAM	2 GB minimum
Hard Disk Space	40 GB hard drive with at least 15 GB of available space.
Operating System	Microsoft Vista (32 bit) with SP1 or SP2.
Monitor	VGA color monitor with 1024x768 resolution. Support for DirectX 9 graphics with: WDDM Driver, minimum 128 MB of graphics memory, Pixel Shader 2.0 in hardware and 32 bits per pixel.
Network Adapter	Network connection with NDIS-compliant network device driver.

ClearSight Agent Manager and Agent System Requirements

Table 1-3 and Table 1-4 list the minimum system requirements for ClearSight Distributed when the Agent Manager and Agent are installed on the same PC.

Table 1-3: ClearSight Distributed Minimum System Requirements — Agent Manager and Agent on same PC (Windows XP)

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with a CD drive for software installation.
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum (2 GHz recommended).
RAM	512 MB minimum (1 GB recommended)
Hard Disk Space	250 MB. In addition, you should have space to store saved trace files. Individual trace files can be as large as 1 GB, but it is not recommended to open a trace file larger than 256 MB.
Operating System	Microsoft Windows XP Home Edition with SP2. Disable the firewall. Microsoft Windows XP Professional with SP2. Disable the firewall.
Monitor	VGA color monitor with 800x600 resolution and 16 colors. 1024x768 resolution and 256 colors recommended.
Network Adapter	Network connection with NDIS-compliant network device driver.
Internet Browser	Microsoft Internet Explorer 6.0 or higher.

Table 1-4: ClearSight Distributed Minimum System Requirements — Agent Manager and Agent on same PC (Windows Vista)

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with audio output and a DVD-ROM drive for software installation.
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum (2 GHz recommended).
RAM	2 GB minimum
Hard Disk Space	40 GB hard drive with at least 15 GB of available space.
Operating System	Microsoft Vista (32 bit) with SP1 or SP2.
Monitor	VGA color monitor with 1024x768 resolution. Support for DirectX 9 graphics with: WDDM Driver, minimum 128 MB of graphics memory, Pixel Shader 2.0 in hardware and 32 bits per pixel.
Network Adapter	Network connection with NDIS-compliant network device driver.
Internet Browser	Microsoft Internet Explorer 6.0 or higher.

ClearSight Agent Manager Only System Requirements

Table 1-5 and Table 1-6 list the minimum system requirements for ClearSight Distributed when only the Agent Manager is installed on the PC.

Table 1-5: ClearSight Distributed Minimum System Requirements — Agent Manager Only (Windows Versions earlier than Vista)

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with a CD drive for software installation.
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum (2 GHz recommended).
RAM	512 MB minimum (1 GB recommended)
Hard Disk Space	250 MB. In addition, you should have space to store saved trace files. Individual trace files can be as large as 1 GB, but it is not recommended to open a trace file larger than 256 MB.
Operating System	Microsoft Windows XP Home Edition with SP2. Disable the firewall. Microsoft Windows XP Professional with SP2. Disable the firewall.
Monitor	VGA color monitor with 800x600 resolution and 16 colors. 1024x768 resolution and 256 colors recommended.
Network Adapter	Network connection with network device driver for accessing remote Agents.
Internet Browser	Microsoft Internet Explorer 6.0 or higher.

Table 1-6: ClearSight Distributed Minimum System Requirements — Agent Manager Only (Windows Vista)

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with audio output and a DVD-ROM drive for software installation.
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum (2 GHz recommended).
RAM	2 GB minimum
Hard Disk Space	40 GB hard drive with at least 15 GB of available space.
Operating System	Microsoft Vista (32 bit) with SP1 or SP2.
Monitor	VGA color monitor with 1024x768 resolution. Support for DirectX 9 graphics with: WDDM Driver, minimum 128 MB of graphics memory, Pixel Shader 2.0 in hardware and 32 bits per pixel.
Network Adapter	Network connection with network device driver for accessing remote Agents.
Internet Browser	Microsoft Internet Explorer 6.0 or higher.

ClearSight Distributed Agent Only System Requirements

Table 1-7 and Table 1-8 list the minimum system requirements for the ClearSight Distributed when only the Agent is installed.

Table 1-7: ClearSight Minimum System Requirements — Agent Only (Windows XP)

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with a CD drive for software installation.
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum (2 GHz recommended).
RAM	512 MB minimum (1 GB recommended)
Hard Disk Space	250 MB. In addition, you should have space to store saved trace files. Individual trace files can be as large as 1 GB, but it is not recommended to open a trace file larger than 256 MB.
Operating System	Microsoft Windows XP Home Edition with SP2. Disable the firewall. Microsoft Windows XP Professional with SP2. Disable the firewall.
Network Adapter	Network connection with network device driver — for accessing remote Agents.
Internet Browser	Microsoft Internet Explorer 6.0 or higher.

Table 1-8: ClearSight Minimum System Requirements — Agent Only (Windows Vista)

Item	Minimum Requirement
Computer	Industry standard computer system (laptop or desktop), with audio output and a DVD-ROM drive for software installation.
Processor	Pentium 4 (or equivalent) running at 1 GHz minimum (2 GHz recommended).
RAM	2 GB minimum
Hard Disk Space	40 GB hard drive with at least 15 GB of available space.
Operating System	Microsoft Vista (32 bit) with SP1 or SP2.
Network Adapter	Network connection with network device driver — for accessing remote Agents.
Internet Browser	Microsoft Internet Explorer 6.0 or higher.

Before Installing ClearSight

Before installing ClearSight, ensure that:

- The target system meets or exceeds the minimum system requirements.
- You have the installation files, either on the ClearSight application CDs or downloaded from the ClearSight Networks website.
- If you have any earlier ClearSight Analyzer version installed, it will be automatically uninstalled before installing the new version. A series of dialog boxes will guide you through the uninstallation of the old version.

Installing ClearSight Analyzer Standalone

Follow the instructions below for installing ClearSight Analyzer Standalone on Windows XP or Windows Vista.

Installing on Windows XP

To install the standalone version of ClearSight Analyzer on Windows XP, proceed as follows:

1. Insert the ClearSight product CD into the target PC's CD-ROM drive.
2. If the InstallShield Wizard does not launch automatically (or if you have downloaded the software) navigate to the location of the install program and run it from there.
3. Follow the instructions in the InstallShield Wizard to install the ClearSight Analyzer software. During the installation:
   a. Accept the terms of the End User Software License Agreement.
   b. Enter your Customer Information.
   c. Specify the installation directory for the ClearSight Analyzer software.

NOTE: ClearSight recommends that you accept the default installation directory.

4. Verify that the directory listed is correct. Click **Install**.
5. When the installation has completed, click **Finish** to exit the InstallShield Wizard.
6. When the program asks you to reboot, click **No**.
7. The next screen asks you to insert the second CD. Insert the Third Party Decode Engine CD.
8. If the InstallShield Wizard does not launch automatically (or if you have downloaded the software) navigate to the location of the install program and run it from there.
9. Follow the instructions in the InstallShield Wizard to install the Third Party Decode Engine. During the install:
   a. Accept the terms of the Software License Agreement.
   b. Specify the installation directory for the Third Party Decode Engine.

      NOTE: ClearSight recommends that you accept the default installation directory.
10. Verify that the directory listed is correct. Click **Install**.
11. When the installation has completed, click **Finish** to exit the InstallShield Wizard.
12. Manually restart your computer.
13. Start the ClearSight Analyzer software from the Start menu **(Start Menu > (All) Programs > ClearSight > ClearSight Analyzer)**.
14. Activate your license (see *Activating the Standard Version* on page 45). Then log in to ClearSight Analyzer and choose your adapter.

Installing on Windows Vista

To install the standalone version of ClearSight Analyzer on windows Vista, proceed as follows:

1. Insert the ClearSight product CD into the target PC's DVD-ROM drive.
2. If the InstallShield Wizard does not launch automatically (or if you have downloaded the software) navigate to the location of the install program and run it from there.
3. If you are logged on to Vista as Administrator, go directly to Step 5.
4. If you are logged onto Vista as other than Administrator but have Administrator permission, you will see the User Account Control dialog box. The message "An unidentified program wants access to your computer" will appear in the User Account Control dialog box. Click **Allow**.
5. Follow the instructions in the InstallShield Wizard to install the ClearSight Analyzer software. During the installation:
   a. Accept the terms of the End User Software License Agreement.
   b. Enter your Customer Information.
   c. Specify the installation directory for the ClearSight Analyzer software.

      NOTE: ClearSight recommends that you accept the default installation directory.
6. Verify that the directory listed is correct. Click **Install**.
7. When the installation has completed, click **Finish** to exit the InstallShield Wizard.
8. When the program asks you to reboot, click **No**.
9. The next screen asks you to insert the second CD. Insert the Third Party Decode Engine CD.
10. If the InstallShield Wizard does not launch automatically (or if you have downloaded the software) navigate to the location of the install program and run it from there.

11. If you are logged on to Vista as Administrator, go directly to Step 13.
12. If you are logged onto Vista as other than Administrator but have Administrator permission, you will see the User Account Control dialog box. The message "An unidentified program wants access to your computer" will appear in the User Account Control dialog box. Click **Allow**.
13. Follow the instructions in the InstallShield Wizard to install the Third Party Decode Engine. During the install:
    a. Accept the terms of the Software License Agreement.
    b. Specify the installation directory for the Third Party Decode Engine.

       NOTE: ClearSight recommends that you accept the default installation directory.
14. Verify that the directory listed is correct. Click **Install**.
15. When the installation has completed, click **Finish** to exit the InstallShield Wizard.
16. Manually restart your computer.
17. Start the ClearSight Analyzer software from the Start menu **(Start Menu > All Programs > ClearSight > ClearSight Analyzer)**.
18. If you are logged on to Vista as Administrator, go directly to Step 20.
19. If you are logged onto Vista as other than Administrator but have Administrator permission, you will see the User Account Control dialog box. The message "An unidentified program wants access to your computer" will appear in the User Account Control dialog box. Click **Allow**.
20. Activate your license (see *Activating the Standard Version* on page 45). Then log in to ClearSight Analyzer and choose your adapter.

Installing ClearSight Distributed

You install ClearSight Distributed in much the same way that you install the ClearSight Analyzer standalone product. However, when installing ClearSight Distributed, you have the option of installing:

- Agent Manager and Agent
- Agent Manager Only
- Agent Only

When you install the Agent Manager only, there is no "local" monitoring and analysis interface for the Agent — it is not the same as installing the standalone version of the ClearSight Analyzer. Installing the Agent Manager only lets you perform monitoring and analysis using a remote Agent.

Similarly, installing the Agent only does not let you manage the Agent from that PC. It installs a ClearSight Distributed Agent that can be managed by an Agent Manager installed on another PC.

Finally, you can install both Agent Manager and Agent on the same PC. You can then manage both the local Agent and remote Agents using just the local Agent Manager.

Installing on Windows XP

To install the ClearSight Distributed on Windows XP, proceed as follows:

1. Insert the product CD into the target PC's CD-ROM drive.
2. If the InstallShield Wizard does not launch automatically (or if you have downloaded the software) navigate to the location of the install program and run it from there.
3. Follow the instructions in the InstallShield Wizard to install the ClearSight Distributed software. During the install:
   a. Accept the terms of the End User Software License Agreement.
   b. Enter your Customer Information.

c. Specify the installation directory for the ClearSight Distributed software.

   NOTE: ClearSight recommends that you accept the default installation directory.

d. Select the ClearSight Distributed components you want to install (see Figure 1-1).

   NOTE: If you want to change to a different configuration after the initial installation, the original configuration must first be uninstalled, and the system rebooted. Then the new installation can be started.

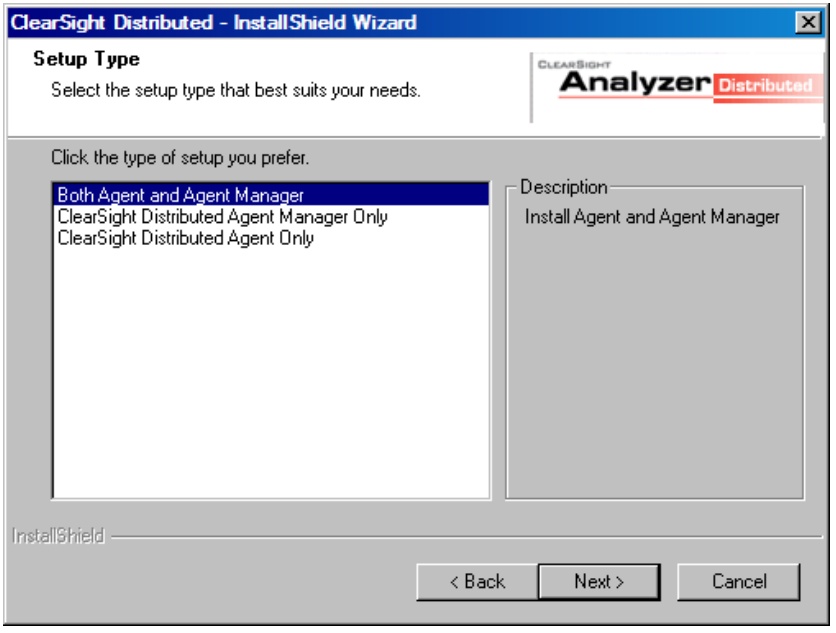


Figure 1-1: Selecting the ClearSight Distributed Components to Install

4. Verify that the directory listed is correct. Click **Install**.
5. When the installation has completed, click **Finish** to exit the InstallShield Wizard.
6. When the program asks you to reboot: Click **No** if you want to install the Third Party Decode Engine. Otherwise, click **Yes**.
7. If you want to install the Third Party Decode Engine, navigate to the location of the install program and run it from there.

8. Follow the instructions in the InstallShield Wizard to install the Third Party Decode Engine. During the install:
   a. Accept the terms of the Software License Agreement.
   b. Specify the installation directory for the Third Party Decode Engine.

      NOTE: ClearSight recommends that you accept the default installation directory.
9. Verify that the directory listed is correct. Click **Install**.
10. When the installation has completed, click **Finish** to exit the InstallShield Wizard.
11. Manually restart your computer.
12. If the Manager is installed on this PC, start the ClearSight Distributed Agent Manager software from the **Start** menu (**Start Menu > (All) Programs > ClearSight Distributed > ClearSight Distributed Agent Manager**).

    The ClearSight Distributed Agent Manager is your "home base" to connect to multiple ClearSight Distributed Agents. Once connected to a Distributed Agent, you work with the standard ClearSight Analyzer functions just as you would with a standalone version of the software.

Installing on Windows Vista

To install the ClearSight Distributed on Windows Vista, proceed as follows:

1. Insert the product CD into the target PC's CD-ROM drive.
2. If the InstallShield Wizard does not launch automatically (or if you have downloaded the software) navigate to the location of the install program and run it from there.
3. If you are logged on to Vista as Administrator, go directly to Step 5.
4. If you are logged onto Vista as other than Administrator but have Administrator permission, you will see the User Account Control dialog box. The message "An unidentified program wants access

to your computer" will appear in the User Account Control dialog box. Click **Allow**.

5. Follow the instructions in the InstallShield Wizard to install the ClearSight Distributed software. During the install:

   a. Accept the terms of the End User Software License Agreement.

   b. Enter your Customer Information.

   c. Specify the installation directory for the ClearSight Distributed software.

      NOTE: ClearSight recommends that you accept the default installation directory.

   d. Select the ClearSight Distributed components you want to install (see Figure 1-2).

      NOTE: If you want to change to a different configuration after the initial installation, the original configuration must first be uninstalled, and the system rebooted. Then the new installation can be started.

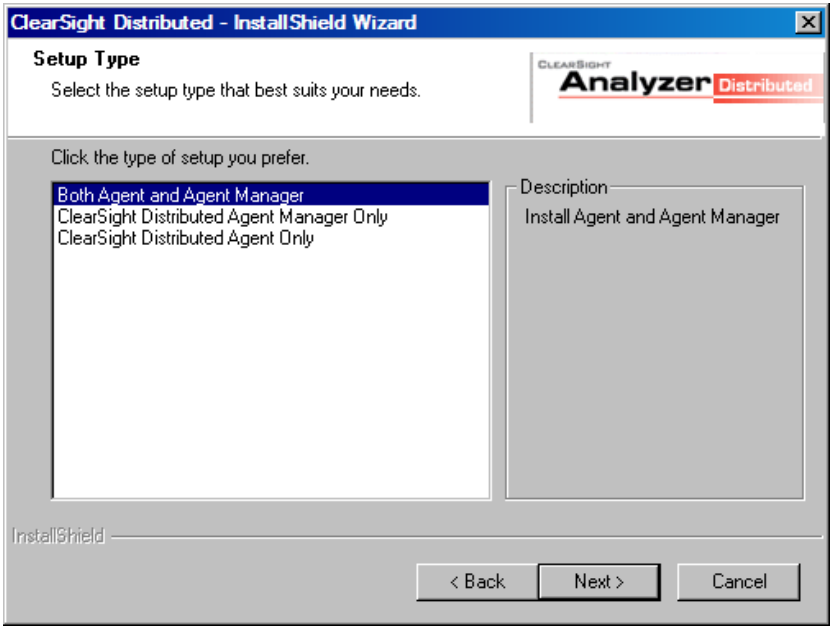


Figure 1-2: Selecting the ClearSight Distributed Components to Install

6. Verify that the directory listed is correct. Click **Install**.
7. When the installation has completed, click **Finish** to exit the InstallShield Wizard.
8. When the program asks you to reboot: Click **No** if you want to install the Third Party Decode Engine. Otherwise, click **Yes**.
9. If you want to install the Third Party Decode Engine, navigate to the location of the install program and run it from there.
10. If you are logged on to Vista as Administrator, go directly to Step 12.
11. If you are logged onto Vista as other than Administrator but have Administrator permission, you will see the User Account Control dialog box. The message "An unidentified program wants access to your computer" will appear in the User Account Control dialog box. Click **Allow**.
12. Follow the instructions in the InstallShield Wizard to install the Third Party Decode Engine. During the install:
    a. Accept the terms of the Software License Agreement.
    b. Specify the installation directory for the Third Party Decode Engine.

       NOTE: ClearSight recommends that you accept the default installation directory.
13. Verify that the directory listed is correct. Click **Install**.
14. When the installation has completed, click **Finish** to exit the InstallShield Wizard.
15. Manually restart your computer.
16. If the Manager is installed on this PC, start the ClearSight Distributed Agent Manager software from the **Start** menu (**Start Menu > (All) Programs > ClearSight Distributed > ClearSight Distributed Agent Manager**).
17. If you are logged on to Vista as Administrator, the program will start. If you are logged onto Vista as other than Administrator but have Administrator permission, you will see the User Account Control dialog box. The message "An unidentified program

wants access to your computer" will appear in the User Account Control dialog box. Click **Allow**.

You use the ClearSight Distributed Agent Manager as your "home base" to connect to multiple ClearSight Distributed Agents. Once connected to a Distributed Agent, you work with the standard ClearSight Analyzer functions just as you would with a standalone version of the software.

Licensing ClearSight Standalone

You can request a license for the ClearSight Analyzer by contacting ClearSight directly, or you can use a **Registration** option within the trial version.

See also:

- *Using the Trial Version to Request a License* on page 44
- *Activating the Standard Version* on page 45

Using the Trial Version to Request a License

The trial version of the ClearSight Analyzer software is installed with a temporary license that expires 14 days from the date the program is first run. It is not possible to upgrade this trial version to the standard version. However, the **Help** menu in the trial version contains a **Registration** option that you can use (within the 14-day trial period) to request a license for the standard version.

If you select **Help > Registration**, you will see a dialog box that gives you a choice of registration by Phone or by Internet.

If you choose **Phone**, ClearSight will display a Locking Code, which you can read over the phone to ClearSight Customer Service. This information will be used to create a license file that will be sent to you by email. This file can be used to activate the standard version of the ClearSight Analyzer.

If you choose **Internet**, the **ClearSight Networks Registration** dialog box will appear (Figure 1-3). By filling in the required information in this dialog box, you are requesting a license file. When you click **Send**, information identifying your computer will be sent to ClearSight Customer Service. This information will be used to create a license file that will be sent to you by email. This file can be used to activate the standard version of the ClearSight Analyzer.

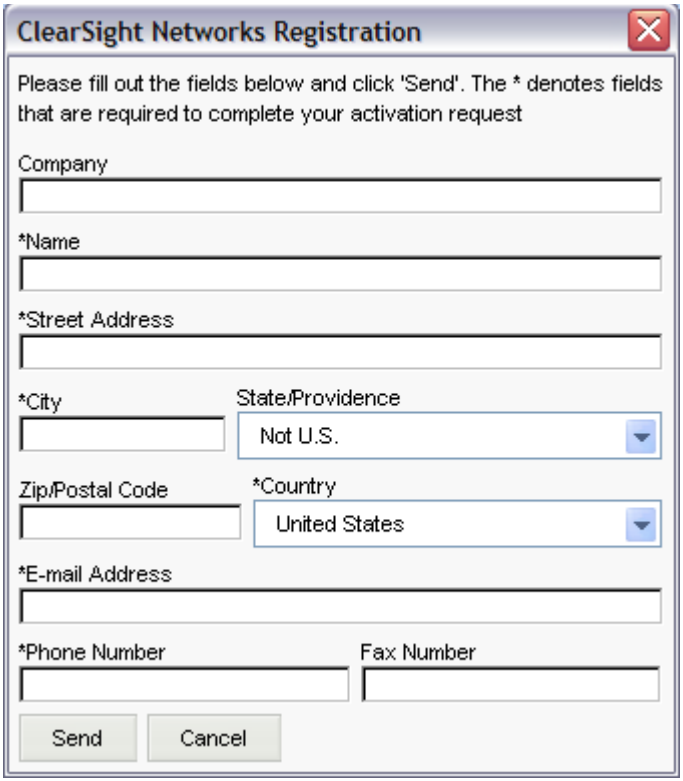


Figure 1-3: ClearSight Networks Registration Dialog Box

Activating the Standard Version

You can obtain the ClearSight Analyzer software from ClearSight Networks, either on CDs or by downloading the setup files from the ClearSight Networks website using FTP.

In either case you will need a license file, which you can also obtain from ClearSight, usually by email. If you have the trial version of the ClearSight Analyzer, you may have requested this license file from within the trial version, as explained in *Using the Trial Version to Request a License* on page 44.

If you have the trial version installed (or any earlier version of the ClearSight analyzer) you must uninstall it and restart your computer

before installing the standard version (see *Uninstalling ClearSight Standalone* on page 49 and *Uninstalling ClearSight Distributed* on page 50).

Install the standard version as described in *Installing ClearSight Analyzer Standalone* on page 34. Then, when you start the ClearSight Analyzer program, it will look for a valid license file. If it does not find this file, the program will present the **ClearSight Networks Activation** dialog box (Figure 1-4).

To enter the license code, either copy and paste the contents of the license file to the **License Code** box, or simply browse to the location of the file. In either case, click **Activate**, and the program will start.

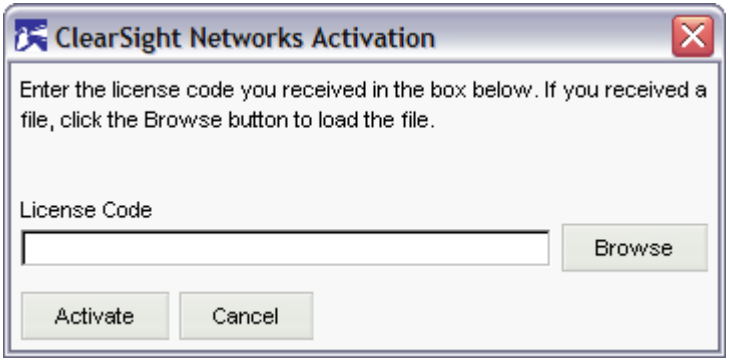


Figure 1-4: ClearSight Networks Activation Dialog Box

Once you have done the activation, ClearSight will subsequently start without showing this dialog box.

NOTE: The license is for use of the ClearSight Analyzer on one computer only. The information in the license file is specific to that computer. It will not work if you try to use it on another computer.

Licensing ClearSight Distributed

Whether you obtain the ClearSight Distributed software on CDs or by download, you will need a license file in order to activate the software. You will need a separate license file for each Agent.

To license ClearSight:

1. Make arrangements with a ClearSight Customer Service representative to purchase ClearSight Distributed. The Customer Service representative will tell you how to provide locking codes that are specific to the computers on which you plan to install the Agent software.
2. Based on these locking codes, ClearSight Customer Service will provide you with a corresponding set of license files, usually by email.
3. Copy each of these license files to a convenient location on the corresponding computer on which the Agent is installed.
4. After you have installed the ClearSight Distributed software, start the ClearSight Agent Manager by selecting **Start > (All) Programs > ClearSight Distributed > ClearSight Distributed Agent Manager**.
5. As you connect to each Agent, the **ClearSight Networks Activation** dialog box (Figure 1-4) will appear. *Chapter 4, Using ClearSight Distributed* explains how to set up an Agents list and how to connect to an Agent from the Manager.

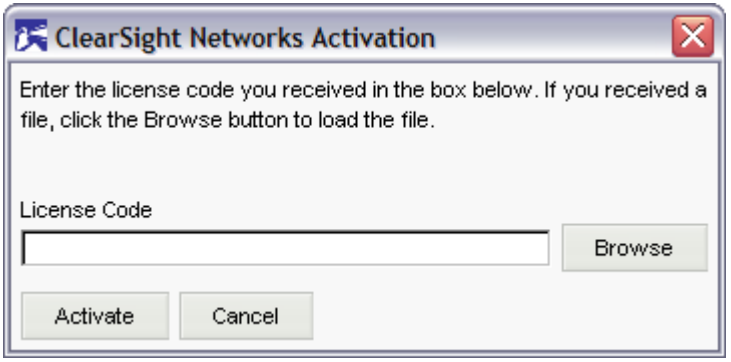


Figure 1-5: ClearSight Networks Activation Dialog Box

6. To enter the license code, either copy and paste the contents of the license file to the **License Code** box, or simply browse to the location of the file. In either case, click **Activate**, and the Agent program will start.

   NOTE: The license file for a given Agent can reside on that Agent's computer, or on the Manager's computer. It is only necessary that you have access to that file at the time that you initially connect to that Agent.

   Once you have done this activation, that particular Agent will subsequently start without showing this dialog box.

NOTE: The license is for use of the ClearSight Agent on one computer only. The information in the license file is specific to that computer. It will not work if you try to use it on another computer.

Uninstalling ClearSight Standalone

To uninstall ClearSight Analyzer:

1. Select the **Start > (All) Programs > ClearSight > Uninstall ClearSight Analyzer** command.
2. If you have Windows Vista, you may see the User Account Control dialog box. If so, click **Allow**.
3. Follow the on-screen instructions to uninstall ClearSight.

   NOTE: Depending on your installation, you may have the option of removing modified files during the uninstallation. Leaving in the modified files will not harm anything. However, if you want to free up the space, you can choose to remove them.
4. Reboot the computer. The uninstall process is not complete until you have rebooted the computer.

   NOTE: You must reboot the computer before re-installing ClearSight.

To uninstall the Third Party Decode Engine:

1. Select the **Start > (All) Programs > Third Party Decode Engine x.x.x > Uninstall Third Party Decode Engine** command.
2. If you have Windows Vista, you may see the User Account Control dialog box. If so, click **Allow**.
3. Follow the on-screen instructions to uninstall the Third Party Decode Engine.
4. Reboot the computer. The uninstall process is not complete until you have rebooted the computer.

   NOTE: You must reboot the computer before re-installing the Third Party Decode Engine.

Uninstalling ClearSight Distributed

To uninstall ClearSight Distributed:

1. Select **Start > (All) Programs > ClearSight Distributed > Uninstall**.
2. Follow the on-screen instructions to uninstall ClearSight.

   NOTE: Depending on your installation, you may have the option of removing modified files during the uninstallation. Leaving in the modified files will not harm anything. However, if you want to free up the space, you can choose to remove them.
3. Reboot the computer. The uninstall process is not complete until you have rebooted the computer.

   NOTE: You must reboot the computer before re-installing ClearSight.

To uninstall ClearSight 3rd Party Decode Engine:

1. Select the **Start > (All) Programs > Third Party Decode Engine x.x.x > Uninstall Third Party Decode Engine** command.
2. If you have Windows Vista, you may see the User Account Control dialog box. If so, click **Allow**.
3. Follow the on-screen instructions to uninstall the Third Party Decode Engine.
4. Reboot the computer. The uninstall process is not complete until you have rebooted the computer.

   NOTE: You must reboot the computer before re-installing any new 3rd Party Decode Engine for ClearSight.

Chapter 2

Connecting the ClearSight Analyzer to the Network

This chapter discusses how to connect ClearSight to the network in a way that maximizes the effectiveness of your network monitoring and analysis. ClearSight can only provide analysis of network data that it "sees." This chapter helps you connect ClearSight to the network in a way that ensures the sharpest vision. The chapter includes the following topics:

- Fundamentals of analyzer placement.
- Typical connection scenarios and their benefits and drawbacks, including:
  - Hubs
  - Network taps
  - Port mirroring
- Special considerations for connecting ClearSight Distributed Agents.

Analyzer Placement Fundamentals

One of the fundamentals of effective network monitoring and analysis is *analyzer placement* — connecting the analyzer to the network in a way that ensures maximum data visibility. A few years ago, most networks made extensive use of shared media — network hubs and the like. In a shared media environment, each station on the network segment sees every packet, checking to see whether it is addressed to that station. Individual stations simply copy the frames addressed to them, allowing the others to flow by. This makes network analysis easy, since an analyzer can simply be placed in promiscuous mode, copying all frames on the segment into the capture buffer for analysis.

Over time, the widespread deployment of network switches has made analyzer placement more complicated. Unlike hubs, network switches forward packets only to the port where a destination address actually resides. This results in a far more effective use of network bandwidth than that achieved by hubs, but it also makes network monitoring and analysis more difficult. Whereas connecting the analyzer to an open port on a hub allowed you to see all the traffic flowing over the device, connecting the analyzer to an open switch port shows you only broadcast and multicast packets.

There are several common methods used to gain visibility into a switched network, including:

- Inserting a hub on each segment to be monitored (page 53).
- Inserting a tap on each segment to be monitored (page 55).
- Setting up port mirroring on a switch (page 57).

The following sections discuss the benefits and drawbacks of each of these methods.

Inserting a Hub

The easiest and most inexpensive way to gain visibility to a switched network is to insert a *hub* between any two devices. Because each packet received by a hub is replicated to every port on the device, ClearSight can be connected to an open port on the hub and see all the data flowing between the two devices.

Figure 2-1 shows one example of how hubs can be used to allow network monitoring and analysis. In this example, hubs have been inserted between switch ports and connected devices on both **Switch A** and **Switch B**. By connecting to an open port on the hub placed between **Switch A** and the WAN cloud, ClearSight can see all the traffic between the switch port and the WAN.

Advantages and Disadvantages

Hubs have the advantage of being both cost-effective and easy to install. However, hubs are not appropriate for all networks. For example, inserting a hub on a full duplex link limits the link to half duplex speeds, slowing response times and reducing throughput.

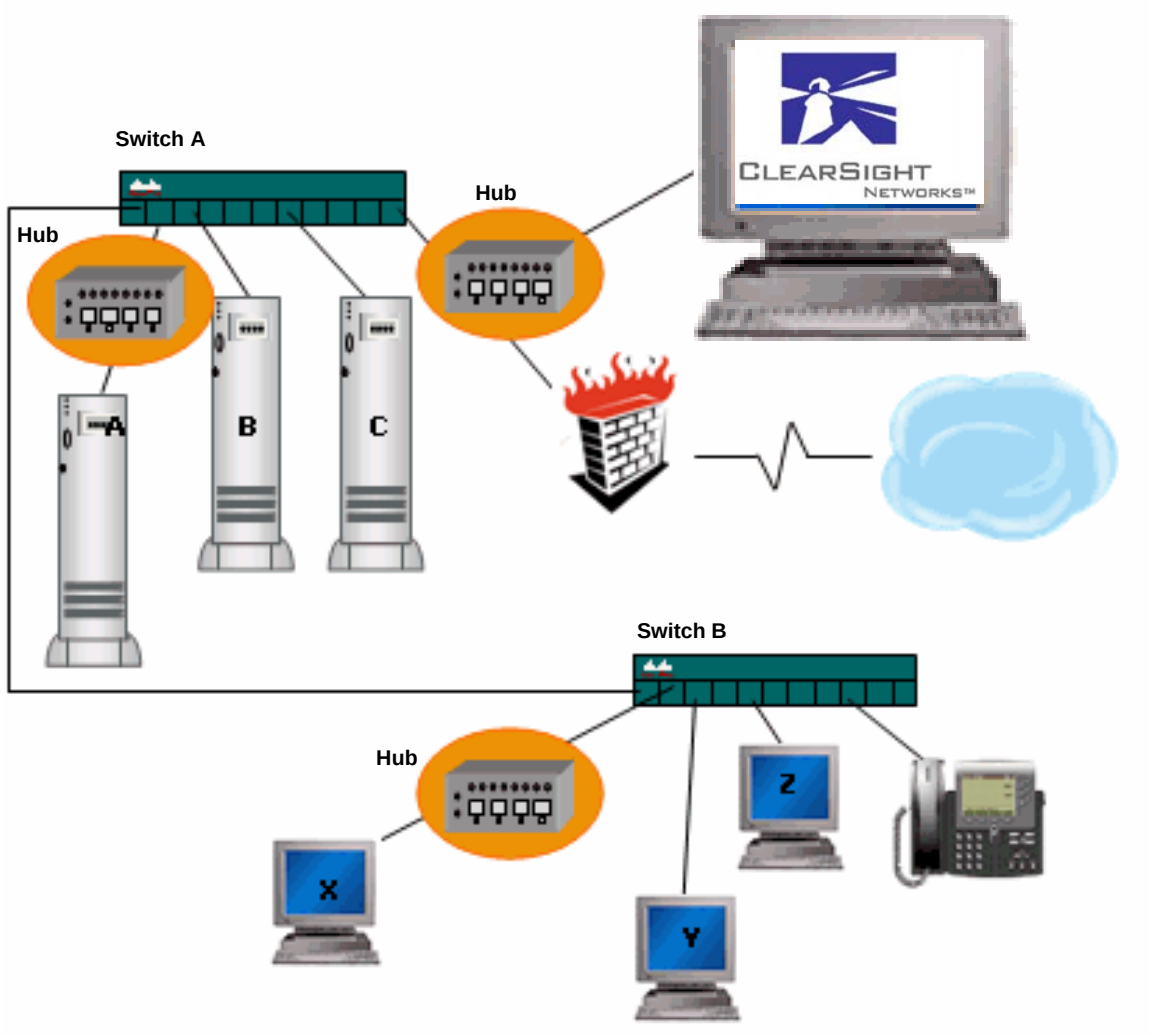


Figure 2-1: Inserting a Hub

Inserting a Tap

ClearSight can connect to the network using a *network tap*. A network tap is a passive device that sits on a link and copies the data flowing over the line to one or more monitor ports. Network taps are available for a wide variety of network media, including copper and fiber. Many networks are designed with taps already in place, allowing easy access to particular network segments.

Figure 2-2 shows one example of how a network tap can be used to allow network monitoring and analysis. In this example, the tap between **Switch A** and **Switch B** splits both sides of the full duplex link off to a separate monitor port where separate ClearSight Analyzers are connected.

NOTE: If you have purchased ClearSight's optional 10/100 Full Duplex Ethernet adapter, you could also make the connection shown in Figure 2-2 using a single ClearSight Analyzer; see *Configuring the Gigabit-XD Ethernet Card* on page 423 for details.

Advantages and Disadvantages

Network taps have several key advantages over hubs:

- Unlike a hub, a network tap preserves the integrity of a full duplex link, splitting out both sides of the link separately for monitoring and analysis.
- Because taps are passive devices, they can be left on a link indefinitely, letting you monitor whenever necessary without taking the link down to insert a hub.

Network taps also have disadvantages. For example:

- Inserting a network tap adds another potential point of failure to your network. If a tap fails, it can take down the link along with it.
- To see all of the traffic on your network, taps need to be installed on each full duplex network segment. This can be a costly investment.
- When inserted on a full duplex link, a tap splits out each side of the link (DTE and DCE) to a separate monitor port. To monitor

both sides of the link, you either need to connect two ClearSight Analyzers (one for each side of the link; see Figure 2-2) or a version of ClearSight using the optional 10/100 Full Duplex Ethernet card. This card is capable of monitoring each side of the link simultaneously.

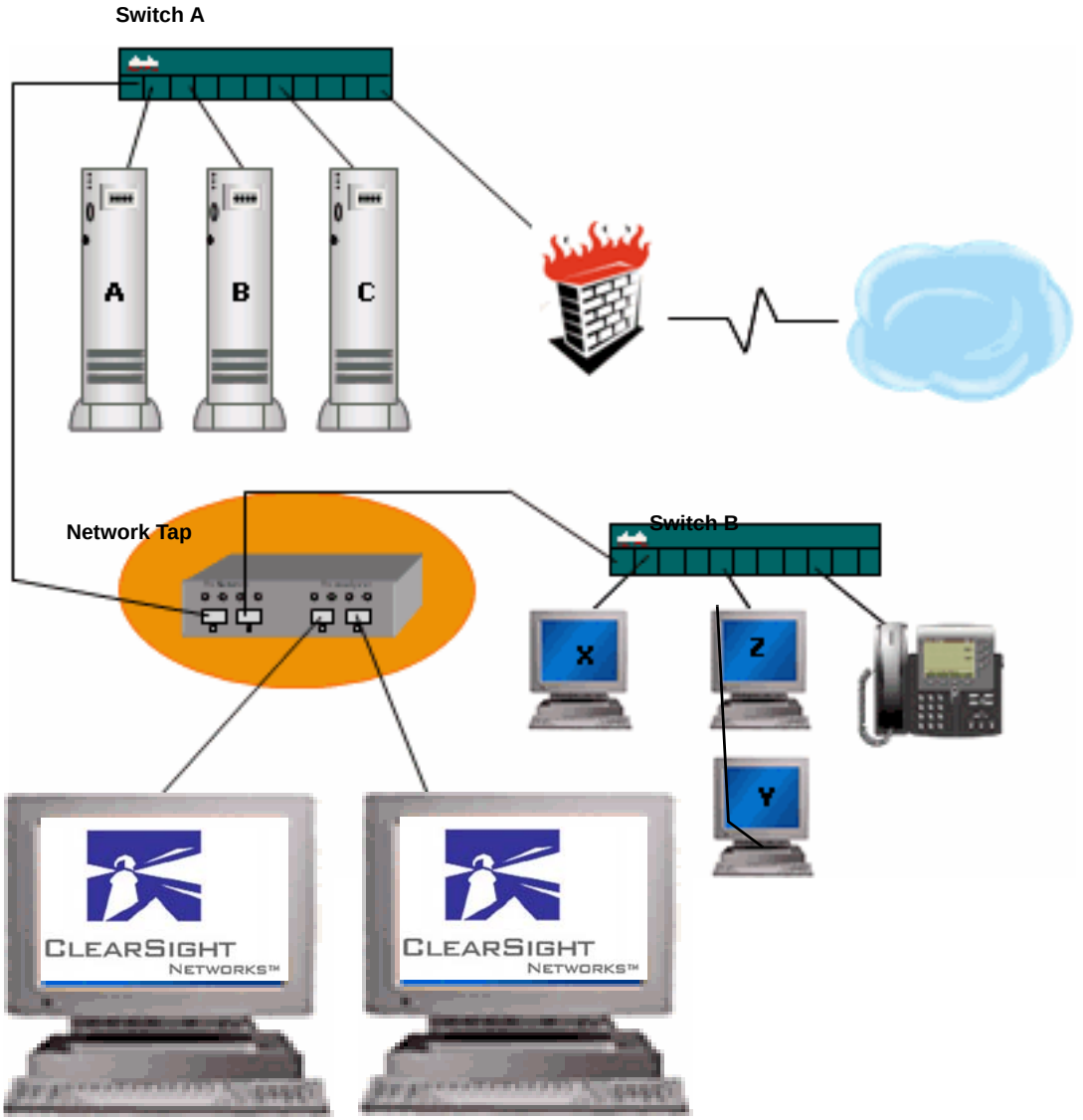


Figure 2-2: Inserting a Tap

Using Port Mirroring

Many switches support some form of *port mirroring* to allow network monitoring. Port mirroring lets you copy the traffic flowing over one or more ports on the switch to a designated monitor port (sometimes referred to as a "mirror port" or a "span port"). You can connect ClearSight to this monitor port to see the copied traffic.

Figure 2-3 shows one example of how port mirroring can be used to allow network monitoring and analysis. In this example:

- On **Switch A**, traffic sent and received on the switch-switch link with **Switch B** is mirrored to **Switch A**'s monitor port. ClearSight is connected to the monitor port.
- On **Switch B**, traffic sent and received on the ports for **Workstations X**, **Y**, and **Z** is mirrored to **Switch B**'s monitor port. ClearSight is connected to the monitor port.

Advantages and Disadvantages

Port mirroring has several key advantages over both hubs and network taps, including:

- Port mirroring lets you monitor or capture traffic from multiple switch ports instead of just a single port. Most implementations also let you copy all traffic for a particular VLAN to the monitor port, allowing quick analysis of a problematic configuration.
- With port mirroring, there is no hardware to install.

Port mirroring also has disadvantages. For example:

- Not all switches support port mirroring.
- Different switches implement port mirroring differently, requiring you to learn how to configure it on the switch.
- When used incorrectly, port mirroring can potentially cause a network loop.
- Port mirroring places a burden on the switch's processor and memory buffer. In extreme cases, port mirroring can potentially overtax the switch processor to the point where the switch reboots.

- The more ports mirrored, the more the switch must buffer data before sending it to the monitor port. This can affect the accuracy of delta times when measuring latency between commands and responses. It can also cause the switch to drop packets before sending them to the monitor port, resulting in false error messages in the analyzer.

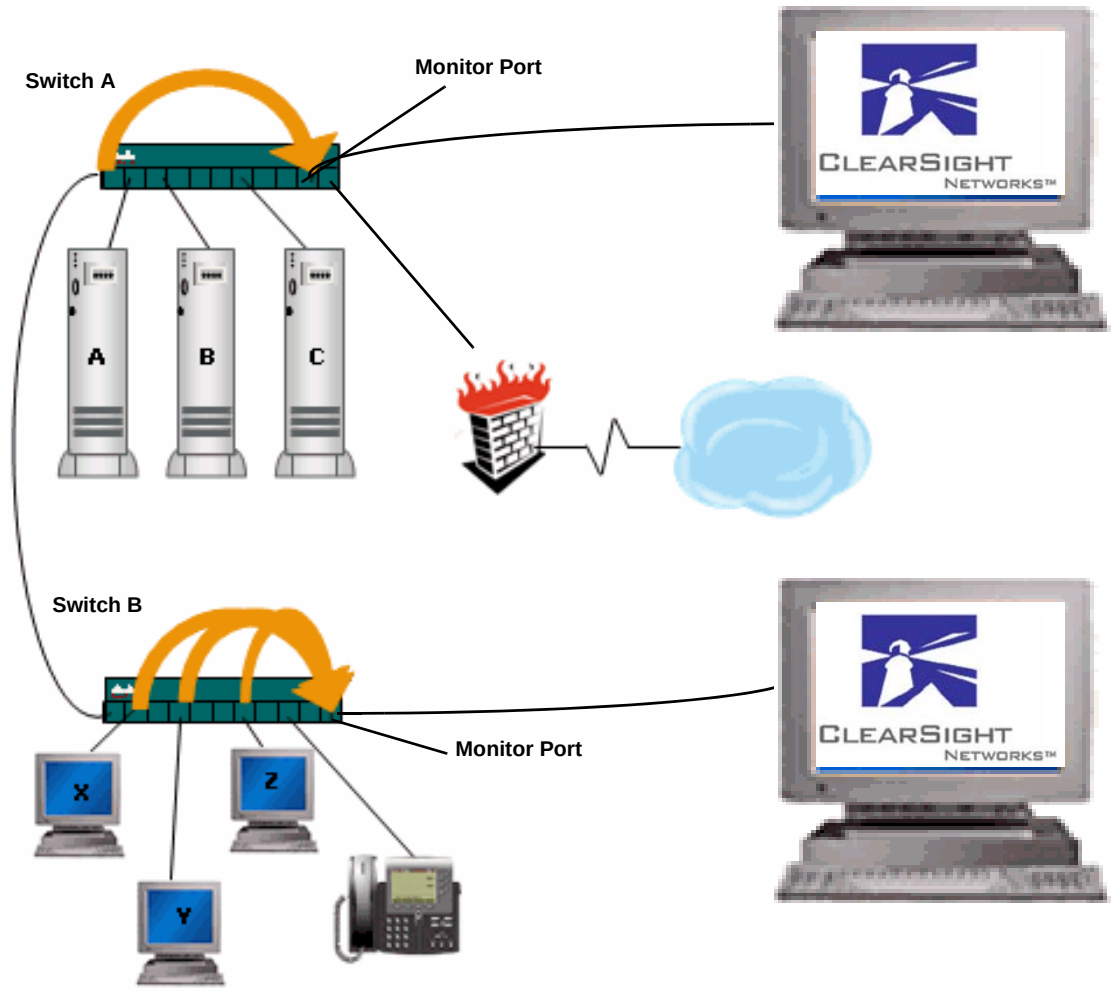


Figure 2-3: Using Port Mirroring

Connecting ClearSight Distributed Agents

When connecting a ClearSight Distributed Agent to the network, you can always use the same interface card for both Agent Viewer-Agent communications and network monitoring. However, if the ClearSight Distributed Agent PC has more than one NIC installed, you can use:

- One card in the Agent for Agent Viewer-Agent communications (the *communications card*).
- A second card for actual network monitoring (the *monitor card*).

Some of the benefits to this sort of implementation include:

- Increased monitoring and analysis performance. If the monitor card is not used for Agent Viewer-Agent communications, its resources are freed up for increased monitoring and capture performance.
- Preserving network monitoring abilities during times of network problems. Connecting the communications and monitor cards to different network segments lets you maintain the connection between the Agent Viewer and the Distributed Agent when the segment to which the monitor card is connected is experiencing problems — one of the times you need ClearSight's capabilities the most.

Figure 2-4 shows a sample Distributed Agent installation using two NICs.

In this example, the Agent Viewer communicates with the ClearSight Distributed Agent over LAN Segment 1 using the communications card. Meanwhile, the Distributed Agent monitors LAN Segment 2 using the monitor card. In this way, the Agent Viewer can still communicate with the Agent, even if LAN Segment 2 is experiencing problems.

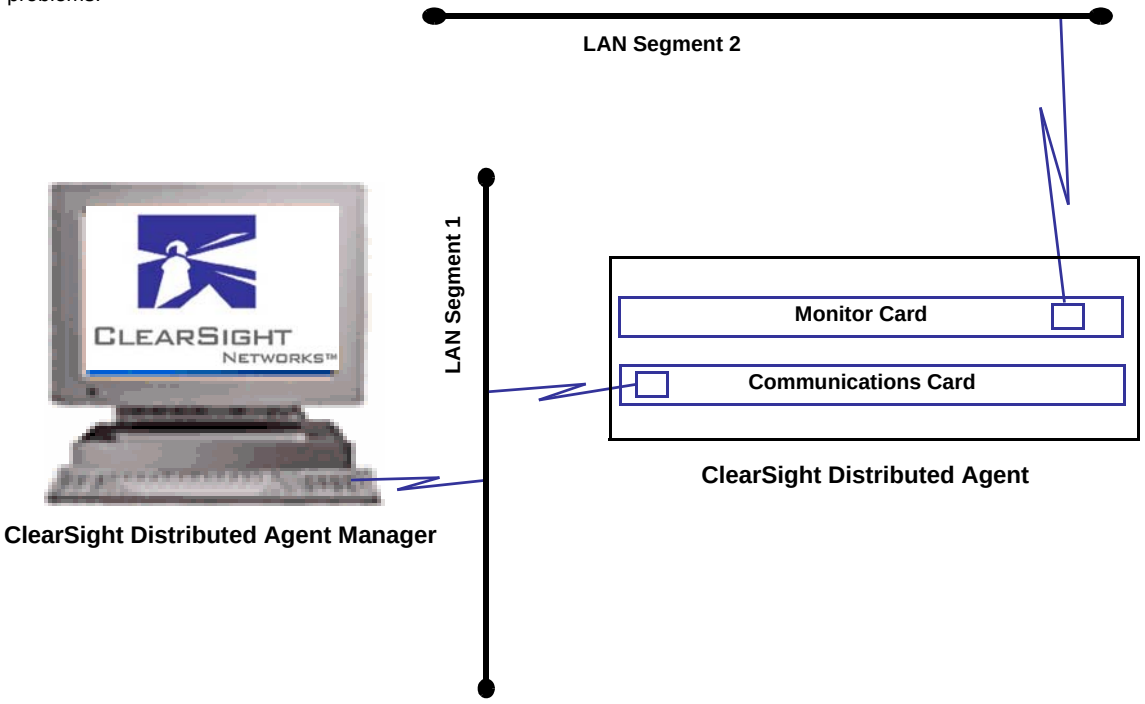


Figure 2-4: Using Two NICs on the Distributed Agent

Setting Up an Agent with Two Interface Cards

As shown in Figure 2-4, setting up an Agent to use two interface cards is relatively simple:

- When adding an Agent to the Agents List, set the **Hostname** field in the Add Agent dialog box to the IP address of the adapter on the Agent with which you want to communicate.

- When the Open Adapter dialog box appears (Figure 2-5), select an adapter to monitor other than the one you are using for Agent Viewer-Agent communications.

NOTE: Adding Agents to the Agents List, using the Open Adapter dialog box, and other ClearSight Distributed concepts are discussed in *Chapter 4, Using ClearSight Distributed*.

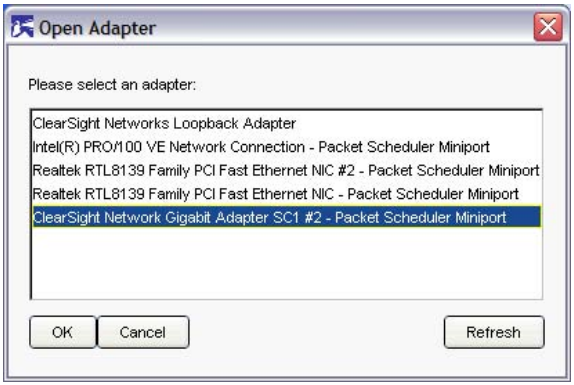


Figure 2-5: Open Adapter Dialog Box

Example — Using Two Interface Cards

In Figure 2-5 four adapters are listed in addition to the standard ClearSight Networks Loopback Adapter. Suppose that the **Realtek RT_8139 Family PCI Fast Ethernet NIC #2** adapter has the IP address of **192.168.1.100** and the **ClearSight Network Gigabit Adapter** has the IP address of **192.168.5.100**. In this example, you could:

- Add an Agent to the Agent List using the IP address of **192.168.1.100** in the **Hostname** field. This means that we will be using the **Realtek RT_8139 Family PCI Fast Ethernet NIC #2** adapter as the communications card.
- Connect to the Agent and select the **ClearSight Network Gigabit Adapter** in the Open Adapter list. This means that we will be using the **ClearSight Network Gigabit Adapter** as the monitor card.

Summary

To connect ClearSight to the network, you must take into account both the design of your network and the data you need to see for effective monitoring and analysis. In general:

- Hubs are most useful when you are interested in quick, easy, cost-effective solutions.
- Network taps are useful for simultaneous monitoring of both sides of a full duplex link. They can also be designed into a network from the outset of your network's implementation.
- Port mirroring is most useful when you need to see data from multiple switch ports or from a single VLAN.
- When connecting a ClearSight Distributed Agent, it can be advantageous to use two cards — a communications card and a monitor card. It can also be a good idea to connect these two cards to different network segments to preserve network communications during times of network problems on the segment being monitored.

Chapter 3

Introducing the ClearSight Analyzer

The ClearSight Analyzer software is a powerful network management tool that combines the features of a traditional network analyzer — network monitoring, packet capture, and protocol decodes — with powerful real-time application monitoring capabilities that let you see problems on your network as they occur.

This chapter covers the following major topics:

- *ClearSight Features*
- *New in CSA 7.0.7*
- *Available Models*
- *Basic Setup for ClearSight Standalone*
- *Setting Up a User List on the Standalone Analyzer*
- *Starting ClearSight Analyzer Standalone*
- *ClearSight User Interface*
- *How to Use ClearSight*

About Standalone and Distributed Features

The features described in this chapter are the same regardless of whether you are using ClearSight in its standalone configuration or connected to a ClearSight Distributed Agent. The major difference is:

- When working with a connected ClearSight Distributed Agent, you enter commands and view ClearSight displays from the Agent Viewer instead of on the local PC. See *Chapter 4, Using ClearSight Distributed* for details on using the Distributed version of ClearSight.

NOTE: CSD is not supported in CSA version 7.0.7.

ClearSight Features

The ClearSight Analyzer software monitors and analyzes the data flowing over the network segment to which it is connected. ClearSight learns about the various IP flows traversing the network, as well as the applications running over them, providing a wide variety of statistics, charts, and graphs that help you understand what is happening on your network. ClearSight provides the following major features:

- Real-time application monitoring focused on common IP-based network applications, including:
  - World-wide web (HTTP)
  - Email (SMTP, POP, and MS-Exchange)
  - Database (MS SQL and Oracle)
  - Voice-over-IP (H.323, SIP, Skinny, MGCP, and Megaco)
  - Streaming media (RTP and RTSP)
  - Security (Kerberos and ISAKMP)
  - Miscellaneous common network applications (DNS, FTP, SMB, Telnet, and Citrix)
- Real-time problem detection and notification for a wide variety of network issues.

- Packet capture and protocol decodes.
- Powerful postcapture analysis with enhanced application monitoring capabilities, allowing you to recreate application flows as seen by the user. For example, you can recreate web transactions, see emails, or even replay VoIP conversations over the ClearSight PC's speaker.
- Powerful filtering capabilities.
- Wide variety of customizable reports for network baselining, maintenance, and eventual expansion.

New in CSA 7.0.7

The following are major new features in CSA 7.0.7, relative to the previous CSA 7.0.6 product:

- **3G-324M Playback —** Media content for 3G-324M flows using AMR or MPEG4 codecs can now be played back.
- **Wireshark version 1.2.2 support—** Wireshark version 1.2.2 is now supported. See *Trace File Open Behavior* on page 238.

Available Models

Table 3-1 shows the available models of CSA 7.0.7.

Table 3-1: ClearSight Analyzer 7.0.7 Models

Platform	Model	Operating System
Regular PC	CSA with regular NIC	Windows XP SP2, Vista SP1/SP2
Dolch	CSA with 1 Gigabit XD adapter (SUS)	Windows XP SP2
	CSA with 10 Gigabit NT20 adapter (SUS)	

NOTE: CSD is not supported in CSA version 7.0.7.

Basic Setup for ClearSight Standalone

After you have installed ClearSight Standalone, you are ready to:

1. Set up a User List for the ClearSight Analyzer. The User List contains all users who are authorized to operate this program.
2. Start the ClearSight Standalone Analyzer.

Each of these topics is described below.

Setting Up a User List on the Standalone Analyzer

For security reasons, every ClearSight Analyzer maintains a list of users who can operate that analyzer. If a user attempts to log in without a valid username and password, the analyzer will not allow it.

IMPORTANT: ClearSight Analyzer Standalone is installed with the following default username and password:

Username **Admin**

Password **<empty string> (no password)**

Managing the User List

You manage the ClearSight's User List via the User Configuration utility, as described in the following procedure:

To set up a User List on a ClearSight Analyzer:

1. Start the User Configuration utility by going to **Start > (All) Programs > ClearSight > User Configuration**. The User Configuration Login dialog box (Figure 3-1) will appear.
2. Enter the default Username **Admin**, and click **OK**.

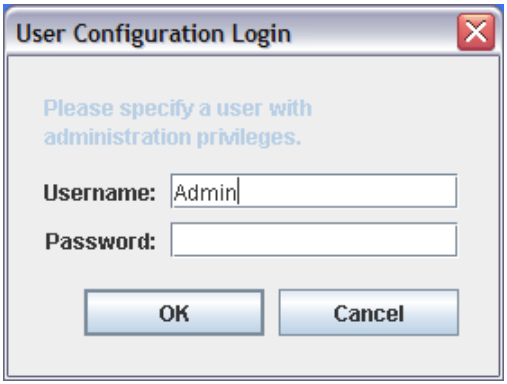


Figure 3-1: User Configuration Login Dialog Box

The **ClearSight User Configuration** utility appears (Figure 3-2). Initially, this window lists only the administrator (Admin) who has just logged in. If you are that administrator, you can add, edit, or remove users from the list using the corresponding buttons in this dialog box.

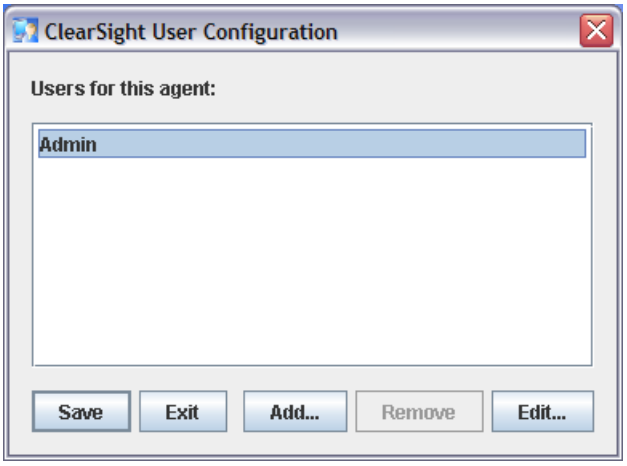


Figure 3-2: Initial Appearance of the User Configuration Utility

3. Note that Admin itself cannot be removed. If you are Admin, it is a good idea to choose a new password. To do so, click the **Edit** Button. The Edit User dialog box will appear (Figure 3-3). Simply type in the new password (twice) and click **OK**. The new password will take effect immediately, and you will return to the ClearSight User Configuration dialog box (Figure 3-2).

   NOTE: The function of the **Permissions** box will be discussed later.



Figure 3-3: Edit User Dialog Box for Admin

4. You can add other users to the user list. To do so, click the **Add** button. In response, the Add User dialog box appears, prompting you to supply the username and password (twice) for the new user. For example, if we add user David, the Add User dialog box will look like Figure 3-4.

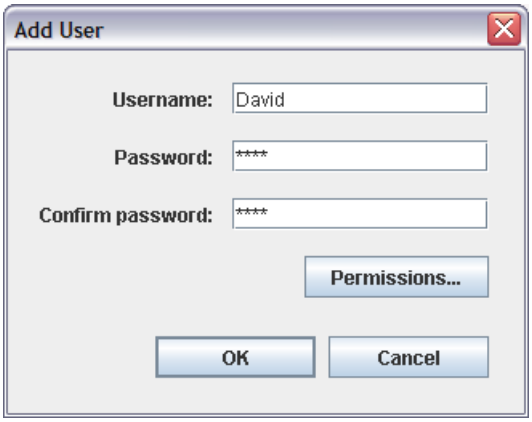


Figure 3-4: Add User Dialog Box for David

IMPORTANT: Be sure to remember the username/password combinations you add to the User List. You will need to supply the same usernames/passwords to those authorized users.

5. In addition to establishing the username and password for a new user, you can set that user's *permissions*. Click **Permissions**. The Permissions for user: David dialog box will appear (Figure 3-5).

   There are three types of permissions that you can grant:

   - **Administer User Settings** lets this user:

     - Create, edit, and remove other users.

     - Change settings on the **Configuration** page.

     NOTE: No one can remove Admin or disable any of Admin's permissions. However, any user with **Administer User Settings** enabled can change Admin's password.

   - **View Application Content** lets this user view the content (such as VoIP conversations and emails) of applications.



Figure 3-5: Permissions for User David Dialog Box

6. When you have set the permissions you want to give this user, click **OK**. You will return to the Add User dialog box. Click **OK** again. You will return to the ClearSight User Configuration dialog box, and your new user will appear in the list, as in Figure 3-6.

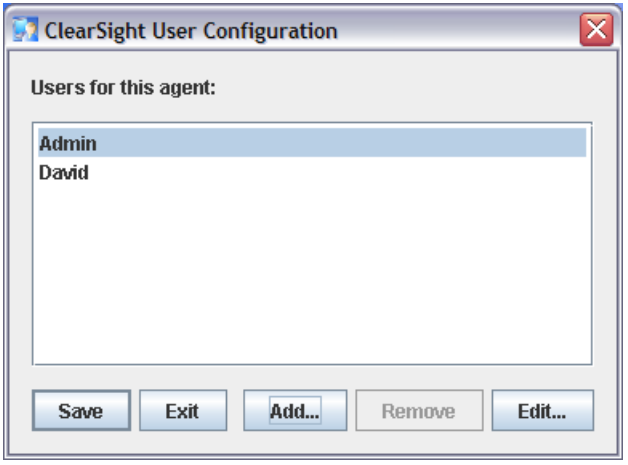


Figure 3-6: User List with David Added

7. When you have finished adding users to the list, click the **Save** button to save your changes.

   Most of the changes you have made will take effect immediately. However, if you have removed a user that is currently logged in, that user will be allowed to finish any currently active session.

Starting ClearSight Analyzer Standalone

1. Start ClearSight Analyzer Standalone by going to **Start > (All) Programs > ClearSight > ClearSight Analyzer**. The User Configuration Login dialog box (Figure 3-7) will appear.

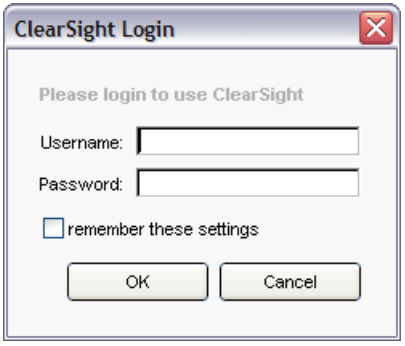


Figure 3-7: ClearSight Login Dialog Box

2. Enter a valid username and password, and click **OK**.
3. If this is the first time you have started the ClearSight Analyzer, the Open Adapter dialog box (Figure 3-8) will appear.

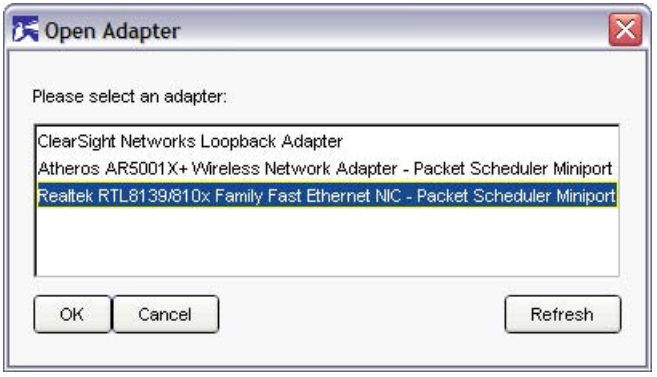


Figure 3-8: Open Adapter Dialog Box

4. Select the network adapter you want to use, and click **OK**.
5. The ClearSight user interface (Figure 3-9) will appear.

ClearSight User Interface

As shown in Figure 3-9, ClearSight's user interface has several key components:

- The *toolbar* provides you easy access to ClearSight's main features — the real-time monitor, alert log, reports, and so on. *ClearSight Toolbar* on page 74 provides details on each of the buttons in the toolbar.
- The *main workspace* updates according to the feature currently selected in the toolbar. When you first start ClearSight, the Monitor feature is selected; its button is highlighted in the toolbar. Accordingly, the workspace shows the real-time Monitor interface.
- The *menus* provide you with access to additional ClearSight commands, including those used to open and save trace files, change the currently selected adapter, reset the Monitor's counters, start and stop capture, access the online help files, and so on. In general, the buttons in the toolbar provide access to the features you will use most of the time; the menus provide access to additional complementary functions.

In addition to these main components, ClearSight provides valuable information in its *title bar* and *caption bar*:

- The *title bar* indicates the adapter ClearSight is currently monitoring.
- The *caption bar* (the bar at the bottom of the display) indicates:
  - The amount of time the current monitoring session has been in progress (**Duration**).
  - The date and time ClearSight started gathering monitoring statistics (**Start Time**).
  - A real-time **Network Activity** LED that provides a quick indication of the amount of network traffic ClearSight is seeing.
  - The **Gigabit Link Status** LED provides status if you have the ClearSight Gigabit Ethernet card selected. Red indicates the link is down; green indicates the link is up and active.

ClearSight's menus — **File**, **Capture**, **Monitor**, **Tools**, and **Help** — let you open and save trace files, switch adapters, start and stop capture, reset monitor statistics, perform trace route, and access the online help files.

ClearSight's toolbar provides access to its most commonly used features and options. When you first start ClearSight, the **Monitor** feature is selected. Its entry is highlighted in the toolbar.



The main workspace shows the interface for the feature currently selected in the toolbar. In this case, the real-time **Monitor** feature is selected. Accordingly, the Application Monitoring Summary appears, providing you with a broad view of the overall health of the applications running over your network, as well as the network layer connections and physical statistics underlying them. From here, you can access more detailed displays by clicking on a particular entry in the display.

In general, you can always navigate the ClearSight user interface by clicking on an entry in the display. If a particular entry in the display can be clicked, the mouse cursor turns into a pointing hand, indicating that you can click on the entry to see more detailed statistics and analysis.

Figure 3-9: ClearSight User Interface

ClearSight Toolbar

Figure 3-10 shows the ClearSight toolbar. The toolbar provides you easy access to ClearSight's most commonly used features.

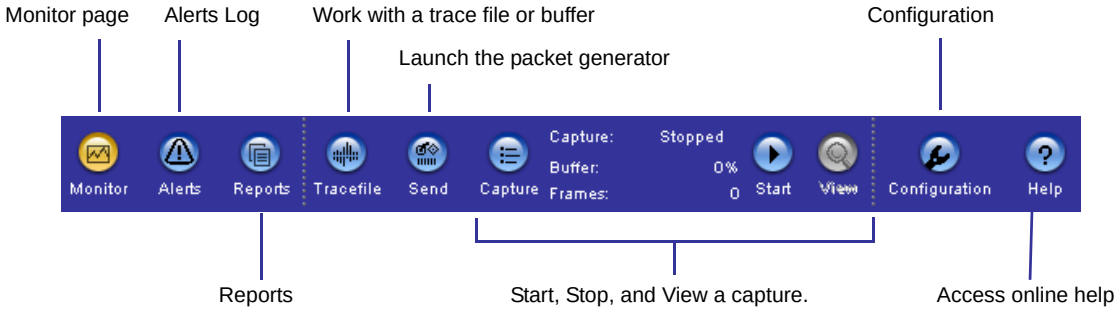


Figure 3-10: ClearSight Toolbar

As shown in Figure 3-10, the ClearSight toolbar provides the following buttons:

Monitor — Click this button to display the real-time monitoring interface. Real-time monitoring is described in Chapter 5, *Monitoring the Network with ClearSight*.

Alerts — Click this button to display the Alert Log. Working with Alerts is described in Chapter 10, *Working with Alerts*.

Reports — Click this button to view reports on the data gathered by the monitor. Reports are described in Chapter 12, *Using Reports*.

Tracefile — Click this button to work with saved trace files in the postcapture analysis pages. Postcapture analysis of trace files and buffers is described in Chapter 7, *Postcapture Analysis*.

Send — Click this button to launch the embedded packet generator (if present). The packet generator is described in Chapter 13, *Using the Packet Generator*.

Capture	Click this button to set up a capture session. Capturing data is described in Chapter 6, *Capturing Data with ClearSight*.
Start\Stop	Click this button to start and stop a capture session. Capturing data is described in Chapter 6, *Capturing Data with ClearSight*.
View	Click this button to perform postcapture analysis of the data currently in the capture buffer. Postcapture analysis is described in Chapter 7, *Postcapture Analysis*.
Configuration	Click this button to access pages that let you work with ClearSight configuration options, including those for filters (Chapter 9, *Using Filters*), alerts (Chapter 10, *Working with Alerts*), the Address Book (Chapter 11, *Using the Address Book*), and so on.
Help	Click this button to access ClearSight's online help system.

How to Use ClearSight

Although you can use ClearSight in whatever way makes the most sense for your particular network, all approaches will use some of the following *phases*:

- *Real-Time Monitoring*
- *Packet Capture*
- *Postcapture Analysis*

Figure 3-12 illustrates these phases. In addition, the sections that follow suggest one methodology for using ClearSight to monitor, manage, and troubleshoot your network.

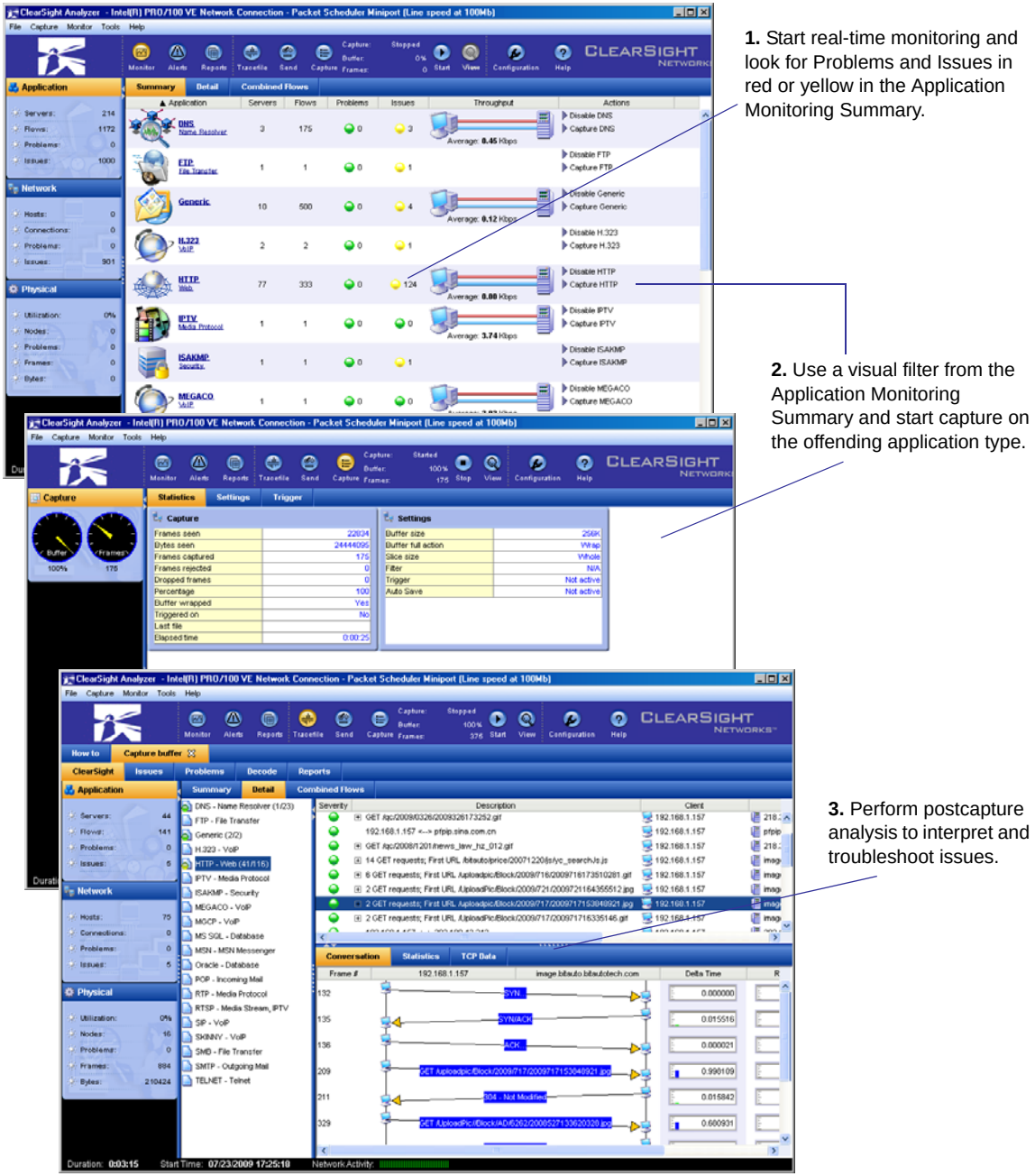


Figure 3-11: Network Analysis with ClearSight – One Approach

Real-Time Monitoring

ClearSight starts monitoring the network as soon as you start the application, updating its displays with statistics and information related to the network layer connections and *application flows* on the network. An *application flow* is a set of packets that performs a specific function, such as a **Get** or a **Post** on a web server, sending or receiving an email message, resolving a domain name, or making a phone call. Depending on the nature of the transaction, flows can consist of as little as 5 packets or as many as 200.

During monitoring, ClearSight does not save data to the capture buffer. Instead, ClearSight gathers statistics and alerts you to problems and issues on the network, allowing you to start a capture when you are more sure of what you want to look at.

Using Real-Time Monitor Displays

During real-time monitoring, pay attention to the **Problems** and **Issues** counters in the Application Monitoring Summary. If these counters start to increment and turn yellow, orange, or red, you have an indication of a possible problem with the corresponding application flow or network layer connection. In this situation, you can start a capture focused on the offending application.

You should also pay attention to the **Charts** and **Hosts** tabs at the **Network** layer. These tabs can give you a quick overview of which protocols are consuming the most bandwidth on your network and point you to the responsible nodes. Network problems often originate from bandwidth-intensive streaming media applications (for example, private use of SIP calls) or the misuse of Web access. ClearSight points you directly to the offending user(s) so you can take corrective action.

Packet Capture

Once ClearSight's real-time application monitoring has alerted you to potential issues on the network, you can start a capture to zoom in on the data behind the problem. During capture, ClearSight provides the same statistics as it does during real-time monitoring. However, during capture, the analyzer stores the captured packets in a capture buffer for later analysis. You can specify how large this buffer is, how much of each frame is captured, and what ClearSight should do when the buffer becomes full.

In addition, you can set filters to focus your capture on just the frames that interest you. For example, you can set filters directly from the Application Monitoring Summary that focus a capture on a single offending application type (HTTP, VoIP, RTP, and so on). This way, you can make sure that you capture only the frames necessary to solve your problem and avoid filling up the buffer with frames that do not interest you.

Postcapture Analysis

After capture, ClearSight provides powerful postcapture analysis capabilities for the packets in the capture buffer, helping you zero in quickly and precisely on the frames displaying problems.

Start in the same screen as you would for real-time monitoring — the Application Monitoring Summary. The Application Monitoring Summary's graphical interface speeds you to potential bottlenecks, problems, and issues. Scan the Summary for yellow or red entries in the **Problems** and **Issues** columns. Click these entries to access detailed statistical displays for problematic flows or connections. In response, ClearSight rebuilds the request and reply exchanges between a client and server and visually displays them in a network ladder diagram (Figure 3-12).

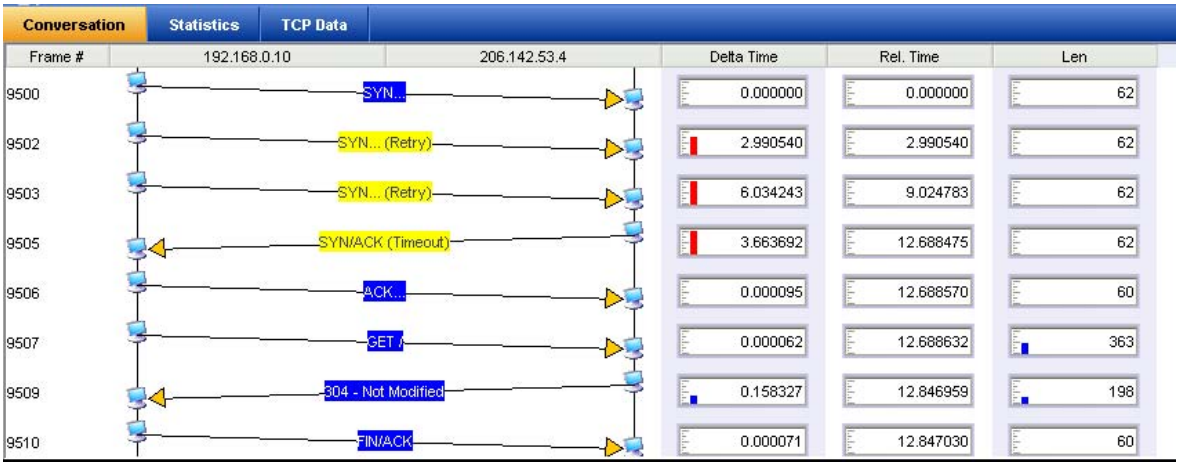


Figure 3-12: Sample Network Ladder Diagram

Within this diagram, the exact request or reply displaying the problem is shown in either yellow or red, depending on the severity of the problem. For example, Figure 3-12 shows that a GET request to an HTTP server had to be retried. From here, you can click on the offending request or response to go directly to the protocol decode for the exact offending frame in the exact selected flow. This way, ClearSight takes the work out of protocol analysis — it shows you the problematic frames and takes you straight to a protocol decode filtered specifically for the flow containing the frame, with the offending frame selected.

In addition to network ladder diagrams reconstructing the request\reply exchanges making up a flow, ClearSight's postcapture detail displays provide application-specific features that show you how a problematic flow appeared to the user. For example, you can:

- Replay VoIP conversations over the PC speaker.
- Re-attempt problematic HTTP requests within the ClearSight interface.
- View email messages as seen by the user.
- View database requests as made by the user.
- View Telnet sessions as seen by the terminal user.

The exact features available depend on the type of application flow you are analyzing. Chapter 5, *Monitoring the Network with ClearSight* describes the features available for each application type.

Chapter 4

Using ClearSight Distributed

This chapter introduces the ClearSight Distributed system, describes its main components, and explains how to use ClearSight features specific to the Distributed version of the product. The chapter includes the following major topics:

- *The ClearSight Distributed System*
- *Getting Started with ClearSight Distributed*
- *Setting Up a User List on an Agent*
- *Using the Agent Manager*
- *Other CSD-Specific Features*

The ClearSight Distributed System

The ClearSight Distributed system consists of a **ClearSight Distributed Agent Manager** connecting to and controlling one or more **ClearSight Distributed Agents**.

- The **ClearSight Distributed Agent Manager** manages the Agents in the ClearSight Distributed system. From an **Agent Manager** window, you can connect to multiple Agents, opening separate **ClearSight Agent Viewer** windows for each connected Agent. In

addition, the **Agent Manager** provides centralized alarm management capabilities in its **Central Problem Manager**.

- **ClearSight Distributed Agents** monitor and analyze the local network segment to which they are connected, sending the results of their analysis as screen updates to the ClearSight Agent Viewer.

  Once you are connected to a Distributed Agent from the Distributed Agent Manager, you interact with the Distributed Agent just as if you were sitting at its keyboard entering commands and analyzing traffic. This way, you can receive all of the real-time application monitoring and analysis capabilities available in the standalone version of ClearSight from a remote location.

- When working with a connected ClearSight Distributed Agent, you enter commands and view ClearSight displays from the Agent Viewer instead of on the Agent's local PC.

Figure 4-1 shows a simple ClearSight Distributed system.

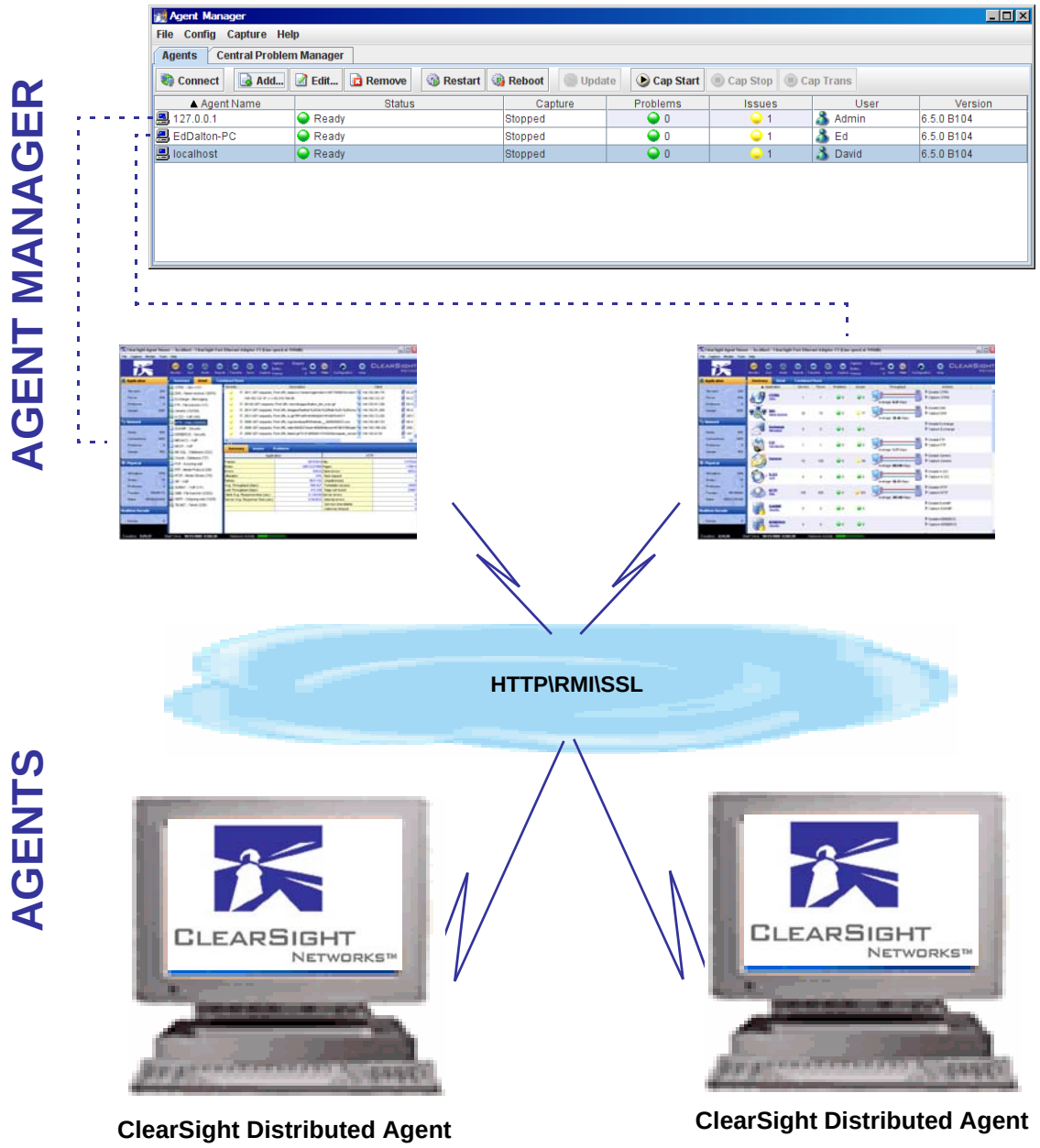


Figure 4-1: ClearSight Distributed System

About ClearSight Distributed Communications

During installation of the ClearSight Distributed Agent software, Setup automatically:

- **Binds the ClearSight kernel** to all available network interface cards on the Agent PC. The ClearSight kernel enables the Agent to monitor and capture from the network.
- **Installs the ClearSight Server service** and configures it to start automatically at system startup. The ClearSight Server service listens for connections from the Agent Viewer. Once a successful connection is established, the Agent begins sending network monitoring and analysis data back to the Agent Viewer for display.

As shown in Figure 4-1, ClearSight Agent Viewers communicate with ClearSight Distributed Agents using HTTP and Java RMI. Optionally, this communication can use HTTP and Java RMI over SSL for secure transfer of data.

Getting Started with ClearSight Distributed

After you have installed the ClearSight Distributed Agent Manager and at least one Distributed Agent, you are ready to:

1. Set up a User List on each Distributed Agent. The User List contains all users who are authorized to connect to the Agent from a Viewer.
2. Start the ClearSight Distributed Agent Manager and add Agents to the Agents List in the Agent Manager.
3. Connect to Agents from the **Agents** tab in the Agent Manager.
4. Configure and manage system-wide Problem reporting in the **Central Problem Manager** tab.

Each of these topics is described below.

Setting Up a User List on an Agent

For security reasons, every ClearSight Distributed Agent maintains a list of users who can connect to the Agent. If an Agent Viewer user attempts to log in without a valid username and password, the Agent will reject the connection.

IMPORTANT: ClearSight Distributed Agents are installed with the following default username and password:

Username **Admin**

Password **<empty string> (no password)**

Managing the Agent's User List

You manage the ClearSight Distributed Agent's User List via the User Configuration utility, as described in the following procedure:

To set up a User List on a Distributed Agent:

1. On the computer on which the Agent is installed, start the User Configuration utility on that Agent by going to **Start > (All) Programs > ClearSight Distributed > User Configuration**. The User Configuration Login dialog box (Figure 4-2) will appear.
2. Enter the default Username **Admin**, and click **OK**.

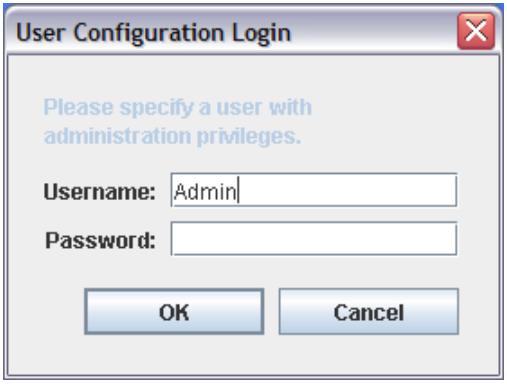


Figure 4-2: User Configuration Login Dialog Box

The **ClearSight User Configuration** utility appears (Figure 4-3). Initially, this window lists only the administrator (Admin) who has just logged in. If you are that administrator, you can add, edit, or remove users from the list using the corresponding buttons in this dialog box.

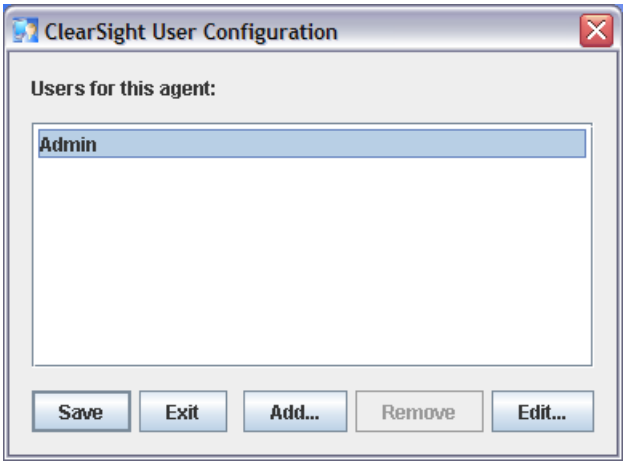


Figure 4-3: Initial Appearance of the User Configuration Utility

3. Note that Admin itself cannot be removed. If you are Admin, it is a good idea to choose a new password. To do so, click the **Edit** Button. The Edit User dialog box will appear (Figure 4-4). Simply type in the new password (twice) and click **OK**. The new password will take effect immediately, and you will return to the ClearSight User Configuration dialog box (Figure 4-3).

   NOTE: The function of the **Permissions** box will be discussed later.

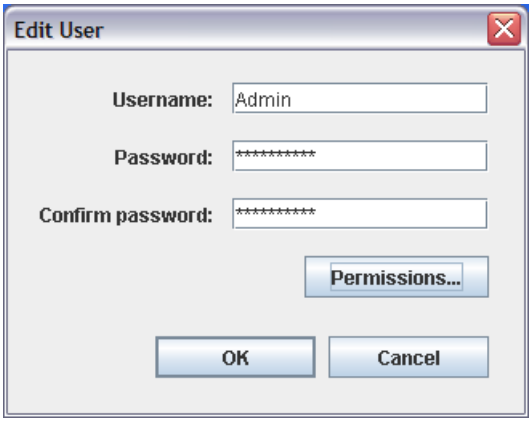


Figure 4-4: Edit User Dialog Box for Admin

4. You can add other users to the user list. To do so, click the **Add** button. In response, the Add User dialog box appears, prompting you to supply the username and password (twice) for the new user. For example, if we add user David, the Add User dialog box will look like Figure 4-5.

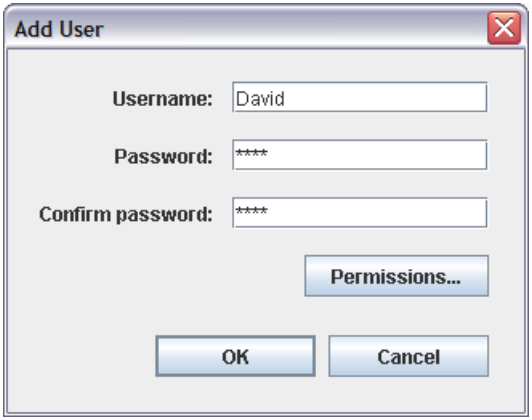


Figure 4-5: Add User Dialog Box for David

IMPORTANT: Be sure to remember the username/password combinations you add to the User List. A user must supply a valid username/password in the ClearSight Distributed Agent Manager when adding this Agent to the Agents List.

5. In addition to establishing the username and password for a new user, you can set that user's *permissions*. Click **Permissions**. The Permissions for user: David dialog box will appear (Figure 4-6).

   There are three types of permissions that you can grant:

   - **Administer User Settings** lets this user:

     - Create, edit, and remove other users.

     - Switch adapters, restart and reboot agents.

     - Change settings on the **Configuration** page.

     - Exit into modes other than Unattended mode.

     NOTE: No one can remove Admin or disable any of Admin's permissions. However, any user with **Administer User Settings** enabled can change Admin's password.

   - **View Application Content** lets this user view the content (such as VoIP conversations and emails) of applications.

   - **Start/Stop/View Capture** lets this user Start, Stop, and View captures on this Agent.



Figure 4-6: Permissions for User David Dialog Box

6. When you have set the permissions you want to give this user, click **OK**. You will return to the Add User dialog box. Click **OK** again. You will return to the ClearSight User Configuration dialog box, and your new user will appear in the list, as in Figure 4-7.

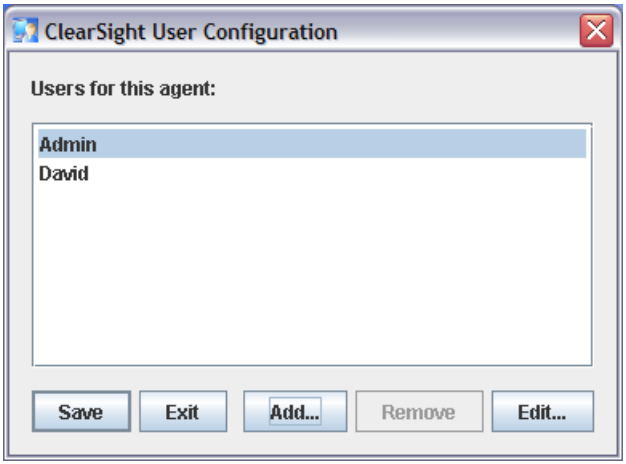


Figure 4-7: User List with David Added

7. When you have finished adding users to the list, click the **Save** button to save your changes.

   Most of the changes you have made will take effect immediately. However, if you have removed a user that is currently logged in, that user will be allowed to finish any currently active session.

Using the Agent Manager

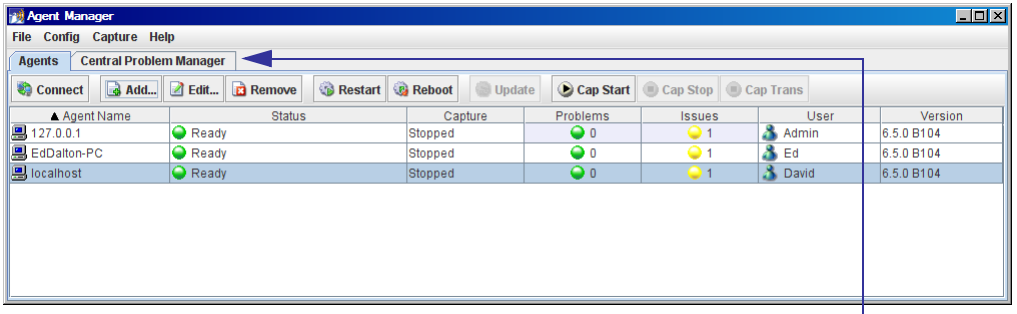
Use the Agent Manager as a "home base" to:

- Manage ClearSight Distributed Agents in the **Agents** tab (page 93).
- Connect to ClearSight Distributed Agents (page 97).
- Manage Problems reported by ClearSight Distributed Agents in the **Central Problem Manager** tab (page 101).
- Copy configuration data from one Agent to one or more others (page 105).

Start the ClearSight Distributed Agent Manager by selecting **Start > (All) Programs > ClearSight Distributed > ClearSight Distributed Agent Manager**. The Agent Manager window (Figure 4-8) appears.

The Agents List shows each of the Distributed Agents you have added to the Agent Manager. Each Agent is listed with its **Agent Name**, **Status**, **Capture** Status, **Problems** and **Issues** detected, the **User** configured to connect to the Agent, and the software **Version** installed on that Agent.

You can connect to an Agent either by double-clicking its entry in the list or by selecting the Agent and clicking the Connect button. If connection is successful, a ClearSight Agent Viewer window will open in which you can work with the Distributed Agent just as if you were sitting at its keyboard.



You can click the **Central Problem Manager** tab to view a consolidated log of Problems reported to this Agent Manager from Distributed Agents. For effective centralized Problem reporting and management, you must configure each Agent to send its Problems to this Agent Manager.

Figure 4-8: The Agent Monitor

Managing Distributed Agents in the Agent Manager

You manage ClearSight Distributed Agents in the Agent Manager's **Agents** tab (also known as the *Agents List)*. As shown in Figure 4-8, the Agents List shows each of the ClearSight Distributed Agents you have added to the Agent Manager. From here, you can use the buttons in the command bar to:

- **Add**, **Edit**, and **Remove** Distributed Agents.
- **Connect** to Distributed Agents.
- **Restart** the Agent service for one or more Agents.
- **Reboot** the computers on which one or more Agents are installed.
- **Update** the software on an Agent.
- **Start** and **Stop** capture on an Agent, or on multiple Agents simultaneously.

Each of these tasks is described below.

Adding Agents to the Agents List

Add an Agent to the Agents List by clicking the **Add** button in the Agent Manager. In response, the Add Agent dialog box appears (Figure 4-9).

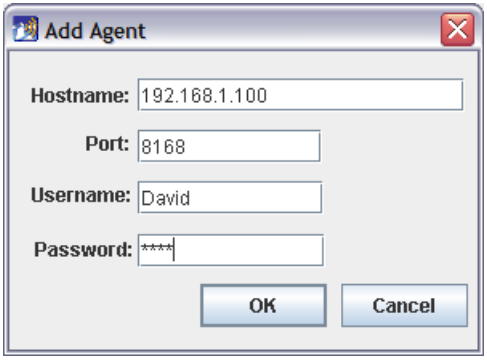


Figure 4-9: The Add Agent Dialog Box

Set the fields in the Add Agent dialog box as follows:

Hostname Enter either a resolvable hostname or an IP address for the Distributed Agent.

NOTE: ClearSight Distributed Agent Manager will connect to this Distributed Agent using the hostname or IP address you specify here. If you are adding a Distributed Agent with two interface cards (one to be used for Agent Viewer communications and one for network monitoring and analysis), you should enter the address of the card to be used for Agent Viewer communications here. See *Connecting ClearSight Distributed Agents* on page 59 for details on this sort of configuration.

Port The default port for Distributed Agent connections is 8168. Under normal circumstances, you should not need to change this setting unless instructed to do so by a Technical Support Representative.

Username Enter the username to be used for connections to this Distributed Agent.

Password Enter the password to be used for connections to this Distributed Agent

IMPORTANT: The **Username** and **Password** you specify here must match a username and password in the User List on the Agent. See *Setting Up a User List on an Agent* on page 87 for details on how to add users to the User List on the Agent.

Once you have finished filling out the fields in the Add Agent dialog box, click **OK** to add the Agent to the list.

What Happens After Adding an Agent to the Agent List

After you click **OK** in the Add Agent dialog box to add an Agent to the Agent List, ClearSight Distributed Agent Manager attempts to connect to the Agent to determine its status. This is not a full-fledged connection attempt. Instead, ClearSight Distributed Agent Manager verifies:

- The ClearSight service is up and running on the Agent machine.
- Whether any other users are logged into the Agent from other Agent Viewers.
- The version of the ClearSight software on the Distributed Agent.

This information is reported in the Agents List for each Agent (shown in Figure 4-8 and detailed in Table 4-1).

Fields for an Agent in the Agents List

Table 4-1 lists and describes the fields provided for each Agent in the Agents List.

Table 4-1: Fields for an Agent in the Agents List

Field	Description
Agent Name	The hostname or IP address of that Agent.
Status	The last status reported for that Agent. This field can report a variety of messages indicating: • Whether that Agent is up, running, and ready for connections. • Whether a user is connected to that Agent and, if so, the Username used for that connection. • Whether that Agent is in Unattended or Ready Mode, which is necessary for starting a capture. • Whether there are any communication errors with that Agent.

Table 4-1: Fields for an Agent in the Agents List

Field	Description
Capture	The current capture status for that Agent. Possible values are Starting, Started, Start Failed, Stopping, Stopped, and Stop Failed. This column can also be blank (when no capture is running and the Agent is not otherwise connected).
Problems	The current problem count for that Agent and the maximum problem severity. This field is sortable but sorts by count only - not the maximum severity.
Issues	The current issue count for that Agent and the maximum issue severity. This field is sortable but sorts by count only - not the maximum severity.
User	The Username configured for connections to that Agent.
Version	The version of the ClearSight software installed on that Agent.

NOTE: In addition to ClearSight Distributed Agents, the Agent Manager can connect to and control Network Time Machine (NTM) Agents via NTM Agent Viewer windows. If any such NTM Agents appear in the Agents List, they will be identified by **(NTM)** in the **Status** column and **NTM** in the **Version** column.

Editing an Agent in the Agents List

You can edit the information for an Agent in the Agents List by selecting that Agent, and then clicking the **Edit** button. In response, the Edit Agent dialog box appears. This dialog box looks exactly like the Add Agent dialog box (Figure 4-9) except that the title bar says Edit Agent. Make the changes you want, and click **OK**.

Removing Agents from the Agents List

You can remove one or more Agents from the Agents list by selecting those Agents, and then clicking the **Remove** button.

Connecting to Agents in the Agents List

Once you have added a Distributed Agent to the Agents list, you can connect to it in either of the following ways:

- Double-clicking its entry in the Agents List
- Selecting the Agent in the list and clicking the **Connect** button.

In either case, the result is the same — ClearSight attempts to connect to the IP address or hostname specified in the Agents List. If connection is successful, ClearSight displays the Open Adapter dialog box (Figure 4-10).

NOTE: If the Distributed Agent to which you are connecting already has a connected user, you will be asked if you want to take over the existing session. If you click **Yes**, the other user will be disconnected and you will take control of the Agent.

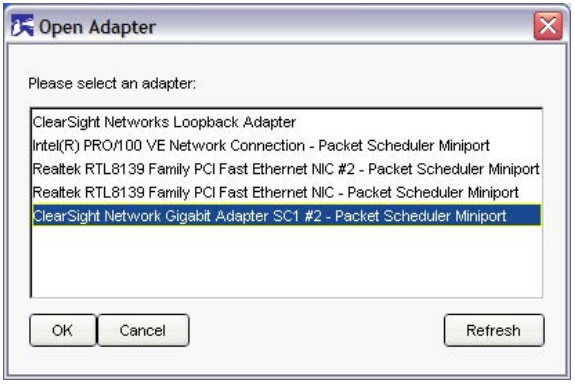


Figure 4-10: Open Adapter Dialog Box

The Open Adapter dialog box lets you select the adapter you want that Agent to monitor. It lists each of the network interface cards on the Agent that have the ClearSight kernel bound. By default, this

includes all of the NICs that were installed in the Agent PC when the Agent software was installed.

Select the adapter you want ClearSight to monitor and click **OK** to continue. In response, a ClearSight Agent Viewer window will open, in which you can work with the standard ClearSight Analyzer functions just as you would with a standalone version of the software.

Disconnecting a Connected Agent

You disconnect a connected Agent either by closing its ClearSight Agent Viewer window or by selecting the **File > Exit** command. When you disconnect a connected Agent, ClearSight displays the dialog box shown in Figure 4-11.



Figure 4-11: Disconnecting an Agent Session

This dialog box gives you the option of letting the Agent continue to monitor your network:

- If you click **Yes**, the Agent continues to monitor your network, updating its counters and statistics. In addition, detected Problems are still reported to the Agent Manager's Central Problem Manager as configured on the Agent. When you reconnect to the Agent from the Distributed Agent Manager, the statistics shown in ClearSight's displays are valid from the beginning of monitoring, not just from the start of this new connection.
- If you click **No**, the Agent stops monitoring the network and waits for a new connection to be initiated from the Distributed Agent Manager.

Rebooting Agents in the Agents List

You can reboot a Distributed Agent from the Agents List by selecting its entry and clicking the **Reboot** button.

Updating the Software on an Agent

This feature allows an Agent Manager to remotely update the software on an Agent to a later version.

The appropriate files must first be present on the Agent Manager's computer. Then the remote update can be initiated by selecting the desired Agent in the Agents List, and clicking the **Update** button.

NOTE: The **Update** button will be grayed out (function not available) unless the software version on the Agent is earlier than the current version available on the Agent Manager's computer.

Starting and Stopping Capture

You can use the **Cap Start** and **Cap Stop** buttons to start and stop capture on an Agent or on multiple Agents simultaneously.

If you want to start or stop capture on more than one Agent, use ctrl-click to select them.

Agents selected for starting a capture must be in Unattended or Ready mode as displayed in the **Status** column of the Agent Manager. Agents that are connected to a viewer must be disconnected before a capture can be started. To put an active viewer into Unattended mode, simply close the Viewer Window, and then click **Yes** in the Confirm dialog box (Figure 4-11 on page 98). The Agent will enter unattended mode *using the network adapter selected during the previous connection.*

NOTE: Users without **Administer User Settings** permission can exit only into Unattended Mode. They will not be prompted by the Confirm dialog box.

When the **Cap Start** button is pressed a capture operation will be automatically started on all currently selected Agents - providing they are in the appropriate state (Unattended or Ready mode) and the configured user has capture permission (see Figure 4-6 on page 90).

The **Capture** status column will change value to indicate the capture status of any Agent. It will switch to **Started** once capture has started — via this feature or any other way.

The **Cap Stop** button lets the user stop capture on one or more Agents for which capture has been started. Again, the configured user must have capture permission and the Agent must be in the **Started** capture state for the stop to be successful.

NOTE: The following special conditions will prevent an Agent from starting the capture:

- The Agent has been newly installed and has not yet been connected by any viewer. In such a state there is no defined adapter card from which to capture. The capture will fail with an appropriate error message.
- Another capture is already taking place on that Agent, either via an Agent Viewer or another Agent Manager, or in unattended mode. An appropriate error message will be displayed.
- The Agent is in the process of restarting.

Saving an Agent's Capture Buffer to a Trace File

If capture has successfully stopped, and one or more packets are contained in the Agent's capture buffer, then the **Cap Trans** button will be enabled, and the Capture column will read **Stopped (has buffer)**. Clicking the **Cap Trans** button will display the "Save tracefile from agent" dialog box (Figure 4-12).

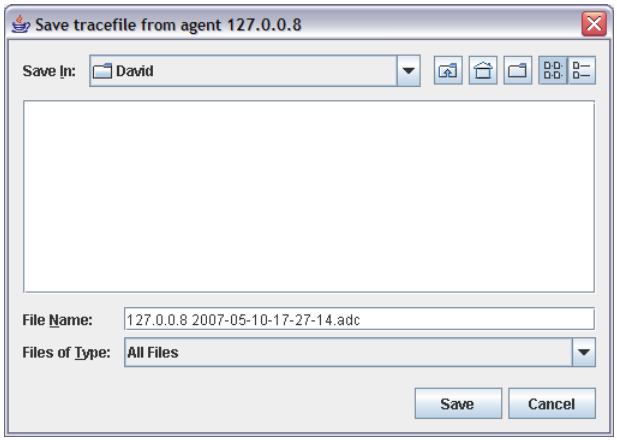


Figure 4-12: The Save Tracefile from Agent Dialog Box

Browse to a location of your choice. Choose a suitable file name and click **Save**. The file will be transferred from the Agent. You can follow the status of the transfer via the **Status** column of the Agent Manager.

Using the Central Problem Manager

Agent Manager's **Central Problem Manager** tab (Figure 4-13) provides a consolidated log of *Problems* sent to it from Distributed Agents. Problems are network error conditions detected by Distributed Agents.

Setting up effective centralized problem reporting from Agents to the Central Problem Manager consists of the following major steps:

- Enable problem generation and set problem thresholds and severities on the Agent in the **Configuration > Preferences > Problem > Thresholds** page. See Chapter 10, *Working with Alerts* for more information on setting thresholds and severities for problems.
- Specify an Agent Manager as a destination for problem reports in each Distributed Agent's **Configuration > Preferences > Problem > Central Alarm** option. Once you have specified an Agent Manager as a destination for Problem reports, all enabled Problems on the Agent will be reported to the Agent Manager

and listed in the **Central Problem Manager** tab. See *Configuring Agents to Report Problems* on page 104 for details.

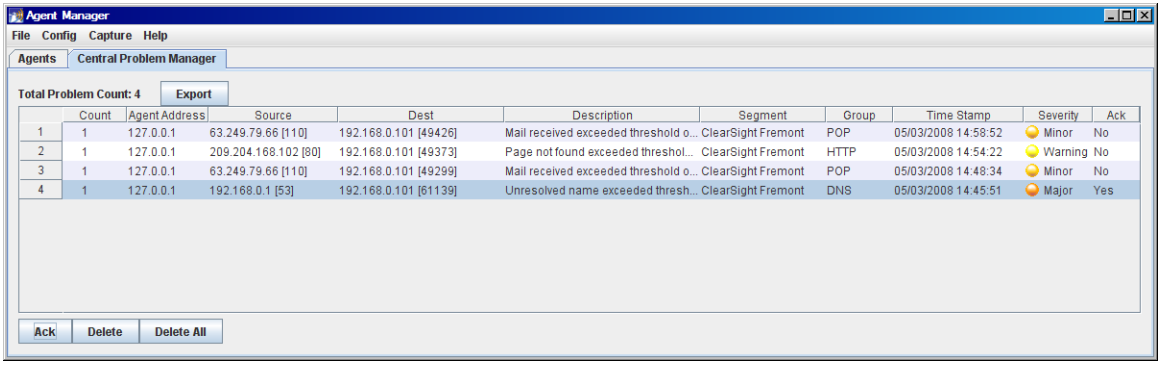


Figure 4-13: The Central Problem Manager Tab

Fields in the Central Problem Manager

The **Central Problem Manager** tab lists problems reported by ClearSight Distributed Agents with the following fields:

Count	The number of similar type problems grouped together.
Agent Address	The IP address of the Distributed Agent reporting this problem.
Source	The IP address of the source station for this problem.
Dest	The IP address of the destination station for this problem.
Description	A short description of the problem.
Segment	The network segment on which the problem was detected.
Group	The network segment on which the problem was detected.
Time Stamp	The time the problem was detected.
Severity	A color-coded icon indicating the severity of the problem.
Ack	Whether or not this problem has been acknowledged. You can acknowledge problems you have already dealt with by selecting them and clicking the **Ack** button. This way, you can sort the Central Problem Manager quickly to view only those problems you have not yet dealt with.

You can sort the **Central Problem Manager** tab by each parameter type by clicking in the corresponding column heading; click again to reverse the order. A triangle icon appears in the column heading of the parameter by which the pane is currently sorted.

Use the **Ack** button to acknowledge problems; use the **Delete** button to remove them from the display. Clicking the **Delete All** button removes all problems from the display.

You can save the Problems list to a CSV file by selecting **Save Problems As...** from the **File** menu.

Configuring Agents to Report Problems

You configure Distributed Agents to send Problems to a Central Problem Manager by clicking the **Configuration > Preferences > Problem > Central Alarm** option (Figure 4-14). Then, specify the following information:

Host to Send — The hostname or IP address to which you want this Agent to report Problems — either the ClearSight Distributed Agent Manager or a standard SNMP Traps server.

Community — The SNMP Community string (if sending to an SNMP Traps server).

Segment — The name of the network segment you would like the Central Problem Manager to display in the Segment field for problems reported by this Agent. If blank, the Agent will send the name of the adapter card reporting the problem.

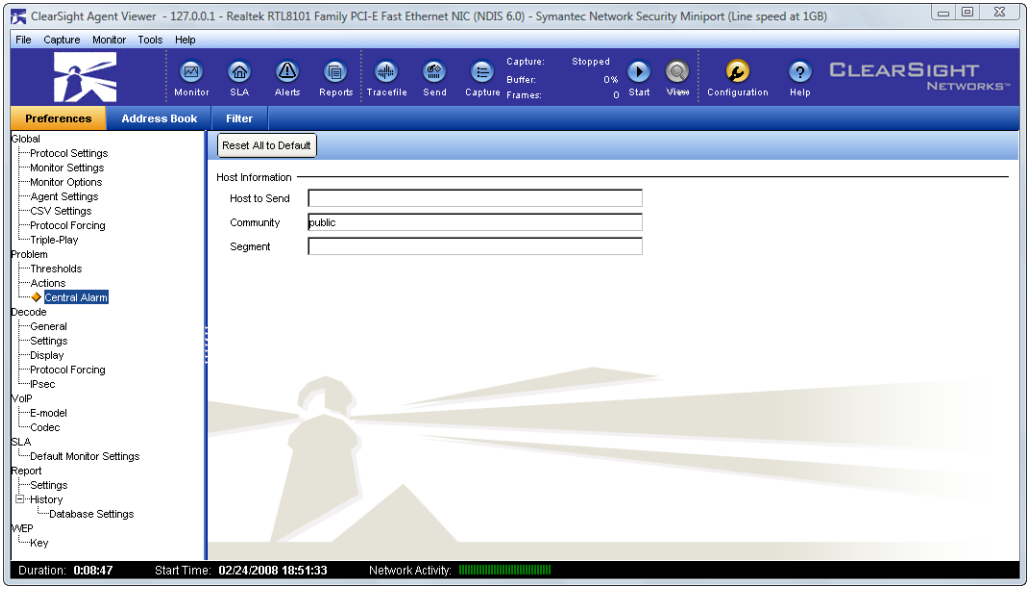


Figure 4-14: Configuring an Agent to Report Problems

Copying Configuration Data

You can copy the configuration data from any given Agent to one or more others. To do this, use the options in the **Config** menu (Figure 4-15).

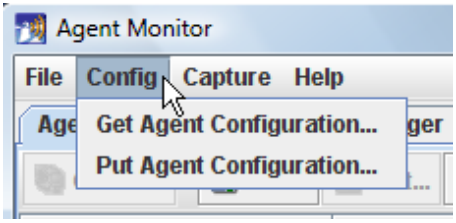


Figure 4-15: The Config Menu

Get Agent Configuration

This menu item lets you upload the configuration of the currently selected Agent to the console PC. When you select **Get Agent Configuration**, the Get CFG dialog box (Figure 4-16) will appear. If you click **Yes** the configuration of the selected Agent will be uploaded. While it is being uploaded, appropriate status information will be displayed in the **Status** column of the selected Agent.

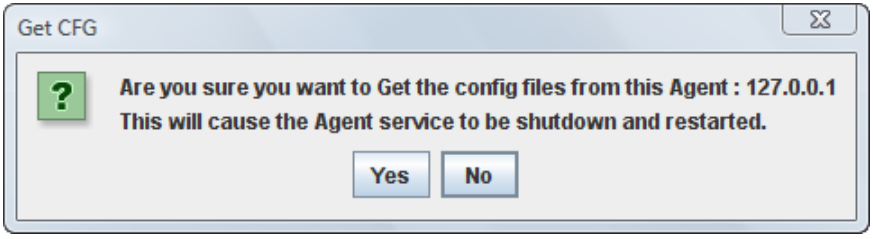


Figure 4-16: The Get CFG Dialog Box

Put Agent Configuration

This menu item lets you download the previously uploaded Agent configuration to one or more target Agents. The target Agents must be selected in the **Agent** tab before this option is selected.

When you select **Put Agent Configuration**, the Put CFG dialog box (Figure 4-17) will appear. If you click **Yes** the previously uploaded

configuration will be sent to the Agents currently selected in the **Agents** tab. As the configuration is sent to each Agent its status column will be updated to indicate progress.

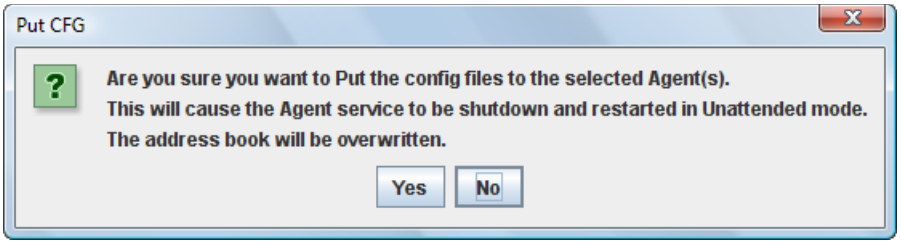


Figure 4-17: The Put CFG Dialog Box

Configuration Merging

Configuration files sent to a target agent are generally copied "as is" to the target agent, replacing any previously existing configuration. However, certain settings related to network cards are merged using the criteria described below.

NOTE: The existence of general.xml or interfaces.xml is controlled by the Agents' history — if the Agent has been run since installation these files will exist.

Adapter Settings in Interfaces.xml

If the destination Agent does not have an **interfaces.xml** file the new one will be copied as-is. If the destination Agent does have a previous **interfaces.xml**, then a merge operation will take place. The merge operation modifies the previously existing **interfaces.xml** file. All interfaces in the new **interfaces.xml** file will be checked against the previously existing **interfaces.xml** file. Interfaces that match by name (not case sensitive) will be copied along with their associated settings to the existing **interfaces.xml** file - replacing the previous settings for that adapter. No new interfaces will be copied from the selected adapter setting in **general.xml**.

If **general.xml** does not exist on the target Agent, then the new **general.xml** is copied "as is" to the target — including any selected adapter setting. If **general.xml** does exist, then the selected adapter

setting is copied only if the specified adapter exists in the target Agents' **interfaces.xml**.

Other CSD-Specific Features

ClearSight Distributed (CSD) includes all of the features of the standalone ClearSight Analyzer (CSA) plus the following CSD-specific features:

- *Secure Socket Layer (SSL) Option*
- *Windows Security Manager Option*

Secure Socket Layer (SSL) Option

This feature allows you to use Java RMI over SSL. To activate this feature, check the **Use SSL for data between Agent and Viewer** check box in **Configuration > Preferences > Global > Agent Settings > Communication**. (see Figure 4-18).

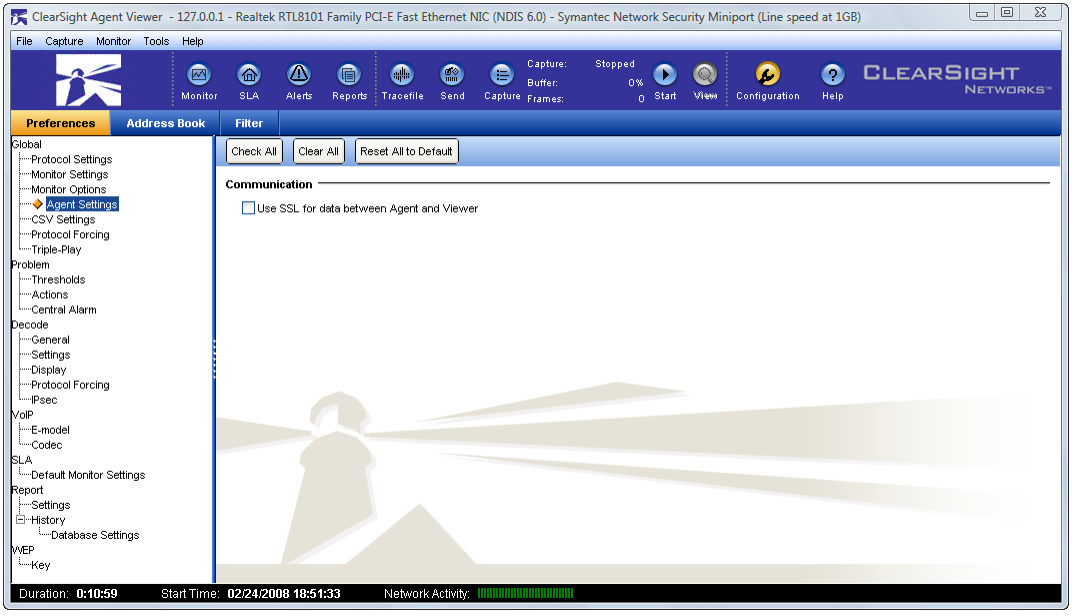


Figure 4-18: Choosing to Use SSL for Data Between Agent and Viewer

Windows Security Manager Option

CSD gives you the option of using a Microsoft Windows Security Server instead of ClearSight's own user security implementation. If you want to do this, use the following structure:

- Make sure that all the Agents are in the same Windows Domain.
- Create these User Groups:

  - Group 1: ClearSightUsersGroup: these users can log into ClearSight.

  - Group 2: ClearSightContentViewGroup: these users can view application content — equivalent to the **View Application Content** permission in the ClearSight User Configuration (see Figure 4-6).

  - Group 3: ClearSightCaptureGroup: these users can start and stop capture, and view captured traffic — equivalent to the **Start/Stop/View Capture** permission in the ClearSight User Configuration (see Figure 4-6).

  - Group4: ClearSightAdminGroup: these users can perform software updates (see *Updating the Software on an Agent* on page 99).
- Assign users to Group 1 if you want to allow them to log into ClearSight. Also assign users to either or both of the other groups according to the permissions you want them to have.

To switch from ClearSight's default user security to Windows User security, navigate to your ClearSight Distributed installation directory and rename the Windows_ActiveUserSecurityManager.txt file to ActiveUserSecurityManager.txt.

To switch from Windows User security back to ClearSight's default user security, rename ActiveUserSecurityManager.txt back to Windows_ActiveUserSecurityManager.txt.

NOTE: This file renaming procedure must be done on both the Manager PC and the Agent PC. Be sure that both the Manager and the Agent are stopped before renaming these files.

Chapter 5

Monitoring the Network with ClearSight

This chapter describes how to use ClearSight's real-time network monitoring features. It includes the following major topics:

- *Working with Real-Time Monitor Displays*
- *Application Layer Monitoring*
- *Network Layer Monitoring*
- *Physical Layer Monitoring*
- *Configuring the ClearSight Analyzer*

Working with Real-Time Monitor Displays

When you first start ClearSight, the Application Monitoring Summary screen appears, providing you with easy access to all of ClearSight's functionality (Figure 5-1). The Application Monitoring Summary screen is a valuable "home base" for network analysis and troubleshooting with ClearSight. It provides you with immediate feedback on the health of the applications running over your network, alerting you to potential issues and problems in real time. From here, you can access ClearSight's more detailed displays for the

various application flows, as well as the network connections and physical layer statistics underlying them.



Figure 5-1: The Application Monitoring Summary

Choosing Which Applications to Display

You can select which applications you want to see displayed on the Summary tab. If you right-click anywhere on the Summary tab, you will see a pop-up button that reads either:



When you click on Show All Applications, ClearSight displays all of the applications that it is able to monitor. When you click on Show Active Applications Only, ClearSight displays only those

applications for which it has detected traffic during the current session. You can toggle between these two situations.

In addition, you can disable applications individually. For example, you can click on Disable HTTP to stop monitoring HTTP traffic. If you have selected Show Active Applications Only, the HTTP line will simply disappear from the Summary tab. If you have selected Show All Applications, the HTTP icon will display as follows:



To restore monitoring of HTTP traffic, simply click on Enable HTTP .

If, however, you have selected Show Active Applications Only, there will be no HTTP line on the screen. In that case, right-click anywhere on the Summary tab, and you will see a modified button that contains an Enable HTTP option. For example:



Then simply click on HTTP to resume monitoring of HTTP traffic.

Understanding and Navigating the ClearSight Workspace

ClearSight's real-time monitoring workspace is organized in a flexible, intuitive set of panes. Figure 5-2 on page 114 shows a sample ClearSight display.

ClearSight's workspace consists of the following types of panes:

- The **Layers pane** is found at the left side of the display. The Layers pane contains three separate layers — **Application**, **Network**, and **Physical**. For each layer, there are counters showing the data ClearSight is currently tracking — the number of servers, flows, hosts, connections, problems, issues, and so on.

  Clicking on a numerical entry in the Layers pane displays more detailed statistics about that entry in the Main pane.

  NOTE: ClearSight's three network layers are described in more detail in *ClearSight's Model of the Network* on page 117.

- The **Main** pane shows detailed information about the currently selected entry in the Layers pane. The displays available in the main pane vary greatly depending on what is selected in the Layers pane. However, the general rules for working with these panes are the same:

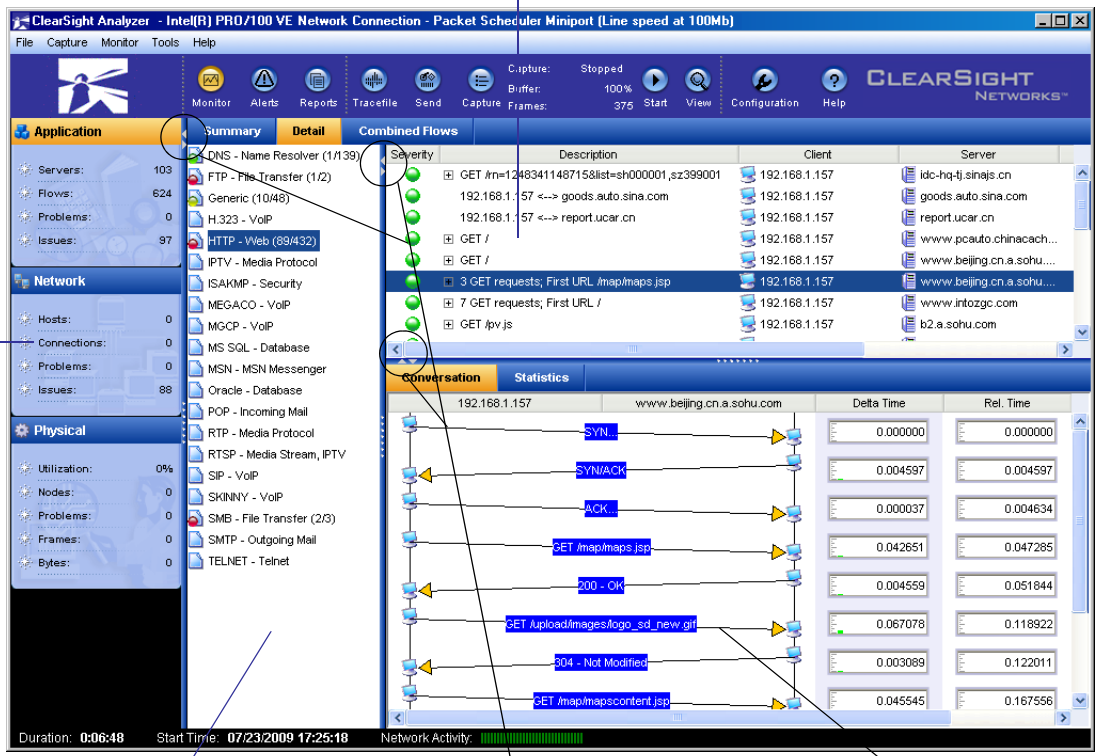
  - The main pane is often divided into multiple sub-panes. In these cases, selecting an entry in one pane typically causes more detailed information about the selected entry to appear in an adjacent pane. Figure 5-2 shows a main pane divided into several sub-panes.
  - In many cases, the displays in the main pane are *tabbed* — different tabs at the top of a display let you select different data to view. For example, in Figure 5-2, the Detail pane includes two tabs — **Conversation** and **Statistics**.
  - You can usually find more detailed information about an entry in the ClearSight display by clicking on it. This is also referred to as "drilling down." To return to a less detailed display, use the entries in the Layers pane to return to summary or overview information.
  - When you click on a **Problems** or **Issues** counter in the Layers pane, ClearSight's **Alerts** display for the selected layer

appears. Alerts are described in detail in Chapter 10, *Working with Alerts*. You can return to the Monitor display by clicking the **Monitor** button in the toolbar.

The best way to learn the ClearSight user interface is by trying it. As ClearSight learns about your network and its data, click each of the items in the user interface to see what statistics are shown.

The **Layers pane** shows the data ClearSight is currently tracking at each of three network layers — **Application**, **Network**, and **Physical**. Click an entry in the Layers pane to select what displays in the Main pane.

A **Flows** pane. Selecting an item here causes the **Statistics** pane below it to update with related details. For example, a problematic flow is selected in the **Flows** pane; the **Statistics** pane shows the exact problematic error message highlighted in color.



A **Statistics** pane showing details on the entry selected in the **Flows** pane. Notice that this pane is *tabbed* — it includes both a **Conversation** and a **Statistics** tab. Many ClearSight displays are tabbed, letting you view extensive statistics about a selected server, flow, connection, node, and so on.

The **Main** pane updates according to the entry selected in the Layers pane.

The Main pane displays vary considerably but usually include multiple panes that work together to show data on whatever entity you select. In this example, the **Main** pane includes three separate sub-panes — Application, Flows, and Statistics.

Note that you can collapse panes in which you are not interested, by using these toggles.

Figure 5-2: Common Panes in the Real-Time Monitor

About the Use of Color in ClearSight Displays

ClearSight's displays use color to guide you intuitively to problems detected by the analyzer. Color works exactly as one would expect:

- Red buttons indicate problems that require immediate attention.
- Orange buttons indicate potential problems you might want to look at.
- Yellow buttons indicate minor errors.
- Green buttons indicate healthy functions.

  NOTE: When you see a red button in ClearSight, click it to find out what is going wrong.

Color Coding for Alert Levels

In addition, color coding corresponds to different alert levels in the Alert Log as follows:

- **Critical** — Red
- **Major** — Orange
- **Minor** — Orange
- **Warning** — Yellow
- **Informational** — Yellow

Chapter 10, *Working with Alerts* describes how to assign different alert levels to different alarms, as well as how to associate different actions with alerts of a given level.

ClearSight Terminology

When you start the ClearSight Analyzer software, it immediately begins to detect and track the various Application layer *flows* on your network. In addition, ClearSight uses real-time analysis to alert you to *problems* and *issues*. These terms are defined as follows:

- **Flow —** A *flow* is a set of packets that performs a specific application layer function, such as a **Get** or a **Post** on a web server, sending or receiving an email message, resolving a domain name, or making a phone call. Depending on the nature of the transaction, flows can consist of as little as 5 packets or as many as 200.
- **Issue —** An *issue* is a minor error condition detected on the network. A single issue does not necessarily need to be investigated. However, multiple recurrences of an issue warrant further investigation. In addition, issues can be useful when troubleshooting a **Problem** detected by ClearSight for the same server, flow, connection, or node.

  A typical issue might be something as simple as a **404 - Not Found** error received by an HTTP client.
- **Problem —** A *problem* is a serious error condition that merits immediate investigation. An example of a problem on the network is a duplicate IP address — a condition that can cause degraded or unpredictable network performance.

ClearSight's Model of the Network

ClearSight's real-time monitoring displays track network activity by *layer*. ClearSight uses a three-layer model of the network adapted from the OSI seven-layer model. The three layers are Application, Network, and Physical:

- At the **Application** layer, ClearSight tracks end-to-end performance for common network applications, including email, database, VoIP, media, and file transfer applications. For each application, ClearSight detects and lists individual flows between application clients and servers, providing detailed statistics monitoring the performance of the application.

  Application layer monitor displays are described in *Application Layer Monitoring* on page 119.

- At the **Network** layer, ClearSight tracks the OSI layer three and layer four hosts and connections underlying the application flows displayed at the Application layer. It also tracks TCP/IP communications, including related protocols such as UDP, ARP, and ICMP.

  Network layer monitor displays are described in *Network Layer Monitoring* on page 168.

- At the **Physical** layer, ClearSight provides statistics describing the actual transmission of network data, including counts for various frame and error types (broadcasts, multicasts, CRC errors, and so on). In addition, the Physical layer displays track VLANs.

  Physical layer monitor displays are described in *Physical Layer Monitoring* on page 180.

ClearSight's Model and the OSI Model

ClearSight's three-layer model of the network simplifies network analysis since you are typically most interested in either application performance or the performance of the connections underlying the applications. For example, distinctions between Presentation layer services and Session layer services are not always meaningful for real-world network analysis. Table 5-1 shows how the seven layers of the OSI model map to ClearSight's three layers.

Table 5-1: How OSI Layers Map to ClearSight Layers

OSI Layers	ClearSight Layers
Application	Application
Presentation	
Session	
Transport	Network
Network	
Data Link	Physical
Physical	

Application Layer Monitoring

This section describes how to use ClearSight's Application Monitoring capabilities. The section includes the following major topics:

- A broad discussion of Application Monitoring (*About Application Monitoring*, below).
- How to access ClearSight's Application Monitoring Detail displays (*Viewing Application Monitoring Detail Displays* on page 120).
- How to navigate and work with ClearSight's Application Monitoring Detail displays (*Working with Application Monitoring Detail Displays* on page 120).
- Specific information on the Detail displays for each supported application type (*Application Monitoring Detail Displays* on page 131).

About Application Monitoring

ClearSight provides detailed real-time analysis for many important network applications, including database applications such as Oracle and MS SQL, email applications such as POP and SMTP, VoIP applications such as H.323 and Skinny, and many more. For each supported application type, ClearSight detects servers and flows, providing real-time analysis and statistics that enable you to troubleshoot network problems as they occur. You can view information for a specific server, for a specific flow, or for an application type as a whole.

For each detected flow, ClearSight rebuilds and displays the interactions and transactions between a client and server using a network ladder diagram and including the associated delta and relative timing. For some application flows (HTTP, email, and FTP among them), ClearSight even rebuilds the content flow as the end user sees it. This helps you detect unauthorized application access, abnormal data patterns, and application level errors.

Viewing Application Monitoring Detail Displays

For each supported application type, ClearSight tracks **Servers**, **Flows**, **Problems**, **Issues**, and **Throughput** in the Application Monitoring Summary (Figure 5-1 on page 110). From the Application Monitoring Summary, you can access Application Monitoring Detail displays for each application, server, and flow.

Access an Application Monitoring Detail display by:

- Clicking either the **Servers** or **Flows** entries at the Application layer in the Layers pane.
- Clicking an entry in the **Application**, **Servers**, or **Flows** columns in the Application Monitoring Summary.

Figure 5-3 on page 121 shows a sample Application Monitoring Detail display.

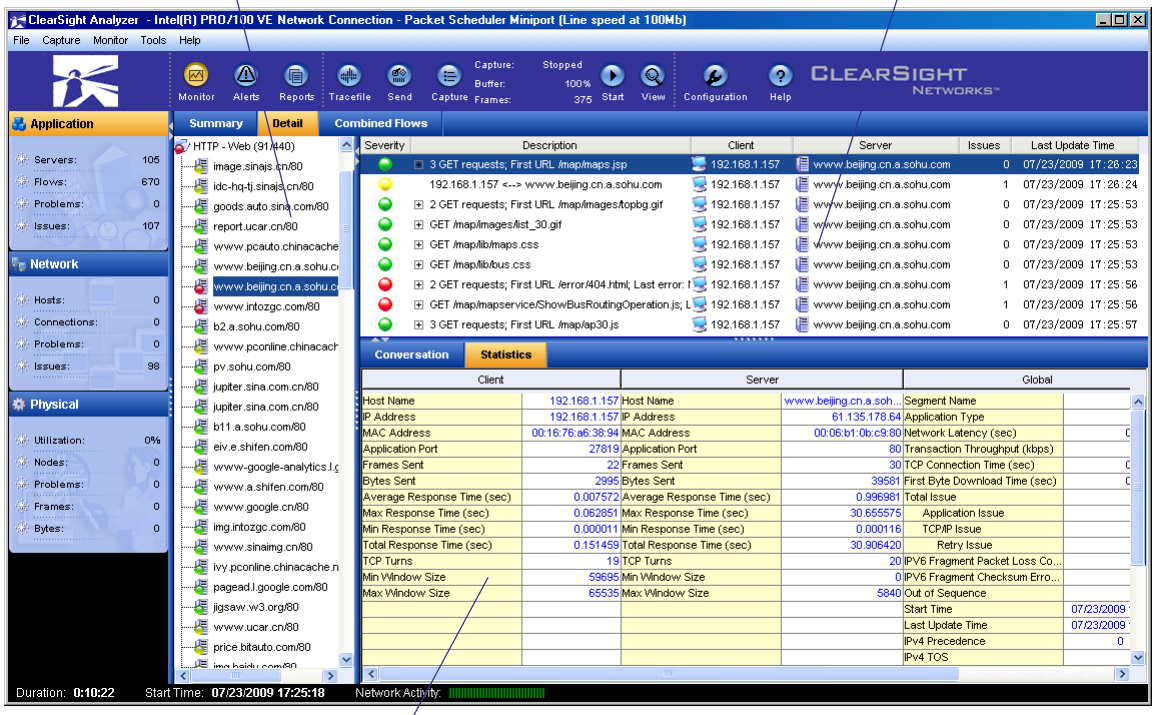
Working with Application Monitoring Detail Displays

As shown in Figure 5-3, Application Monitoring Detail displays consist of the following panes:

- The **Applications** pane lists each supported application type. Each application entry can be cascaded open to show the servers of the corresponding application type ClearSight has detected. You can select either an individual server or an application type as a whole to view corresponding statistics in the **Flows** and **Statistics** panes.
- The **Flows** pane lists each detected flow for the application type or server selected in the Applications pane. If an application type is selected, the Flows pane shows all detected flows for that application type. Similarly, if an individual server is selected, the Flows pane shows only the flows for that server.
- The **Statistics** pane shows detailed information on the application, server, or flow selected in either the Applications or Flows pane. You control what appears in the Statistics pane by the entry you select in the other two panes.

Applications Pane
The Applications pane lists each supported application type. Entries with a button in their icon can be cascaded open to show detected servers; the number in parentheses indicates how many servers/flows have been detected. The color of the button indicates the highest alert level detected on a server of the corresponding application type.

Flows Pane
The Flows pane lists each detected flow for the server or application type selected in the Applications pane.



Statistics Pane
The Statistics pane provides detailed statistics for either the application type or server selected in the Applications pane or the flow selected in the Flows pane.

Figure 5-3: Application Monitoring Detail Display

The Applications Pane

The **Applications** pane lists each supported application type. In the Detail tab, a distinctive button appears in the icon next to an application's entry to indicate that ClearSight has detected servers of the corresponding application type. The numbers in parentheses adjacent to the entry indicate exactly how many servers and flows ClearSight has detected. The color of the icon indicates the highest Alert level detected on a server of the indicated type.

For example, an entry like this 

indicates that ClearSight has detected three HTTP servers and four HTTP flows, and that at least one of the servers shows a red-level Alert. You can double-click application entries to cascade them open and show the detected servers.

Select either application or server entries in the Applications pane to determine what appears in the Flows and Statistics panes:

- Select an application entry to view flows and statistics for the application as a whole. For example, you can select HTTP to see all HTTP flows ClearSight has detected.
- Select a server entry to view flows and statistics for a specific application server. For example, you can select an HTTP server entry to see just the HTTP flows for that server.

Automatic Capture Filters in the Applications Pane

You can right-click on any entry in the Applications pane to start capture with an automatic capture filter on the selected application type or server. For example, right-click on an **H.323** entry to display a context menu with a **Capture H.323** option. Select this option to start a capture that will filter out all traffic except H.323. Similarly, you can right-click on a server entry to start a capture on just that server.

The Flows Pane

The **Flows** pane lists each detected flow for the selected application or server in the Applications pane. If an application type is selected in the Applications pane (for example, FTP), the Flows pane shows all detected flows for that application type. Similarly, if an individual server is selected, the Flows pane shows only the flows for that server. Figure 5-4 shows a sample Flows pane for FTP.

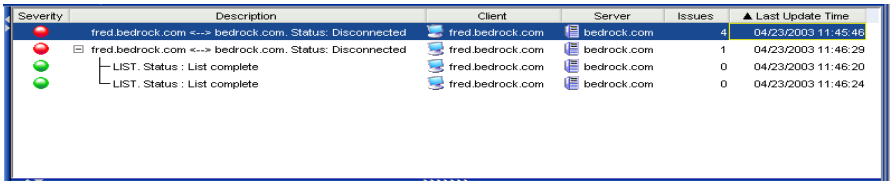


Figure 5-4: Sample Flows Pane

As shown in Figure 5-4, the Flows pane lists each detected flow with the following statistics:

Severity — An icon indicating the highest alert level detected for this flow, from red (most severe) to green (healthy). See *About the Use of Color in ClearSight Displays* on page 115 for details on how ClearSight uses colors.

Description	The type of transaction performed by this flow. For example, this could be a **Get** on an HTTP server, an email on a POP server, a call setup on a VoIP server, and so on. Some transactions will appear with a switch icon ⊞ adjacent to their entries. This icon indicates that you can click the entry to cascade it open and see the actual commands included as part of this flow. For example, Figure 5-4 shows an FTP flow cascaded open to show two **LIST** commands. Selecting a command below a flow entry causes ClearSight to recreate the actual command in the Statistics window — you can see emails, FTP transactions, Telnet sessions, database requests, and VoIP calls as experienced by the end user.
Client	The address of the client side of this flow.
Server	The address of the server side of this flow.

NOTE: You can change how addresses are displayed in the **Client** and **Server** fields by using the context menus accessed by right-clicking on an entry. See *Toggling Address Displays in the Flows Pane*, below, for information on how to do this.

Issues	The number of issues associated with this flow.
Last Update Time	The last time ClearSight updated this flow with new statistics.

Sorting the Flows Pane

You can sort the Flows pane by each statistic type by clicking in the corresponding column heading; click again to reverse the order. A triangle icon appears in the column heading of the statistic by which the pane is currently sorted.

Toggling Address Displays in the Flows Pane

You can change how addresses are displayed in the **Client** and **Server** fields by right-clicking in the **Description** column. In response, a context menu appears that lets you change the address display to IP addresses, IP hostnames, or MAC addresses.

Automatic Capture Filters in the Flows Pane

You can right-click in the **Description** column of any entry in the Flows pane to start capture with an automatic capture filter on the selected flow's IP addresses and port numbers. For example, if you right-click on an FTP flow, it might produce an entry reading something like **Capture 192.168.1.100/3451 <-> 192.168.1.133/21**. Selecting this option would start a capture including all traffic between these two IP addresses on the corresponding ports.

The Statistics Pane

The information shown in the **Statistics** pane depends on what you have selected in either the Applications pane or the Flows pane, as summarized in Table 5-2.

Table 5-2: Statistics Pane Tabs

If you select this...	The Statistic pane displays...
A parent application type in the Applications pane.	Displays statistics for the application as a whole in **Summary**, **Issues**, and **Problems** tabs. In addition, some applications may include an application-specific tab (for example, selecting **DNS** will cause an extra **Name Resolve** tab to appear).
A server in the Applications pane.	Displays statistics specifically for the selected server in **Summary**, **Issues**, and **Problems** tabs.
A flow in the Flows pane.	Displays statistics specifically for the selected flow in **Conversation** and **Statistics** tabs.

NOTE: In addition, you can click the ⊞ icon in the Flows pane to display individual commands from a flow (for example, a **Get** on an HTTP server). Selecting an individual command in the Flows pane displays options in the Statistics pane that let you recreate the exact transaction. These types of displays vary by application type; they are described in detail in the application-specific sections that follow.

Summary Tab Information

The **Summary** tab provides tables of statistics describing and quantifying the traffic from the selected application type or server. ClearSight provides counts for traffic totals (frames, bytes, errors, and so on), as well as application-specific frame type counters. For example, the **Summary** tab for HTTP includes counters for **Hits**, **Pages**, and **Page not found** errors. The exact frame types counted depend on the selected application type.

Issues Tab Information

The **Issues** tab lists detected issues for the selected application or server. Issues are listed with the following statistics:

Count	The number of similar type issues grouped together.
Source	The IP address of the source station for this issue.
Destination	The IP address of the destination station for this issue.
Description	A short description of the issue.
Time Stamp	The time the issue was detected.
Severity	A color-coded icon indicating the severity of the issue.

You can sort the **Issues** tab by each statistic type by clicking in the corresponding column heading; click again to reverse the order. A triangle icon appears in the column heading of the statistic by which the pane is currently sorted.

Problems Tab Information

The **Problems** tab lists all detected problems for the selected application or server. Problems are listed with the following statistics:

Count	The number of similar type problems grouped together.
Source	The IP address of the source station for this problem.
Destination	The IP address of the destination station for this problem.
Description	A short description of the problem.
Group	The offending application type.
Time Stamp	The time the problem was detected.
Severity	A color-coded icon indicating the severity of the problem.

You can sort the **Problems** tab by each statistic type by clicking in the corresponding column heading; click again to reverse the order. A triangle icon appears in the column heading of the statistic by which the pane is currently sorted.

Conversation Tab Information

The **Conversation** tab displays the exchange of data between client and server that makes up the flow selected in the Flows pane. The **Conversation** tab presents this as a standard network ladder diagram so you can follow the conversation as it happened (Figure 5-5). The client is shown on one side of the ladder while the server is on the other; the pane's title bar shows you the address or hostname of each. The arrows show you the direction of the frames in the flow.

In addition, the timing for the conversation is displayed, including:

Delta Time — The time between the indicated frame and the frame that preceded it. Vertical colored bars highlight unusual values.

Relative Time — The time between the indicated frame and the first frame in the flow.

Length — The length of the frame in bytes. Vertical colored bars provide a visual cue to the length.

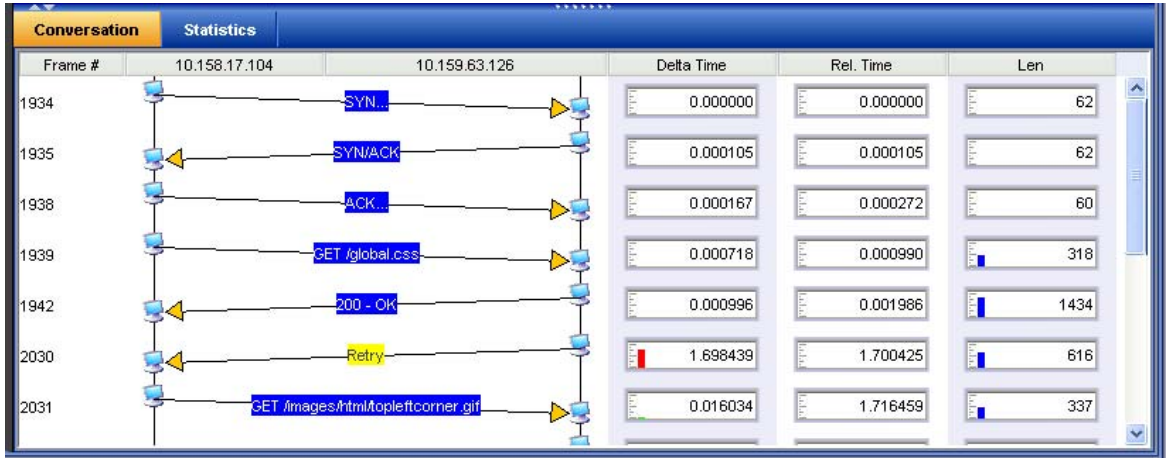


Figure 5-5: Sample Conversation Tab (HTTP Flow)

In addition, ClearSight color codes the exchanges in the **Conversation** tab so you can speed your analysis to problematic messages. For example, Figure 5-5 shows a **GET request** retry on an

HTTP flow in yellow. More serious errors (for example, a **404 - Object not Found** error on an HTTP flow) would appear in red, while messages without any errors appear in blue.

NOTE: You can print the conversation (ladder diagram) by selecting **File > Print** in the pull-down menu.

NOTE: You can save the conversation to a pdf file. To do that, simply right-click anywhere on the ladder diagram. An **Export** button will appear. Clicking on the **Export** button brings up an **Export** dialog box, which lets you specify where you want to save the file.

Statistics Tab Information

The **Statistics** tab provides tables of statistics describing and quantifying the traffic on the flow selected in the Flows pane. ClearSight provides counts for traffic totals on both sides of the connection (frames, bytes, errors, and so on), as well as statistics measuring response times for the flow and application-specific frame type counters. For example, the **Statistics** tab for FTP includes counters for **Number of Downloaded Files** and **Last Downloaded Filename.** The exact frame types available depend on the selected application type.

Report Tab Information

The **Report** tab (available for VoIP flows only) provides a QoS (quality of service) report for the selected flow. See *Viewing VoIP QoS Reports* on page 153 for details.

Application Monitoring Detail Displays

This section provides specific information on the Detail displays for each of ClearSight's supported application types, as follows:

- Citrix Detail Display (page 132)
- DNS Detail Display (page 133)
- FTP Detail Display (page 134)
- Telnet Detail Display (page 136)
- HTTP Detail Display (page 138)
- POP Detail Display (page 140)
- SMTP Detail Display (page 142)
- MS SQL Detail Display (page 144)
- Oracle Detail Display (page 147)
- Exchange Detail Display (page 149)
- MSN Detail Display (page 150)
- H.323 Detail Display (page 152)
- SIP Detail Display (page 152)
- Skinny Detail Display (page 152)
- MGCP Detail Display (page 152)
- Megaco Detail Display (page 152)
- RTP Detail Display (page 159)
- RTSP Detail Display (page 161)
- IPTV Detail Display (page 162)
- Kerberos Detail Display (page 164)
- ISAKMP Detail Display (page 165)
- SMB Detail Display (page 166)
- Generic Detail Display (page 167)

Citrix Detail Display



ClearSight monitors Citrix traffic in real time, creating flows for remote access sessions between a user (Citrix client) and a remote computer (Citrix server). Citrix sessions let a client operate a remote machine as if it were directly connected. Keystrokes and mouse actions entered at the client's computer are passed to the remote machine, and screen displays from the remote machine appear on the client's screen as well.

NOTE: You must use the ClearSight decode engine to properly display Citrix information. To select the ClearSight decode engine, go to **Configuration > Decode > General > Decode Engines** and select the **ClearSight** radio button.

ClearSight shows Citrix sessions in a ladder view, showing each interaction as it occurs. To see the ladder view for a Citrix session, simply select a Citrix flow in the Flows pane.

Figure 5-6 shows a typical Citrix Detail display.

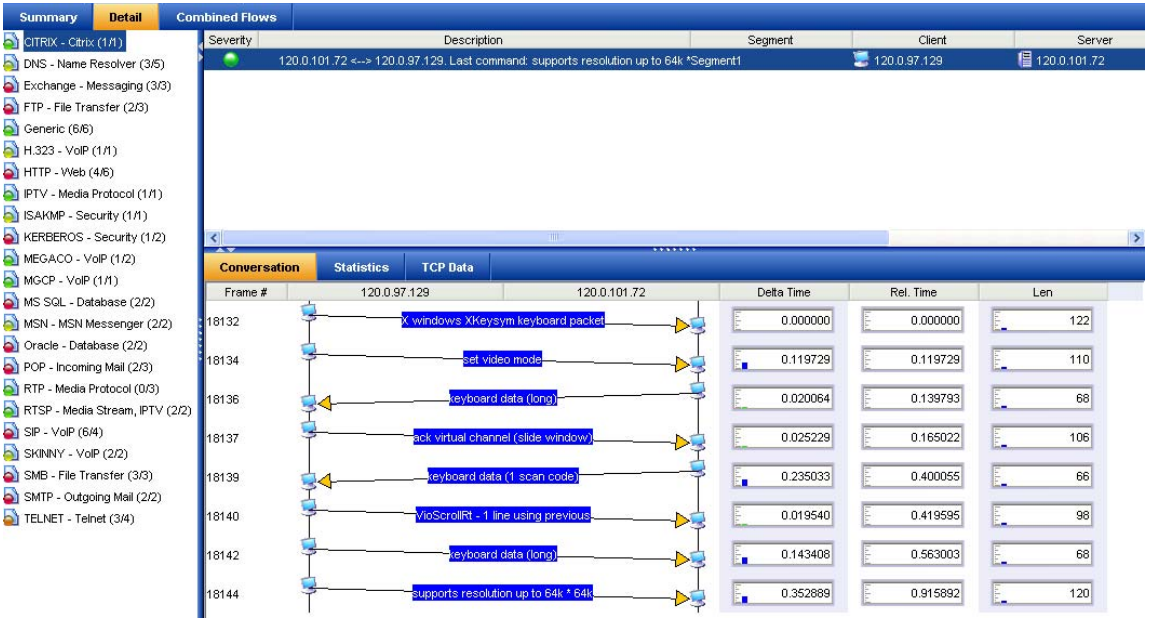


Figure 5-6: Sample Citrix Detail Display

DNS Detail Display



ClearSight monitors Domain Name Service (DNS) traffic in real time, creating flows for name resolution transactions between clients and DNS servers. Stations use DNS to obtain the IP address associated with a particular hostname. This is called “resolving a domain name.”

Figure 5-7 shows a typical flow for a DNS query in the Detail display.

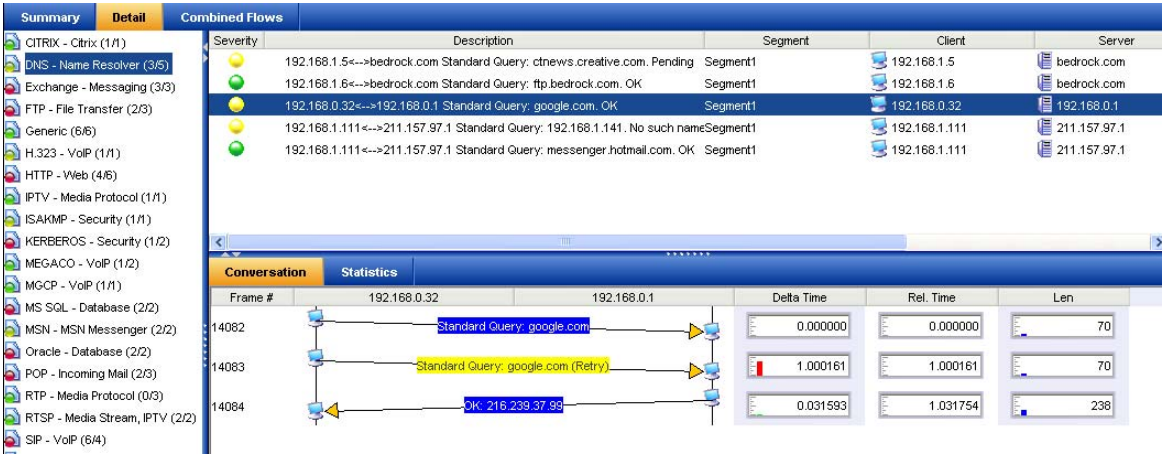


Figure 5-7: Sample DNS Detail Display

Name resolution can account for a surprisingly high percentage of network traffic. Monitor the response times on your DNS servers — are responses to name requests timely, or are your DNS servers lagging? The **Delta Time** fields in the **Conversation** tab can show you in real time the delay between when a request was made of a DNS server and when it actually responded. In addition, you can use the **Configuration > Problem Settings > DNS > Response time (msec)** threshold to specify the highest acceptable response time for a DNS server. This way, ClearSight can generate an alert when it detects a DNS server that is responding more slowly than the threshold specifies.

Adding Names to the Address Book from DNS Discovery

During real-time monitoring, ClearSight keeps track of the name\address pairs resolved from DNS servers and lets you add them to the Address Book.

To add names to the Address Book from the DNS Detail display:

1. Select the parent **DNS - Name Resolver** entry in the Applications pane.

   A new **Name Resolve** tab appears in the Statistics pane.

2. Click on the **Name Resolve** tab in the Statistics pane.

3. The **Name Resolve** tab lists each of the name\address pairs resolved from DNS servers during the current monitoring session. You can add individual name\address pairs to the Address Book by checking the boxes next to their entries and clicking the **Add** button. You can also enable the automatic generation of address book entries.

For more information on working with the Address Book, see Chapter 11, *Using the Address Book*.

FTP Detail Display

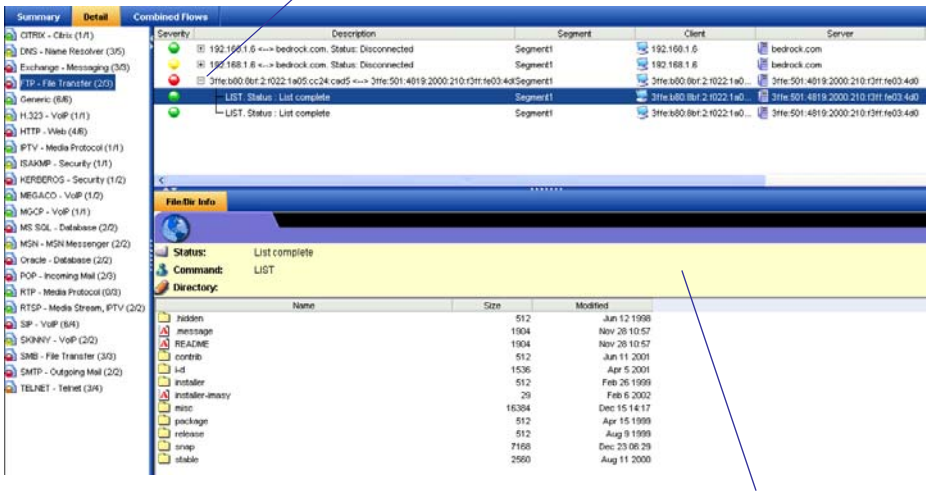


ClearSight monitors File Transfer Protocol (FTP) traffic in real time, creating flows for the various commands making up a file transfer session between a client and an FTP server. In addition, ClearSight recreates FTP transactions as they occur, showing you graphically which files are being transferred, which directories are being listed (and by whom), incorrect passwords, and so on.

You can use the information in the FTP Detail display to maintain visibility on your FTP servers, easily seeing which files are being requested most often, which FTP servers are in danger of becoming overloaded, and whether there is any unauthorized access taking place.

Figure 5-8 shows how ClearSight recreates FTP transactions in the Statistics pane.

Click this icon to cascade open the flow. Then, select an individual command in the flow to see ClearSight recreate the command as seen by the user.



In this example, a LIST command is selected in the Flows pane. In the Statistics pane, ClearSight shows the current status of the transaction, the last command, and the results of the command — all the files listed from the FTP server are listed within ClearSight. You see the transaction as the user saw it.

Figure 5-8: Recreating an FTP Transaction

Recreating an FTP Transaction

As shown in Figure 5-8, ClearSight can recreate an FTP transaction from the user's perspective.

To recreate an FTP transaction:

1. Click the switch icon ⊞ adjacent to an entry in the Flows pane.

   The selected flow cascades open to show the individual commands that make up the flow.

2. Select a command from the flow.

   The Statistics pane automatically recreates the command as seen from the user's perspective. In this example, ClearSight shows the current status of the FTP transaction, the last command (**LIST**),

and the results of the command — all of the files listed from the FTP server are listed in ClearSight.

Telnet Detail Display



ClearSight monitors Telnet traffic in real time, creating flows for remote terminal sessions between a client and a Telnet server. Telnet sessions let a client operate a remote machine as if they were directly connected. Keystrokes entered at the client terminal are passed to the remote machine while screen displays from the remote machine appear on the client terminal.

ClearSight shows Telnet sessions as they occur, displaying the character-oriented data passing from server to client as seen by the client. To view a Telnet session from a client's perspective, simply select a Telnet flow in the Flows pane. In response, the Statistics pane adds a Terminal tab to show you the Telnet session from the client's perspective (Figure 5-9).

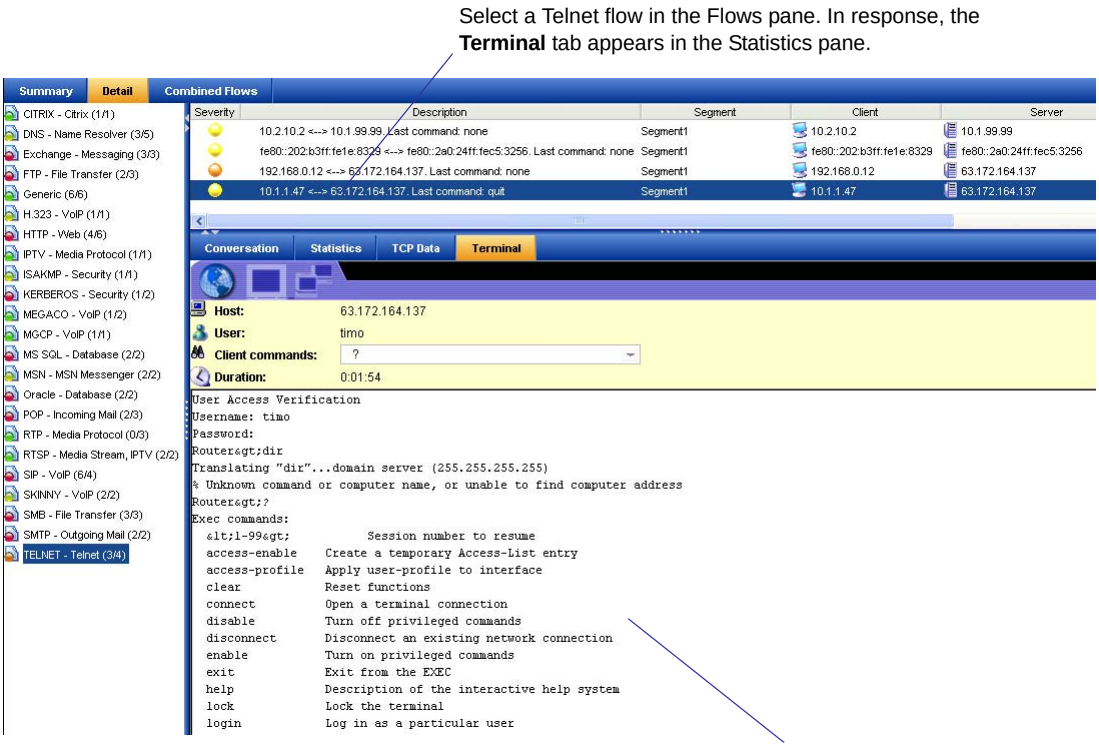


Figure 5-9: Viewing a Telnet Session

HTTP Detail Display



ClearSight monitors HyperText Transfer Protocol (HTTP) traffic in real time, keeping track of web servers and creating flows for web page requests, posts, and so on.

You can use the information in the HTTP Detail display to keep track of:

- **Web server performance**. The **Delta Time** fields in the **Conversation** tab can show you in real time the delay between when a request was made of an HTTP server and when the server actually responded. In addition, you can use the **Configuration > Problem Settings > HTTP > Response time (msec)** threshold to specify the highest acceptable response time for an HTTP server. This way, ClearSight can generate an alert when it detects an HTTP server that is responding more slowly than the threshold specifies.
- **Internet attacks**. Distributed denial of service attacks may show up with sudden spikes in accesses to particular servers or files.
- **Inappropriate access**. Check if employees are accessing inappropriate material from within the corporate network.

Recreating an HTTP Transaction

In addition to various statistics, alerts, and diagrams detailing HTTP transactions, ClearSight can recreate an HTTP transaction from the user's perspective within the ClearSight user interface.

To recreate an HTTP transaction:

1. Click the switch icon ⊞ adjacent to an HTTP entry in the Flows pane.

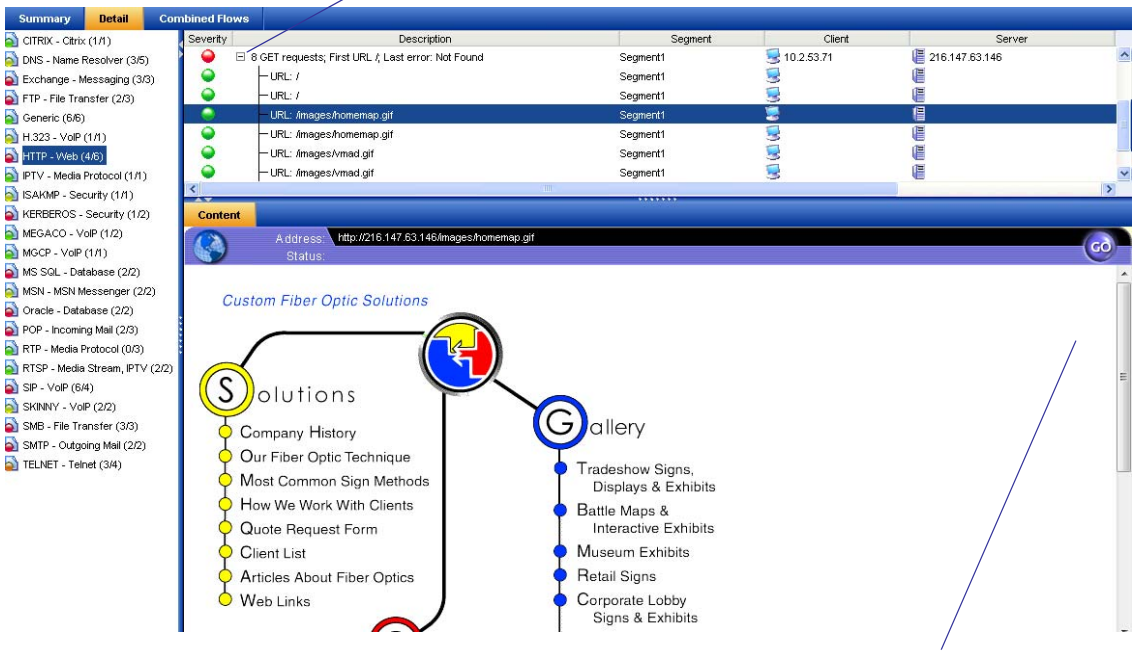
   The selected flow cascades open to show the individual requests that make up the flow.

2. Select an HTTP request from the flow.

   The Statistics pane updates to display the **Content** tab (Figure 5-10). Click the **GO** button in the upper right hand corner of the **Content** tab to issue the selected HTTP request and see the

results within the ClearSight user interface. Figure 5-10 shows the results of a sample GET request from an HTTP server.

Click this icon to cascade open the flow. Then, select an individual request in the flow to see ClearSight recreate the request as seen by the user. Note that this particular flow includes several GET requests — you can select any of the GETs seen on this flow and recreate the request in the **Content** tab below.



When an individual HTTP request is selected in the Flows pane, the **Content** tab appears in the Statistics pane, and recreates the HTTP command as seen by the user. You can also go to the website involved. Simply click the **GO** button in the upper right corner of the Statistics pane to issue the selected HTTP command and see the results.

Figure 5-10: Recreating an HTTP Transaction

NOTE: You must enable **Show HTTP Child Flows** in **Configuration > Preferences > Global > Monitor Options** in order to use this function. See *Global Monitor Options* on page 192.

POP Detail Display



ClearSight monitors Post Office Protocol (POP) traffic in real time, creating flows for email transactions between clients and POP servers. POP is a standard protocol typically used by clients to retrieve email messages from a server.

As with other Detail displays, you can use the information in this display to monitor the health of your POP servers. You can determine how much of an effect unsolicited ("spam") emails are having on your servers' performance. In addition, you can detect unauthorized use of your POP servers.

As with other servers monitored by ClearSight, the delta timers in the **Conversation** tab and the response time alerts configured in the **Configuration > Problem Settings** page can be useful tools for determining the responsiveness of a POP server.

Viewing Emails

In addition to displaying the sequence of requests and responses used to retrieve email from a POP server, ClearSight also shows the actual email messages in natural language. You can view emails as seen by the end user within the ClearSight user interface.

IMPORTANT: Viewing another party's email may be considered an invasion of privacy. Make sure that you understand the ramifications of what you are doing before using ClearSight to view another party's email.

To view an email:

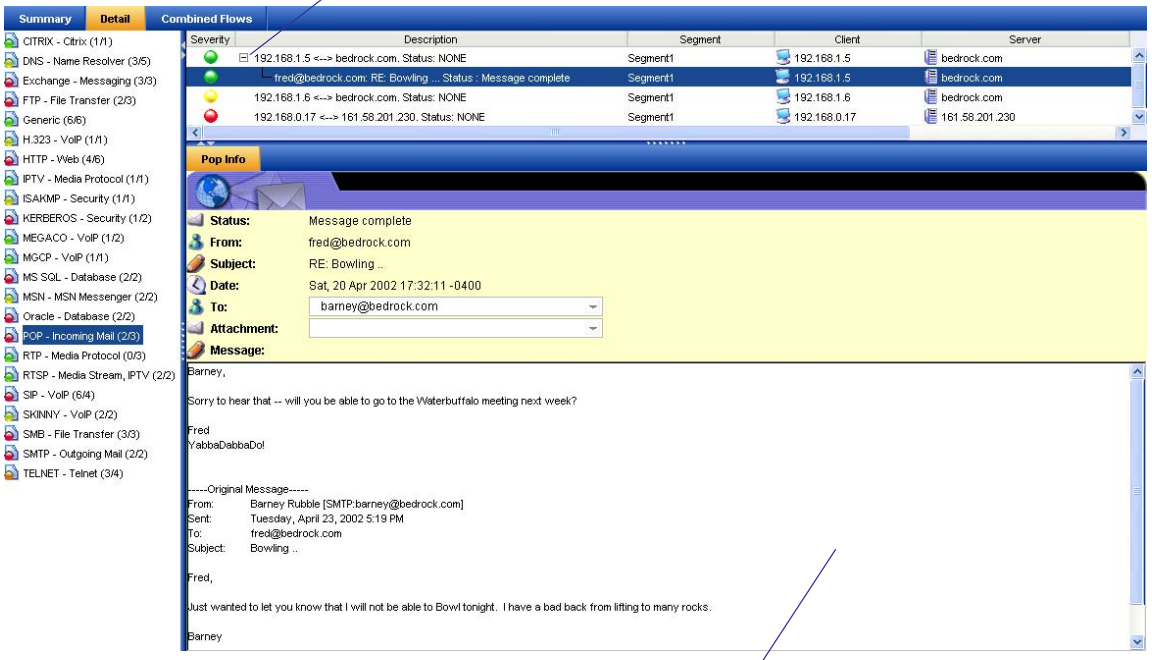
1. Click the switch icon ⊞ adjacent to a POP entry in the Flows pane.

   The selected flow cascades open to show the emails received on the flow.

2. Select an email message from the flow.

   The Statistics pane updates to display the **Pop Info** tab (Figure 5-11). The **Pop Info** tab shows the email message as a user might have seen it within their email client — all fields are included.

Click this icon to cascade open the flow. Then, select an individual email in the flow to see ClearSight display the message as seen by the user in the **Pop Info** tab below.



When an individual email is selected in the Flows pane, the **Pop Info** tab appears in the Statistics pane, displaying the selected email message as seen by the user.

Figure 5-11: Viewing an Email Retrieved on a POP Flow

SMTP Detail Display



ClearSight monitors Simple Mail Transfer Protocol (SMTP) traffic in real time, creating flows for email transactions between clients and SMTP servers. SMTP is a standard protocol typically used by clients to send email messages to a server for forwarding to their eventual destinations.

As with other Detail displays, you can use the information in this display to monitor the health of your SMTP servers. SMTP servers are a popular target of unsolicited emailers ("spammers"). Many spammers abuse private SMTP servers by using them to "bounce" their unsolicited commercial emails. This can result in degraded performance for your SMTP servers. In extreme cases, such abuse can amount to a denial of service attack. ClearSight can help you monitor the email flowing over your SMTP servers, ensuring that only authorized messages are forwarded.

As with other servers monitored by ClearSight, the delta timers in the Detail display's **Conversation** tab and the response time alerts configured in the **Configuration > Problem Settings** page can be useful tools for determining the responsiveness of an SMTP server.

Viewing Emails

In addition to displaying the sequence of requests and responses used to send email to an SMTP server, ClearSight also shows the actual email messages in natural language. You can view emails as sent by the end user within the ClearSight user interface.

IMPORTANT: Viewing another party's email may be considered an invasion of privacy. Make sure that you understand the ramifications of what you are doing before using ClearSight to view another party's email.

To view an email:

1. Click the switch icon ⊞ adjacent to an SMTP entry in the Flows pane.

The selected flow cascades open to show the emails sent on the flow.

2. Select an email message from the flow.

   The Statistics pane updates to display the **Mail Info** tab (Figure 5-12). The **Mail Info** tab shows the email message as the user sent it — all fields are included.

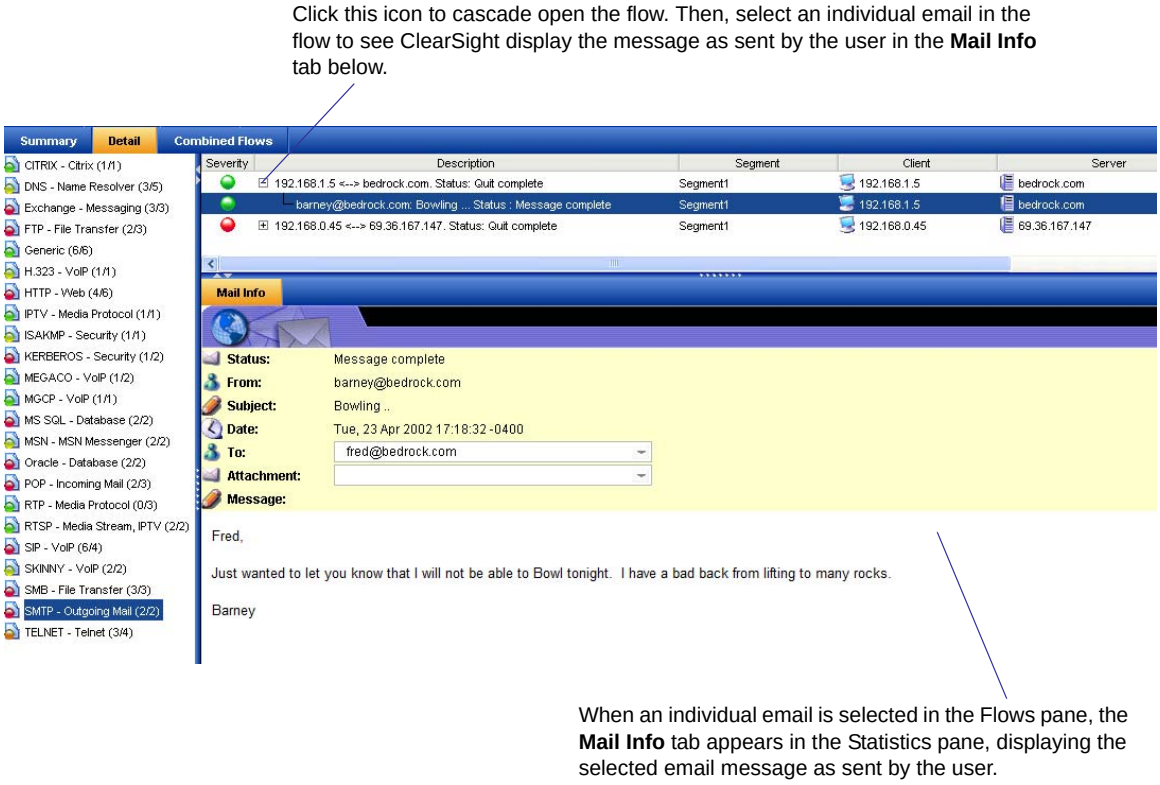


Figure 5-12: Viewing an Email Sent on an SMTP Flow

MS SQL Detail Display



ClearSight monitors Microsoft SQL Server (MS SQL) traffic in real time, creating flows for transactions between database clients and MS SQL servers. MS SQL is Microsoft's proprietary implementation of an enterprise database system using the Structured Query Language (SQL).

As with other Detail displays, you can use the information in this display to monitor the health of your MS SQL servers. ClearSight keeps track of a wide variety of common SQL commands, including **Selects**, **Inserts**, **Deletes**, and so on.

As with other servers monitored by ClearSight, the delta timers in the Detail display's **Conversation** tab can be useful tools for determining the responsiveness of an MS SQL server. In addition, the counters in the **Statistics** tab provide details on the average transaction time for the selected flow. These statistics can help you determine whether your current MS SQL server is powerful enough for your needs.

Recreating an MS SQL Transaction

In addition to various statistics, alerts, and diagrams detailing MS SQL transactions, ClearSight can also recreate an MS SQL transaction from the user's perspective within the ClearSight user interface.

You can see the results of **Select** statements and **Cursor Open** statements (among others) from the database client's perspective. ClearSight shows the actual tabular data returned from such statements so you can see exactly what queries are being performed against your database.

To recreate an MS SQL transaction:

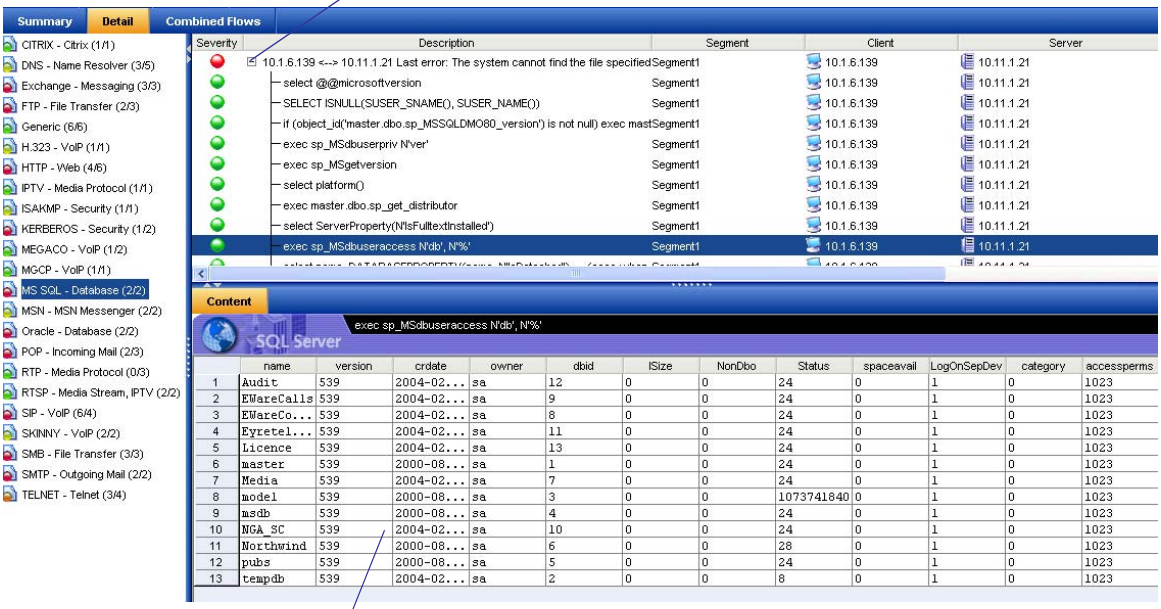
1. Click the switch icon ⊞ adjacent to an MS SQL entry in the Flows pane.

   The selected flow cascades open to show the individual queries and commands that make up the flow.

2. Select an MS SQL command from the flow (for example, a **Select** or a **Cursor Open**).

The Statistics pane updates to display the **Content** tab (Figure 5-13). The **Content** tab shows the actual tabular data returned from the selected query or command.

Click this icon to cascade open the flow. Then, select an individual SQL query or command in the flow to see ClearSight recreate it as seen by the user.



When an individual MS SQL command is selected in the Flows pane, the **Content** tab appears in the Statistics pane, allowing you to view the results of the command as seen by the user. ClearSight shows you in tabular format exactly which data was returned for an SQL query.

Figure 5-13: Recreating an MS SQL Transaction

Viewing Errors on MS SQL Flows

In addition to displaying the results of queries to MS SQL servers, ClearSight also provides an extra tab showing any error messages issued against an MS SQL flow.

To view MS SQL error messages:

1. Select a parent flow with associated errors in the Flows pane. Flows with errors usually appear with a yellow icon in their **Severity** column.

   A new Error Log tab appears in the Statistics pane displaying any SQL errors generated against the selected transaction. Figure 5-14 shows a sample of several SQL errors generated against an MS SQL transaction.

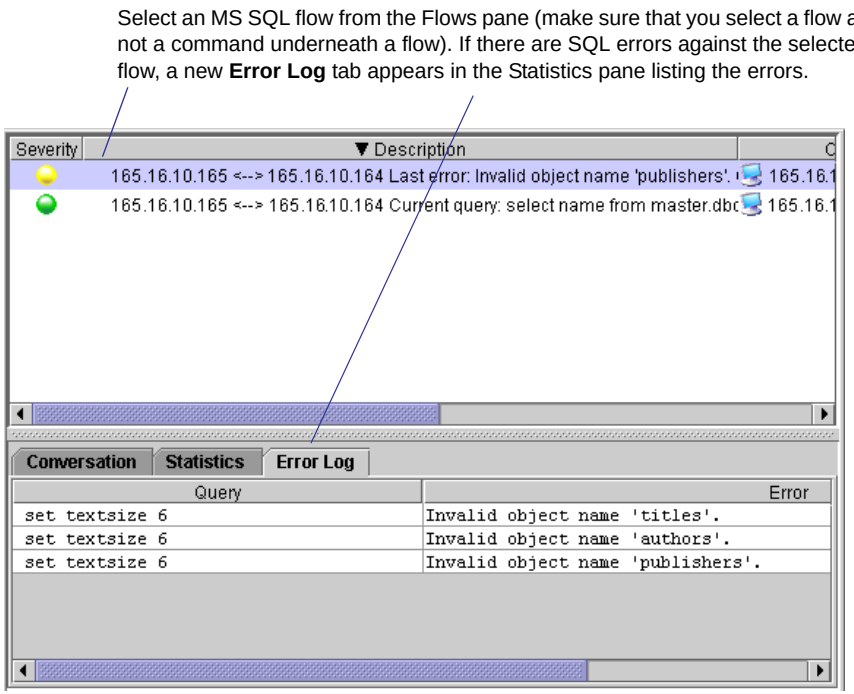
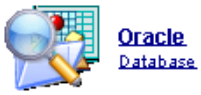


Figure 5-14: Viewing Errors Against an MS SQL Flow

Oracle Detail Display



ClearSight monitors Oracle traffic in real time, creating flows for transactions between database clients and Oracle servers. Oracle's implementation of the Structured Query Language (SQL) is widespread on corporate intranetworks.

As with other Detail displays, you can use the information in this display to monitor the health of your Oracle servers. ClearSight keeps track of a wide variety of common SQL commands, including **Selects**, **Inserts**, and **Deletes**.

As with other servers monitored by ClearSight, the delta timers in the Detail display's **Conversation** tab can be useful tools for determining the responsiveness of an Oracle server. In addition, the counters in the **Statistics** tab provide details on the average transaction time for the selected flow. These statistics can help you determine whether your current Oracle server is powerful enough for your needs.

Recreating an Oracle Transaction

In addition to various statistics, alerts, and diagrams detailing Oracle transactions, ClearSight can recreate transactions from the user's perspective within the ClearSight user interface.

You can see the results of **Select** statements and **Cursor Open** statements (among others) from the database client's perspective. ClearSight shows the actual tabular data returned from such statements so you can see exactly what queries are being performed against your database.

To recreate an Oracle transaction:

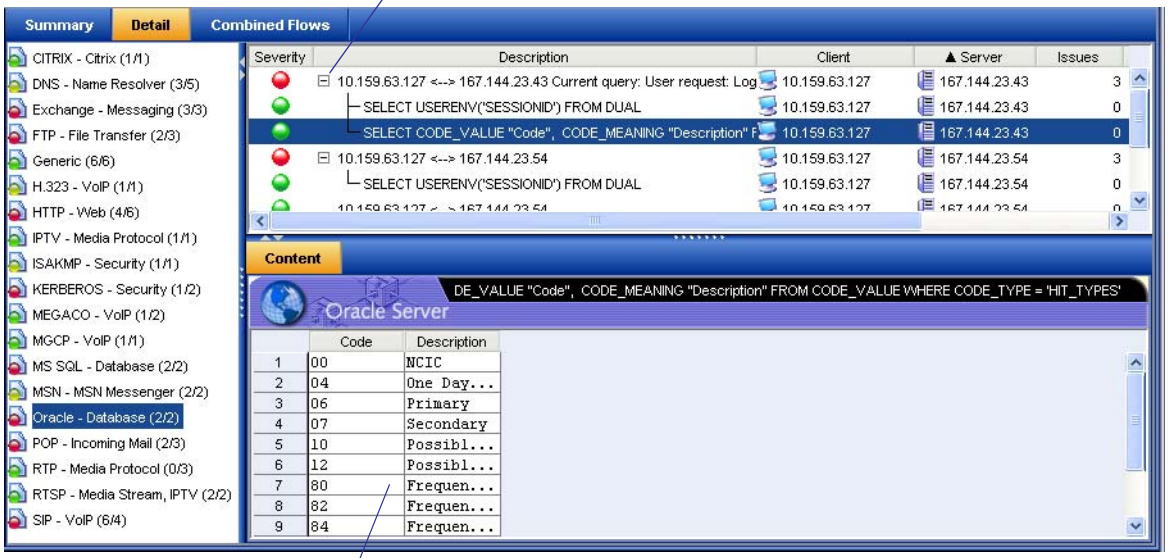
1. Click the switch icon ⊞ adjacent to an Oracle entry in the Flows pane.

   The selected flow cascades open to show the individual queries and commands that make up the flow.

2. Select an Oracle command from the flow (for example, **Select** or **Cursor Open**).

The Statistics pane updates to display the **Content** tab (Figure 5-15). The **Content** tab shows the actual tabular data returned from the selected query or command.

Click this icon to cascade open the flow. Then select an individual query or command in the flow to see ClearSight recreate it as seen by the user.



When an individual Oracle command is selected in the Flows pane, the **Content** tab appears in the Statistics pane. This lets you view the results of the command as seen by the user. ClearSight shows you in tabular format exactly which data was returned for an SQL query.

Figure 5-15: Recreating an Oracle Transaction

Viewing Errors on Oracle Flows

In addition to displaying the sequence of requests and responses used to perform queries and other transactions on Oracle servers, ClearSight provides an extra tab showing any error messages issued against a flow. Use the following procedure to view Oracle error messages.

To view Oracle error messages:

1. Select a flow with associated errors in the Flows pane. Flows with errors will most likely appear with a yellow icon in their **Severity** column.

   NOTE: Make sure that you select a parent flow and not a command underneath a flow entry.

   A new **Error Log** tab appears in the Statistics pane displaying any SQL errors generated against the selected transaction. The display is very similar to that for MS SQL flows, shown in Figure 5-14 on page 146.

Exchange Detail Display



ClearSight monitors Microsoft Exchange transactions in real time, creating flows for transactions between messaging clients and Exchange servers. Exchange is Microsoft's proprietary server for email, instant messaging, scheduling, and so on.

As with other Detail displays, you can use the information in this display to monitor the health of your Exchange servers. Exchange servers typically move an enormous amount of data — as your network's needs grow, their hardware resources can become overwhelmed. The delta timers in the Detail display's **Conversation** tab and the counters in the **Statistics** tab can help you determine if your Exchange servers are responsive enough for your needs.

In addition, ClearSight can help you determine whether you have tuned Exchange's built-in anti-spam measures effectively. Because ClearSight lets you view the emails running across your Exchange server, you can quickly see how much of the total volume is spam and how much is legitimate traffic. Armed with this knowledge, you

can gauge the effectiveness of your current anti-spam measures and, if necessary, take corrective action.

Viewing Emails

In addition to displaying the sequence of requests and responses used to send and receive messages between an Exchange client and server, ClearSight can show the actual email messages in natural language. You can view emails as seen by the end user within the ClearSight user interface.

IMPORTANT: Viewing another party's email may be considered an invasion of privacy. Make sure that you understand the ramifications of what you are doing before using ClearSight to view another party's email.

To view an email:

1. Click the switch icon ⊞ adjacent to an Exchange entry in the Flows pane.

   The selected flow cascades open to show the emails sent on the flow.

2. Select an email message from the flow.

   The Statistics pane updates to display the email message as a user sent it — all fields are included.

MSN Detail Display



Microsoft Network Messenger (MSN) is Microsoft's proprietary server for instant messaging.ClearSight monitors MSN transactions in real time, creating flows for transactions between messaging clients and MSN servers.

When the MSN Application is selected, ClearSight displays overall application statistics, including total frames, total bytes, average throughput, and client and server average response times. It also shows the number of file transfers, voice conversations, video conversations, IM (instant messaging) conversations, and the associated number of bytes transferred.

When a server is selected, ClearSight displays Application Host, Server Statistics, and MSN Server Statistics (for that server) in the **Summary** tab. When a flow is selected, ClearSight displays Conversation and Statistics information specific to that flow.

Viewing MSN Messages

In addition to displaying the sequence of requests and responses used to send and receive traffic between an MSN client and server, ClearSight can show the actual MSN messages in natural language. You can view messages as seen by the end user within the ClearSight user interface.

IMPORTANT: Viewing another party's messages may be considered an invasion of privacy. Make sure that you understand the ramifications of what you are doing before using ClearSight to view another party's messages.

To view an MSN message:

1. Click on an MSN flow in the Flows pane.
2. If an MSN message is present in the flow, the contents will be displayed in the **MSN Message** tab in the Statistics pane.

VoIP Detail Displays



ClearSight monitors Voice over IP (VoIP) calls in real time, creating flows for individual calls and monitoring VoIP Gateways, Gatekeepers, Multipoint Control Units, Clients, Call Managers, and so on.

ClearSight's displays for H.323, SIP, Skinny, MGCP, and Megaco are similar in content. All of these VoIP applications use RTP for the actual transmission of voice data. ClearSight displays both RTP and TCP information, and can actually reproduce the voice or video content extracted from the RTP stream (see *Replaying Voice Calls* on page 155 and *Replaying Video Content* on page 157).

Some specific characteristics of these VoIP applications are:

- **H.323** is an overarching term for a suite of protocols providing real-time VoIP functionality. In general, H.323 includes the H.225 Call Signaling, H.245 Media Control, and H.225 RAS protocols.
- **SIP** (Session Initiation Protocol) is a signaling protocol used to connect and tear down VoIP calls, multimedia sessions, and so on. SIP handles call setup, connection, and control. It also includes T.38 Fax over IP.
- **Skinny** refers to Cisco's Skinny Client Control Protocol (SCCP). In the Skinny world, "thin" IP telephony devices operate by implementing just those parts of the H.323 specification necessary for minimum operations. For the rest of their VoIP services, they communicate with full-blown H.323 proxies called *Call Managers*.
- **MGCP** (Media Gateway Control Protocol) coordinates the functions of an H.323-compliant *Call Agent* with those of a *Media Gateway*. The Call Agent takes care of signaling and call processing, while the media gateway handles audio signal translation and connectivity to a telephone endpoint.
- **Megaco** (also known as H.248) is similar to MGCP, but it supports a wider range of networks, including ATM. Additionally, Megaco enables the Media Gateway Controller to exercise more control over the operation of the Media Gateway.

Viewing VoIP QoS Reports

ClearSight provides a wide variety of QoS (Quality of Service) information describing and quantifying VoIP calls. Using this information, you can determine whether your existing network is delivering an acceptable VoIP quality of service. Pay particular attention to jitter statistics when evaluating the quality of VoIP service — a high level of jitter can make VoIP calls unintelligible.

To view a VoIP QoS report:

1. Click on an entry in the Flows pane for **H.323**, **SIP**, **Skinny, MGCP, or Megaco**.
2. Note that the Statistics pane now shows two tabs — the familiar Conversation tab, and a Reports tab that is unique to VoIP applications.
3. Click on the Reports tab. The resulting display will be similar to Figure 5-16.

The QoS Report applies to the selected flow, and contains the following information:

Summary	Shows the VoIP protocol involved, plus various parameters, including call duration and the number of frames transferred under RTP.
VoIP Index	A numerical index (scale of 1 to 5) characterizing the overall quality of the call. This is also shown as a "star" rating in the upper right hand corner of the report.
Performance Index	Summarizes the overall quantities of Packet Loss, Jitter, Out of Sequence packets, and Latency observed on the selected flow.

The remainder of the report shows detailed bar charts and tables, including:

- Packet Loss Report

- Jitter Analysis
- Out of Sequence Report
- R Value and MOS
- VQFactor (for video flows)

Controls at the top of the Reports tab let you adjust the image size for easier viewing. You can move forward and backward if there are multiple pages. You can also save and/or print the report.

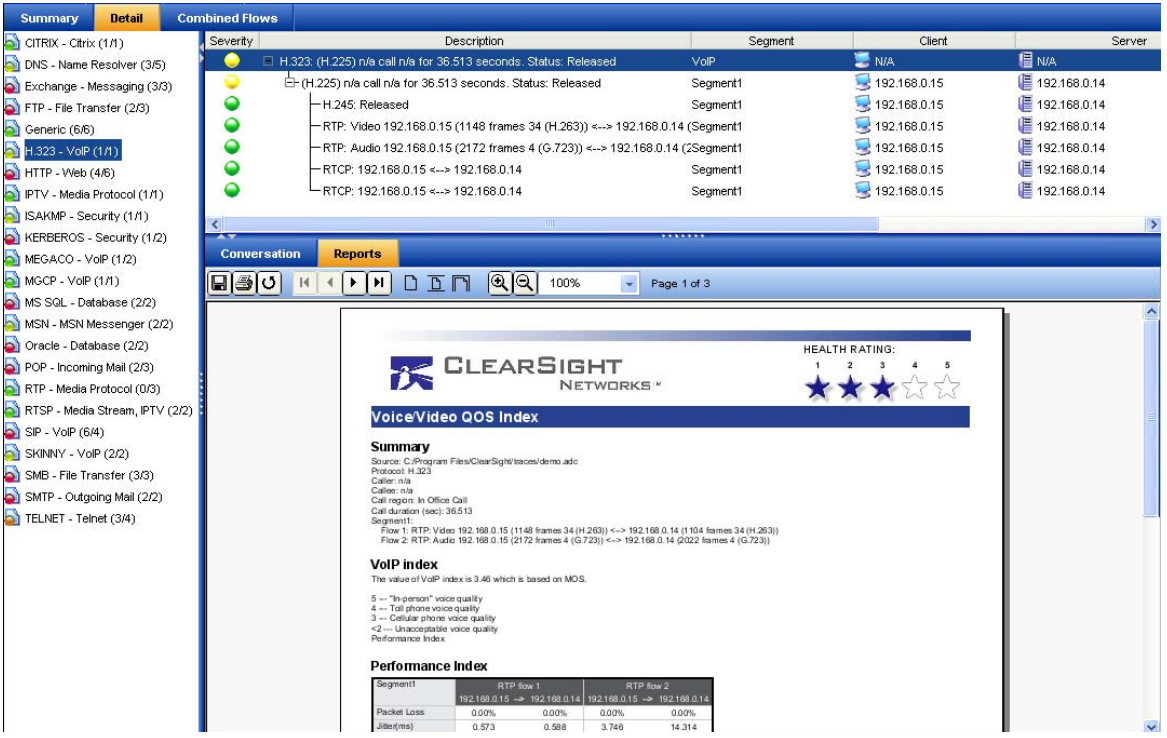


Figure 5-16: Viewing a VoIP QoS Report

Replaying Voice Calls

ClearSight also lets you replay Voice calls over the PC's speaker from within the ClearSight user interface. Use the following procedure to do so.

IMPORTANT: Listening to a private VoIP conversation may be considered an invasion of privacy. Make sure that you understand the ramifications of what you are doing before using ClearSight to listen to a private VoIP call.

To replay a VoIP call:

1. Click the switch icon ⊞ adjacent to an entry in the Flows pane for a VoIP flow.

   The selected flow cascades open to show the various commands and streams seen on the flow.

2. Select an entry for an RTP audio stream below the selected flow.

   The Statistics pane updates to include an area with a built-in media player. Click the **Play** button to play the selected RTP audio stream over the PC's speaker.

Figure 5-17 shows a sample screen with a VoIP call ready for playback (in this case, a Skinny call).

Click this icon to cascade open the flow. Then select an individual RTP audio stream. The left side of the pane below lets you play the selected audio stream over the PC's speaker.

Click this button to play the selected RTP audio stream.

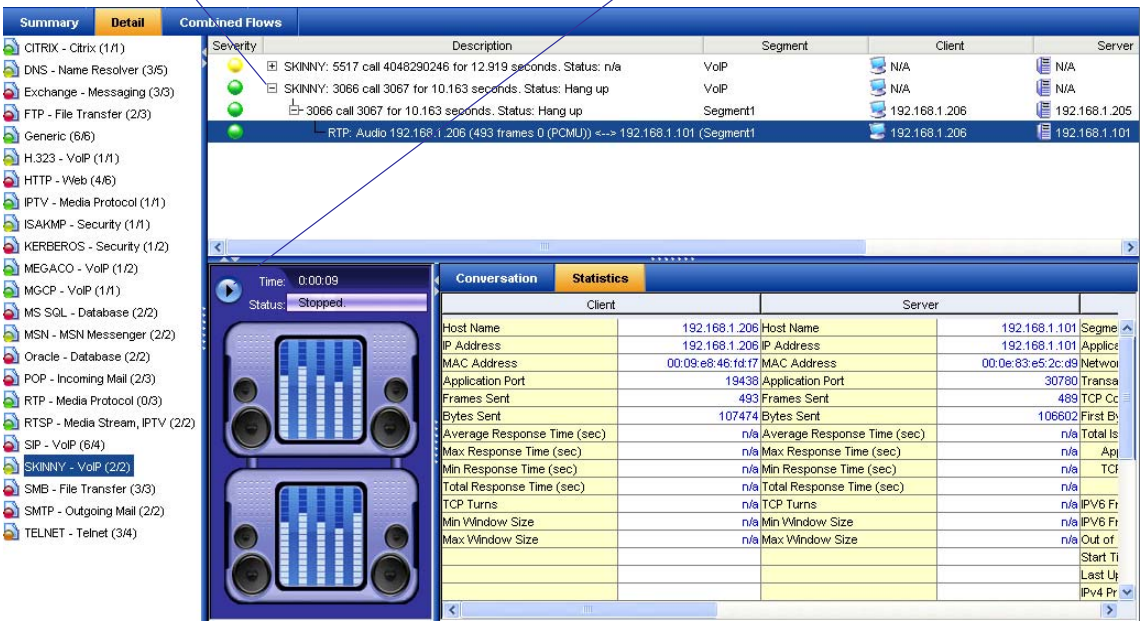


Figure 5-17: Replaying a VoIP Call over the PC's Speaker

NOTE: Depending on the Codec used, you might be able to save the audio content to a wav file. See *Saving an RTP Audio Stream to a Wav File* on page 160.

Replaying Video Content

ClearSight also lets you replay Video content within the ClearSight user interface. Use the following procedure to do so.

To replay Video Content:

1. Click the switch icon ⊞ adjacent to an entry in the Flows pane for a VoIP flow.

   The selected flow cascades open to show the various commands and streams seen on the flow.

2. Select an entry for an RTP video stream below the selected flow.

   The Statistics pane updates to include an area with a built-in media player. Click the **Play** button to play the selected RTP video stream.

Figure 5-18 shows a sample screen showing a VoIP video stream being played back.

Click on a flow to select an individual RTP video stream. The left side of the pane below lets you play the selected video stream.

Click this button to play the selected RTP video stream.

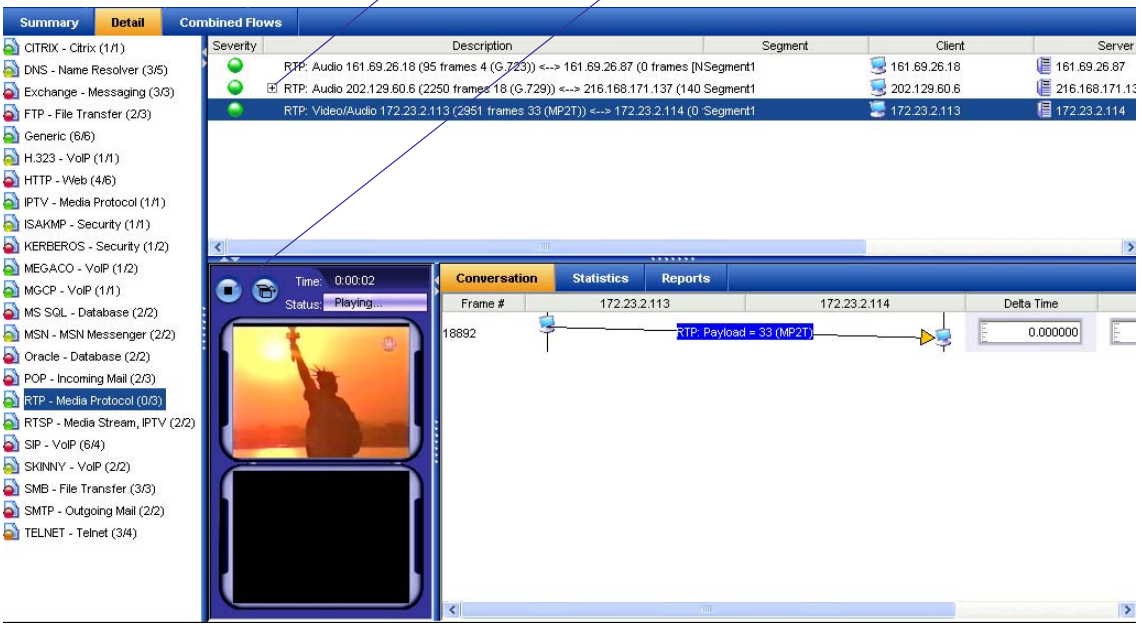


Figure 5-18: Replaying Video Content

To increase the size of the video display, click the button.

NOTE: Depending on the Codec used, you might be able to save the video content to an mpg file. See *Saving an RTP Video Stream to an Mpg File* on page 160.

RTP Detail Display



ClearSight monitors Real-Time Transport Protocol (RTP) transactions, creating flows for individual multimedia streams. RTP is widely used by real-time multimedia delivery applications, providing time-critical delivery of audio and video. Among other common applications, RTP is used for delivery of audio data by H.323, SIP, Skinny, MGCP, and Megaco.

ClearSight provides a variety of statistics describing and quantifying RTP streams. Using these statistics, you can troubleshoot RTP streams to ensure timely delivery of multimedia data.

Replaying RTP Streams

ClearSight also lets you replay RTP streams within the ClearSight user interface.

To replay an RTP stream:

1. Click the switch icon ⊞ adjacent to an RTP entry in the Flows pane.

   The selected flow cascades open to show the various commands and streams seen on the flow.

2. Select an entry for an RTP stream below the selected flow.

   The Statistics pane updates to include an area with a built-in media player. Click the **Play** button to play the selected RTP stream.

Saving an RTP Audio Stream to a Wav File

For certain supported Codecs, you can save the audio content of an RTP stream to a wav file. For a two-way RTP stream, the two streams are put into separate channels.

To create the wav file, simply right-click anywhere on the media player. An **Export** button will appear. Clicking on the **Export** button brings up a **Save** dialog box, which lets you specify where you want to save the file.

Saving an RTP Video Stream to an Mpg File

For certain supported Codecs, you can save the video content of an RTP stream to an mpg file. For a two-way RTP stream, the two streams are put into separate channels.

To create the mpg file, simply right-click anywhere on the media player. An **Export** button will appear. Clicking on the **Export** button brings up a **Save** dialog box, which lets you specify where you want to save the file.

RTSP Detail Display



ClearSight monitors Real-Time Streaming Protocol (RTSP) transactions, creating flows for individual multimedia streams, including Microsoft IPTV. RTSP is a control protocol for coordinating the delivery of real-time multimedia, such as audio and video. The actual delivery is typically done by another protocol, such as RTP, but under the control of RTSP. A single RTSP session can control several multimedia servers, and can also perform important functions such as synchronizing audio with a corresponding video stream. The structure of RTSP is intentionally similar to HTTP, and therefore it has an inherent compatibility with HTTP applications, such as web browsers. For example, an RTSP session can be initiated by clicking on a link on a web page.

Figure 5-19 shows a typical flow for an RTSP stream in the Detail display.

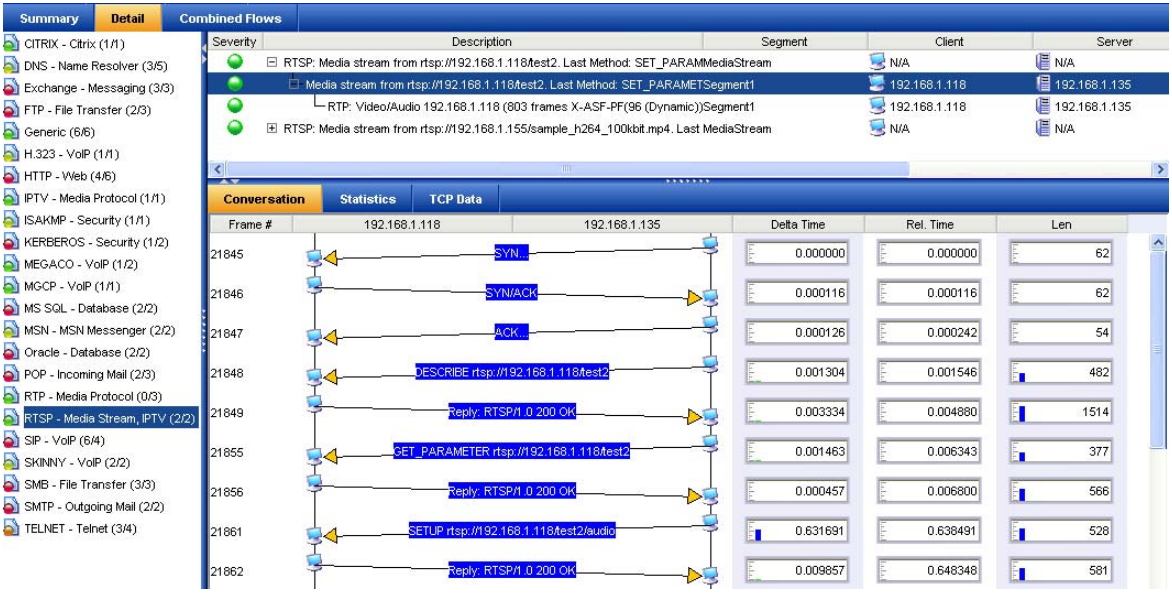


Figure 5-19: Sample RTSP Detail Display

The ladder view in the **Conversation** tab shows the sequence of transactions that control the media stream. The exploded view in the

Flows pane shows how the actual deliveries of the audio and video content are carried by the RTP protocol.

IPTV Detail Display



ClearSight monitors IP Television (IPTV) transactions, creating flows for individual multimedia streams.

Figure 5-20 shows a typical flow for an IPTV stream in the Detail display.

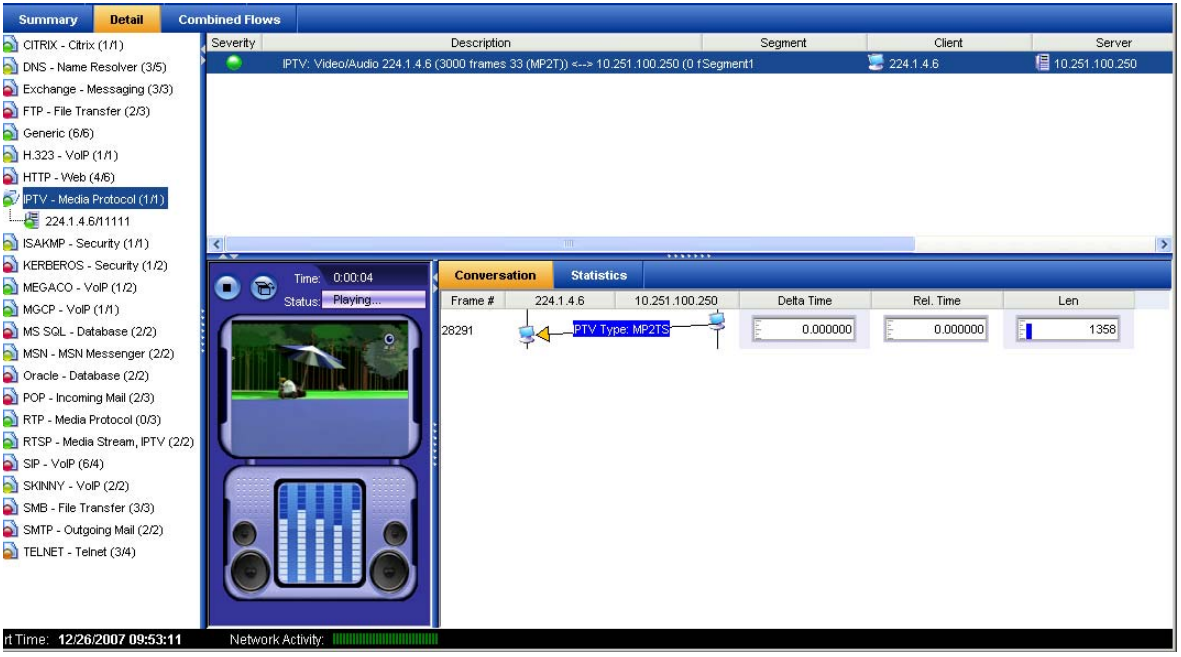


Figure 5-20: Sample IPTV Detail Display

The ladder view in the **Conversation** tab shows the IPTV type.

NOTE: You must use the ClearSight Decode Engine to decode MPEG2 over UDP.

Replaying IPTV content

ClearSight also lets you replay IPTV streams within the ClearSight user interface.

To replay an IPTV stream:

Click the play button  above the video screen.

To increase the size of the video display, click the  button.

Saving an RTP Video Stream to an Mpg File

You can save the video content of an IPTV stream to an mpg file.

To create the mpg file, simply right-click anywhere on the media player. An **Export** button will appear. Clicking on the **Export** button brings up a **Save** dialog box, which lets you specify where you want to save the file.

Kerberos Detail Display



ClearSight monitors Kerberos transactions in real time, creating flows for transactions between clients and Kerberos servers. Kerberos servers provide a means of verifying the identities of clients, and for issuing tickets that can be used to establish credentials by means of which the clients can authenticate themselves to other servers.

You can use the information in this display to track the security related activity on your network. For example, the Statistics pane Summary tab shows you the number of tickets issued, the number of clients involved, and the number of errors. Errors can occur, for example, when a server cannot be found in the Kerberos database, or when a client's credentials have been revoked.

As with other servers monitored by ClearSight, the delta timers in the Detail display's **Conversation** tab can be useful tools for determining the responsiveness of a Kerberos server. In addition, the counters in the **Statistics** tab provide details on the average transaction time for the selected flow. These statistics can help you determine whether your current Kerberos server is powerful enough for your needs.

ISAKMP Detail Display



ClearSight monitors ISAKMP transactions in real time, creating flows for transactions between clients and ISAKMP servers. ISAKMP servers establish, maintain, and delete Security Associations, which provide the framework through which parties to a conversation can authenticate each other and conduct secure transactions.

You can use the information in this display to track the security related activity on your network. For example, the Statistics pane Summary tab shows you the number of sessions, and the number of Phase 1, Phase 2, and Quick Mode successes and failures.

As with other servers monitored by ClearSight, the delta timers in the Detail display's **Conversation** tab can be useful tools for determining the responsiveness of an ISAKMP server. In addition, the counters in the **Statistics** tab provide details on the average transaction time for the selected flow. These statistics can help you determine whether your current ISAKMP server is powerful enough for your needs.

SMB Detail Display



ClearSight monitors SMB traffic in real time, creating flows for transactions between SMB clients and SMB servers. SMB (Server Message Block) is also known as CIFS (Common Internet File System). It is the most common application through which Microsoft computer users access files and other resources (such as printers) on a network.

Figure 5-21 shows a typical flow for a series of request-response interactions between an SMB client and an SMB server in the Detail display.

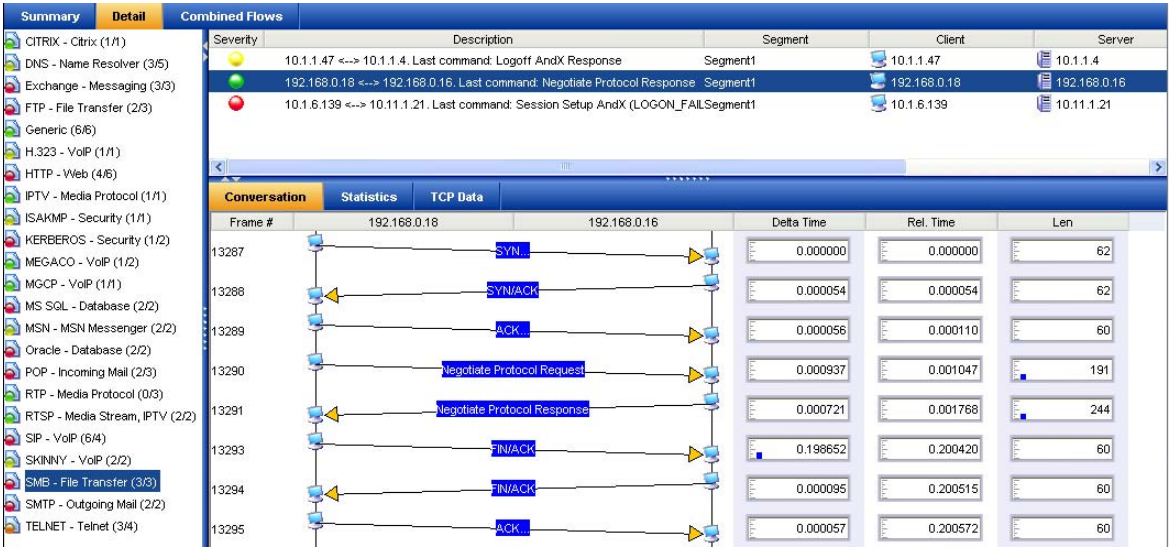


Figure 5-21: Sample SMB Detail Display

The ladder view in the **Conversation** tab shows the specific sequence of requests sent by the client, each followed by a response from the server.

SMB-specific counters in the **Statistics** tab keep track of the number of sessions, the number of directory and file requests, and the number of various kind of errors.

Generic Detail Display



ClearSight creates “generic” flows for those application layer transactions which either do not fit into any of the explicitly supported application types (those shown elsewhere on the **Application > Summary** page) or which have not yet been conclusively identified.

ClearSight provides traffic statistics describing and quantifying generic flows in the Statistics tab. In addition, the **Conversation** tab includes the standard network ladder diagram showing the TCP handshaking between the endpoints of the flow.

Network Layer Monitoring

This section describes ClearSight's real-time monitoring displays at the Network layer. At the Network layer, ClearSight tracks the layer three and layer four hosts and connections underlying the application flows displayed at the Application layer. Counters and statistics are provided for protocols in the TCP/IP family, including UDP, ARP, and ICMP.

You view real-time monitoring displays at the Network layer by clicking **Network** in the Layers pane. In response, the Main pane updates with the following tabs of Network layer monitoring displays:

Overview Tab	Provides frame-level counters describing total network layer traffic observed (page 169).
Connections Tab	Lists detected network layer connections with various statistics (page 170).
Hosts Tab	Lists detected network layer nodes with various statistics (page 175).
Charts Tab	Provides graphs of either the protocol composition of observed traffic or response time distribution (page 177).
Multicast Tab	Lists detected multicast groups and servers with various statistics (page 178).

Overview Tab (Network Layer)

The **Overview** tab provides a wide variety of counters and statistics describing total observed network layer traffic. Separate frame counts and response time counters are provided for a wide variety of TCP/IP traffic (for example, IP, TCP, UDP, ARP, and ICMP). Figure 5-22 shows the **Overview** tab.

The Network layer is currently selected in the Layers pane, providing access to several tabs displaying network layer information. As shown below, the **Overview** tab is currently selected, providing a variety of counters and statistics for the total network layer traffic observed.

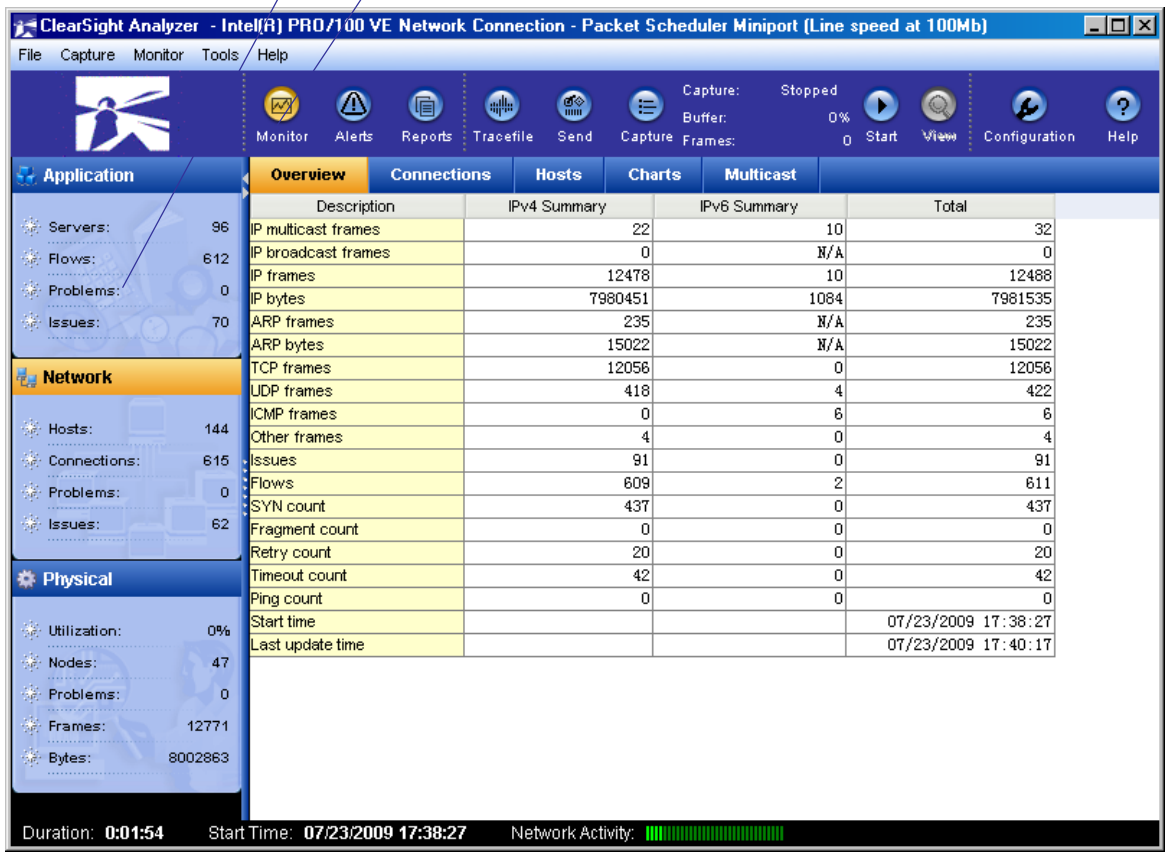


Figure 5-22: Overview Tab at the Network Layer

Connections Tab (Network Layer)

The **Connections** tab provides counters and statistics describing and quantifying each detected network layer client-server connection. Figure 5-23 shows an example of the **Connections** tab.

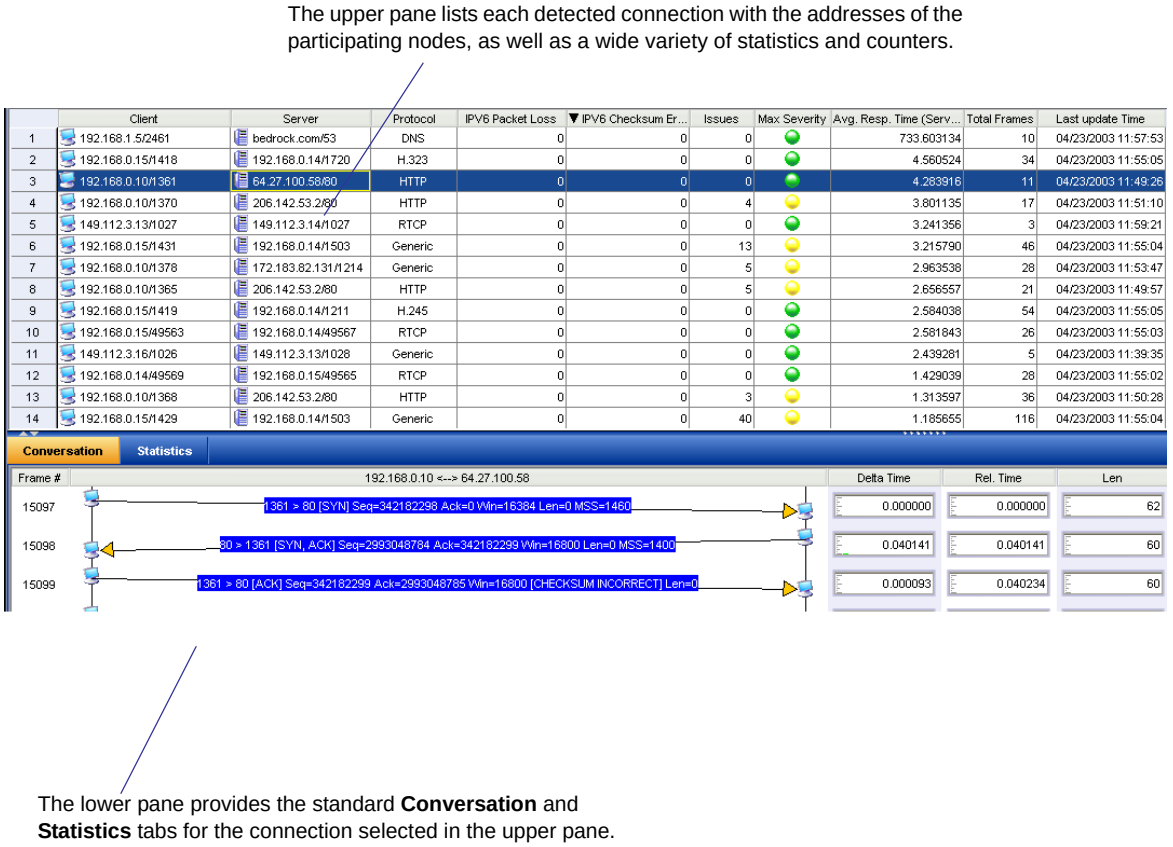


Figure 5-23: Connections Tab at the Network Layer

As shown in Figure 5-23, the **Connections** tab is divided into two panes:

- The upper pane lists each detected connection with the following statistics:

Client	The address of the client side of the connection.
Server	The address of the server side of the connection.
Protocol	The upper layer protocol in use on the connection.
IPV6 Packet Loss	The number of IPv6 fragments lost on this connection. ClearSight maintains fragmentation analysis to a depth of 20 packets. This means that when ClearSight receives the first fragment of a given packet, it waits for all of the fragments in the packet to arrive for the time it takes 19 more packets to arrive. If the entire packet has not arrived by then, ClearSight will declare a lost fragment for the packet. **NOTE:** Packets are removed from this data structure in a first-in first-out manner.
IPV6 Checksum Errors	The total number of IPv6 packets on this connection that show checksum errors. Checksum errors are calculated using the standard checksum algorithm from RFC 768. **NOTE:** The checksum error count is not incremented until all fragments for a given packet are received. The counter will not be incremented for a packet unless all fragments for the packet are received.

NOTE: The **IPV6 Packet Loss** and **IPV6 Checksum Errors** statistics appear only if you have purchased the optional IPv6 Multicast Analysis Option.

Issues	The total number of issues associated with this connection. Click the **Issues** entry at the Network layer in the Layers pane to see all detected issues.
Max Severity	A color-coded icon showing the highest alert level detected on this connection.
Avg Resp Time	The average response time from the server to all client requests on this connection.
Total Frames	The total number of frames seen on this connection.
Last Update Time	The last time ClearSight updated the statistics for this connection.

- The lower pane provides the standard **Conversation** and **Statistics** tabs describing the connection selected in the upper pane. The **Conversation** and **Statistics** tabs provide the same type of information as they do at the Application layer (see *Conversation Tab Information* on page 129 and *Statistics Tab Information* on page 130 for details), except for network layer data.

  In general:

  - The **Conversation** tab displays the exchange of data between client and server that makes up the connection selected in the upper pane. The **Conversation** tab presents this as a standard network ladder diagram so you can follow the conversation as it happened. The client is shown on one side of the ladder while the server is on the other; the pane's title bar shows you the address or hostname of each. The arrows show you the direction of the messages in the flow.

    NOTE: You can print the ladder diagram by selecting **File > Print** in the pull-down menu.

In addition, the timing for the conversation is displayed, including:

Delta Time	The time between the indicated message and the message that preceded it.
Relative Time	The time between the indicated message and the first message in the flow.

- The **Statistics** tab provides tables of statistics describing and quantifying the traffic on the connection selected in the upper pane. ClearSight provides counts for traffic totals on both sides of the connection (such as frames, bytes, and errors), as well as for the connection as a whole.

Toggling Address Displays in the Connections Tab

You can change how addresses are displayed in the **Client** and **Server** fields of the **Connection** tab's upper pane by right-clicking in the pane. In response, a context menu appears that lets you change the address display to IP addresses, IP hostnames, or MAC addresses.

Automatic Capture Filters in the Connections Tab

The **Connections** tab provides a wide variety of automatic capture filters. Access the automatic capture filters by right-clicking a connection in the upper pane of the Connections tab. In response, a context menu appears with a variety of available automatic capture filters. Automatic capture filters are available explicitly for the selected connection's addresses and ports, as well as for a variety of common wild-card filtering scenarios using different combinations of the selected addresses and ports.

IPv6 Fragmentation Analysis in the Connections Tab

ClearSight users with the IPv6 Multicast Analysis Option enabled will receive information on fragmented packet loss and UDP checksum errors for each detected IPv6 multicast flow. These

statistics will appear in the **Connections** tab of the Network layer monitoring display.

As described above, both the **Packet Loss** and **Checksum Errors** counters appear in the upper pane of the **Connections** tab. In addition to these counters, the lower pane's **Statistics** tab provides an **Out of Sequence** counter. This shows the number of packets that had at least one fragment arriving at the destination out of order. ClearSight increments the **Out of Sequence** counter only once for a given packet, even if more than one fragment for the packet arrived out of order.

To ensure accurate fragmentation analysis, ClearSight checks each fragment's VLAN ID and Fragment ID. This way, a given fragment is not mistakenly associated with a different parent packet.

NOTE: Packets and **Fragments** are two different things. A packet consists of one or more fragments.

Hosts Tab (Network Layer)

The **Hosts** tab provides counters and statistics describing and quantifying the traffic for each detected network layer host. Figure 5-24 shows an example of the **Hosts** tab.

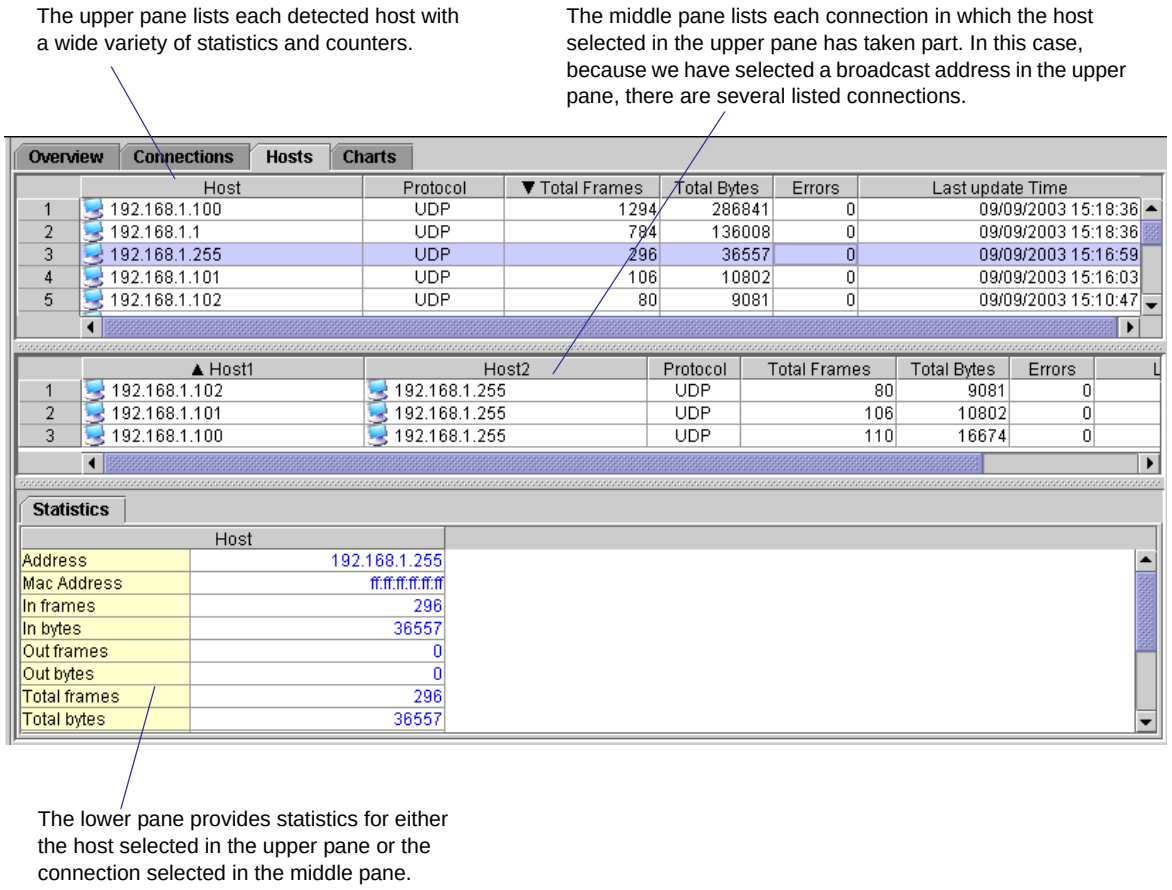


Figure 5-24: Hosts Tab at the Network Layer

As shown in Figure 5-24, the **Hosts** tab is divided into three panes:

- The top pane lists each detected host with a variety of statistics describing and quantifying the traffic seen for the host.

- The middle pane lists each connection in which the host selected in the top pane has participated. Each connection is listed with a variety of counters and statistics for the traffic on the connection.
- The lower pane provides statistics on either the host selected in the top pane or the connection selected in the middle pane, depending on which is selected.

Toggling Address Displays in the Hosts Tab

You can change how addresses are displayed in the **Hosts** tab by right-clicking in the pane. In response, a context menu appears that lets you change address display to IP addresses, IP hostnames, or MAC addresses.

Automatic Capture Filters in the Hosts Tab

The **Hosts** tab provides a variety of automatic capture filters. Access the automatic capture filters by right-clicking a connection or host in the top two panes of the **Hosts** tab. In response, a context menu appears with a variety of available automatic capture filters. Automatic capture filters will be available explicitly for the selected host or connection's address(es) and port(s), as well as for a variety of common wild-card filtering scenarios using different combinations of the selected addresses and ports.

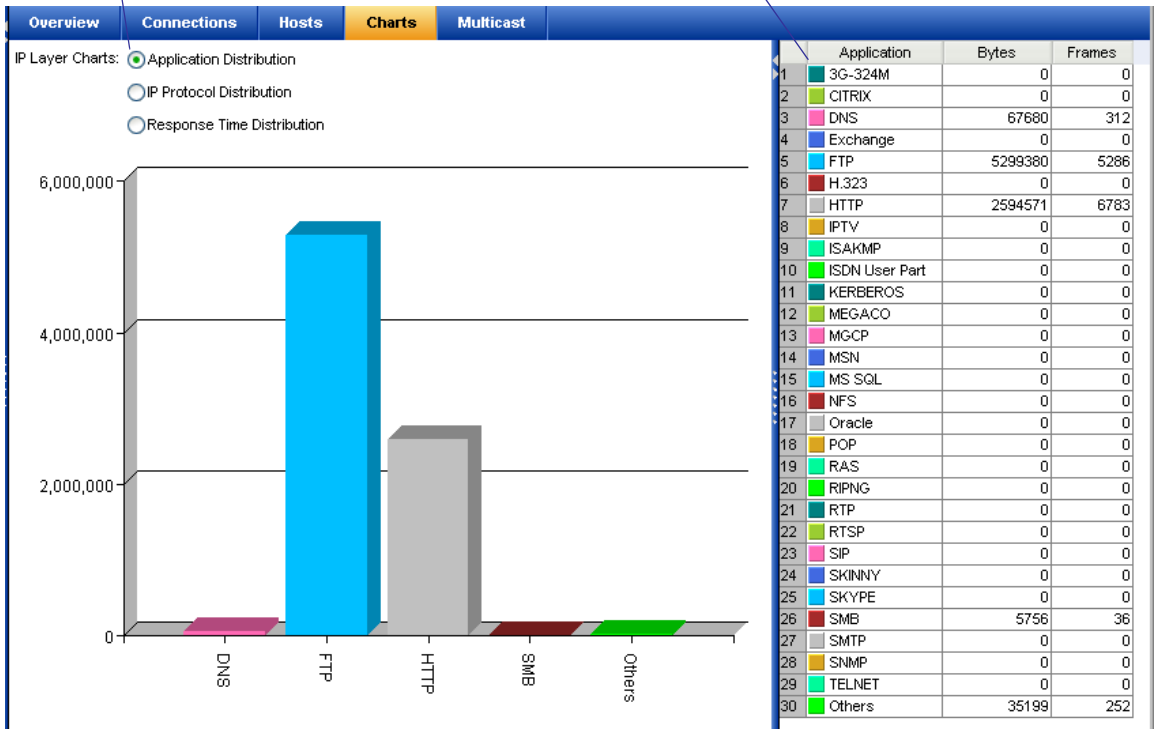
Charts Tab (Network Layer)

The **Charts** tab provides you with a broad overview of the distribution of protocols on your network. Bar charts for both application layer and network layer protocols show you which protocols are consuming most of your bandwidth. In addition, you can view graphs showing you response times for all servers detected on the network.

Figure 5-25 shows an example of the **Charts** tab.

Use these options to specify what type of charts you want to view.

This table provides both a legend to the color codes used in the charts as well as byte and frame counts for each of the listed protocols. You can use this table to monitor bandwidth-eating protocols you may not want on your corporate network.



	Application	Bytes	Frames
1	3G-324M	0	0
2	CITRIX	0	0
3	DNS	67680	312
4	Exchange	0	0
5	FTP	5299380	5286
6	H.323	0	0
7	HTTP	2594571	6783
8	IPTV	0	0
9	ISAKMP	0	0
10	ISDN User Part	0	0
11	KERBEROS	0	0
12	MEGACO	0	0
13	MGCP	0	0
14	MSN	0	0
15	MS SQL	0	0
16	NFS	0	0
17	Oracle	0	0
18	POP	0	0
19	RAS	0	0
20	RIPNG	0	0
21	RTP	0	0
22	RTSP	0	0
23	SIP	0	0
24	SKINNY	0	0
25	SKYPE	0	0
26	SMB	5756	36
27	SMTP	0	0
28	SNMP	0	0
29	TELNET	0	0
30	Others	35199	252

Figure 5-25: Charts Tab at the Network Layer

Multicast Tab (Network Layer)

The **Multicast** tab provides counters and statistics describing and quantifying the traffic on each detected multicast address. ClearSight extracts multicast group addresses (IGMP for IPv4 and MLD for IPv6) from packets sent by hosts to routers. Figure 5-26 shows an example of the **Groups** tab in the **Multicast** tab.

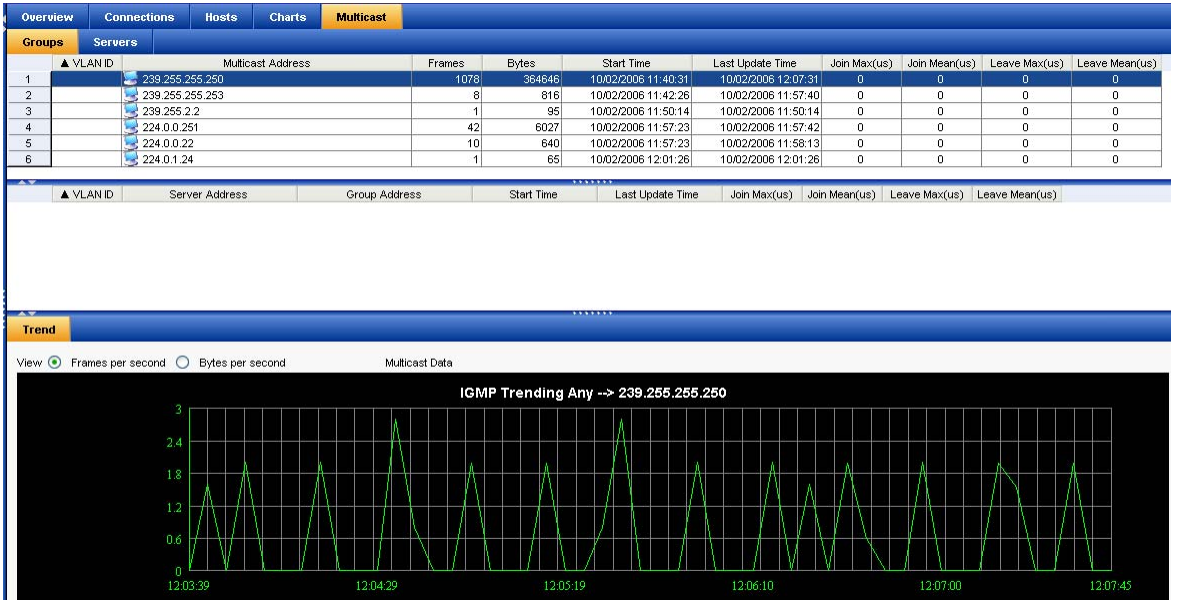


Figure 5-26: Multicast Tab at the Network Layer

As shown in Figure 5-26, the **Groups** tab in the **Multicast** tab lists each detected multicast address with the following statistics:

VLAN ID	The ID of the VLAN (if any) from which the MLD Report or IGMP message was sent.
Multicast Address	The multicast address extracted from an MLD or IGMP packet.
Frames	The number of frames sent to this multicast address.

Bytes	The number of bytes sent to this multicast address.
Start Time	The time at which the first MLD Report or IGMP message for this multicast address was seen.
Last Update Time	The time at which the most recent MLD Report or IGMP message for this multicast address was seen.
Join Max (us)	The maximum time it took for multicast traffic to start flowing after the initial Join packet was issued.
Join Mean (us)	The average time it took for multicast traffic to start flowing after the initial Join packet was issued.
Leave Max (us)	The maximum time it took for multicast traffic to stop flowing after the initial Leave packet was issued.
Leave Mean (us)	The average time it took for multicast traffic to stop flowing after the initial Leave packet was issued.

The statistics in the **Servers** tab are the same as in the Groups tab, except that the **Server Address** is shown instead of the **Multicast Address**.

Reserved IPv6 Multicast Addresses

As you use ClearSight to analyze the multicast traffic on your network, certain reserved IPv6 addresses may appear in the **Multicast** tab more frequently than others. Table 5-3 shows some common reserved IPv6 multicast addresses you may see while using ClearSight to monitor your IPv6 multicast traffic. The complete list can be found in RFC 2373.

Table 5-3: Common Reserved IPv6 Multicast Addresses

IPv6 Multicast Address	Description
FF02::1	**All-nodes**. Used to reach all nodes on the same link.
FF02::2	**All-router**. Used to reach all routers on the same link.
FF02::4	**DVMRP routers**. Used to reach all DVMRP multicast routers on the same link.
FF02::5	**OSPF routers**. Used to reach all OSPF routers on the same link.

Physical Layer Monitoring

This section describes ClearSight's real-time monitoring displays at the Physical layer. At the Physical layer, ClearSight provides statistics describing the actual transmission of network data, including counts for various frame and error types (such as broadcasts, multicasts, and CRC errors). Counts are provided both globally and for each individual detected MAC address. In addition, ClearSight tracks VLANs and Subnets at the Physical layer.

You view real-time monitoring displays at the Physical layer by clicking **Physical** in the Layers pane. In response, the Main pane updates with the following tabs of Physical layer monitoring displays:

Overview Tab — Provides counters for various common frame and error types. In addition, graphs are provided charting utilization and error levels in real time (page 182).

VLAN Tab — Lists detected VLANs with various statistics (page 183).

Subnet Tab	Lists detected Subnets with various statistics (page 184).
Nodes Tab	Lists detected MAC nodes with various statistics (page 185).
Charts Tab	Provides a graph showing the percentage utilization of network bandwidth over time (page 186).

Overview Tab (Physical Layer)

The **Overview** tab provides a wide variety of counters for different frame and error types observed during the monitoring session. In addition, real-time graphs show the current and historical network utilization and frequency of errors. Figure 5-27 shows an example of the **Overview** tab.

The Physical layer is currently selected in the Layers pane, providing access to the **Overview**, **VLAN, Subnet, Nodes, and Charts** tabs. As shown below, the **Overview** tab is currently selected, providing frame, error, and utilization counters and graphs for the monitoring session.

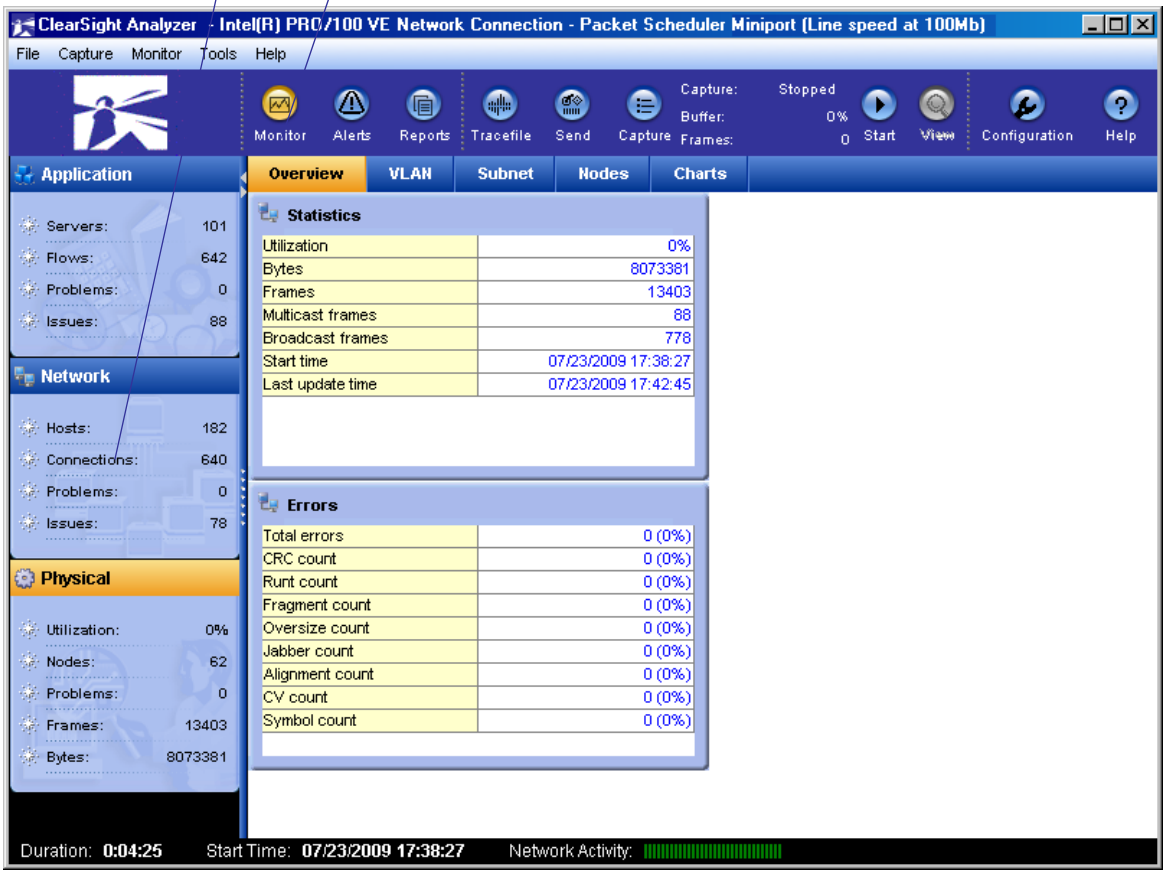


Figure 5-27: Overview Tab at the Physical Layer

VLAN Tab (Physical Layer)

The **VLAN** tab provides counters and statistics describing the traffic seen on each detected VLAN. ClearSight analyzes 802.1Q tags in real time to provide information on detected VLANs.

Figure 5-28 shows an example of the **VLAN** tab.

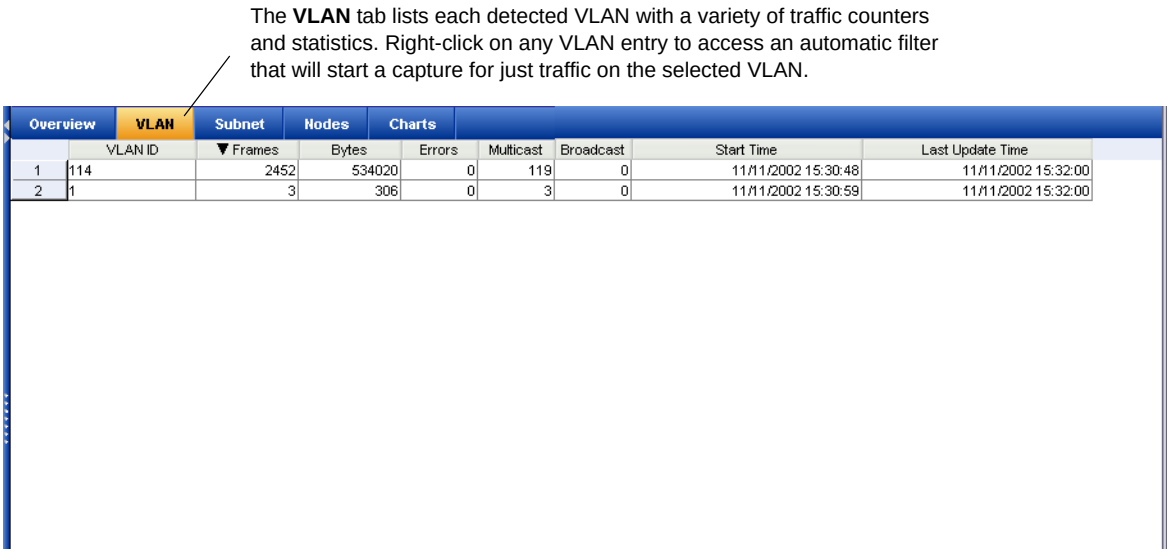


Figure 5-28: VLAN Tab at the Physical Layer

Automatic Capture Filters in the VLAN Tab

You can start a capture on any VLAN listed in the **VLAN** tab by right-clicking its entry and selecting the **Capture VLAN** *xx* entry from the context menu that appears.

Subnet Tab (Physical Layer)

The **Subnet** tab provides counters and statistics describing the traffic seen on each detected subnet.

Figure 5-28 shows an example of the **Subnet** tab.

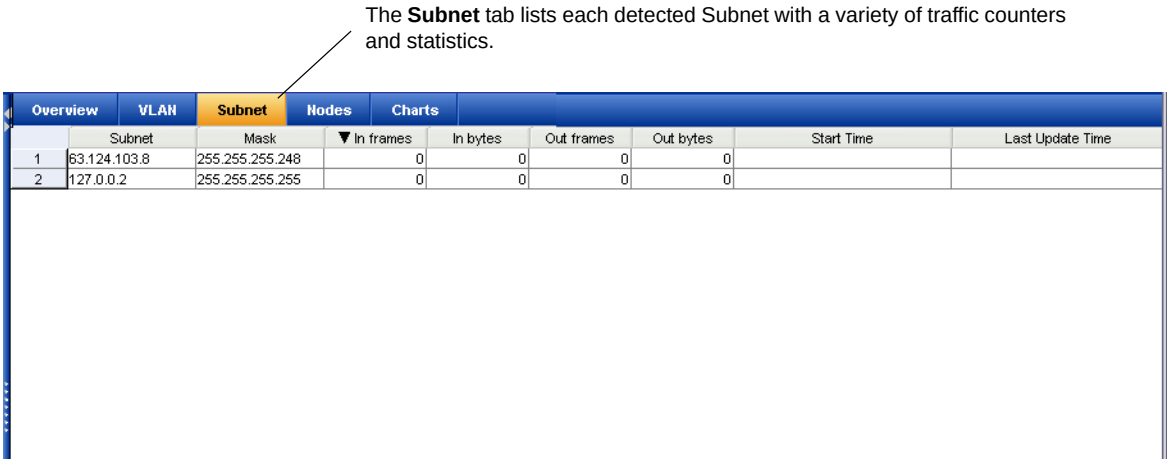
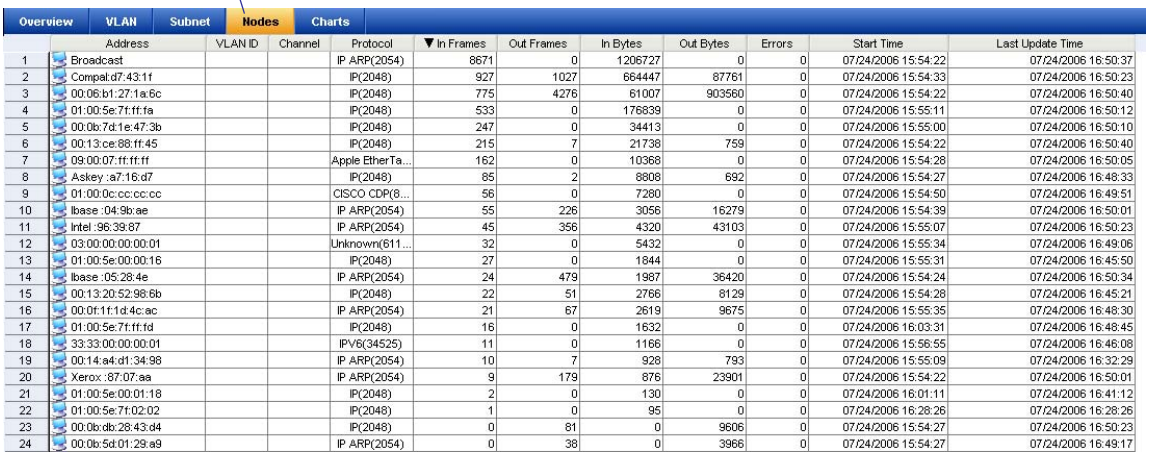


Figure 5-29: Subnet Tab at the Physical Layer

Nodes Tab (Physical Layer)

The **Nodes** tab provides counters and statistics describing and quantifying the traffic for each detected MAC address on the network. Figure 5-30 shows an example of the **Nodes** tab.

The **Nodes** tab lists each detected MAC address with a variety of statistics describing and quantifying the node's traffic. As with most ClearSight displays, you can sort the display by any statistic by clicking in the corresponding column heading.



Overview | VLAN | Subnet | Nodes | Charts

	Address	VLAN ID	Channel	Protocol	▼ In Frames	Out Frames	In Bytes	Out Bytes	Errors	Start Time	Last Update Time
1	Broadcast			IP ARP(2054)	8671	0	1206727	0	0	07/24/2006 15:54:22	07/24/2006 16:50:37
2	Compal:d7:43:1f			IP(2048)	927	1027	664447	87761	0	07/24/2006 15:54:33	07/24/2006 16:50:23
3	00:06:b1:27:1a:6c			IP(2048)	775	4276	61007	903560	0	07/24/2006 15:54:22	07/24/2006 16:50:40
4	01:00:5e:7f:ff:fa			IP(2048)	533	0	176839	0	0	07/24/2006 15:55:11	07/24/2006 16:50:12
5	00:0b:7d:1e:47:3b			IP(2048)	247	0	34413	0	0	07/24/2006 15:55:00	07/24/2006 16:50:10
6	00:13:ce:88:ff:45			IP(2048)	215	7	21738	759	0	07/24/2006 15:54:22	07/24/2006 16:50:40
7	09:00:07:ff:ff:ff			Apple EtherTa...	162	0	10368	0	0	07/24/2006 15:54:28	07/24/2006 16:50:05
8	Askey :a7:16:d7			IP(2048)	85	2	8808	692	0	07/24/2006 15:54:27	07/24/2006 16:48:33
9	01:00:0c:cc:cc:cc			CISCO CDP(8...	56	0	7280	0	0	07/24/2006 15:54:50	07/24/2006 16:49:51
10	Ibase :04:9b:ae			IP ARP(2054)	55	226	3056	16279	0	07/24/2006 15:54:39	07/24/2006 16:50:01
11	Intel :96:39:87			IP ARP(2054)	45	356	4320	43103	0	07/24/2006 15:55:07	07/24/2006 16:50:23
12	03:00:00:00:00:01			Unknown(611...	32	0	5432	0	0	07/24/2006 15:55:34	07/24/2006 16:49:06
13	01:00:5e:00:00:16			IP(2048)	27	0	1844	0	0	07/24/2006 15:55:31	07/24/2006 16:45:50
14	Ibase :05:28:4e			IP ARP(2054)	24	479	1987	36420	0	07/24/2006 15:54:24	07/24/2006 16:50:34
15	00:13:20:52:98:6b			IP(2048)	22	51	2766	8129	0	07/24/2006 15:54:28	07/24/2006 16:45:21
16	00:0f:1f:1d:4c:ac			IP ARP(2054)	21	67	2619	9675	0	07/24/2006 15:55:35	07/24/2006 16:48:30
17	01:00:5e:7f:ff:fd			IP(2048)	16	0	1632	0	0	07/24/2006 16:03:31	07/24/2006 16:48:45
18	33:33:00:00:00:01			IPV6(34525)	11	0	1166	0	0	07/24/2006 15:56:55	07/24/2006 16:46:08
19	00:14:a4:d1:34:98			IP ARP(2054)	10	7	928	793	0	07/24/2006 15:55:09	07/24/2006 16:32:29
20	Xerox :87:07:aa			IP ARP(2054)	9	179	876	23901	0	07/24/2006 15:54:22	07/24/2006 16:50:01
21	01:00:5e:00:01:18			IP(2048)	2	0	130	0	0	07/24/2006 16:01:11	07/24/2006 16:41:12
22	01:00:5e:7f:02:02			IP(2048)	1	0	95	0	0	07/24/2006 16:28:26	07/24/2006 16:28:26
23	00:0b:db:28:43:d4			IP(2048)	0	81	0	9606	0	07/24/2006 15:54:27	07/24/2006 16:50:23
24	00:0b:5d:01:29:a9			IP ARP(2054)	0	38	0	3966	0	07/24/2006 15:54:27	07/24/2006 16:49:17

Figure 5-30: Nodes Tab at the Physical Layer

Automatic Capture Filters in the Nodes Tab

You can start a capture on any node listed in the **Nodes** tab by right-clicking its entry and selecting the **Capture** ***MAC Address*** entry from the context menu that appears.

Charts Tab (Physical Layer)

The **Charts** tab provides you with a broad overview of the percentage utilization of your network. ClearSight measures network utilization over a specific time period called the *Check Interval*. ClearSight makes a measurement of the percentage network utilization during each check interval and records it in the **Charts** tab at the Physical Layer. The chart shows the number of check intervals in each specified percentage utilization range. The specific number of check intervals in each utilization range is provided in the **Occurrences** column in the table at the right of the **Charts** tab (Figure 5-31).

NOTE: You specify the value for the **Check Interval** in the **Configuration > Preferences > Global > Monitor Settings** page (see *Global Monitor Settings* on page 190 for details).

Figure 5-31 shows an example of the **Charts** tab.

The chart illustrates network utilization over time.

This table provides both a legend to the color codes used in the charts as well as counts for the number of **Check Intervals** during which network utilization was in the indicated percentage range. You set the **Check Interval** in the **Configuration > Preferences > Global > Monitor Settings** page; see *Global Monitor Settings* on page 190 for details.

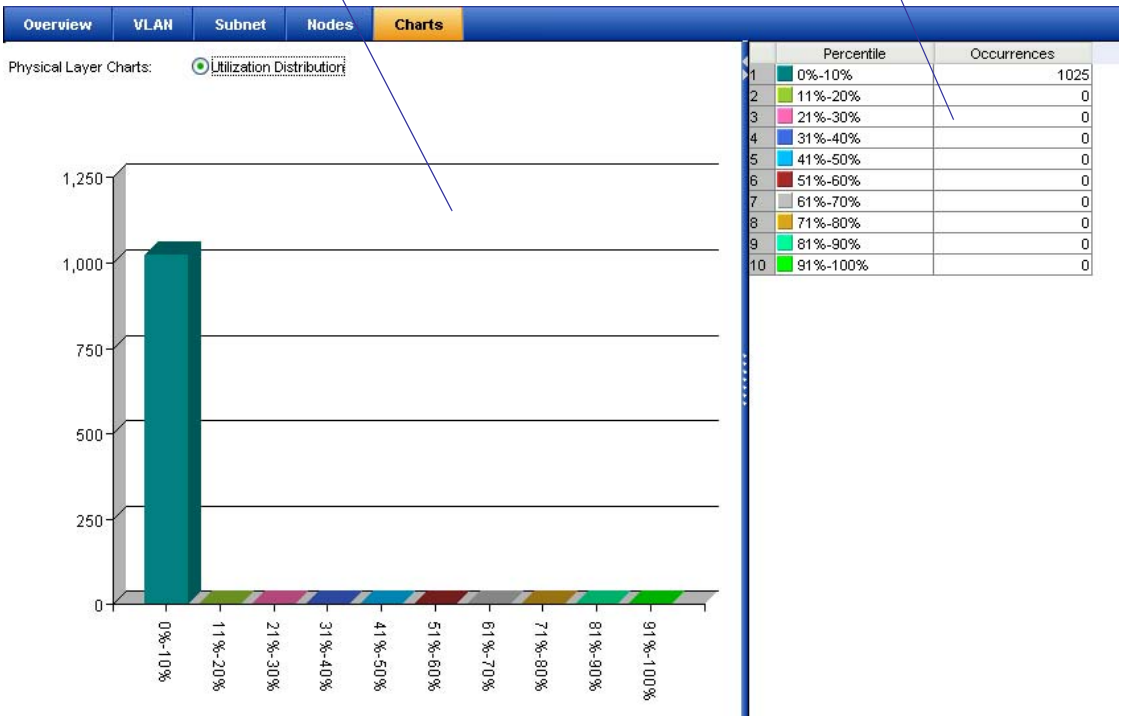


Figure 5-31: Charts Tab at the Physical Layer

Configuring the ClearSight Analyzer

This section describes how to set configuration preferences that affect the operation of the ClearSight Analyzer.

To set configuration preferences:

1. Click the **Configuration** button in the toolbar.
2. Click on the **Preferences** tab.
3. Select which options you want to set from the menu at the left of the display (Figure 5-32).

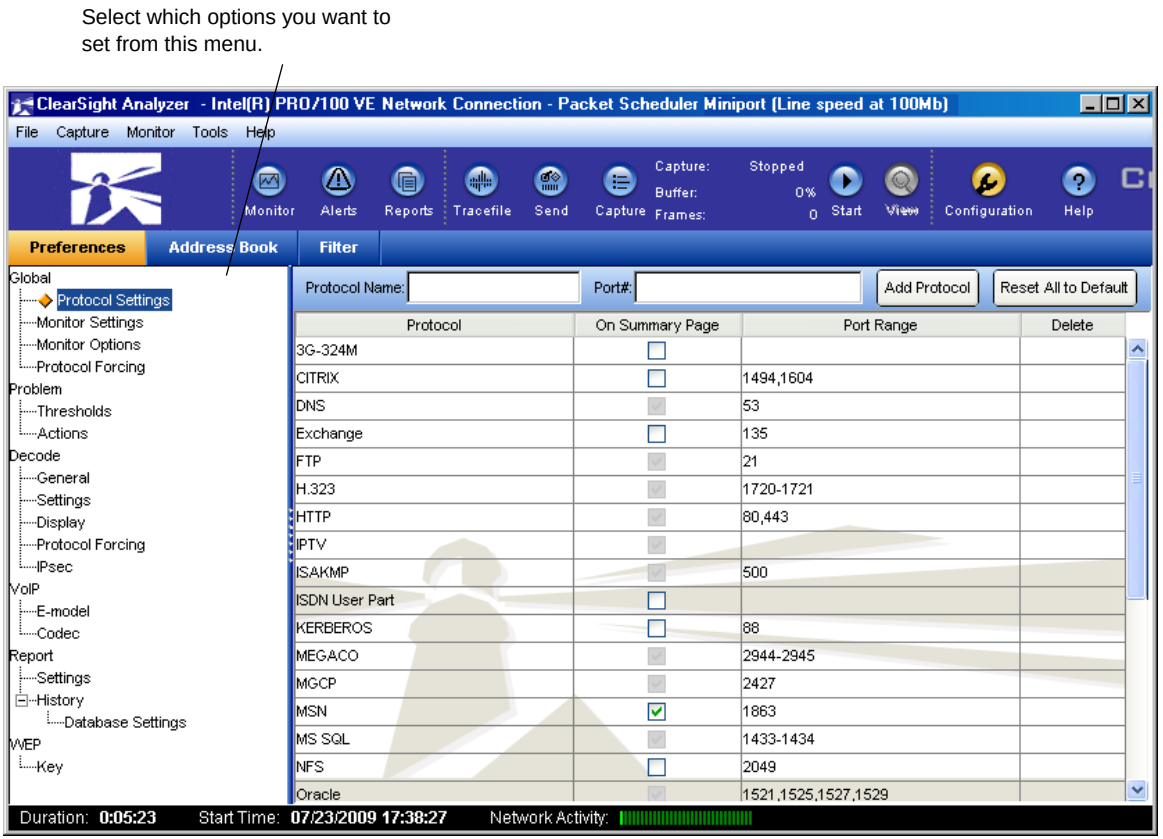


Figure 5-32: Setting Configuration Preferences

Global Protocol Settings

Use **Global > Protocol Settings** (Figure 5-32 on page 188) to:

- Add custom port and protocol combinations to the list of protocols monitored by ClearSight.
- Edit the ports on which ClearSight currently expects to see standard protocols.
- Select the protocols that will display on the Application layer Summary tab.

The **Protocol Settings** options are useful if your network runs either proprietary protocols or standard protocols over non-standard ports.

When you select **Protocol Settings**, ClearSight lists the protocol\port combinations it is currently configured to monitor. ClearSight uses the well-known ports for common protocols. However, you can use the options in this screen to add custom protocols to the list, modify an existing protocol\port combination, or delete a protocol entirely.

NOTE: You can specify multiple ports, separated by commas (such as 80,443) or port ranges (such as 1720-1729).

Indicate whether you want a protocol to display on the **Application** layer **Summary** tab by checking or unchecking the **On Summary Page** box for that application. Note however, that there are certain applications that ClearSight considers fundamental, and it will not let you disable them using this screen. For those applications, simply follow the disable/enable process described in *Choosing Which Applications to Display* on page 110.

If you have added a custom protocol there will be a trash icon in the **Delete** column. Clicking that icon deletes that entire row.

NOTE: Changes made to protocol\port entries take effect immediately. However, new protocols are not positioned in alphabetical order on the Summary Page until you exit and restart ClearSight.

Global Monitor Settings

Use **Global > Monitor Settings** (Figure 5-33 on page 191) to:

- Select a filter that will apply to all packets entering the Monitor.

  If a filter is currently selected, the name of that filter is displayed in the **Filter** area. To deselect that filter, click the **Remove** button. The filter name will then be replaced by **None** to indicate that no filter currently applies. The name of the button changes to **Set** to indicate that you can set (select) a new filter.

  If you click on the **Set** button, the **Filter List** dialog box (Figure 9-31) appears. You can then choose the filter you want from the list of currently defined filters.

  You can create a new filter by clicking the **Create** button at the lower left. For details on how to create new filters (or edit existing filters) see Chapter 9, *Using Filters*.

- Specify (in seconds) the interval over which ClearSight monitors and averages all real-time statistics. This is specified by the **Intervals > Check** option. By default, this is set to five seconds.

  Use this option to change the granularity of the statistics presented by ClearSight's real-time monitor. Larger values will tend to smooth out statistical anomalies while smaller values may place undue importance on momentary bursts. In general, a value close to the default of five seconds provides optimum results.

- Specify (in seconds) the interval over which ClearSight monitors and averages application throughput. This is specified by the **Intervals > Throughput** option. By default, this is set to one second. When traffic is present, the throughput displayed on the Application layer Summary screen (see Figure 5-1 on page 110) toggles between *current* and *average*. The *current* value is the most recent measurement of throughput, averaged over the Throughput Interval. When traffic is not present, only the *average* value is displayed, which is the average throughput since the beginning of that monitoring session.

  Use this option to change the granularity of the throughput values presented by ClearSight's real-time monitor. Larger values will tend to smooth out statistical anomalies while smaller values may place undue importance on momentary bursts. In general, a

value close to the default of one second provides optimum results.

- Specify the maximum number of "rungs" that an individual ladder view can have. You can set this number independently for applications, connections, and others.
- Specify the maximum number of network connections that ClearSight will track.
- Specify the maximum number of servers and flows of each supported application type for which ClearSight will maintain statistics. Once the upper limit for a particular type of server or flow has been reached, ClearSight will not create new entries in the monitor displays for new servers and flows.

  TIP: Use these options to configure ClearSight's performance for the types of servers and flows in which you are most interested. The more servers and flows you specify that ClearSight monitor, the more of the ClearSight PC's resources you consume. Direct your monitoring resources to the servers and flows in which you are most interested.

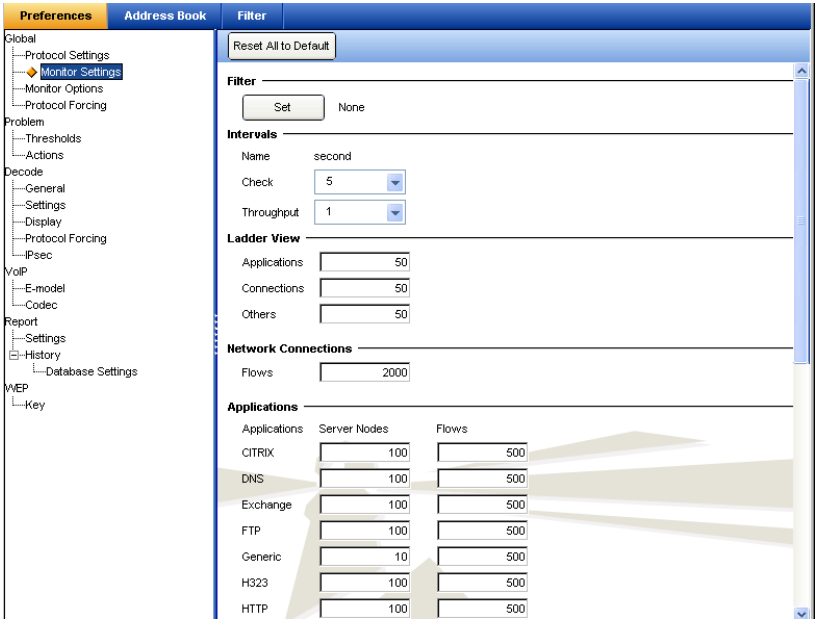


Figure 5-33: The Monitor Settings Configuration Screen

Global Monitor Options

Use **Global > Monitor Options** (Figure 5-34) to specify which statistics ClearSight should gather at each layer (**Application**, **Network**, and **Physical**. Statistics with checked boxes are gathered while statistics with unchecked boxes are not.

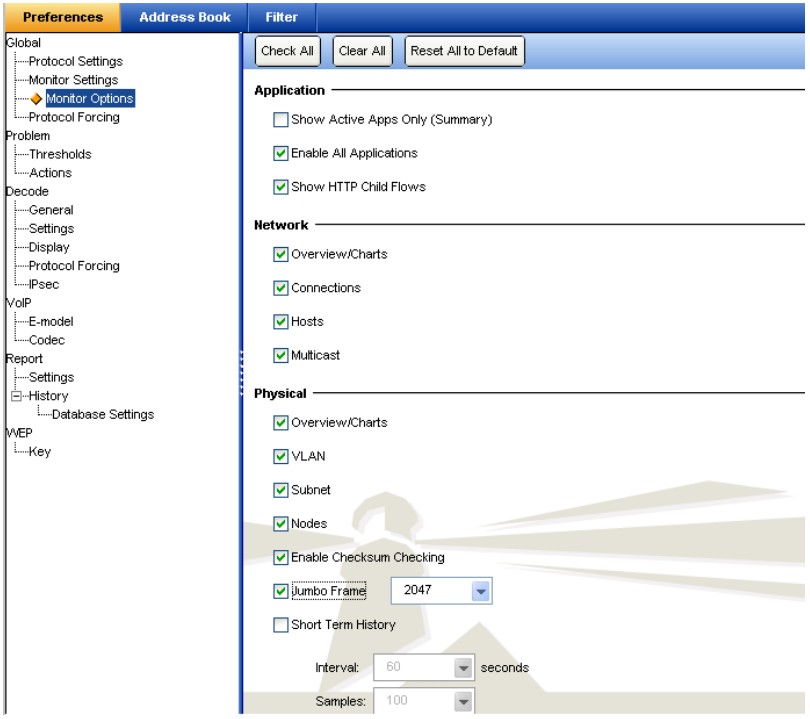


Figure 5-34: The Monitor Options Configuration Screen

Application Layer Options

The **Show Active Apps Only (Summary)** check box lets you set ClearSight's default view to show only active applications in the Application layer Summary screen. However, you can toggle this view between showing active applications only or all applications, as explained in *Choosing Which Applications to Display* on page 110.

The **Enable All Applications** check box lets you control whether application information is processed and displayed. This is useful

when you are not interested in application information, to improve ClearSight's performance for the statistics you *are* interested in. Unchecking this box disables all applications. Checking this box restores all otherwise enabled applications.

The **Show HTTP Child Flows** check box lets you control whether or not child flows will be shown under HTTP flows. This option affects the Monitor, Capture, and Decode functions.

Network and Physical Layer Options

If you know that you are not interested in a particular type of statistic on the network layer or physical layer, you can turn off its collection to improve ClearSight's performance for the statistics you *are* interested in. After restarting ClearSight, the tabs for deselected statistics appear in the display but remain blank.

Specifying Jumbo Frames

If an Ethernet Frame is larger than 1518 bytes (or larger than 1522 bytes if a VLAN ID is included), that frame will normally be classified as an Oversize or Jabber frame. However, you can specify a larger than 1518 (or 1522) value in the **Jumbo Frame** field in **Configuration > Preferences > Global > Monitor Options > Physical**. In that case, frames that are larger than 1518 (or 1522) bytes but equal to or less than the value you specify will be classified as Jumbo frames. If the such a frame has a CRC error, it will be included in the CRC count.

You can select one of four values from the **Jumbo Frames** drop-down list: 2047, 4085, 8191, or 9018.

Suppressing Checksum Messages

Some newer network adapter cards have an option to offload checksum calculation to the card as a performance enhancement. Some cards don't even have that option — their drivers always defer checksum calculations to the card. When such adapters are used, ClearSight will flag many packets as having checksum errors, when in fact the checksum calculation has only been deferred to the card.

To handle this situation, there is an option to suppress these extraneous messages. Simply uncheck the **Enable Checksum Checking** box in **Configuration > Preferences > Global > Monitor Options > Physical**.

Short Term History

If you enable **Short Term History**, the **Overview** tab in the **Physical** layer will be changed to a history view showing trending charts. From the drop-down lists you can choose the number of samples and the time interval between samples.

NOTE: Short Term History applies to real-time monitoring, not to postcapture analysis.

NOTE: Changes made to **Monitor Options** do not take effect until you restart ClearSight.

Global Protocol Forcing Options

Figure 5-35 shows the **Global > Protocol Forcing** screen.

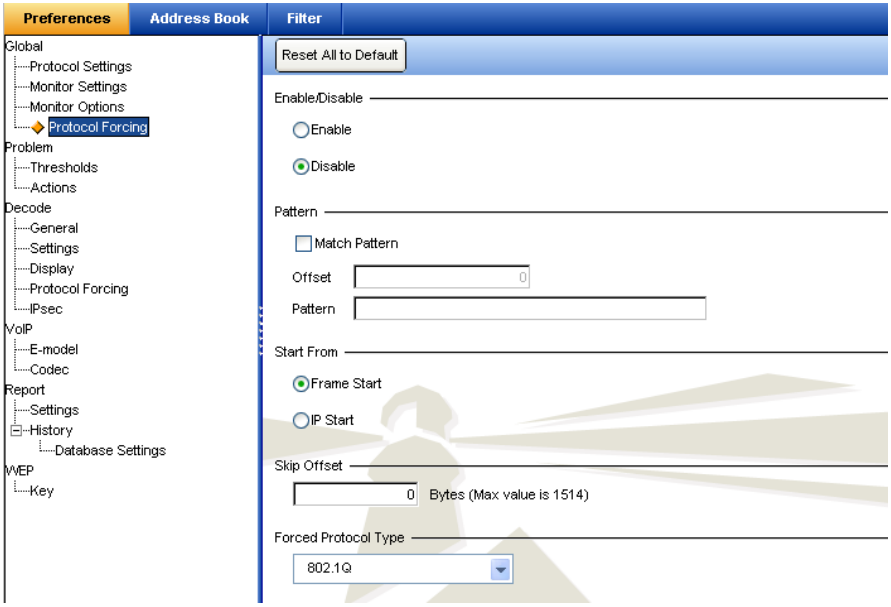


Figure 5-35: The Global Protocol Forcing Configuration Screen

Enable/Disable

The **Enable/Disable** area lets you turn protocol forcing on and off. If you select **Disable**, you can still set the options in the other areas, but they will not be effective until you select **Enable** from this area.

Pattern

The **Pattern** area lets you enter a pattern to be matched for protocol forcing purposes. The **Offset** you enter is always from start of frame. The **Pattern** entry should be in hex. To enable the pattern match, check the **Match Pattern** box.

Start From and Skip Offset

The **Start From** area lets you tell ClearSight where to start looking for a forced protocol.

- If you select **Frame Start**, ClearSight will look at the start of frame plus **Skip Offset**.
- If you select **IP Start**, ClearSight will look at the start of the IP stack plus **Skip Offset**.

Forced Protocol Type

The **Forced Protocol Type** area lets you select a forced protocol from a drop-down list. Note that contents of the list are a function of the choice you make in the **Start From** area.

Problem Thresholds

Use **Problem > Thresholds** to:

- Specify (in milliseconds) the interval over which ClearSight averages quantities, before comparing them with their corresponding threshold values. This is specified by the **Interval** option. By default, this is set to one second (1000 milliseconds).

  Use this option to change the granularity used when identifying a condition as a problem. Larger values will tend to smooth out statistical anomalies while smaller values may place undue importance on momentary bursts. In general, a value close to the default of 1000 seconds provides optimum results.

- Set the actual threshold that define each kind of problem. For more details, see *Setting Thresholds for Problem Reporting* on page 334.

Problem Actions

Use **Problem > Actions** to specify what clearSight should do when a problem is detected. For more details, see *Defining Severities and Actions* on page 324.

Decode

The options available in **Decode** affect the **Decode** tab in post analysis. For details, see *Configuration Options for the Decode Tab* on page 237.

VoIP E-model

Use **VoIP > E-model** (Figure 5-36) to specify values for the quantities you want to use in the calculation of R-values for VoIP flows.

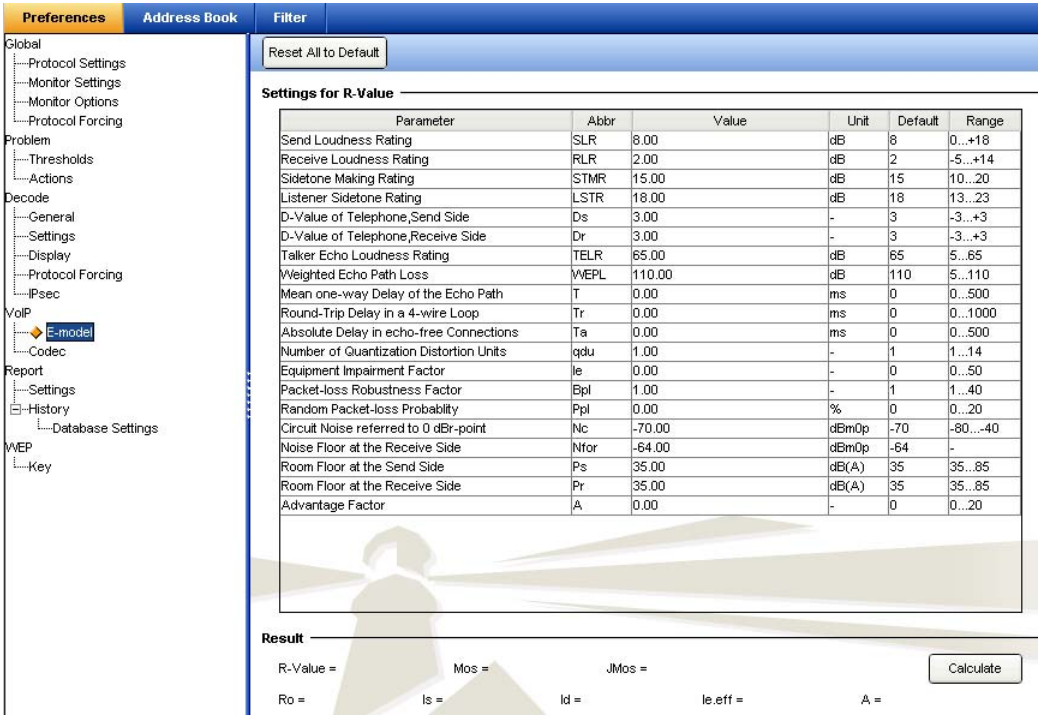


Figure 5-36: E-Model Calculator

VoIP Codec

Use **VoIP > Codec** to specify whether you want the **AMR** to be **GSM** or **3GPP**.

Report Settings

Use **Report > Settings** to customize the format of reports, and to add customer identifying information. For details, see *Controlling the Report Format* on page 371.

History Report Database Settings

Use **Report > History > Database Settings** to specify what data the History reporter should accumulate, and how long it should retain that data. For details, see *Controlling the Accumulation of Data* on page 392.

WEP Key

Use **WEP > Key** to specify whether the WEP encryption keys for wireless traffic should be 128 bits, 64 bits, or none.

The Address Book Tab

Use the **Address Book** tab to build an address book. For details, see *Working with the Address Book* on page 364.

The Filter Tab

Use the **Filter** tab to open the **Filter List** dialog box. From there you can click a Create button to access the **New Filter** dialog box, where you can create a new filter. For details, see *Using Defined Filters* on page 274.

Changing Window Styles

You can change the appearance of the windows in ClearSight by selecting **Look and Feel** from the **Tools** menu. Figure 5-37 shows the available window styles.

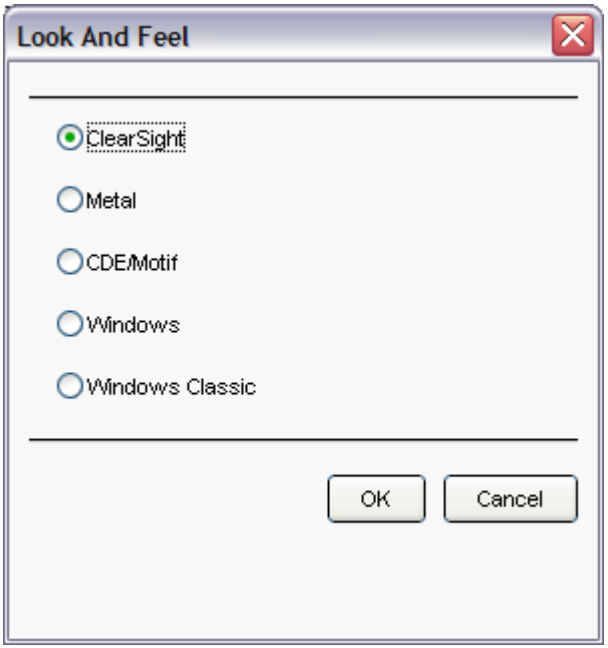


Figure 5-37: The Look and Feel Dialog Box

Chapter 6

Capturing Data with ClearSight

This chapter describes how to use ClearSight to capture data. It includes the following major topics:

- *About Capture*
- *The Capture Workspace*
- *Observing the Capture in Progress*

About Capture

In contrast to real-time monitoring, ClearSight's *capture* feature stores traffic that passes your capture filters into a *capture buffer* for postcapture analysis. Capturing data can provide you with the level of detail you need to solve tough network problems. Once you have a buffer or trace file of captured data, you can use ClearSight's postcapture analysis capabilities (described in Chapter 7, *Postcapture Analysis*) to see what is really happening on your network.

You can also use commands in the **File** menu to save trace files of frames still in the capture buffer for later postcapture analysis. ClearSight provides the same postcapture analysis features for trace files as it does for freshly captured data in the capture buffer.

The Capture Workspace

As with all ClearSight features, you use the toolbar to start working with capture features. The toolbar provides controls for starting and stopping capture, as well as viewing the results of the capture in various postcapture analysis pages.

Click the **Capture** (Figure 6-1) button in the toolbar to display the Capture workspace (Figure 6-2).

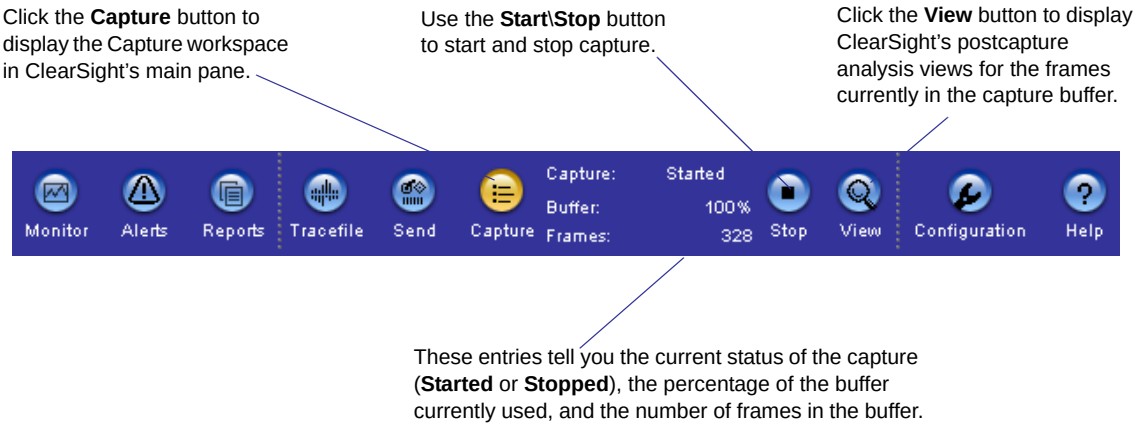


Figure 6-1: Capture Controls in the Toolbar

The Capture workspace adds a **Capture** layer to the standard entries in the Layers pane. The gauges provide you with quick information on the status of the buffer. Click the **Capture** entry in the Layers pane to view the capture workspace in the main pane.

The Capture workspace includes tabs that let you see statistics for the capture in progress, create and select filters, adjust buffer settings, customize the view within the Layers pane, create and select triggers, and view issues and problems.

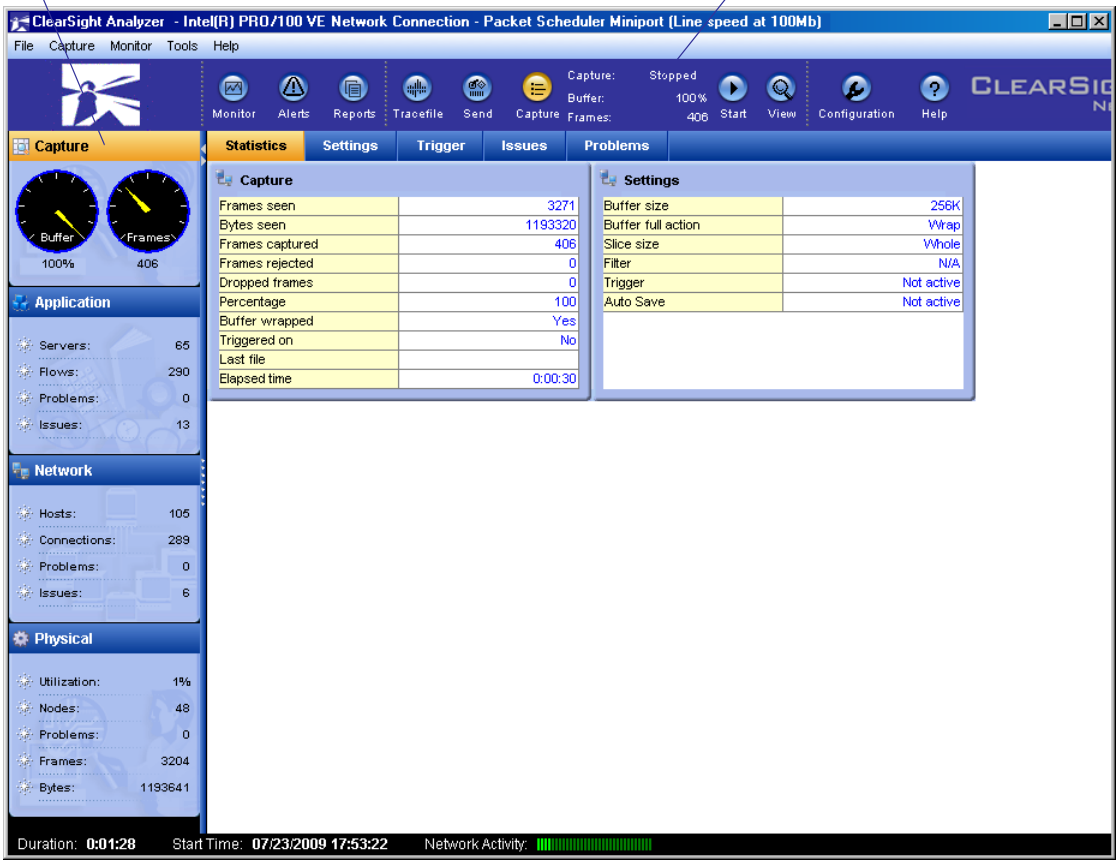


Figure 6-2: The Capture Workspace

The Capture workspace (Figure 6-2 on page 203) consists of the following tabs:

Statistics The **Statistics** tab contains two panes — the **Capture** pane and the **Settings** pane. The **Capture** pane provides statistics for the capture in progress, or if the capture has stopped, the contents of the capture buffer. The **Settings** pane provides a summary of the current buffer settings, which you can change by adjusting parameters in the **Settings** tab. For details, see *The Statistics Tab* on page 205.

Settings Lets you control a variety of functions related to the capture process:

- Lets you select a filter for use in the next capture session. Also lets you create a new filter.
- Lets you set buffer management options for capture.
- Lets you customize the view in the Layers pane.
- Lets you disable the Monitor during capture.

For details, see *The Settings Tab* on page 206.

Trigger Lets you set up specific conditions that determine when capture starts and stops. For details, see *The Trigger Tab* on page 213.

Issues Reports issues detected during the current capture session, but only for packets that pass the current capture filter. For details see *Issues Tab Information* on page 127.

Problems Reports problems detected during the current capture session, but only for packets that pass the current capture filter. For details see *Problems Tab Information* on page 128.

The Statistics Tab

Table 6-1 describes the counters in **Capture** pane of the **Statistics** tab. These counters show values for the capture currently in progress or, if capture has stopped, the frames currently in the capture buffer.

Table 6-1: Statistics Tab Counters in the Capture Pane

Counters	Description
Frames seen	The number of frames ClearSight has seen on the network during this capture session.
Bytes seen	The number of bytes ClearSight has seen on the network during this capture session.
Frames captured	The number of frames ClearSight has copied from the network and into the capture buffer during this capture session.
Frames rejected	The number of frames ClearSight has seen but not captured because of a capture filter.
Dropped frames	The number of frames ClearSight has dropped during this capture session. For the Gigabit-SC1 or Gigabit-XD card, this counter increments when an exception occurs while ClearSight is processing the current frame. For all other adapter cards, this counter increments while ClearSight is processing the current frame, or if ClearSight's internal buffer is overrun.
Percentage	The percentage of the capture buffer currently occupied by captured data.
Buffer wrapped	Whether or not the capture buffer has wrapped (Yes or No).
Triggered on	Whether or not a trigger was used to start or stop capture (Yes or No).
Last file	The file name used the last time the buffer was saved.
Elapsed time	The amount of time that has elapsed since the start of capture.

The **Settings** pane lists the current values of the buffer settings. You can change these values through selections you make in the **Settings** tab. For details, see *The Settings Tab* on page 206.

The Settings Tab

Before starting a capture, set the options in the **Settings** tab to tune capture buffer performance for your network analysis needs. Set these options carefully to make sure that the frames you need are still available in the buffer for postcapture analysis when you have finished capturing data.

Figure 6-3 shows the **Settings** tab.

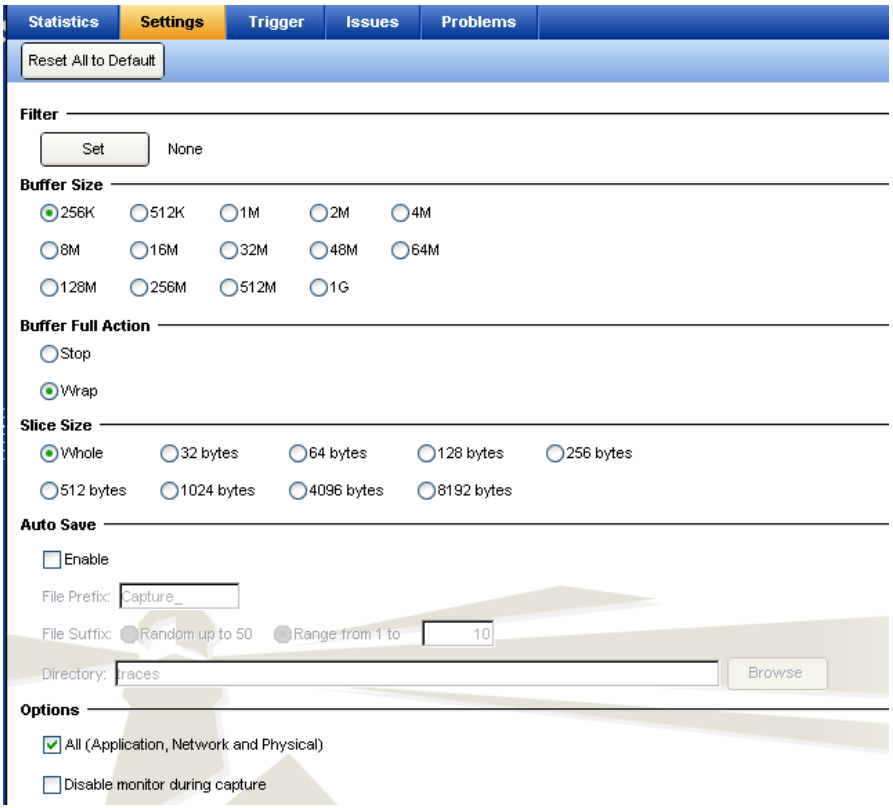


Figure 6-3: The Settings Tab

As shown in Figure 6-3, you can set the following:

- **Filter** (page 207)
- **Buffer Size** (page 208)
- **Buffer Full Action** (page 208)
- **Slice Size** (page 209)
- **Auto Save** (page 209)
- **Options** (page 210)

Selecting a Filter

The **Filter** area in the **Settings** tab lets you select a filter to apply to a capture session. Capture filters limit which frames are stored in the capture buffer, providing you with the means of focusing the capture on just that data which interests you.

ClearSight's postcapture analysis capabilities rely on the data gathered by the capture feature. However, the bandwidth and speed of modern networks make it easy to overwhelm your capture buffer with data that doesn't interest you. Filters give you a way to sharpen ClearSight's focus, examining the data that interests you and ignoring the data that does not.

If a filter is currently selected, the name of that filter is displayed in the **Filter** area. To deselect that filter, click the **Remove** button. The filter name will then be replaced by **None** to indicate that no filter currently applies. The name of the button changes to **Set** to indicate that you can set (select) a new filter.

If you click on the **Set** button, the **Filter List** dialog box (Figure 6-4) appears. You can then choose the filter you want from the list of currently defined filters.

You can create a new filter by clicking the **Create** button at the lower left. For details on how to create new filters (or edit existing filters) see Chapter 9, *Using Filters*.

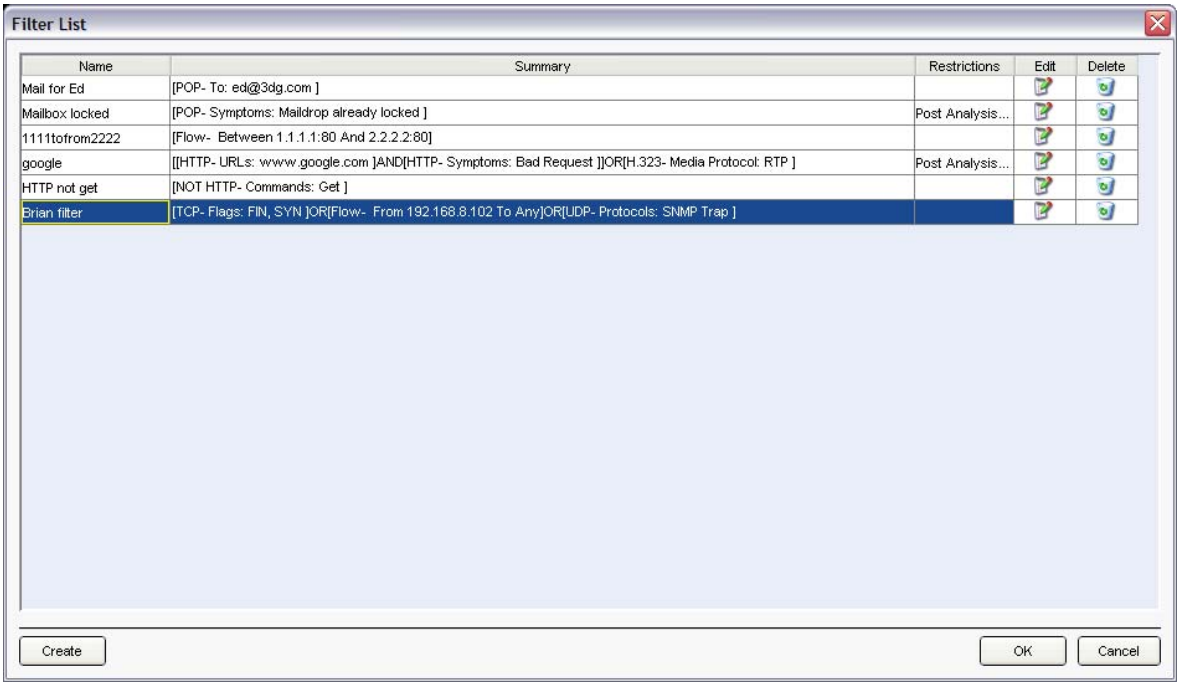


Figure 6-4: The Filter List Dialog Box

Setting the Buffer Size

The **Buffer Size** option specifies how much memory ClearSight uses for captured frames. ClearSight supports large buffer sizes, up to 25% of the physical memory installed in the PC. However, the larger the capture buffer, the longer it will take ClearSight to perform postcapture analysis. Try to balance buffer sizes with your need for speed.

Specifying the Buffer Full Action

The **Buffer Full Action** tells ClearSight what to do when the capture buffer fills with incoming frames. ClearSight can either **Stop** capture or **Wrap** the buffer:

- If you select the **Stop** option, ClearSight stops capturing data when the buffer fills. No more frames will be captured.

- If you select the **Wrap** option, ClearSight overwrites the oldest frames in the buffer with newly arriving frames. ClearSight continues to do this, wrapping the buffer continuously until the capture is stopped.

If you enable the **Wrap** option, and you have not enabled any form of trigger to stop capture, make sure that you stop the capture manually after you have the data you need for postcapture analysis. Otherwise, you may overwrite the data you need.

Setting the Slice Size

The **Slice Size** option tells ClearSight how much of each lower layer frame to capture. The remaining portion of each frame is "sliced" off and not stored in the capture buffer.

Slicing frames reduces the amount of data stored in the buffer for each captured frame. Because of this, your available buffer space will last longer with slicing enabled. However, you should be careful to set the **Slice Size** option in such a way that it does not slice off data you need for postcapture analysis.

Lower layer frames include upper layer data. You typically want to preserve the headers of upper layer frames for postcapture analysis. When an upper layer frame is encapsulated completely within a single lower layer frame, most normal slice sizes will leave the header of the encapsulated upper layer frame. However, frames from many upper layer protocols can span multiple lower layer frames, with a header starting at any point in the lower layer frame. In situations like this, you may want to select **Whole** so that you capture the data you need for postcapture analysis.

Setting the Auto Save Parameters

The **Auto Save** feature lets you automatically save trace files when the capture buffer becomes full. The options are:

- By default, **Auto Save** is **Disabled**. If you want to enable **Auto Save**, click the **Enable** check box.

- **File Prefix** is the first part of the name for the trace files you want to save. The default is Capture_.
- **File Suffix** adds a number sequence to your trace files. You can select **Range from 1 to:** or add incremental wraps to an already completed range of files. For example, if you have completed a range of 1-20 files, select **Random** and you can continue to save the trace files starting at Capture_21.

  NOTE: The size of each file is approximately equal to the buffer size. The disk space required will be determined by the number entered in the **Range from 1 to:** option. For example, if you enter 10, and the buffer size is 128 MB, these 10 files will occupy approximately 1.28 GB of hard drive space.
- In the **Directory** box, type in the directory name where you want to save your files. The default is *traces*. Alternatively, you can browse to the desired directory.

  NOTE: Prior to Version 5.1 ClearSight Distributed did not allow this browse option — the files had to be saved in the *traces* directory. Beginning with Version 5.1, ClearSight Distributed lets you save these files to a directory of you own choosing. The only remaining restriction is that the directory must be on the Agent's PC.

Setting the Capture Options

The **Options** area provides the following additional settings that help you to optimize performance versus features while capturing.

The All (Application, Network and Physical) Option

The **All (Application, Network and Physical)** check box lets you determine whether ClearSight will process network traffic while capturing frames to a capture buffer. If this box is unchecked, ClearSight will not process the frames, thus reducing the processing overhead while the capture is in progress. The processing can be done later, either by using the **View** button on ClearSight's toolbar, or by saving the buffer as a trace file.

Figure 6-5 shows how the state of the **All (Application, Network and Physical)** check box affects the appearance of the Layers pane in the capture display, when you are actively capturing frames.

In addition, checking this box causes the **Issues** and **Problems** tabs to be present in the capture workspace.

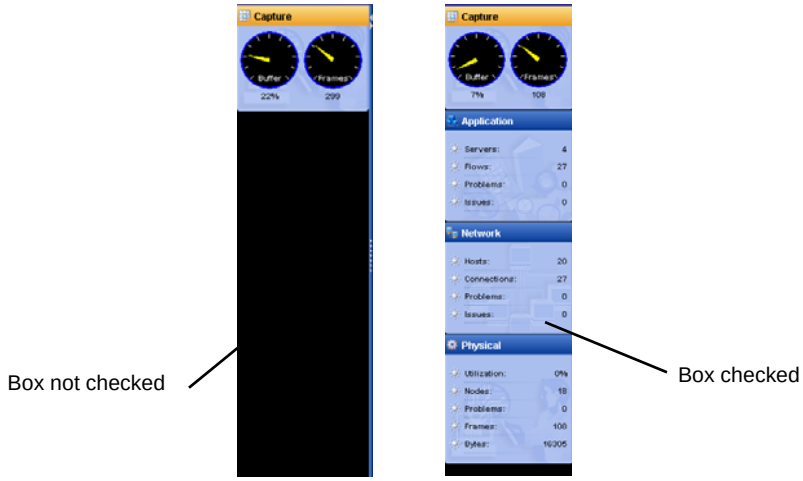


Figure 6-5: Changing the ClearSight View

NOTE: When you change this option, the change will take effect the next time you start ClearSight.

The Disable monitor during capture Option

If the **Disable monitor during capture** box is checked, the operation of the Monitor will be paused when a capture starts, and will resume when the capture stops.

NOTE: When you change this option, the change will take effect the next time you start a capture.

Real-Time Monitoring During Capture

During capture (unless you have checked **Disable monitor during capture**) you can still use all of the real-time monitoring displays described in Chapter 5, *Monitoring the Network with ClearSight*. ClearSight does not stop updating the real-time monitoring displays during capture — it just provides some additional displays detailing the capture in progress. See *Observing the Capture in Progress* on page 216 for details on these displays.

The Trigger Tab

The **Trigger** tab lets you specify when ClearSight should start and stop capturing frames. Figure 6-6 shows the **Trigger** tab.

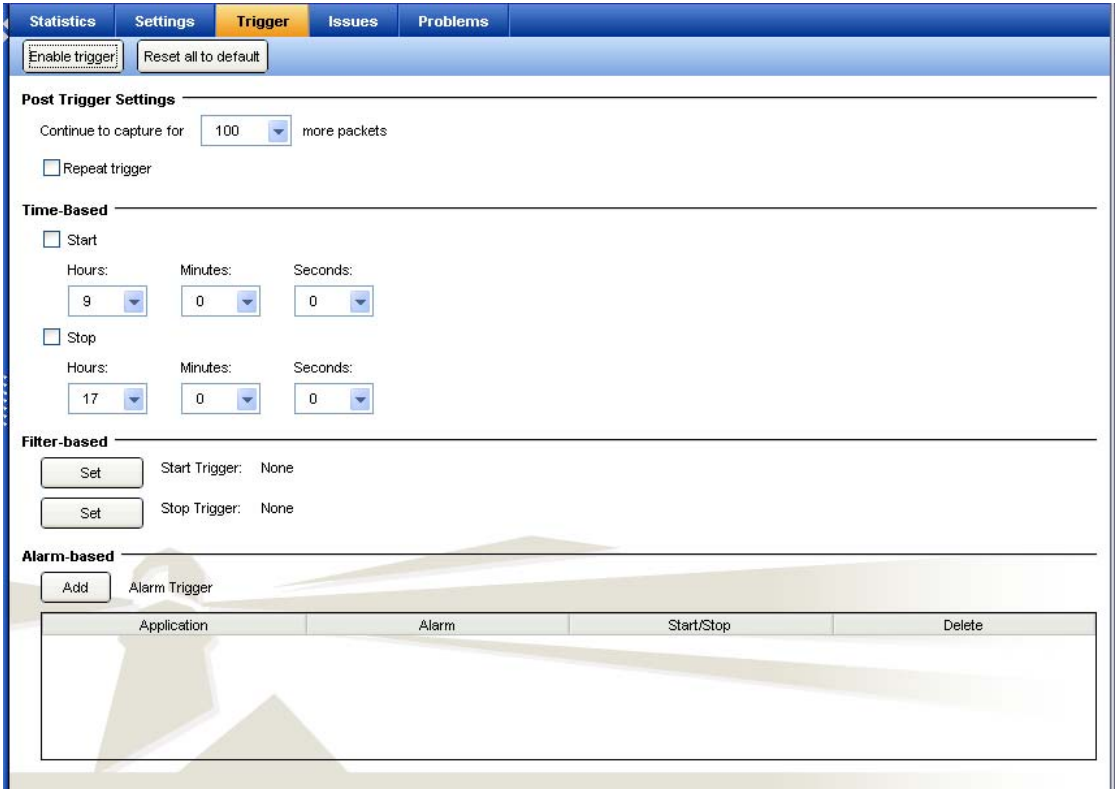


Figure 6-6: The Trigger Tab

As shown in Figure 6-6, you can set the following trigger options:

- **Post-Trigger Settings** (page 214)
- **Time-Based** (page 214)
- **Filter-Based** (page 214)
- **Alarm-Based** (page 214)

To actually use the trigger settings, click the **Enable trigger** button. To stop using the trigger settings, click **Disable trigger**.

Setting the Post-Trigger Settings

In this area you can specify how many more packets ClearSight should capture after a trigger event occurs. Choose the value you want from the drop-down list.

If you check the **Repeat Trigger** box, capturing will again start or stop if the trigger event occurs again.

Setting Time-Based Triggers

In this area you can set a simple time-of-day criterion for starting and/or stopping capture. Check the **Start** and/or **Stop** box and select the appropriate time(s) of day from the drop-down lists.

Setting Filter-Based Triggers

In this area you can use a filter to trigger start or stop of capture when ClearSight sees a packet that passes the specified trigger. If such a trigger is already selected, its name will be shown and the corresponding button will say **Remove**. If no trigger is selected, **None** will be shown and the button will say **Set**. Clicking on that button will then display the **Filter List** dialog box, and you can select the filter you want from the list of defined filters.

NOTE: If a filter shows **Post Analysis Only** in the **Restrictions** column, you cannot use it as a trigger.

Setting an Alarm-Based Trigger

In this area you can create a list of alarm-based triggers to start or stop capture. Initially, the list will be empty, as shown in Figure 6-6. If you click on the **Add** button, the Alarm-Based Trigger dialog box (Figure 6-7) will appear.

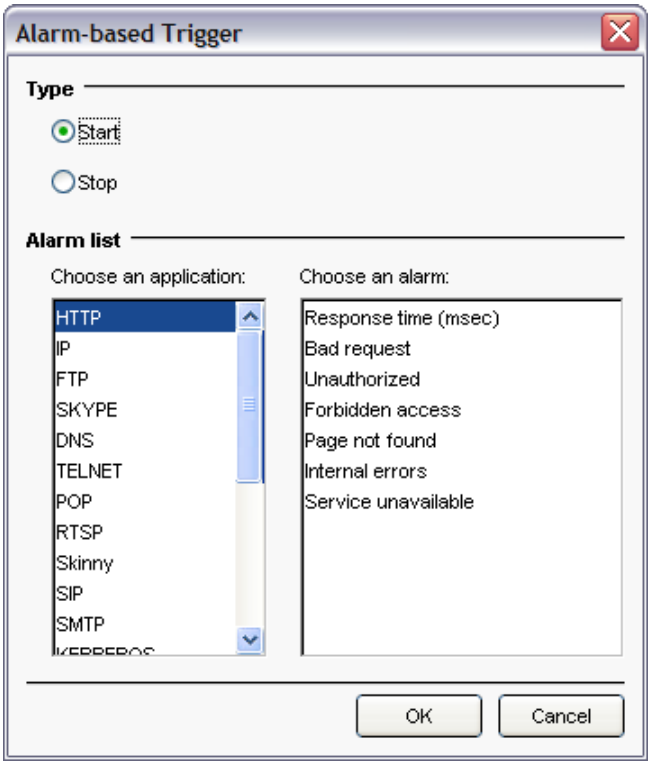


Figure 6-7: The Alarm-Based Trigger Dialog Box

In the **Type** area, you can select whether the trigger will start or stop capture. Then, in the **Alarm list** area, you select an application, and then choose a pre-defined alarm from the application-specific list that appears in the **Choose an alarm:** box. When you have chosen the alarm, click **OK**, and that alarm will be added to the **Alarm-Based Trigger** list.

To actually use an alarm trigger, set the corresponding problem's threshold in **Configuration > Preferences > Problem > Thresholds > Problems**, and enable problem generation by checking the box in **Configuration > Preferences > Decode > General > Problem Generation**.

Observing the Capture in Progress

Once you have set up the capture buffer for your needs, you can start the capture by clicking the **Start** button in the toolbar or, alternatively, selecting the **Start** option from the **Capture** menu. In response, ClearSight starts capturing frames off the network and storing those that pass your capture filters in the capture buffer. Also:

- The gauges in the **Capture** layer in the Layers pane begin to increment, showing you how many frames are in the buffer and what percentage of available buffer space they occupy.
- If the **All (Application, Network and Physical)** box is checked, the displays in the Capture workspace for all of the other usual layers — **Application**, **Network**, and **Physical** — begin to increment as well, though only for traffic that passes the current capture filter.
- If the **Disable monitor during capture** box is unchecked, the real-time monitoring displays continue to update with newly detected flows, statistics, and counters.

  NOTE: As mentioned above, the real-time monitoring displays are unfiltered. While the layer displays in the Capture workspace only show flows, connections, and nodes from traffic that has passed the current capture filter, the real-time monitoring displays show *all* traffic. The displays are identical with the exception of the **Capture** layer entry at the top of the Layers pane — use this entry to determine which displays you are viewing. Switch between the two workspaces using the **Monitor** and **Capture** buttons in the toolbar.
- The counters in the Capture workspace's **Statistics** tab begin to increment, providing you with real-time feedback on the progress of the capture. The counters in the **Statistics** tab are described below.
- If the **All (Application, Network and Physical)** box is checked, the **Issues** and **Problems** tabs begin to fill with any issues and problems associated with traffic that passed the current capture filter.

Chapter 7

Postcapture Analysis

This chapter describes ClearSight's postcapture analysis capabilities. The chapter includes the following topics:

- *About Postcapture Analysis*
- *Working with Postcapture Analysis Displays*
- *Working with the Decode Tab*
- *Configuration Options for the Decode Tab*
- *Working with Trace Files*

About Postcapture Analysis

During postcapture analysis, ClearSight brings all of its troubleshooting capabilities together in a single workspace to help you understand and analyze captured network data. Postcapture analysis takes place in a set of integrated tabs, each of which provides access to a specific set of analysis functions.

Foremost among the tabs in the postcapture analysis workspace is the **ClearSight** tab (located under **Tracefile** in the tool bar). The **ClearSight** tab provides for postcapture analysis all of the same

functionality found in the real-time monitoring displays, tracking application layer servers and flows, network layer connections and hosts, and physical layer VLANs and nodes.

In addition to the **ClearSight** tab, the postcapture analysis workspace provides the familiar tri-paned **Decode** display for detailed protocol analysis. In most cases, however, the other tabs in ClearSight's postcapture display help you troubleshoot your problems before you have to go through the hexadecimal code.

When you do need to go to the **Decode** tab, ClearSight's *smart navigation* and *automatic filtering* capabilities make it easy to move between the **ClearSight** and **Decode** tabs and see just those frames that interest you.

- *Smart navigation* lets you click on a command in a **Conversation** tab in the **ClearSight** tab and go directly to a **Decode** tab filtered on the parent flow with the corresponding frame selected. Similarly, options in the **Decode** tab let you go directly to a selected frame's IP or Application flow in the **ClearSight** tab.
- *Automatic filters* let you right-click on an entry in the **ClearSight** tab and temporarily filter the **Decode** tab of all traffic except that from a selected application, flow, server, host, or station.

Working with Postcapture Analysis Displays

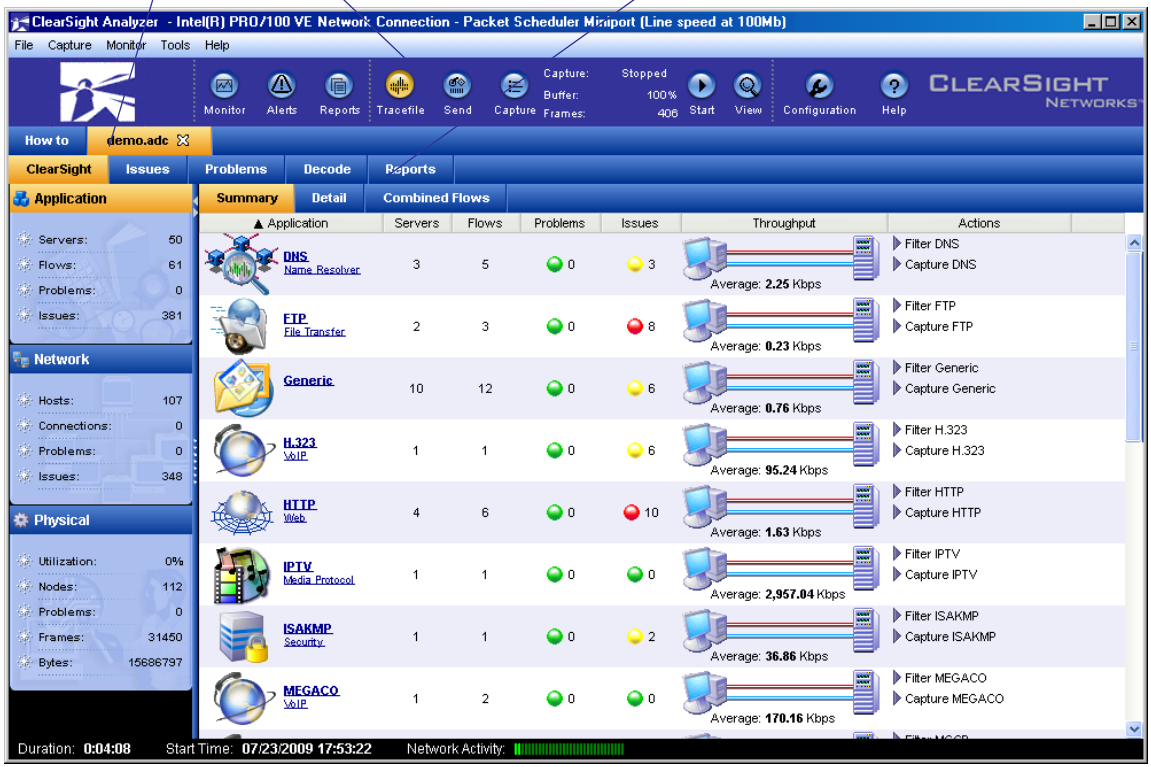
ClearSight can perform postcapture analysis on either the frames currently in the capture buffer or in a saved trace file.

- To perform postcapture analysis of the frames currently in the capture buffer, click the **View** button in the toolbar.
- To perform postcapture analysis of a trace file, use the **File > Open** command to open the desired trace file.

Regardless of whether you are analyzing a buffer or trace file, the postcapture analysis workspace appears in the same way (Figure 7-1).

As you can see from the selected icon in the toolbar, the postcapture analysis workspace is currently showing a trace file. The title bar for the workspace shows the name of the trace file.

Postcapture analysis takes place in a set of integrated tabs. The **ClearSight** tab (shown) gives you access to all of the same features available during real-time monitoring. In addition, you can see traditional, tri-paned protocol analysis in the **Decode** tab. Smart navigation and automatic filters make it easy to move between the two tabs.



In addition to the **ClearSight** and **Decode** tabs, the postcapture analysis workspace also provides alert tabs (**Issues** and **Problems**), and a **Reports** tab.

Figure 7-1: The Postcapture Analysis Workspace

As shown in Figure 7-1, the postcapture analysis workspace consists of multiple integrated tabs. Table 7-1 lists and describes the tabs available in the postcapture analysis workspace.

Table 7-1: Tabs in the Postcapture Analysis Workspace

Tab	Description
ClearSight	The **ClearSight** tab provides for postcapture analysis all of the same functionality found in the real-time monitoring displays, tracking application layer servers and flows, network layer connections and hosts, and physical layer VLANs and nodes. For detailed information on working with and understanding the displays in the **ClearSight** tab, see Chapter 5, *Monitoring the Network with ClearSight*. **NOTE:** In the postcapture analysis workspace, there is an additional tab, **TCP Data**, in the **Detail** tab whenever the TCP protocol is involved. You can view the TCP Data in either ASCII or Hex characters. You can copy and paste from the TCP Data tab, and you can also save its contents to a file.
Issues	The **Issues** tab provides for postcapture analysis all of the same functionality found in the **Issues** tab in the Alert Log, reporting minor network errors. See Chapter 10, *Working with Alerts* for information on working with the **Issues** tab. In postcapture analysis, the **Issues** tab provides an additional *drill-down* feature. If you right-click on a particular issue, you are given a chance to jump to detailed information on the specific application flow, network connection, or other item that is the source of the issue.
Problems	The **Problems** tab provides for postcapture analysis all of the same functionality found in the **Problems** tab in the Alert Log, reporting network problems detected in the current buffer or trace file. See Chapter 10, *Working with Alerts* for information on working with the **Problems** tab. In postcapture analysis, the **Problems** tab provides an additional *drill-down* feature. If you right-click on a particular problem, you are given a chance to jump to detailed information on the specific application flow, network connection, or other item that is the source of the problem.

Table 7-1: Tabs in the Postcapture Analysis Workspace (Continued)

Tab	Description
Decode	The **Decode** tab provides you with the familiar tri-paned protocol decode display, breaking out each captured frame by protocol layer and translating the protocols into natural language text. This chapter describes how to understand and work with this tab, as well as how to access it in an intelligent way from the **ClearSight** tab.
Reports	The **Reports** tab provide the same reports for postcapture analysis that are available during real-time monitoring by clicking the **Reports** button in the ClearSight toolbar. See Chapter 12, *Using Reports* for information on working with reports.

Smart Navigation between the ClearSight and Decode Tabs

During postcapture analysis, you will spend most of your time in the **ClearSight** and **Decode** tabs. ClearSight provides *smart navigation* techniques that let you move quickly and precisely between these two tabs to locate the frames displaying problems. Specifically, smart navigation lets you:

- Click on a command in a **Conversation** tab in the **ClearSight** tab and go directly to a **Decode** tab filtered on the parent flow with the corresponding frame selected.

  This technique is described in *Smart Navigation from the ClearSight Tab* on page 222.

- Select a frame in the **Decode** tab and click the **Jump to a related page** button  to go directly to the selected frame's IP or Application flow in the **ClearSight** tab.

  This technique is described in *Smart Navigation from the Decode Tab* on page 224.

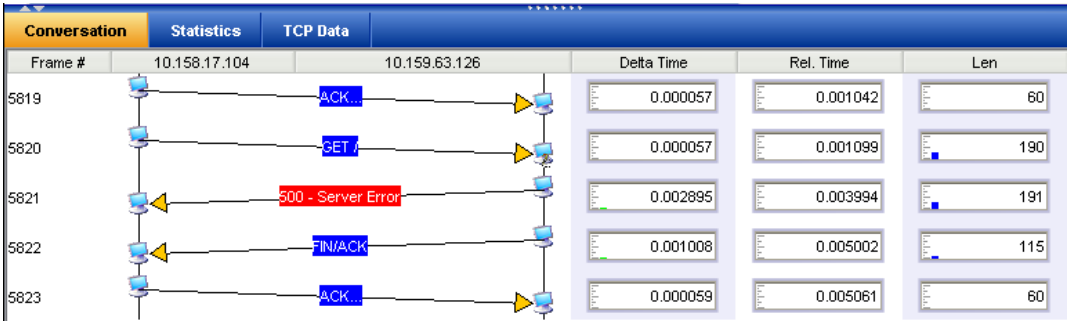
Smart Navigation from the ClearSight Tab

Just as in the real-time monitoring displays, postcapture analysis in the **ClearSight** tab rebuilds the request and reply exchanges between clients and servers and visually displays them in network ladder diagrams in the **Conversation** tab for a selected flow.

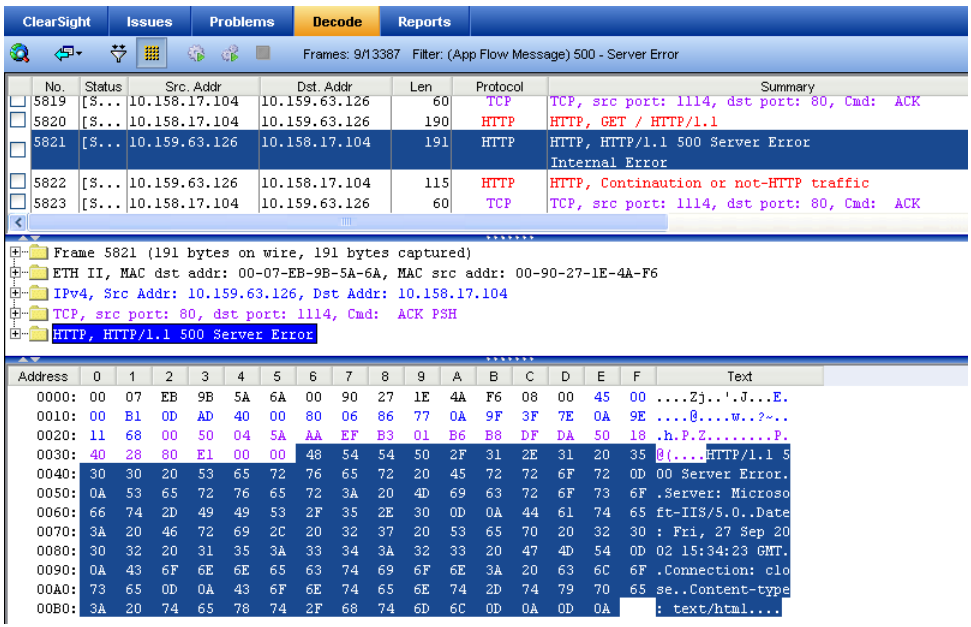
Within a **Conversation** tab diagram, requests or replies displaying problems are shown in different colors depending on the severity of the problem. You can click on an offending request or response in a **Conversation** tab diagram to go directly to the protocol decode for the exact offending frame in the exact selected flow. This way, ClearSight takes the work out of protocol analysis — it shows you a problematic frame and takes you straight to a protocol decode filtered specifically for the flow containing the frame, with the offending frame selected.

For example, Figure 7-2 illustrates moving from a **404 - Object Not Found** response from an HTTP server in a **Conversation** tab diagram directly to a **Decode** tab filtered on the parent flow with the offending frame selected.

NOTE: You are not limited to clicking on just problematic frames in the **Conversation** tab. Clicking on *any* frame shown in a **Conversation** tab takes you to a **Decode** tab filtered on the parent flow with the corresponding frame selected.



Click the frame in the **Conversation** tab to see the decode.



Clicking on an entry in a **Conversation** tab takes you directly to the entry for that frame in the **Decode** tab. Notice that the selected frame's number matches in both displays (**5821**). This *smart navigation* technique makes it easy to move from the **ClearSight** tab to the **Decode** tab.

In addition, the **Decode** tab is automatically filtered so that only frames in the flow containing the selected frame are shown.

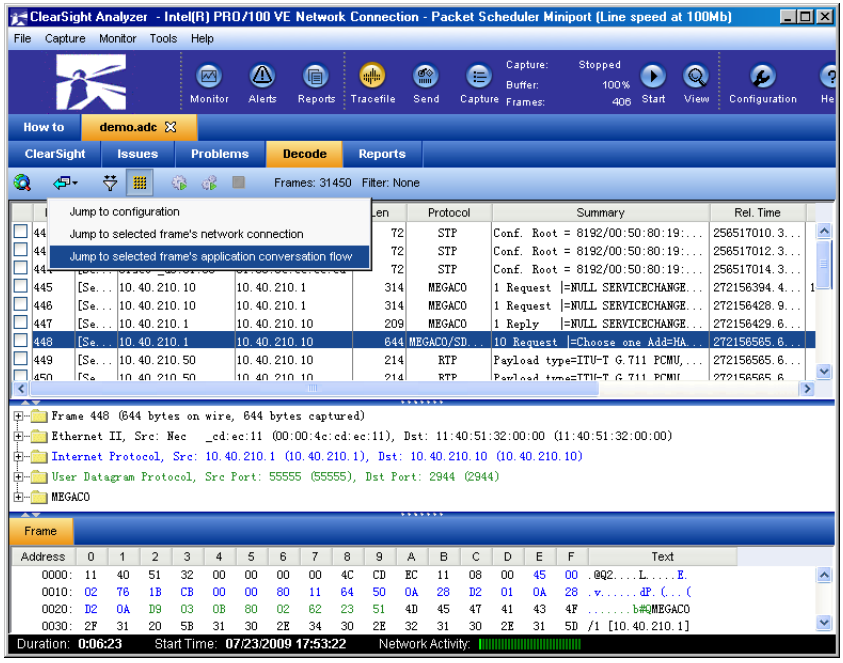
Figure 7-2: Smart Navigation from the Conversation Tab

Smart Navigation from the Decode Tab

Sometimes, working with protocol decodes is the only way to get to the root of a network problem. However, when working with trace files containing tens of thousands of frames, it can be easy to get lost in protocol decodes.

ClearSight provides you with an easy way to climb out of the code and gain an unobstructed view on network traffic as a whole. When you work with the **Decode** tab, you can select a frame in the Summary pane and click the **Jump to a related page** button  to go directly to the selected frame's IP connection or Application Conversation in the **ClearSight** tab. Sometimes, a change of perspective is all that is required to see a network problem clearly.

Figure 7-3 illustrates using the **Jump to a related page** button to navigate from a Q.931 Alerting message in the Decode tab to its parent application flow in the ClearSight tab.



You can use the **Jump to a related page** button to move from a selected frame's entry in the **Decode** tab to its parent Application or IP flow in the **ClearSight** tab.

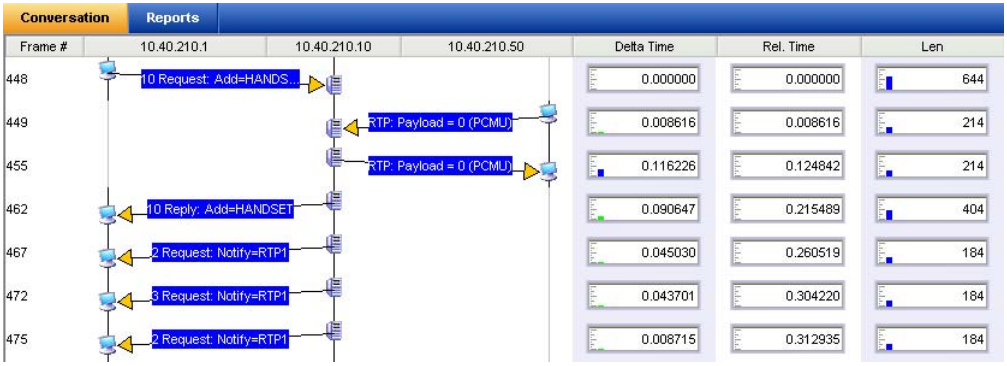


Figure 7-3: Smart Navigation from the Decode Tab

Using Automatic Filters in the Postcapture Displays

Automatic filters are generally available by right-clicking an entry in either the **ClearSight** or **Decode** tabs. In response, a context menu appears with a variety of automatic filters available for the selected entry. Depending on the selected tab, both display and capture filters may be listed. Select a display filter using the commands that start **Filter *xxx*.** Select a capture filter using the commands that start **Capture *xxx***.

The exact filters available depend on the selected layer, pane, and entry. Typically, automatic display filters are available explicitly for the selected entry's address(es) and port(s), as well as for a variety of common wild-card filtering scenarios using different combinations of the selected address(es) and port(s).

Once you select an automatic display filter, ClearSight automatically displays the **Decode** tab with your filter applied. To remove the filter, either apply a new automatic filter from the **ClearSight** tab or click the **Filter On\Off** toggle button  in the **Decode** tab's status bar.

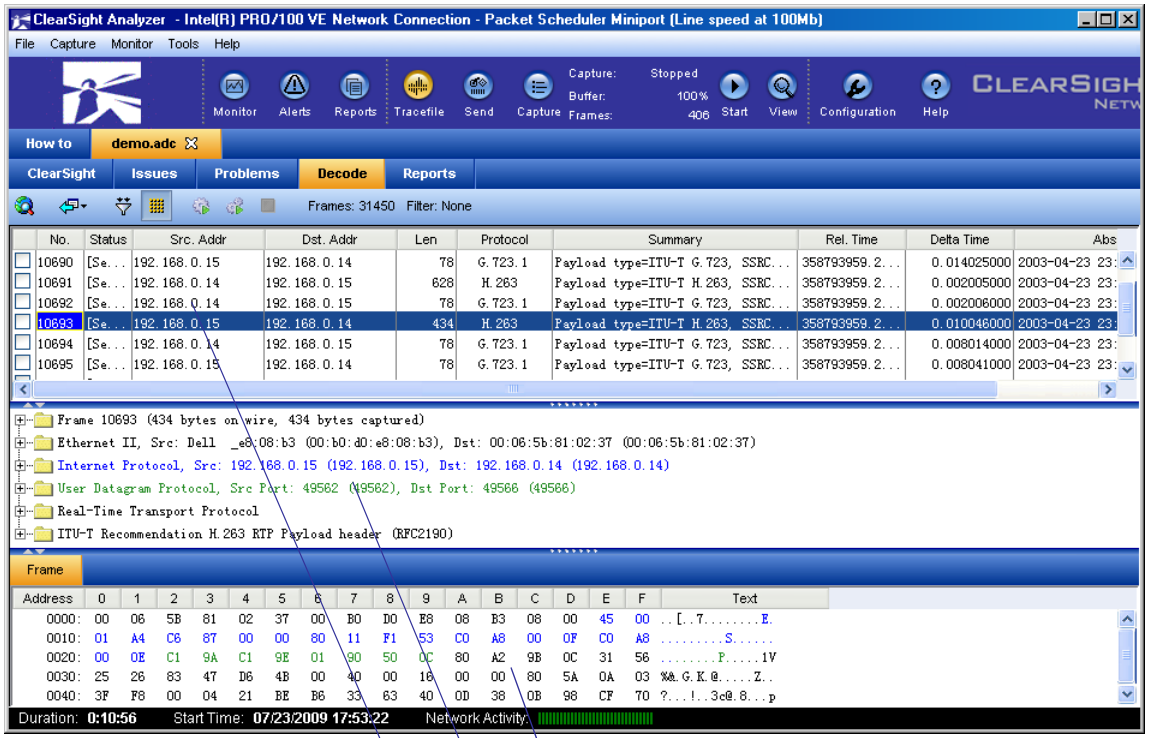
See *Using Automatic Filters* on page 272 for a full discussion of how to use automatic filters.

Working with the Decode Tab

This section describes how to work with the **Decode** tab in the postcapture analysis workspace. In most cases, ClearSight's network analysis capabilities let you troubleshoot your network without ever having to look at a traditional protocol decode. Sometimes, you still want to see a traditional decode breaking out the actual protocol layers embedded in each captured frame. ClearSight provides you with this functionality in the **Decode** tab.

Figure 7-4 shows an example of the **Decode** tab.

ClearSight's **Decode** tab provides a traditional tri-paned protocol decode. A title bar shows the name of the trace file being displayed. The **Search** button lets you search through the display for a particular frame. The **Jump to a related page** button lets you navigate to a selected frame's Application or IP flow in the **ClearSight** tab. The **Apply Filter** button lets you select a filter. The **Filter On/Off** button lets you turn the filter on and off.



The **Decode** tab's three panes — **Summary**, **Detail**, and **Hex** — work together to show you the various protocol layers embedded in a frame. The **Summary** pane lists each captured frame on a single line with an overview of its source and destination addresses, the highest layer protocol in the frame, and various timing information. The **Detail** pane shows each of the layers of the frame selected in the **Summary** pane. You can cascade open each of the layers to see the various fields in the frame decoded into natural language. The **Hex** pane shows both the hexadecimal and ASCII translation of the frame selected in the **Summary** pane. The highlight in the **Hex** pane updates according to the protocol layer selected in the **Detail** pane, so you can see exactly which hex code corresponds to which protocol layer in the frame.

Figure 7-4: The Decode Tab

Panes in the Decode Tab

As shown in Figure 7-4, the **Decode** tab contains three panes that work together to show you the various protocol layers embedded in a frame:

- The **Summary** pane is at the top of the **Decode** tab.
- The **Detail** pane is in the middle of the **Decode** tab.
- The **Hex** pane is at the bottom of the **Decode** tab.

The Summary Pane

The **Summary** pane is at the top of the **Decode** tab. It lists each captured frame on a single line, providing a condensed view of the source and destination addresses, the highest layer protocol in the frame, and various timing information.

You can scroll through the **Summary** pane to see the entries for each of the frames in the buffer or trace file. Selecting an entry causes the **Detail** and **Hex** panes to update with decode information for the selected frame.

If ClearSight finds an address listed in the **Decode** tab in its Address Book, it will substitute the name for the address in the decode displays.

By default, ClearSight lists each frame in the **Summary** pane with the fields listed in Table 7-2. You can use the options in the **Configuration > Decode Settings** tab to select a subset of these fields. See *Configuration Options for the Decode Tab* on page 237 for details.

Table 7-2: Summary Pane Fields

Field	Description
Checkboxes	Use the checkboxes in this column to select multiple frames. You can perform different actions on checked frames by right-clicking in the **Summary** pane and selecting one of the available commands in the context menu that appears. See *Context Menu Commands in the Summary Pane* on page 230 for details on available commands.
No.	This column numbers the frame sequentially.
Status	A status flag, if any, for this frame.
Src Addr	The source and destination addresses found in this frame. If ClearSight finds a name in its Address Book for either of these addresses, it substitutes that name in the display.
Dst Addr	
Len	The length of the frame in bytes.
Protocol	The highest layer protocol seen in the frame.
Summary	A condensed view of the frame's purpose, including the highest layer request, response, or status code seen in the frame. If the **Show Transport Summary Only** option is enabled, the **Summary** column will show information about the transport layer protocol instead (TCP or UDP), including information on source and destination ports.
Rel Time	The interval between this frame and either the start of capture or, if enabled, the frame marked with the **Mark as Rel Time Origin** flag. See *Context Menu Commands in the Summary Pane* on page 230 for information on how to apply the **Mark as Rel Time Origin** flag.
Delta Time	The interval between this frame and the previous frame.
Abs. Time	The timestamp when this frame was captured.

Context Menu Commands in the Summary Pane

You can right-click on any of the entries in the **Summary** pane to access a context menu of **Decode** tab options. Table 7-3 lists and describes the available options.

Table 7-3: Context Menu Commands Available in the Summary Pane

Command	Description
Mark as Rel Time Origin	Set this frame as the mark from which the **Relative Time** fields for the other frames in the **Summary** pane are calculated. After applying this command, the **Relative Time** fields shown in the **Summary** pane are automatically recalculated.
Show Transport Summary Only	Show transport protocol (TCP, UDP, and so on) information in the **Summary** column instead of information on the highest layer protocol in the frame.
Filter Checked Frames	Remove all frames from the display except those with checked boxes in the leftmost column of the **Summary** pane.
Check Range	Display a dialog box where you can check a range of contiguous frames by supplying their starting and ending frame numbers. Use this command in conjunction with the **Filter Checked Frames** command to zoom in on a block of frames quickly.
Uncheck All Frames	Uncheck all checked frames.

The Detail Pane

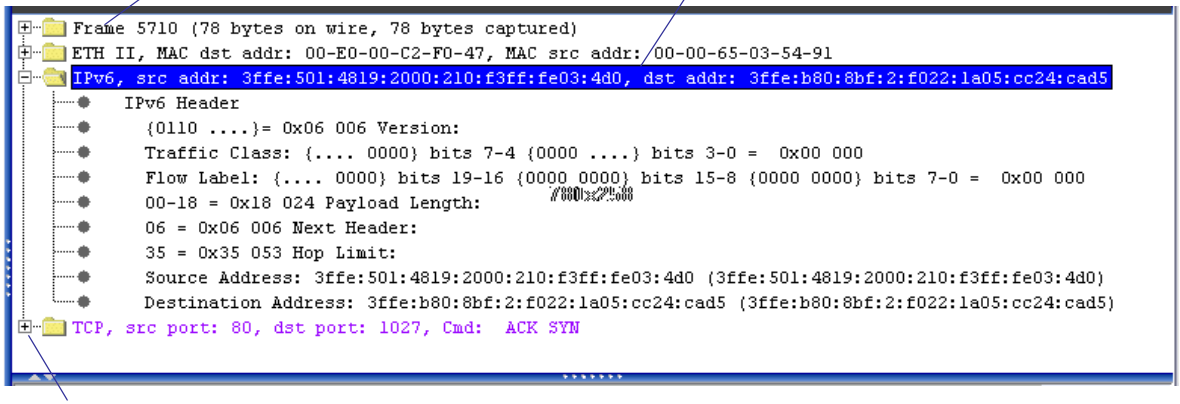
The **Detail** pane is in the middle of the **Decode** tab. It shows each of the layers of the frame selected in the **Summary** pane. The layers of the frame are arranged with the lowest protocol layer at the top of the pane and then work their way up to the highest protocol layers. You can cascade open each of the layers to see the various fields in the frame decoded into natural language.

NOTE: The first layer shown for each frame in the **Detail** pane is the only layer not actually found in the frame itself. Instead, this special **Frame** layer contains "housekeeping" information about the frame as a whole — when it was captured, its frame number, its length, and so on.

Figure 7-5 shows an HTTP frame in the **Detail** pane with its IP layer cascaded open, showing the decodes for the different fields. You can select each line in the **Detail** pane to see the corresponding hex and ASCII code highlight in the **Hex** pane.

The **Frame** layer contains the only information presented in the **Detail** pane that is not actually found in the frame itself. It provides general housekeeping information about the frame — when it was captured, its length, and so on.

Each protocol layer in the frame has its own line in the **Detail** pane (in this case, Ethernet II, IPv6, TCP, and HTTP). A given layer can be cascaded open by clicking the icon adjacent to its entry. In this example, the IPv6 layer of an HTTP frame has been cascaded open to show the decodes of the individual IP fields.



Click these icons to cascade the corresponding layer open.

Figure 7-5: Detail Pane in the Decode Tab

The Hex Pane

The **Hex** pane is at the bottom of the **Decode** tab. It shows both the hexadecimal and ASCII translation of the frame selected in the **Summary** pane. The highlight in the **Hex** pane updates according to the line selected in the **Detail** pane so you can see exactly which hex code corresponds to which layer or field in the frame.

The hex portion of the display shows each byte in the frame as two hex characters. The bytes are arranged in a table, with successive bytes appearing from left to right in a row and continuing down the table, row by row. The hex code at the left of the table shows the offset from the beginning of the frame.

The ASCII portion of the display shows the translations for the hex codes using either the ASCII or EBCDIC method, depending on the current selection in the **Configuration > Decode Settings** page. The default is ASCII.

Searching for Frames in the Decode Tab

You can search for frames containing specific values in the **Summary**, **Detail**, or **Hex** panes by clicking the **Search** button  in the **Decode** tab's title bar. In response, a set of search options appears at the left of the **Decode** tab (Figure 7-6). Enter the text you want to search for, select the fields to search, and click the **Search** button. Alternatively, you can use the **Go To** options to specify a frame number to go to.



Figure 7-6: Search Options in the Decode Tab

Decoding Ethernet OAM Frames

The ability to decode Ethernet OAM frames is an optional feature that requires a special license. Additionally, you must select the ClearSight Decode Engine (**Configuration > Preferences > Decode > General > Decode Engines > ClearSight**). When both of these conditions are satisfied, then frames with EtherType 0x8049 will be displayed as EOAM frames in the **Decode** tab.

ClearSight supports these decodes for both ITU and IEEE OAM frame formats. IEEE frame format support makes it possible to recognize TLV information in the decodes.

It is also possible to decode Ethernet OAM frames that have a different value for the EtherType, provided that the alternative value has been set up in the **EtherOAM** area of **Configuration > Preferences > Decode > Protocol Forcing**. For details see *Decode Protocol Forcing Options* on page 247.

In the current version of CSA, decoding is supported for the following Ethernet OAM frames:\

Opcode Value	OAM PDU Type
0x01	CCM
0x02	LBR
0x03	LBM
0x04	LTR
0x05	LTM

Figure 7-7 shows an example of an Ethernet OAM frame decode as it appears in the **Decode** tab. In this example, protocol forcing has been used to recognize EtherType 0x8042 as an Ethernet OAM frame.

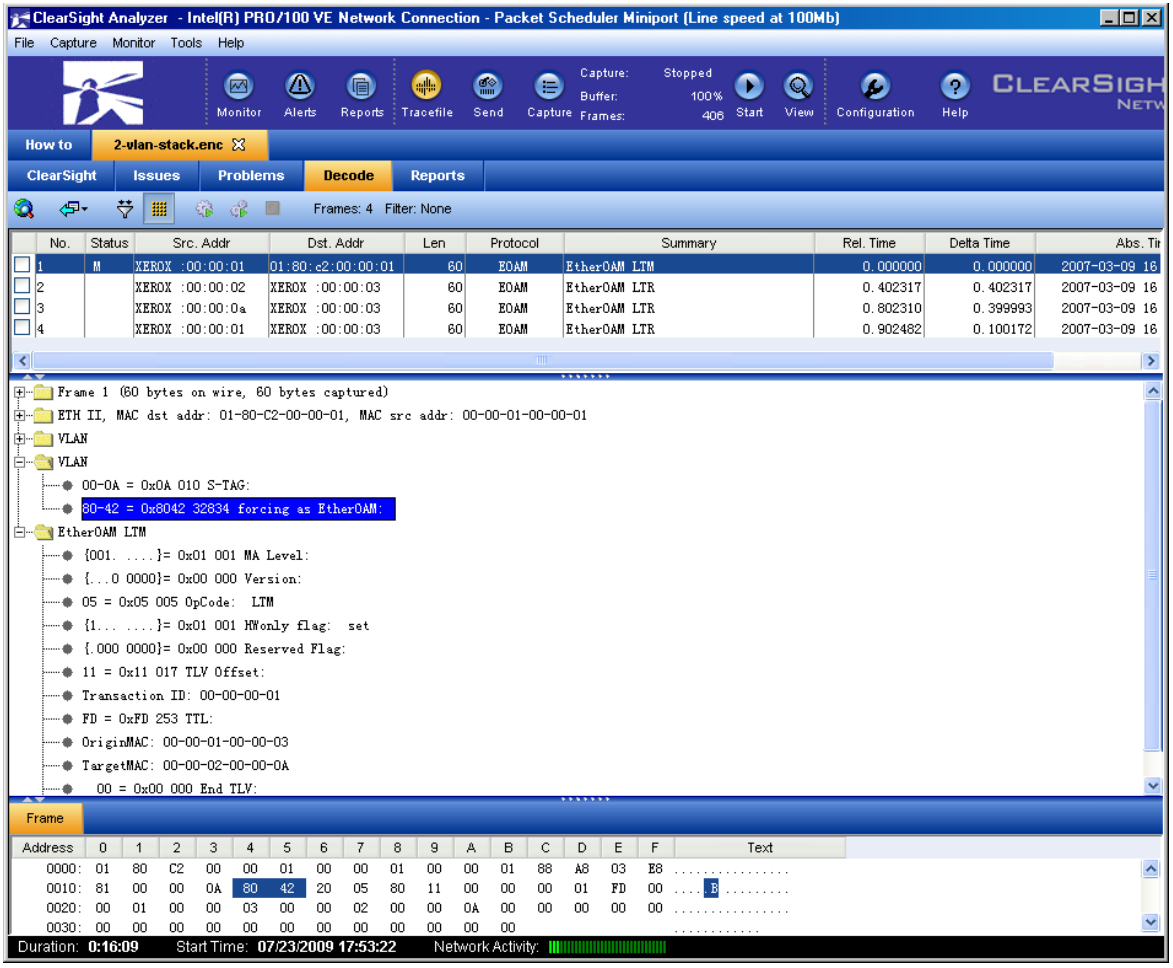


Figure 7-7: Decoding an Ethernet OAM Frame

Decoding 3G-324M Frames

The analyzer can decode 3G-324M frames, and can also construct tabs in the hex pane for reassembled and bit-swapped frames. However, in order to enable the proper decoding of 3G-324M frames, you must specify port number 2000 in the Port Range field for 3G-324M in the **Configuration > Preferences > Global > Protocol Settings** screen (see Figure 7-8).

In order for the analyzer to accept a port number of 2000 for 3G-324M, it is necessary that you first temporarily reassign the port number for Skinny to something other than 2000. While Skinny is set to something other than 2000, the analyzer will not be able to properly decode Skinny frames. They will be decoded simply as TCP frames.

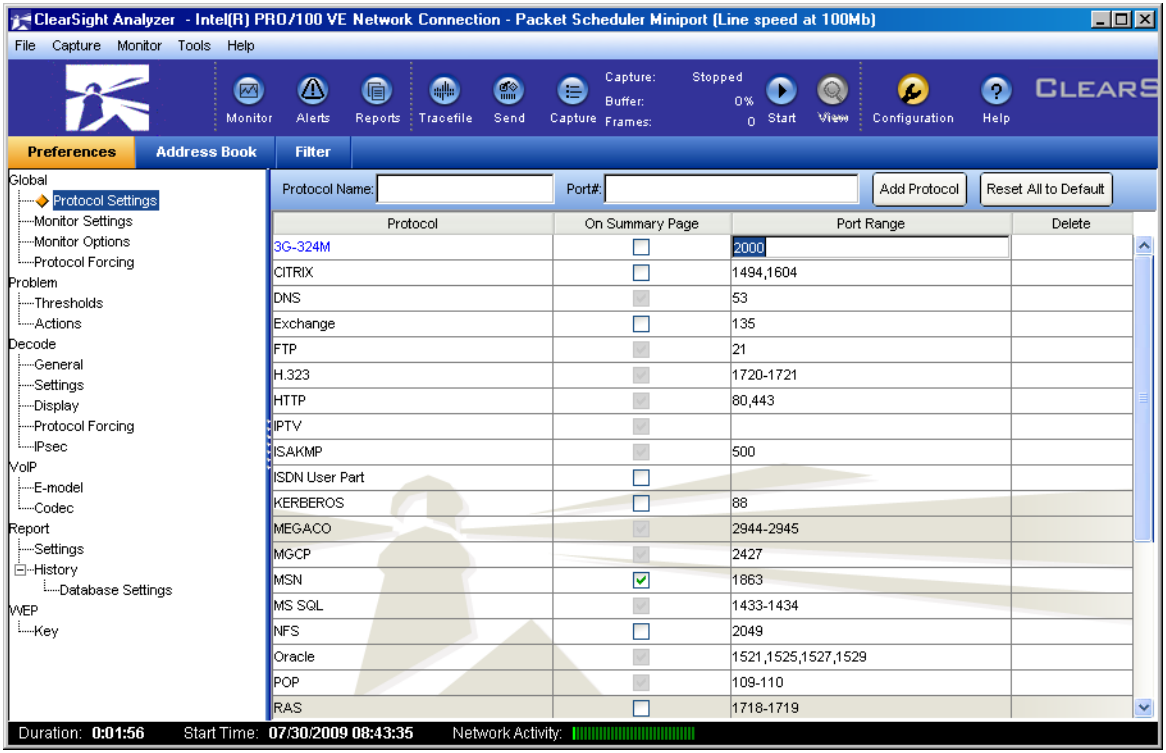


Figure 7-8: Setting the Port Number for 3G-324M Protocol Decodes

Replaying 3G-324M Video Content

ClearSight also lets you replay 3G-324M video content within the ClearSight user interface, if the codec is AMR or MPEG4.

To replay 3G-324M Video Content:

1. Click on a 3G-324M flow in the Flows pane.
2. The Statistics pane updates to include an area with a built-in media player. Click the **Play** button to play the selected 3G-324M video stream.

Figure 7-9 shows a sample screen showing a 3G-324M video stream being played back.

Click on a flow to select an individual 3G-324M video stream. The left side of the pane below lets you play the selected video stream.

Click this button to play the selected 3G-324M video stream.

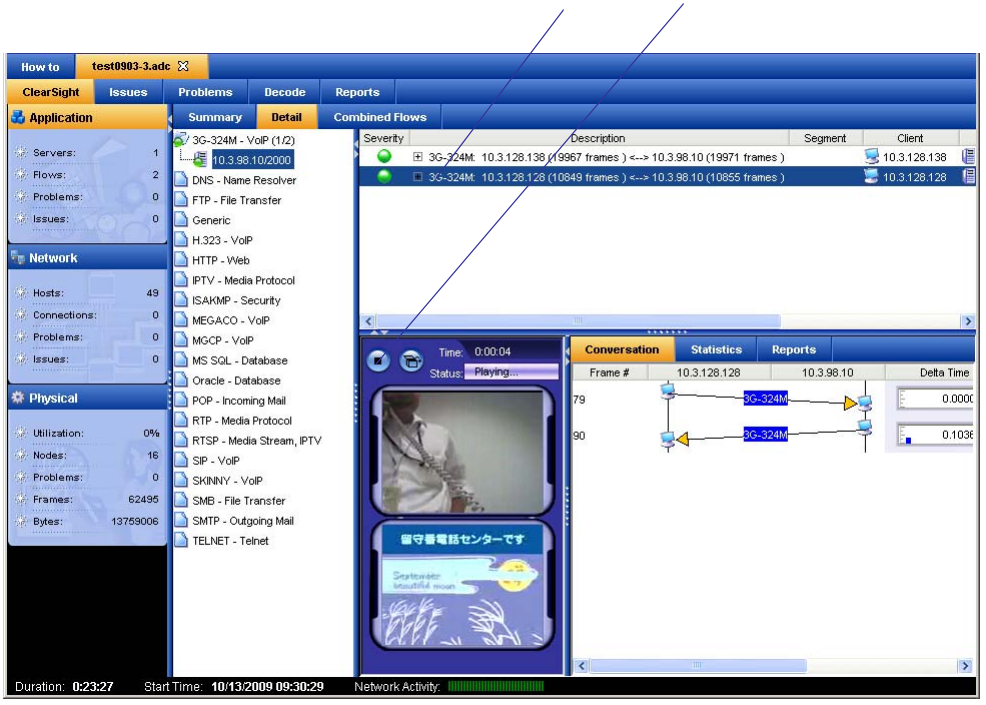


Figure 7-9: Replaying 3G-324M Video Content

To increase the size of the video display, click the button.

Configuration Options for the Decode Tab

You set configuration options for the displays in the **Decode** tab in **Configuration > Preferences > Decode**. The selections in these screens affect how information is displayed when you open a trace file or view the capture buffer. To get to each of these screens click the corresponding entry in the menu at the left of the page.

Decode General Options

Figure 7-10 shows the **Decode > General** screen.

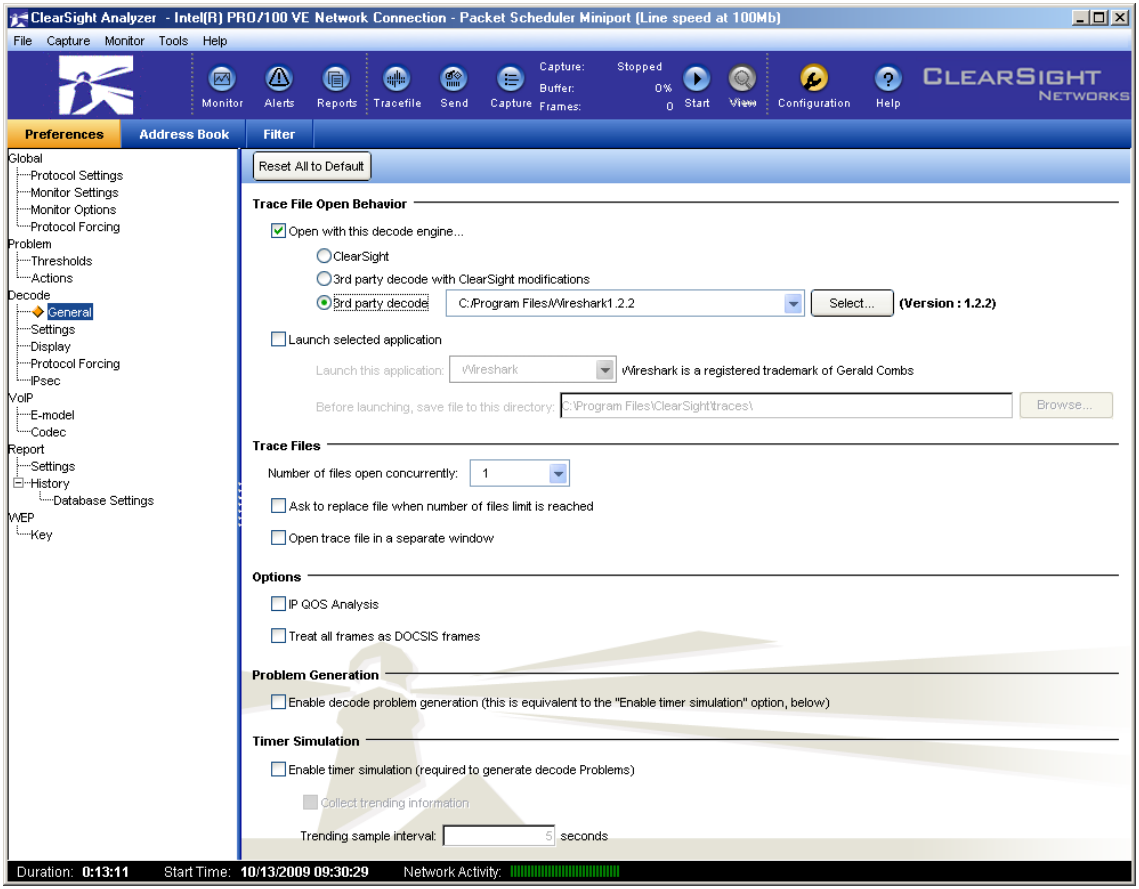


Figure 7-10: The Decode General Configuration Screen

Trace File Open Behavior

You can select which decode engine will be used to construct the displays in the decode tab within CSA. The options available under **Open with this decode engine** are:

ClearSight	ClearSight's own decode engine supplied as part of the ClearSight Analyzer.
3rd party decode with ClearSight modifications	An alternative decode engine packaged with the ClearSight analyzer.
3rd party decode	An alternative decode engine available from a 3rd party's website.

If you installed the **3rd party decode with ClearSight modifications** during the initial installation of the ClearSight Analyzer software, the program recognizes it and automatically selects the **3rd Party with ClearSight modifications** option.

If you have installed a 3rd party decode software (currently only Wireshark® version 1.2.2 has been fully tested), CSA will detect it when the CSA program starts, and will show its folder in the drop-down list. If the list has more than one entry, just select the one you want and click the **Select** button. The version number will then be displayed to the right of the **Select** button. If you select a version other than 1.2.2, you will see an error message warning you that the version you selected has not been fully tested with CSA. If you select a folder that does not contain a 3rd party decode software, an error message will point that out.

External Application Launching

You can also launch an external application, such as Wireshark® or Snort®, instead of or in addition to using the decode engine that you selected in the **Open with this decode engine** area. When you check the **Launch selected application** box, the trace file will be processed and the resulting data will be displayed in the application's own window, separate from CSA.

To appear in the drop-down list and be launchable, an external application must be installed on the viewer machine (the PC on which the Agent Manager and CSA Agent Viewer are installed). By default, Wireshark and Snort are pre-configured, and will display in the drop-down list if present.

If the trace file has been saved on a CSD Agent, it must first be transferred to the viewer machine before launching the application. Specify the name of a local (on the viewer machine) target directory in the **Before launching, save file to this directory:** field.

To open the trace file, choose **Open** from the **File** menu, and browse to the desired file location on the CSD Agent. The file will be transferred, and, if it is not in .pcap format, it will be converted to .pcap. Then the selected application will be launched automatically.

If the trace file you want to open is already on the viewer machine, choose **Open Local File** from the file menu. If the trace file is not in .pcap format, it will be converted. Then the selected application will be launched automatically.

NOTE: You can check **Open with this decode engine** or **Launch selected application**, or you can check both. If you check both, the **Open with decode engine** choice will affect the displays in the decode tab within CSA, and the **Launch selected application** choice will cause the trace file to be opened also in the application's own separate window.

Trace Files

The options available under **Trace Files** let you load more than one trace file at a time. Under **Number of files open concurrently** you can choose 1, 2, 3, 4, or 5 for the maximum number of trace files that can be opened simultaneously.

If you check **Ask to replace file when number of files limit is reached**, then ClearSight will prompt you before replacing the least recently opened trace file. For example, if the limit is 3 and you try to open a fourth trace file, ClearSight will ask you whether you want to replace the first-opened one. If the box is not checked, ClearSight will

automatically close the first-opened file before opening the fourth one.

If you check **Open trace file in a separate window**, then ClearSight opens each trace file in its own window. If the box is not checked, ClearSight opens all the trace files in separate tabs in the same window.

Options

The options available in the **Options** area of **Decode > General** are listed and described in Table 7-4.

*Table 7-4: Options in **Decode > General***

Decode Display Setting	Description
IP QoS analysis	Check this box to replace Type of Service (ToS) decodes with Differentiated Services (DiffServ) decodes in the IP section of the **Detail** pane.
Treat all frames as DOCSIS frames	Check this box to interpret all frames as DOCSIS frames rather than as ordinary Ethernet frames.

Problem Generation

Checking the **Problem Generation** box has the same effect as checking **Enable Timer Simulation**. See *Timer Simulation Settings*.

Timer Simulation Settings

The options available under **Timer Simulation** are listed and described in Table 7-5.

Table 7-5: Timer Simulation Settings in the Decode Settings Tab

Timer Simulation Settings	Description
Enable timer simulation (required to generate decode Problems)	Enable this option if you would like ClearSight to use its analysis capabilities to report Problems when opening a trace file. **NOTE:** Problem reporting can be time consuming when opening large trace files. Enabling this option turns on the post-analysis logic that simulates the passage of time for the duration of the tracefile for the primary purpose of generating Problems for post-analysis in a manner similar to how they would have been generated in real time.
Collect trending information	Enable this option if you want ClearSight to collect trending information. This information will be displayed in the **Trend** tab in the **Statistics** pane of the **Multicast** tab, or in the Jitter section of a VoIP QoS report. Trending information cannot be collected unless the timer-simulation logic is running to drive it. Therefore, if you want to select the **Collect Trending Information** option, you must first select **Enable Timer Simulation**.
Trending sample interval	This field lets you specify (in seconds) how often ClearSight should sample the data from which to compile the trending information.

NOTE: Changes made to **Decode Settings** take effect dynamically. You do not have to exit and restart ClearSight.

Currently the **Collect Trending Information** option controls the collection of trending information collected during post-analysis and stored inside a database (since the number of data points collected can be arbitrarily large - especially if the tracefile has a long duration).

The trending information is displayed in the **Trend** tab (in the lower portion) of the **Multicast** tab. If the trending flag is turned on and there are entries in any of these tables, a graph will be presented (when an entry is selected) showing how octets and frames arrived over time. If the option is not enabled, a panel containing a link to the 'Collect Trending Information' settings is displayed.

Decode Settings

Figure 7-11 shows the **Decode > Settings** screen.

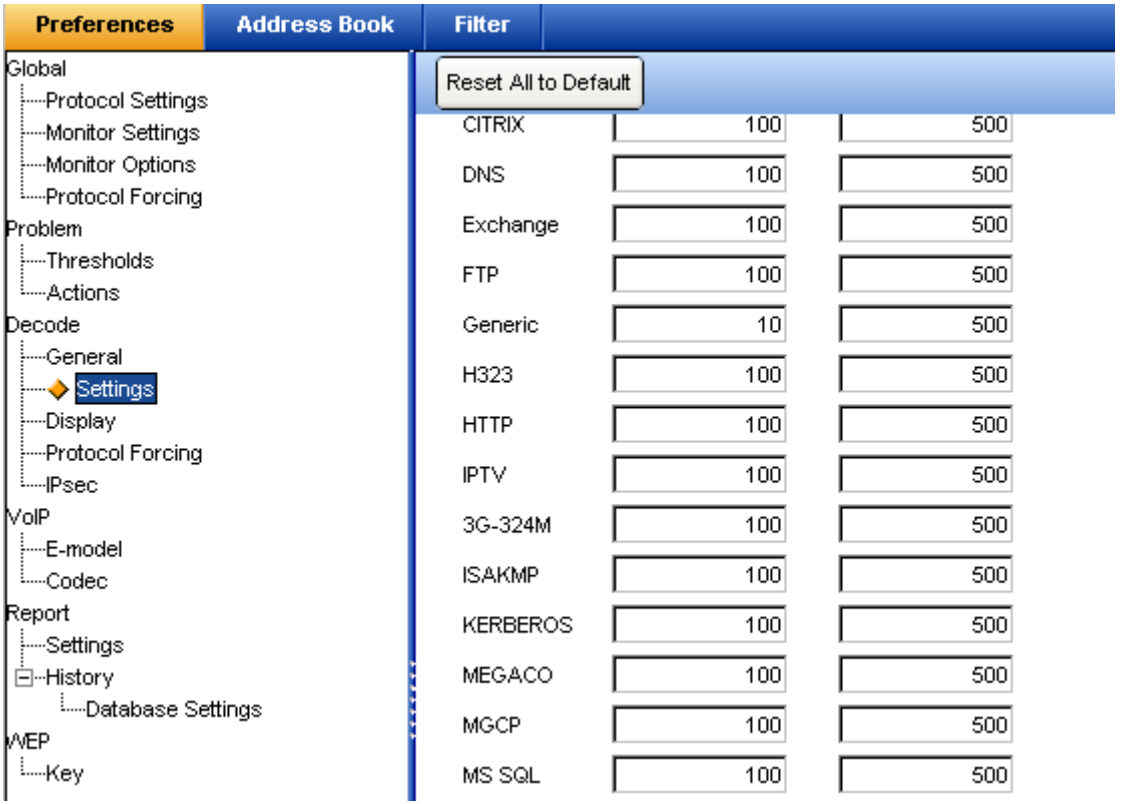


Figure 7-11: The Decode Settings Configuration Screen

Ladder View

The **Ladder View** area lets you specify the maximum number of "rungs" that an individual ladder view can have. You can set this number independently for applications, connections, and others.

Network Connections

The **Network Connections** area lets you specify the maximum number of network connections that ClearSight will track.

Applications

The **Applications** area lets you specify the maximum number of servers and flows of each supported application type for which ClearSight will maintain statistics. Once the upper limit for a particular type of server or flow has been reached, ClearSight will not create new entries in the monitor displays for new servers and flows.

TIP: Use these options to configure ClearSight's performance for the types of servers and flows in which you are most interested. The more servers and flows you specify that ClearSight monitor, the more of the ClearSight PC's resources you consume. Direct your monitoring resources to the servers and flows in which you are most interested.

Decode Display Options

Figure 7-12 shows the **Decode > Display** screen.

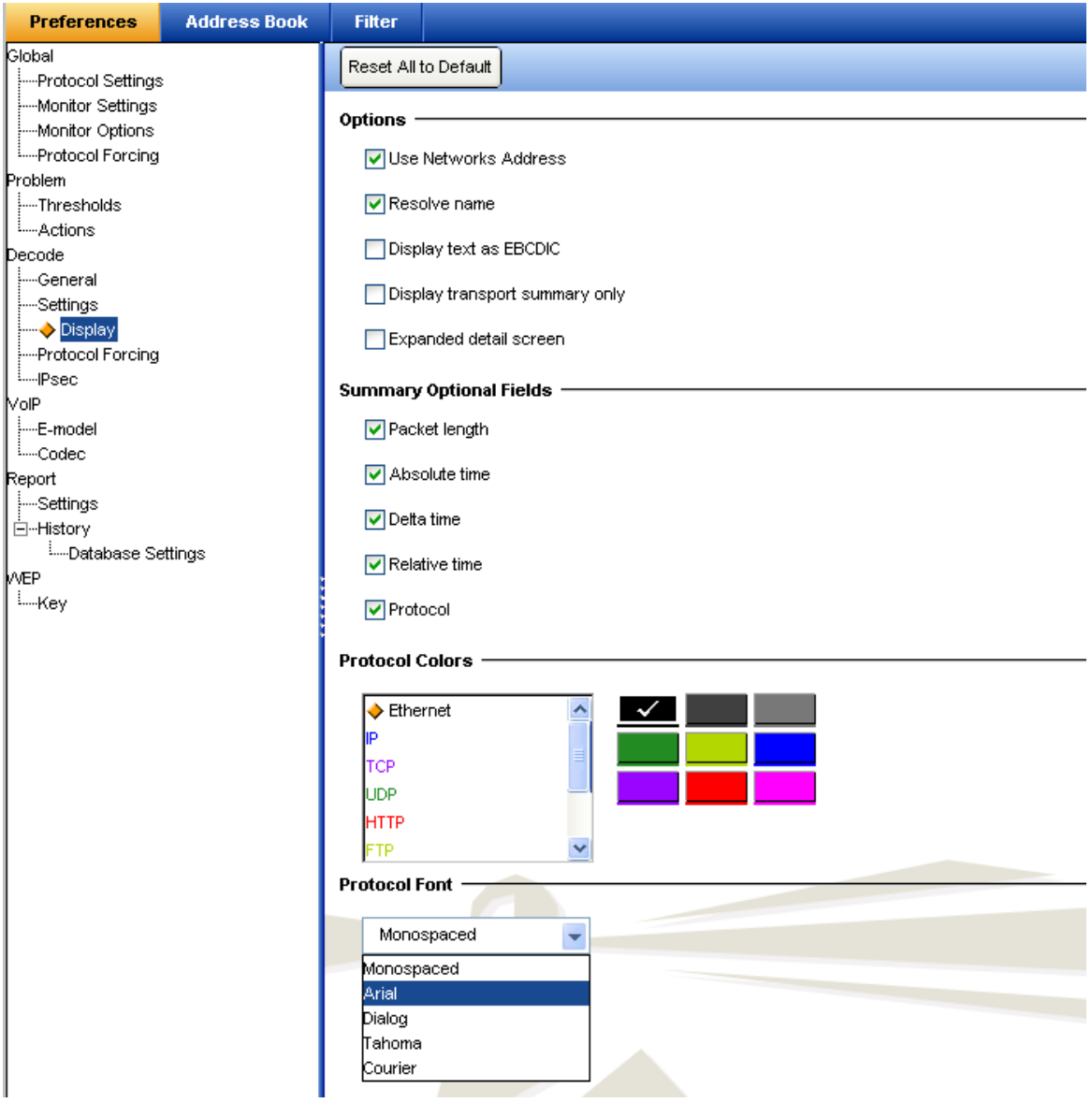


Figure 7-12: The Decode Display Configuration Screen

Options

The choices available under **Options** are listed and described in Table 7-6.

Table 7-6: Decode Display Settings in the Decode Settings Tab

Decode Display Setting	Description
Use network address	Check this box if you want ClearSight to use network addresses in the **Summary** pane instead of MAC addresses.
Resolve name	Check this box if you want ClearSight to display IP addresses using domain names when it can.
Display text as EBCDIC	Check this box if you want ClearSight to use EBCDIC translation in the **Hex** pane instead of ASCII.
Display transport summary only	Check this box if you want ClearSight to show transport protocol (TCP, UDP, and so on) information in the **Summary** column instead of information on the highest layer protocol in the frame.
Expanded detail screen	Check this box to open all ⊞ switches in the **Detail** pane.

Summary Optional Fields

The choices available under **Summary Optional Fields** are listed and described in Table 7-6.

Table 7-7: Decode Display Settings in the Decode Settings Tab

Decode Display Setting	Description
Packet length	Select the fields you want ClearSight to include in the **Summary** pane. For a description of each of these individual options, see Table 7-2 on page 229.
Absolute time	
Delta time	
Relative time	
Protocol	

Protocol Colors

The **Protocol Colors** options on **Decode > Display** let you specify the color coding used for different protocols in the **Decode** tab. Careful configuration of color coding can ease your eyes during prolonged troubleshooting sessions in the **Decode** tab. Select a protocol in the list and then click the color to use from the palette at the right.

Protocol Font

The **Protocol Font** options on **Decode > Display** let you specify the font to be used in the **Decode** tab. Select a font from the drop-down list.

Decode Protocol Forcing Options

Figure 7-13 shows the **Decode > Protocol Forcing** screen.

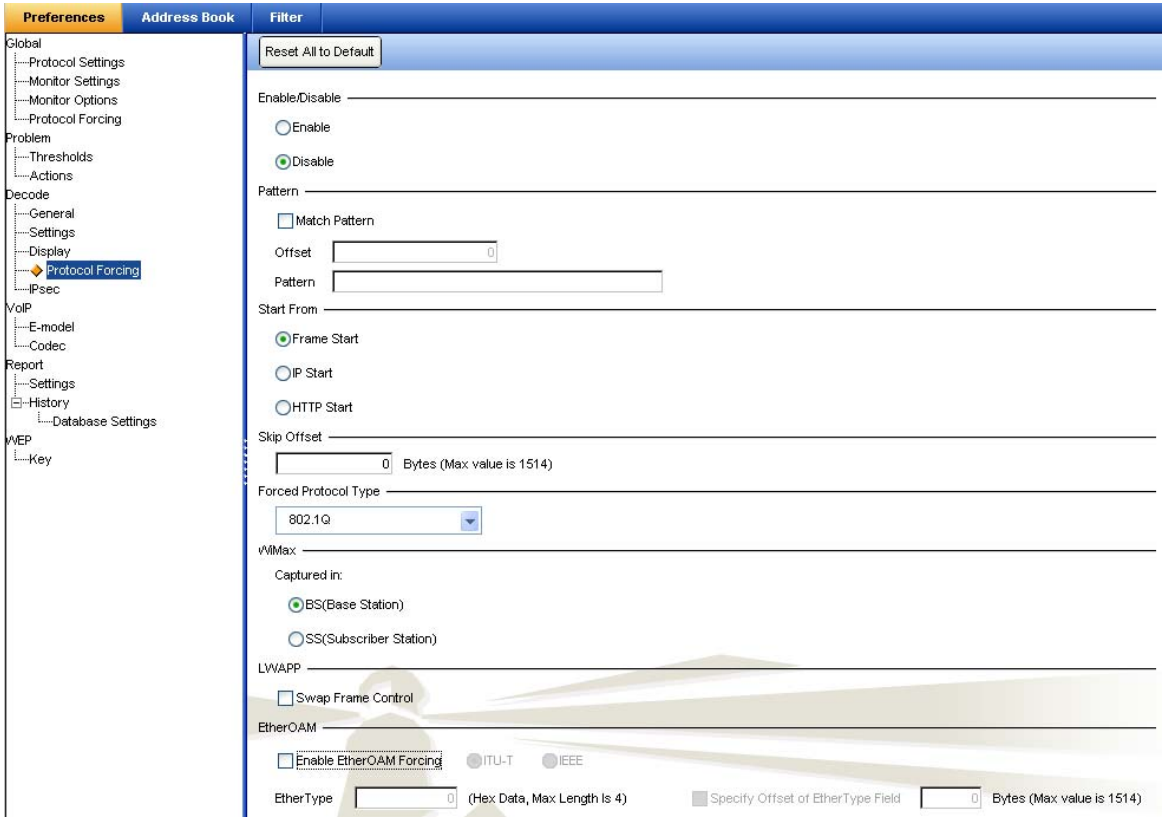


Figure 7-13: The Decode Protocol Forcing Configuration Screen

NOTE: Unless you have selected **3rd party decode with ClearSight modifications**, the decode engine will not necessarily support protocol forcing. If it does not, a warning message will be displayed instead of the options shown in Figure 7-13.

Enable/Disable

The **Enable/Disable** area lets you turn protocol forcing on and off. If you select **Disable**, you can still set the options in the other areas, but they will not be effective until you select **Enable** from this area.

Pattern

The **Pattern** area lets you enter a pattern to be matched for protocol forcing purposes. The **Offset** you enter is always from start of frame. The **Pattern** entry should be in hex. To enable the pattern match, check the **Match Pattern** box.

Start From and Skip Offset

The **Start From** area lets you tell ClearSight where to start looking for a forced protocol.

- If you select **Frame Start**, ClearSight will look at the start of frame plus **Skip Offset**.
- If you select **IP Start**, ClearSight will look at the start of the IP stack plus **Skip Offset**.
- If you select **HTTP Start**, ClearSight will look at the start of the HTTP stack plus **Skip Offset**.

Forced Protocol Type

The **Forced Protocol Type** area lets you select a forced protocol from a drop-down list. Note that contents of the list are a function of the choice you make in the **Start From** area.

LWAPP

In the LWAPP (Lightweight Access Point Protocol) area you can check the **Swap Frame Control** box to swap the bytes within the Frame Control Register. There are two different conventions currently used for the positions of these bytes, so some frames may

need to be decoded with this box checked, while others may need to have this box unchecked.

EtherOAM

Check the **Enable EtherOAM Forcing** box if you want to enable protocol forcing for Ethernet OAM frames. Enter the hex value for the EtherType that you want to have decoded as Ethernet OAM, and also enter the byte offset of that EtherType field from the start of the frame.

NOTE: EtherOAM will be present on this screen only if it is enabled by a special license for Ethernet OAM.

WiMax

In the **WiMax** area you must specify whether you want to capture in **BS (Base Station)** or **SS (Subscriber Station)**.

NOTE: Wimax will be present on this screen only if it is enabled by a special license for WiMax.

Decode IPSec Options

While most other Internet security protocols operate at the transport layer or above, IPsec operates at the Network layer, and hence it can be used in a wide variety of situations. ClearSight can decode IPsec frames, provided that the appropriate **Encapsulating Security Payload (ESP)** selections and parameters have been entered in the **Configuration > Preferences > Decode > IPsec** screen.

Figure 7-14 shows the **Decode > IPsec** screen. This screen lets you set options for IP Security (IPsec) decodes.

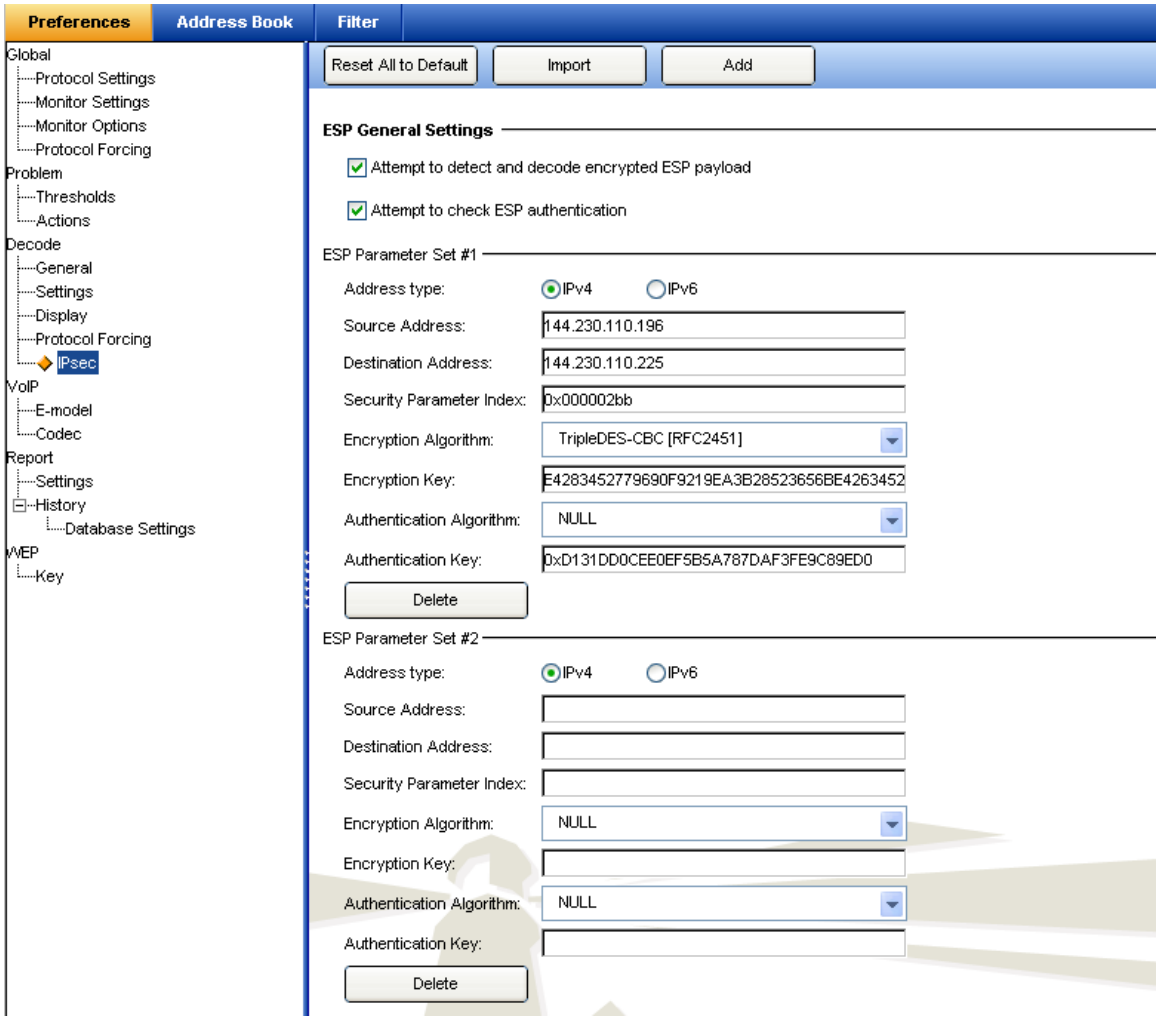


Figure 7-14: The Decode IPsec Configuration Screen

NOTE: If you have selected **3rd party decode**, this function will not be available at the location shown in Figure 7-14. You will have to configure the IPsec decodes in the 3rd party decode software itself. A warning message will be shown directing you to do it that way.

ESP General Settings

The **ESP General Settings** area lets you specify whether you want to detect and decode encrypted ESP frames, and independently, whether you want to check ESP authentication. The use of authentication is strongly recommended, so in practice it is rare to see the encryption used without the authentication.

ESP Parameter Sets

The **ESP Parameter Set** area lets you specify sets of ESP parameters for use in the decoding process.

To add an ESP parameter set, click the **Add** button. A parameter set area will appear, and you can fill it in.

To delete an ESP parameter set, click the **Delete** button for that set.

ESP parameter set files have a standard format, and are typically saved as .txt files. If you have a pre-existing ESP parameter set that you wish to use, click the **Import** button. An Open dialog box will appear, and you can browse to the location of the .txt file.

NOTE: When you change the parameter sets, the change will take effect the next time you open a trace file.

Working with Trace Files

ClearSight can open a variety of common trace file formats, including:

- ClearSight (*.adc)
- Packet capture (*.pcap)
- Generic capture files (*.cap)

Most commands for working with trace files are found under the **File** menu. The **File** menu includes the following commands for working with files:

Open	Displays a common Open dialog box where you can navigate to saved trace files that you want to open.
Recent Files	Lists the most recent trace files you have opened or saved, giving you easy access to frequently used files.
Save	Displays a common Save dialog box in which you specify a path and filename for the trace file (of the frames currently in the capture buffer) to be saved. You can save trace files in either the ClearSight format (*.adc) or in the Network General .enc format.
Save As	Displays a common Save As dialog box in which you can save the current trace file with a different path and filename.
Close	Closes the current trace file.
Merge	Lets you create a new trace file by merging up to four existing trace files. You can merge files that are in .adc or .pcap format. The resulting merged file must be in .adc format.

Chapter 8

Multi-Segment Analysis

This chapter describes ClearSight's multi-segment analysis capabilities. The chapter includes the following topics:

- *About Multi-Segment Analysis*
- *Creating Merged Trace Files*
- *Viewing Combined VoIP Flows*
- *Viewing Other Combined Flows*
- *Using Auto-Combine Filters*
- *Using the Multi-Tiered Tab*
- *Using the NAT Tab*
- *Combining Flows Manually*
- *Real-Time Multi-Segment Monitoring*

About Multi-Segment Analysis

ClearSight has the ability to correlate data that has been collected on multiple network segments. Up to four segments can be involved. Multi-segment analysis lets you view connections end-to-end, to see how transactions propagate, when there are two or more segments

involved. This makes it easier to see where there may be bottlenecks or other problems.

Creating Merged Trace Files

A common first step in multi-segment analysis is to collect data from two or more network segments, and to save the data to respective trace files. It is then necessary to merge the trace files. ClearSight can process the merged trace file in such a way that transactions involving more than one segment can be displayed.

NOTE: You can also do real-time monitoring from multiple segments (see *Real-Time Multi-Segment Monitoring* on page 267). For brevity, however, most of the discussions in this chapter will be in the context of trace file postcapture analysis.

To merge two or more trace files:

1. Select **Merge** from the **File** menu. The **ClearSight Choose File(s) to Merge** dialog box will appear.
2. Navigate to the location of the file(s) you want to include. Click or Ctrl-Click on the specific files. The result will be similar to Figure 8-1.
3. Click **Open**. The **ClearSight File Merge** dialog box will appear, with the file(s) you just selected included (Figure 8-2). You can choose familiar names for the segments. To give a file a different segment name, double-click in the **Segment** column for that file. Type in the new name or select a name from the drop-down list.
4. If the time stamp for the first packet is not the same in all the trace files, you can enter an adjustment factor for any file in the **Time Offset (sec)** column.

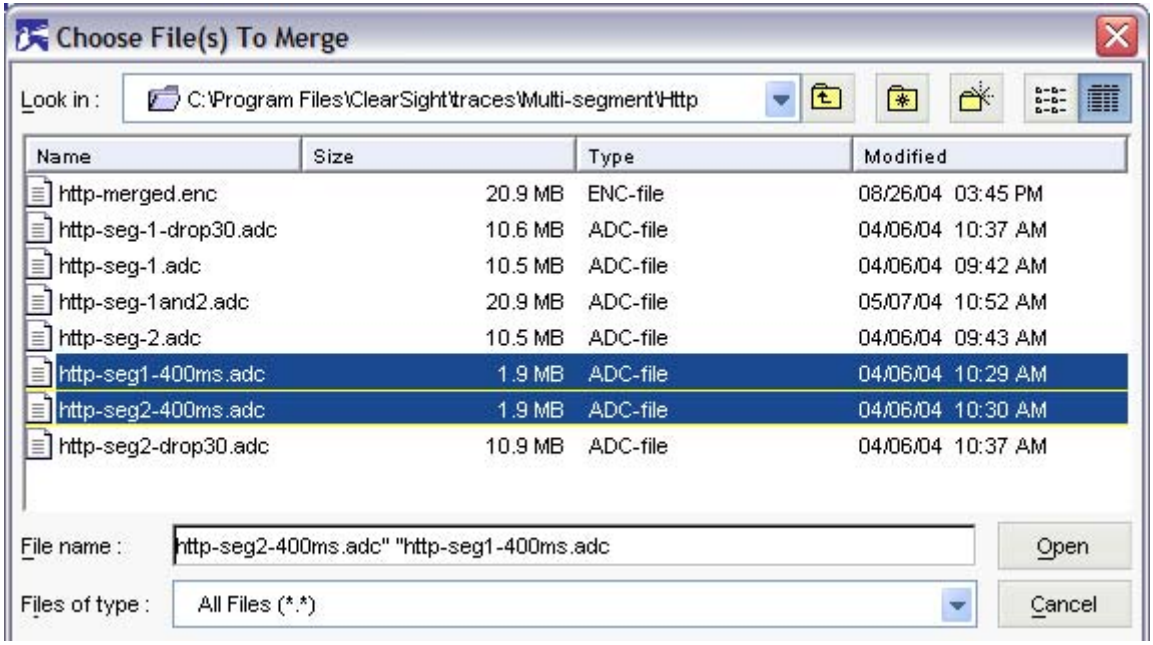


Figure 8-1: Choose File(s) to Merge Dialog Box

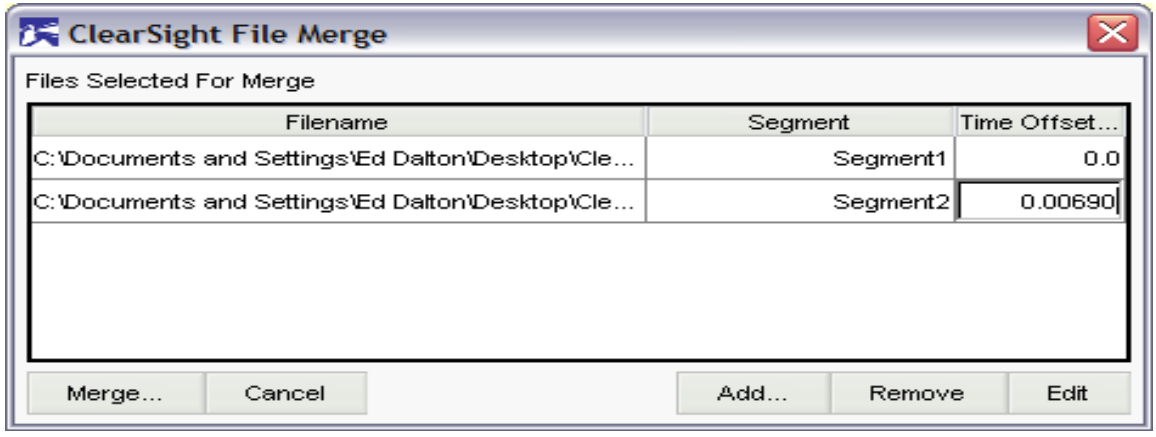


Figure 8-2: Files Selected for Merge

5. Continue the process until you have gathered all the files that you want included. Then click the **Merge** button. The **Save Merge To** dialog box will appear.

6. Navigate to the location where you want to save the file, choose a name for the merged file, and click **Save**. The new merged trace file can now be opened in the ClearSight Analyzer.

   NOTE: You can merge files that are in .adc, .enc, or .pcap format. The resulting merged file must be in .adc format.

Viewing Combined VoIP Flows

ClearSight tracks VoIP flows according to the Call ID. If, for a given VoIP application, the same Call ID appears on more than one flow, ClearSight creates a combined flow.

To view combined flows for VoIP applications:

1. Open a trace file that contains multi-segment VoIP data.
2. In the **Main** pane of the **Detail** tab, select the VoIP application of interest.
3. In the **Flows** pane, cascade open the flows to see which have multiple segments listed.
4. Select one of these flows, and view the multi-segment ladder display in the **Conversation** tab of the **Statistics** pane. Figure 8-3 shows a typical example.

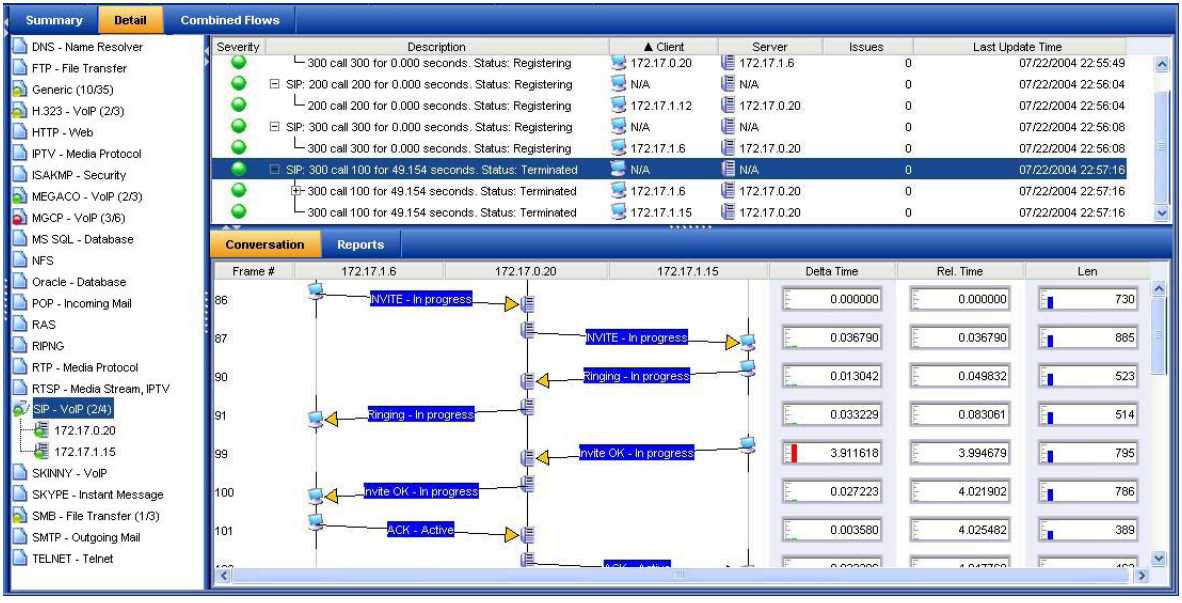


Figure 8-3: Viewing a Multi-Segment VoIP Flow

Working with the Ladder View

Sometimes you may want to switch between the Segment View (Figure 8-4) and the No-Segment View (Figure 8-5). To switch to the No-Segment View, simply right-click anywhere on the ladder diagram, and check the **Show No Segment Info** box from the menu that appears. To return to the Segment view, uncheck that box.

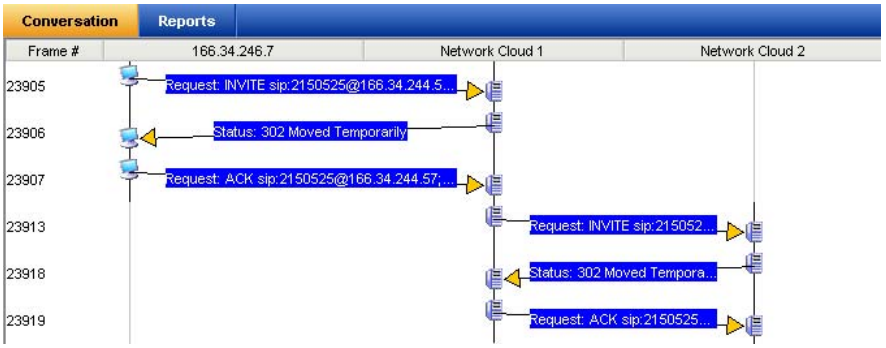


Figure 8-4: The Segment View

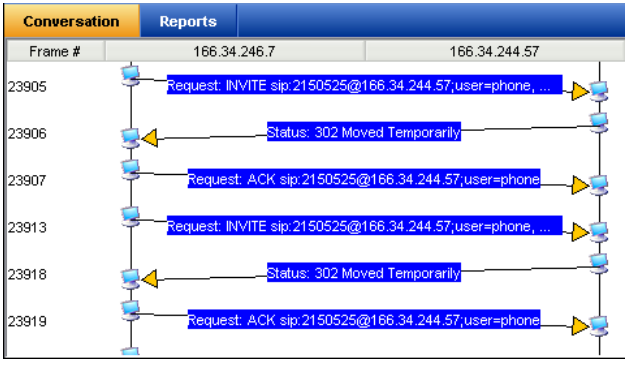


Figure 8-5: The No-Segment View

NOTE: You can print the ladder diagram by selecting **File > Print** in the pull-down menu. You can also save the ladder diagram to a pdf file. To do that, simply right-click anywhere on the ladder diagram. A menu will appear, with an **Export** selection. Clicking on **Export** brings up an **Export** dialog box, which lets you specify where you want to save the file.

Viewing Other Combined Flows

ClearSight tracks flows for applications other than VoIP according to the source IP address and port number. If the same IP address / port pair appears on more than one segment within a suitably short time interval, ClearSight creates a combined flow.

To view combined flows for non-VoIP applications:

1. Open a trace file that contains multi-segment data.
2. Go to the **Application** layer, **Combined Flows** tab.
3. The **Flows** pane will list all of the flows that have been recognized as combined flows, for all active applications in the trace file. If you select an individual flow, the multi-segment ladder view will appear in the **Conversation** tab of the **Statistics** pane. Some performance related statistics and advice will appear in the Reports tab.

Figure 8-6 shows a combined flows display with a DNS query selected.

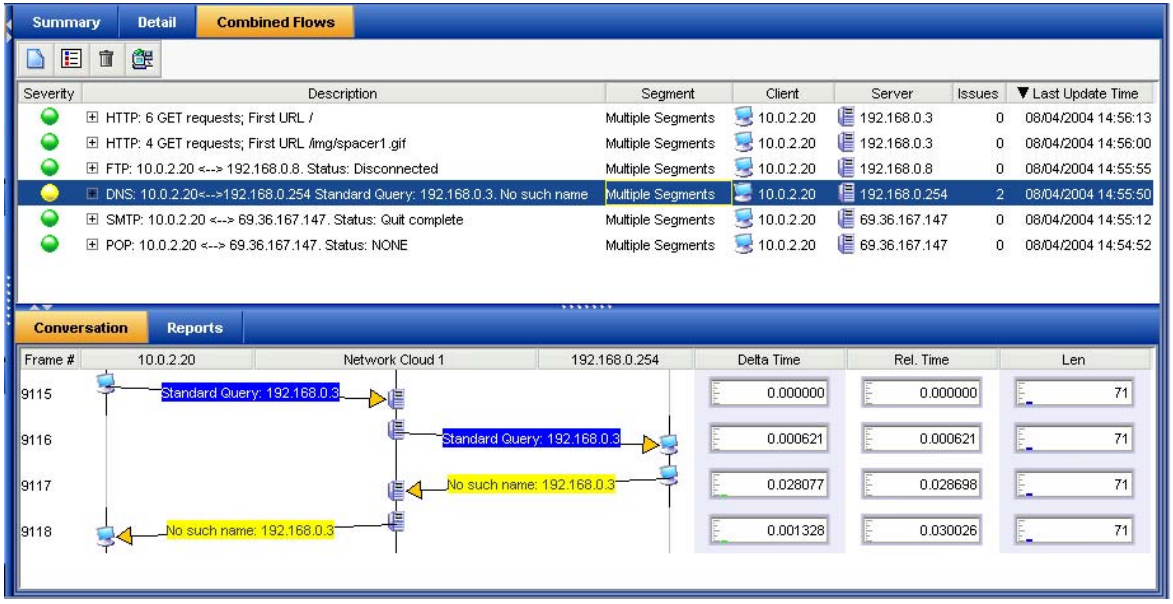


Figure 8-6: Viewing a Multi-Segment DNS Flow

Working with the Ladder View

Sometimes you may want to switch between the Segment View (Figure 8-7) and the No-Segment View (Figure 8-8). To switch to the No-Segment View, simply right-click anywhere on the ladder diagram, and check the **Show No Segment Info** box from the menu that appears. To return to the Segment view, uncheck that box.

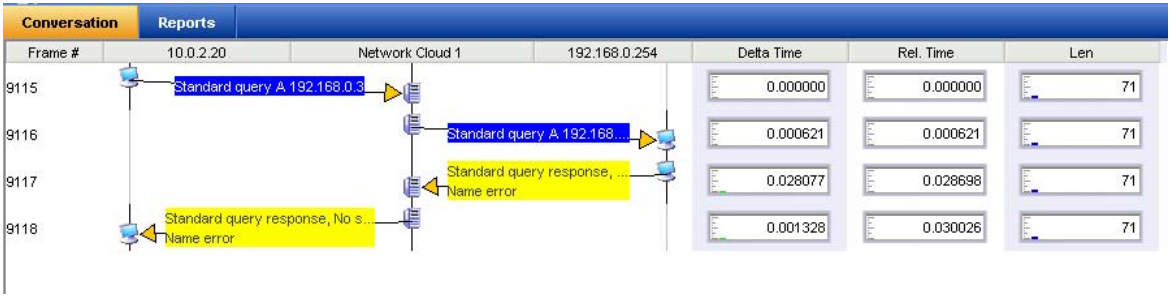


Figure 8-7: The Segment View

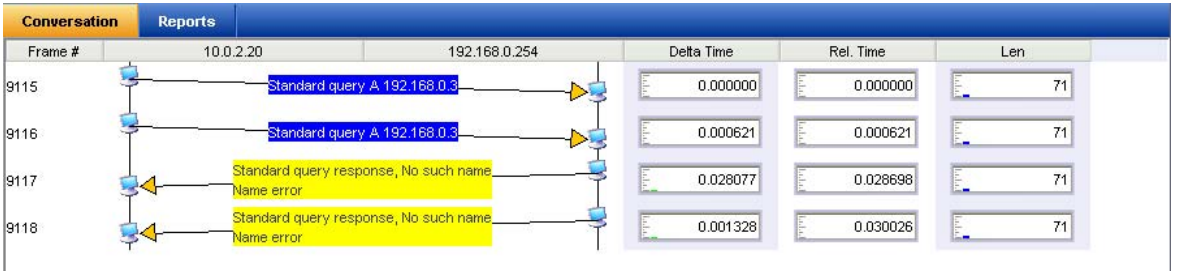


Figure 8-8: The No-Segment View

NOTE: You can print the ladder diagram by selecting **File > Print** in the pull-down menu. You can also save the ladder diagram to a pdf file. To do that, simply right-click anywhere on the ladder diagram. A menu will appear, with an **Export** selection. Clicking on **Export** brings up an **Export** dialog box, which lets you specify where you want to save the file.

Using Auto-Combine Filters

By default, the Combined Flows tab displays all the applications for which combined flows have been recognized in the trace file. In most cases, you will not be interested in all the applications, or you will not be interested in all the source and destination addresses. For this reason, ClearSight lets you filter the display, so that you can concentrate on your areas of interest.

To set up a display filter for combined flows:

1. Open a trace file that contains multi-segment data.
2. Go to the **Application** layer, **Combined Flows** tab.
3. At the top of the tab, click the **Auto-Combine Flows** icon. A multi-segment filter dialog box (such as shown in Figure 8-9) will appear.

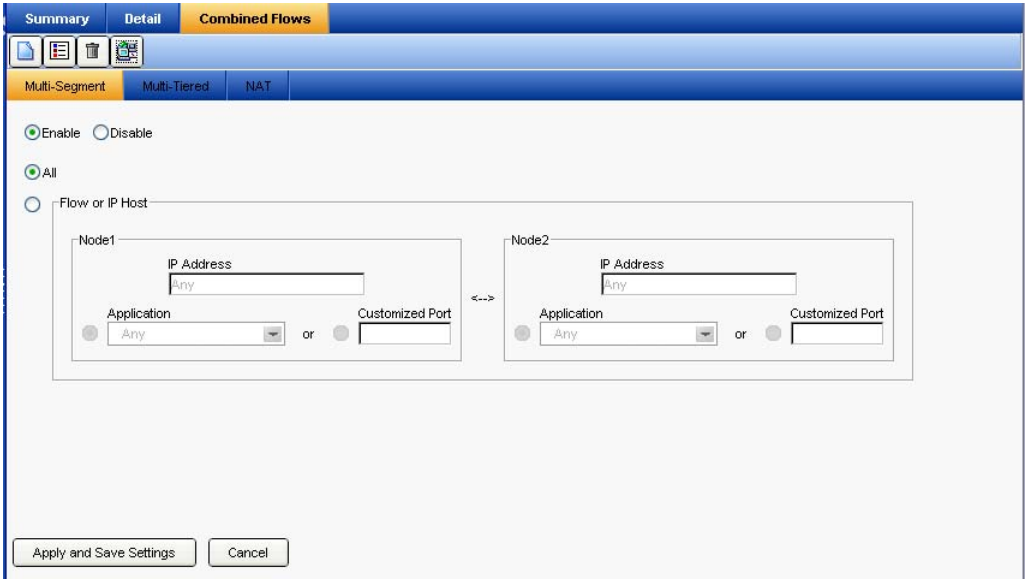


Figure 8-9: Multi-Segment Filter Dialog Box

The **Enable** and **Disable** buttons are a toggle that controls whether or not multi-segment analysis will occur. If you select **Enable**, then you can choose **All** (to process and display all multi-segment flows) or **Flow or IP Host** to be more selective.

4. Choose **Flow or IP Host**. The display will now appear as in Figure 8-10.

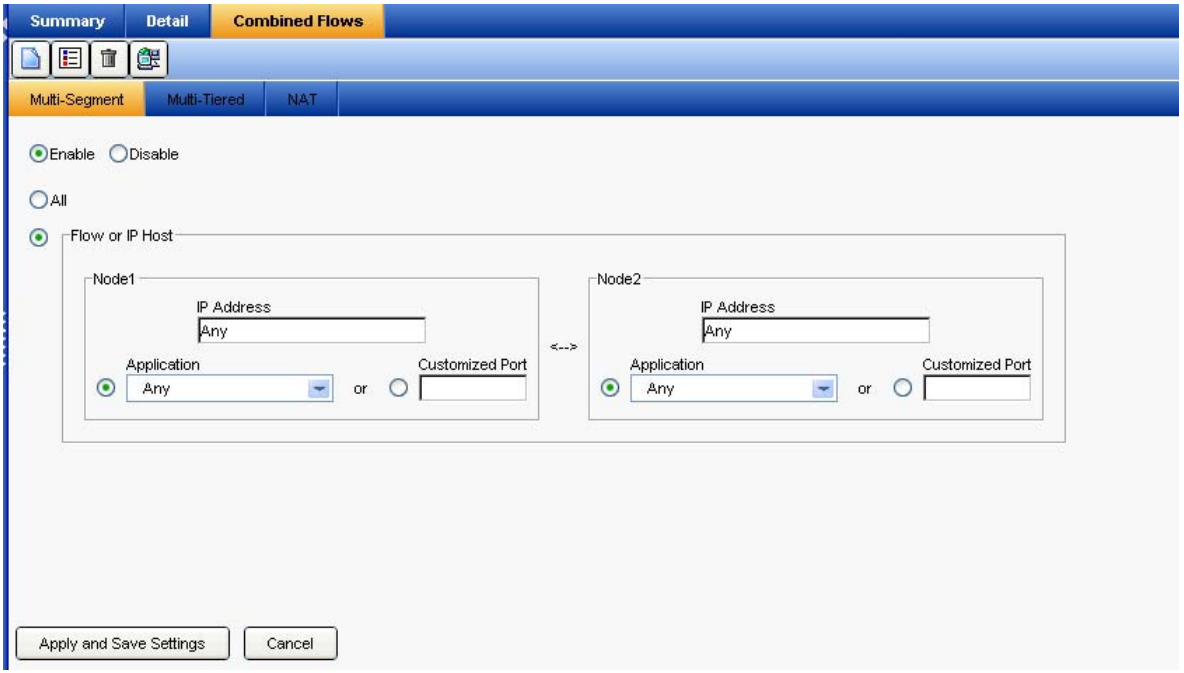


Figure 8-10: Flow or IP Host Selected

5. The two lines in the **Flow or IP Host** box refer to the endpoints of the conversation. Suppose you were interested in analyzing transactions between the hosts at IP addresses 10.0.2.20 and 69.36.167.147. You could simply enter 10.0.2.20 in **IP Address 1** and 69.36.167.147 in **IP Address 2**.

   You can further filter the analysis by limiting it to specific applications or port numbers between the parties specified in the **IP Address** boxes. In that case you would choose an **Application** from the pull-down list, or enter a port number in **Customized Port**. Note that there is an AND relationship between what you enter in **IP Address** and what you enter in **Application** or **Customized Port**.

6. Suppose that you were interested in all the conversations between 10.0.2.20 and 69.36.167.147, regardless of application.

The multi-segment filter dialog box would then look like Figure 8-11.

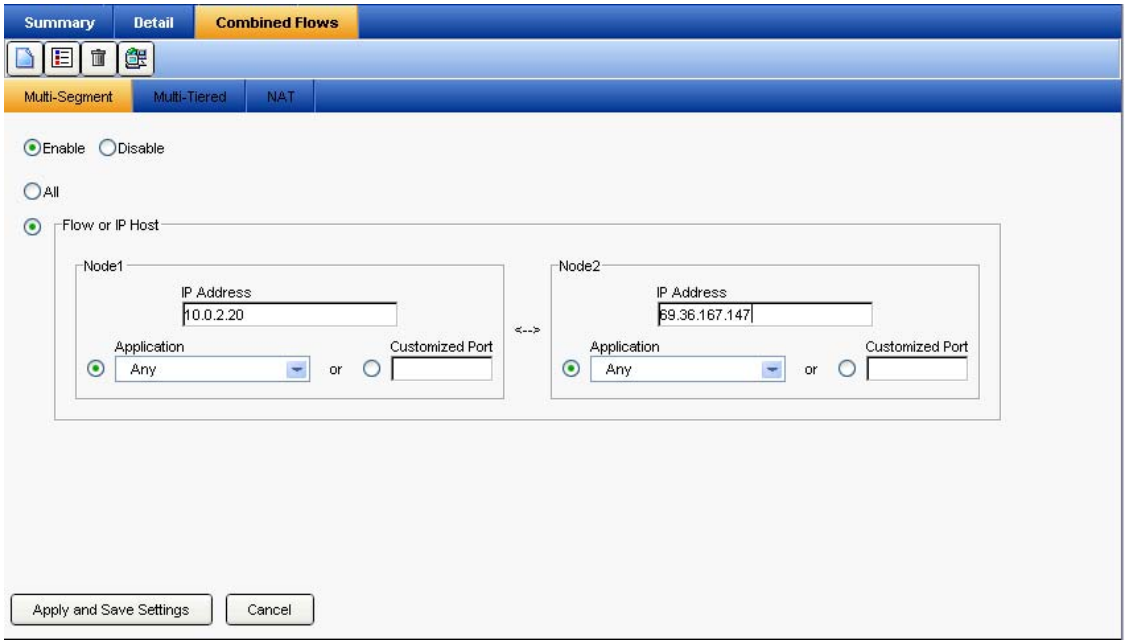


Figure 8-11: Filtering for Transactions Between two IP Hosts

7. Click **Apply and Save Settings**. ClearSight will generate a new filtered display and return you to the Application layer Summary pane.
8. Return to the **Combined Flows** tab. The new display shows only the conversations between 10.0.2.20 and 69.36.167.147, which in this case are SMTP and POP applications. Selecting a flow shows the multi-segment ladder diagram. For the flow selected in Figure 8-11, we see Isun retrieving his email (Figure 8-12).

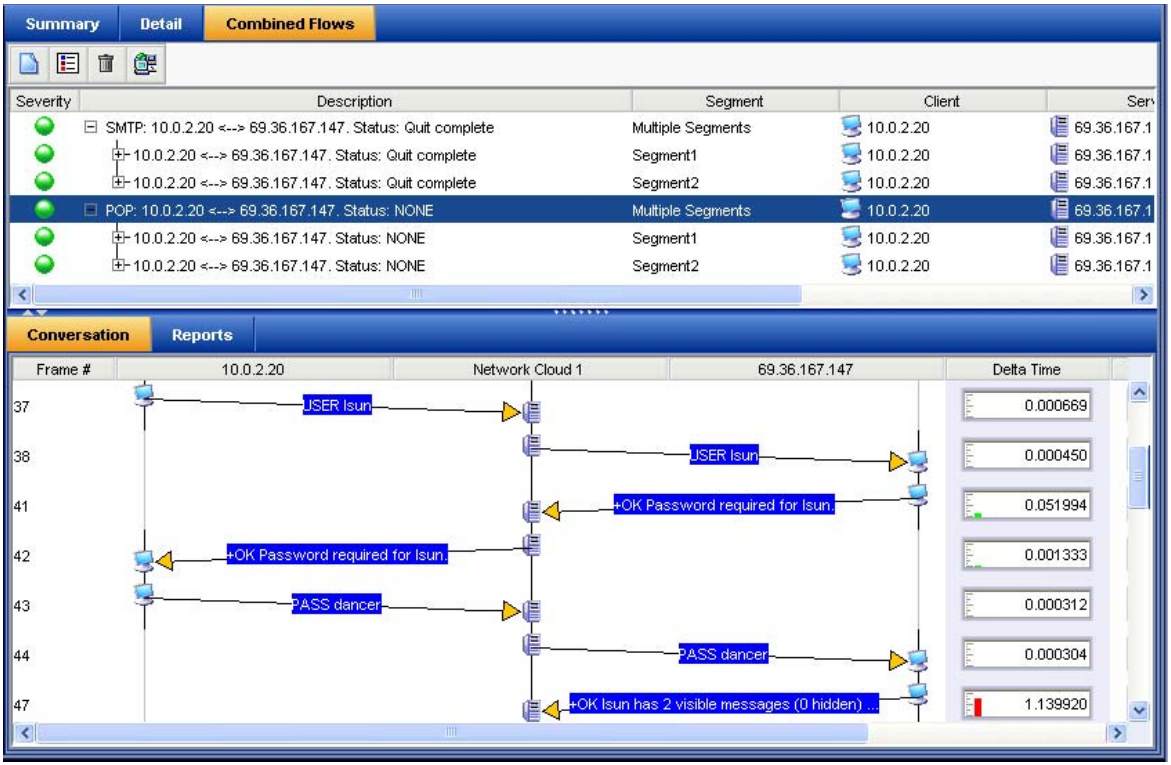


Figure 8-12: Isun Gets His Email

Using the Multi-Tiered Tab

An alternative approach to filtering combined flows uses the **Multi-Tiered** tab within the **Auto-Combine Flows** function. Whereas a filter in the Multi-Segment tab applies to all the segments, filters in the **Multi-Tiered** tab can apply individually to each segment. The tiers are basically segments — **Tier 1** refers to the segment listed on the top line in the ClearSight File Merge dialog box, **Tier 2** refers to the segment listed on the second line, and so on.

The **Enable** and **Disable** buttons are a toggle that controls whether or not multi-tiered analysis will occur. If you select **Enable**, then you can choose 2-Tiered, 3-Tiered, or 4-Tiered analysis.

There is an OR relationship among the tiers — that is, the restrictions set in Tier 1 are ORed with those in Tier 2, Tier 3, and so on.

There is also an OR relationship between the filters defined in the **Multi-Tiered** tab and those defined in **Multi-Segment** tab. When you click **Apply and Save Settings**, the information from both of these tabs is used to update the display.

Multi-Tiered filtering can also be used to analyze situations in which the tiers are not actually physically separate segments. For example, Suppose there is a client at IP address x.x.x.x, a server at IP address y.y.y.y, and a database at IP address z.z.z.z. You can enter the x.x.x.x/y.y.y.y combination in the Tier 1 tab, the y.y.y.y/z.z.z.z combination in Tier 2, and x.x.x.x/z.z.z.z in Tier 3. You will then be able to view the interactions among these three hosts as a multi-segment display, even though all three may be physically connected to the same network segment.

NOTE: Multi-Tiered filtering can be used only with trace files — it cannot be used in conjunction with real-time monitoring.

Using the NAT Tab

You can use the **NAT** tab to effect a further refinement regarding how ClearSight displays combined flows. The **NAT** tab contains a simple pair of radio buttons — **Enable** and **Disable**.

These **Enable** and **Disable** buttons are a toggle that controls whether or not to display combined flows that have been subject to Network Address Translation (NAT).

If you select **Enable**, then combined flows will be displayed even when the IP addresses have been changed because of Network Address Translation. If you select **Disable**, such flows will be treated as independent flows and will not appear in the **Combined Flows** display.

Combining Flows Manually

The Auto-Combine Flows function used in both Multi-Segment and Multi-Tier filtering operates on the entire trace file. Thorough use of filters, you can tailor the display to show you only the combined flows that are of interest to you. However, this particular approach to filtering may not isolate exactly the situations you want to see. Therefore, ClearSight provides a means of hand-selecting the flows that you want to include in your own custom-built combined flow.

To set up a new combined flow manually:

1. Click the **New Combined Flow** icon at the top of the **Combined Flows** tab. A **Prompt** dialog box will appear.
2. Enter the name that you want for the new combined flow. Figure 8-13 shows an example.

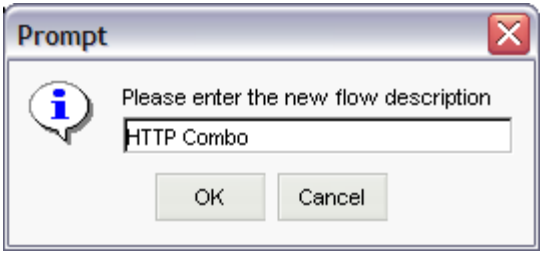


Figure 8-13: Entering a Name for a New Combined Flow

3. Click **OK**. The name of the new combined flow will then appear as one of the flows listed in the **Flow** pane of the **Combined Flows** tab.
4. Select that new combined flow.
5. Go to the **Detail** tab and right-click on a flow that you want to include in your new combined flow.
6. From the drop-down list, select **Add to selected combined flow**. The flow you just selected will then become a part of the new combined flow.
7. Continue this process until you have added all the flows you want.

8. Return to the **Combined Flows** tab and select your new combined flow. If you have selected a meaningful combination of flows, you will see an appropriate multi-segment ladder display in the **Statistics** pane.

To rename a manually constructed combined flow, select that flow and click on the **Edit Combined Flow** icon at the top of the **Combined Flows** tab. The **Prompt** box will return and you can change the name.

To remove a manually constructed combined flow, select that flow and click on the **Remove Flow** icon.

Real-Time Multi-Segment Monitoring

It is possible to perform multi-segment analysis in real time by using an adapter that can monitor more than one network segment simultaneously. Currently available adapters are:

- The 10/100 Full Duplex Ethernet card, which can be used on any two Ethernet segments — it doesn't have to be restricted to a full-duplex environment.
- The Gigabit Ethernet card, which has two Gigabit Ethernet ports.

To use one of these adapters for multi-segment monitoring, go to the **Configuration > Adapter Settings** page, and choose the **Multiple Segment** option. Then enter names for the segments in the **First segment's Name** and **Second segment's Name** boxes.

NOTE: You cannot use the Multi-Segment or Multi-Tier filters in connection with real-time monitoring.

Chapter 9

Using Filters

This chapter describes how to work with *filters*. The chapter includes the following major topics:

- *About Filters*
- *Using Automatic Filters*
- *Using Defined Filters*

About Filters

Filters help you sift through a potentially overwhelming body of data and look at just those frames that interest you. ClearSight provides comprehensive filtering capabilities for a wide variety of application events, flow types, protocols, and addresses.

Automatic Filters vs. Defined Filters

ClearSight provides two kinds of filters — *automatic filters* and *defined filters*:

- You create *automatic filters* by right-clicking an entry either in the real-time monitoring displays or in the **ClearSight** tab during

postcapture analysis. In response, a context menu appears listing available automatic filters for the selected entry.

Automatic filters are described in *Using Automatic Filters* on page 272.

- You create *defined filters* by setting the options in the **New Filter** dialog box. Defined filters are saved in a global list and can be re-used whenever needed.

  For details on how to create defined filters, see *Using Defined Filters* on page 274.

Using Filters in Real-time or During Post Analysis

Automatic filters can be used to filter frames entering the capture buffer, or to filter the display of frames in the **Decode** tab during post analysis:

Defined filters can be used to filter packets entering the Monitor, packets entering the capture buffer, or packets being displayed in the **Decode** tab during post analysis.

- Using a filter as a monitor filter determines which frames enter the Monitor. You can exclude all frames except those matching the current filter. This way, the displays in the monitor do not fill up with data that does not interest you. If a filter is currently being applied to the monitor, the **Filter On** icon () appears in the status bar at the bottom of the window.
- Using a filter as a capture filter determines which frames are stored in the capture buffer during capture. You can exclude all frames except those matching the current filter. This way, the capture buffer does not fill up with frames that do not interest you.
- Using a filter as a decode display filter determines which frames are displayed in the **Decode** tab during postcapture analysis. Decode display filters temporarily remove matching frames from the **Decode** tab, clearing the way for unobstructed analysis. Display filters are temporary — you can always remove them and re-display all of the frames in the buffer or trace file.

ClearSight maintains a global list of the filters you have defined using the options in the **New Filter** dialog box (Figure 9-4). Each defined filter has a unique name so you can select it from the list whenever you need to use it. The defined filter list itself is available from various places depending on where the filter is to be applied:

To filter monitoring	From the **Filter** area of the **Settings** tab in **Configuration > Preferences > Global > Monitor Settings**.
To filter capture	From the **Filter** area of the **Settings** tab in the Capture workspace.
To filter decode displays	From the **Apply Filter** icon  in the status bar of the **Decode** tab in the Postcapture Analysis workspace.

NOTE: Some filters cannot be applied to monitoring or capture, but only to the decode display during post analysis. These filters are listed in the Filter List with the notation **(Post Analysis Only)** in the **Restrictions** column.

Packet-Based Filters vs. Flow-Based Filters

ClearSight uses both *packet-based* and *flow-based* filters:

- *Packet-based* filters are applied, on a packet-by-packet basis. For each packet that arrives, ClearSight checks to see if it meets the criteria for the currently selected filter. If the frame matches these criteria, it is passed into the Monitor or capture buffer, or it appears in the decode display.
- *Flow-based* filters are applied during postcapture analysis only, and are generally available for various error types and status codes. When ClearSight finds a packet that displays a particular error type or status flag, it filters the display to show you all of the packets belonging to the flow. This way, you can see the logic leading up to the error, making troubleshooting easier.

  Flow-based filters are listed in the Filter List with the notation **(Post Analysis Only)** in the **Restrictions** column.

Using Automatic Filters

In addition to the filters you set up manually in the **New Filter** dialog box, ClearSight provides a wealth of automatic capture and display filters. Automatic filters make it easy to see exactly what you are interested in without ever having to bother with manual configuration.

Automatic Capture Filters

Automatic capture filters are generally available by right-clicking an entry in the real-time monitoring displays. In response, a context menu appears with a variety of automatic capture filters available for the selected entry. The exact filters available will depend on the selected layer, pane, and entry. Typically, automatic capture filters will be available explicitly for the selected entry's address(es) and port(s), as well as for a variety of common wild-card filtering scenarios using different combinations of the selected address(es) and port(s). Figure 9-1 shows an example of the automatic capture filters available for a sample connection at the Network layer.

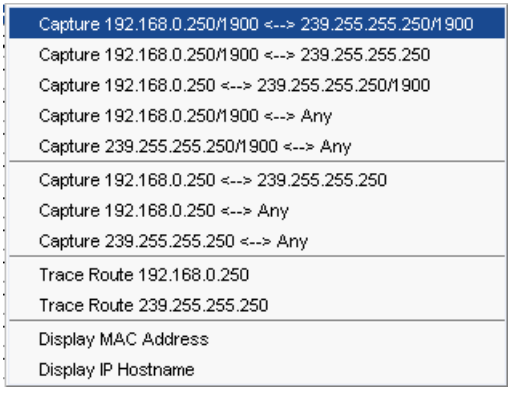


Figure 9-1: Automatic Capture Filters

NOTE: When you select an automatic capture filter, ClearSight immediately begins capturing frames with that filter applied.

Automatic Display Filters

Automatic display filters are applied in much the same way as automatic capture filters. However, instead of right-clicking entries in the real-time monitoring displays, you right-click entries in the **ClearSight** tab in the postcapture analysis display. In response, a context menu appears listing a variety of automatic filters available for the selected entry. Both display and capture filters will be listed. Select a display filter using the commands that start **Filter *xxx*.** Select a capture filter using the commands that start **Capture *xxx***. In the **Decode** tab, you can check frames in the **Summary** pane that interest you, then right click on any frame, and select **Filter Checked Frames** to display only those frames. The exact filters available depend on the selected layer, pane, and entry. Typically, automatic display filters will be available explicitly for the selected entry's address(es) and port(s), as well as for a variety of common wild-card filtering scenarios using different combinations of the selected address(es) and port(s). However, each entry is different. For example, clicking an application entry in the Applications pane in the **ClearSight** tab gives you access to an automatic display filter for just that application type. Once you select an automatic display filter, ClearSight displays the **Decode** tab with your filter applied. To remove the filter, click the **Filter On\Off** toggle button  in the **Decode** tab's status bar.

Figure 9-2 shows an example of the automatic display filters available for a sample flow at the Application layer. In this example, a parent flow has child flows. Two filters are available — one for the entire flow and one for the specific client to server address/port pair to filter for the parent flow only.

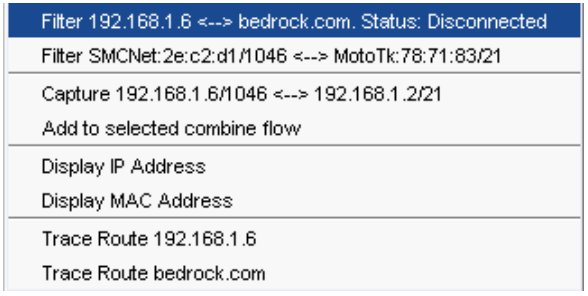


Figure 9-2: Automatic Display Filters

Using Defined Filters

You create defined filters in the **New Filter** dialog box.

To create a defined filter:

1. Click the **Click Here** button in the **Configuration > Filter** tab. The **Filter List** dialog box (containing a list of current filters) appears. Figure 9-3 shows the **Filter List** dialog box.

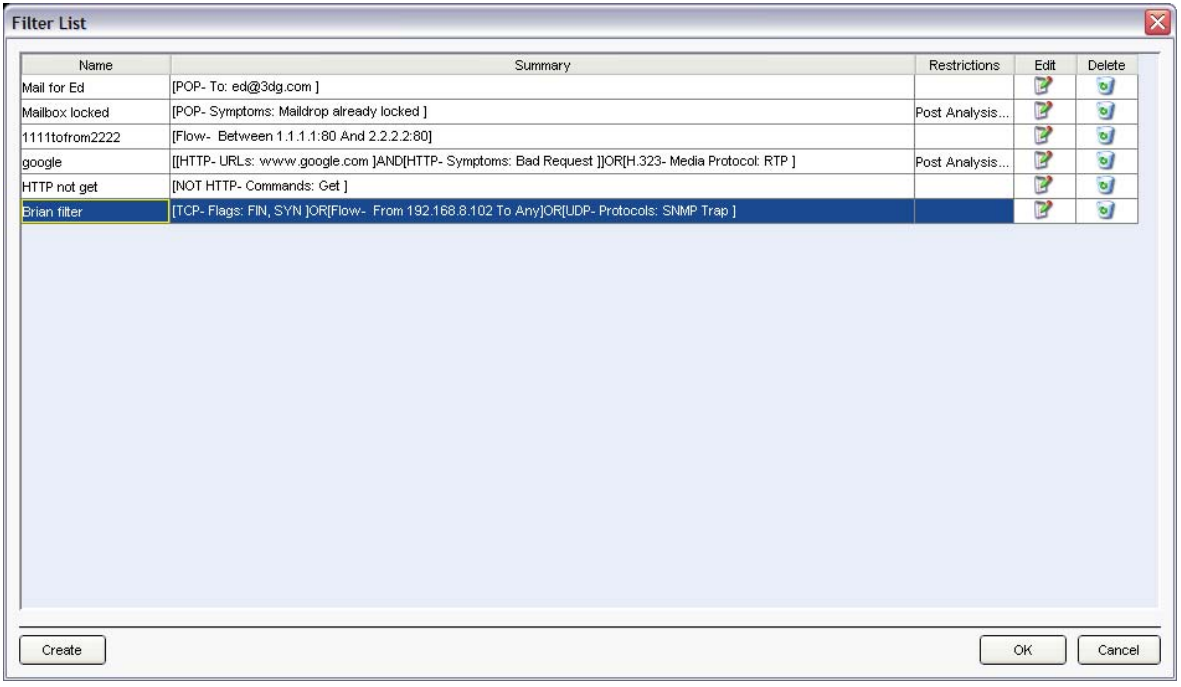


Figure 9-3: The Filter List Dialog Box

2. To define a new filter, click the **Create** button. The **New Filter** dialog box (Figure 9-4) appears.
3. Enter a descriptive name for this filter in the **Filter Name:** field.

   The filter will be known by this name throughout ClearSight's displays. You will be able to apply the filter by selecting this name from the filter list in these places in ClearSight's displays:

   - In **Configuration > Preferences > Global > Monitor Settings**

- In **Capture > Settings > Filter**
- In **Capture > Trigger > Filter-based**
- In **Tracefile > Decode** (using the **Apply Filter** icon in the status bar)

NOTE: You can also access the **Create** button from these locations.

4. Set the filtering criteria for this filter in the various filter dialog boxes. These dialog boxes are listed in the **New Filter Items** menu at the left of the **New Filter** dialog box. The available filtering criteria in these dialog boxes are described in detail in the sections that follow.

   IMPORTANT: An individual filter component, created within a specific filter dialog box, is represented by one rectangle in Figure 9-4. A named filter is made up by grouping these rectangles using logical **AND, OR**, and **NOT** operands. The **AND** and **OR** relationships are determined by the relative positions of the rectangles. The **NOT** operand is created by clicking on a **NOT** icon within the affected rectangle. See Figure 9-4 for details.

   NOTE: Use of the **NOT** operand excludes the specified frames.

5. Click **OK** to save your filter in the filter list.

   The filter list appears showing all available filters and a summary of their definitions.

You build a defined filter from filtering criteria specified in each of the filter configuration dialog boxes that you access by clicking on the selections in the **New Filter Items** list. As you build the filter, the logical structure of the filter is displayed graphically. Each dialog box generates the attributes shown in a corresponding rectangle on this screen. The rectangles are grouped together using AND, OR, and NOT operands. Items located on the same line are ANDed. The separate lines are ORed. You invoke the NOT operand by clicking the NOT button.

If a packet matches the specified logical combination of criteria, it passes the filter and is accepted.

You can go back and edit an item by clicking the Edit button. You can remove the item entirely by clicking the Delete button.

Give your filter a name here. You will select this filter from the filter list using this name.

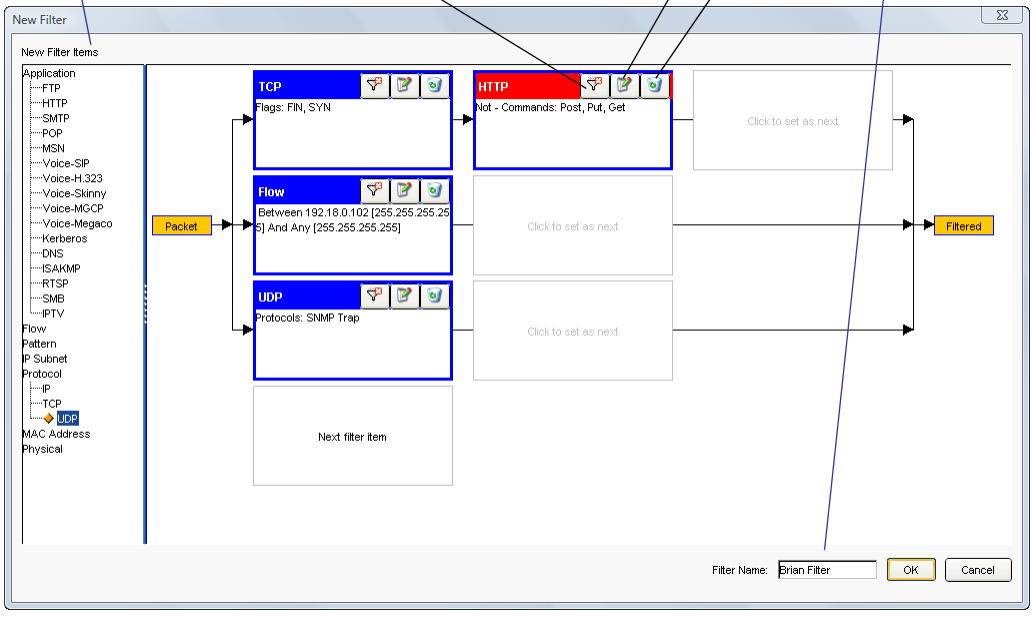


Figure 9-4: Building a Defined Filter

Setting Application Layer Filters

Click the **Application** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **Application Filter** dialog box (Figure 9-5). Here you can select the applications that interest you. Frames from checked applications are included as part of this filter.



Figure 9-5: The Application Filter Dialog Box

In addition to these broad application layer filters, you can select specific filtering criteria for each particular application by clicking its entry in the **New Filter Items** menu at the left of the page. The dialog box that appears lets you select various frame types, commands, and status messages that you can use as filtering criteria. Available filtering criteria for each application are described in the sections that follow.

Setting DNS Filters

Click the **DNS** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **DNS Filter** dialog box. Here you can specify various types of DNS traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-6, you can filter on the following criteria for DNS traffic:

General	Specify values for different fields in a DNS command to be included as part of this filter (**DNS Name, Query ID**). Packets including a specified value for a specified field will be included as part of this filter.
Commands	Select different DNS command types to include as part of this filter.
Status	Select different DNS status flags to include as part of this filter.
Symptoms	Select different DNS error message types to be included as part of this filter.

IMPORTANT: Status and **Symptoms** filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including criteria from these groups is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

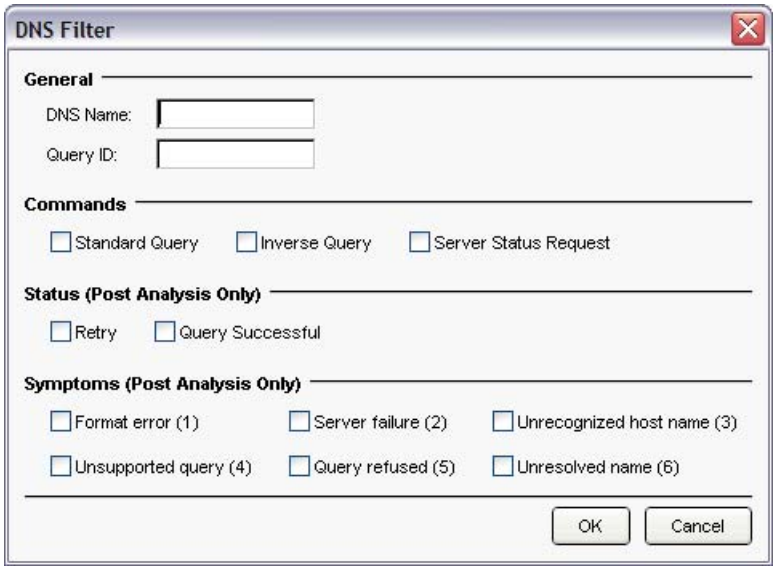


Figure 9-6: Filtering Criteria for DNS

Setting FTP Filters

Click the **FTP** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **FTP Filter** dialog box. Here you can specify various types of FTP traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-7, you can filter on the following criteria for FTP traffic:

General	Specify a file name or user name as filtering criteria. Traffic including the specified file name and/or user name will be included as part of this filter.
Type	Select FTP Control and/or Data frames as part of this filter.
Commands	Select different FTP command types to include as part of this filter.
Symptoms	Select different FTP error message types to be included as part of this filter.

IMPORTANT: Symptoms filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including Symptoms criteria will not be available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

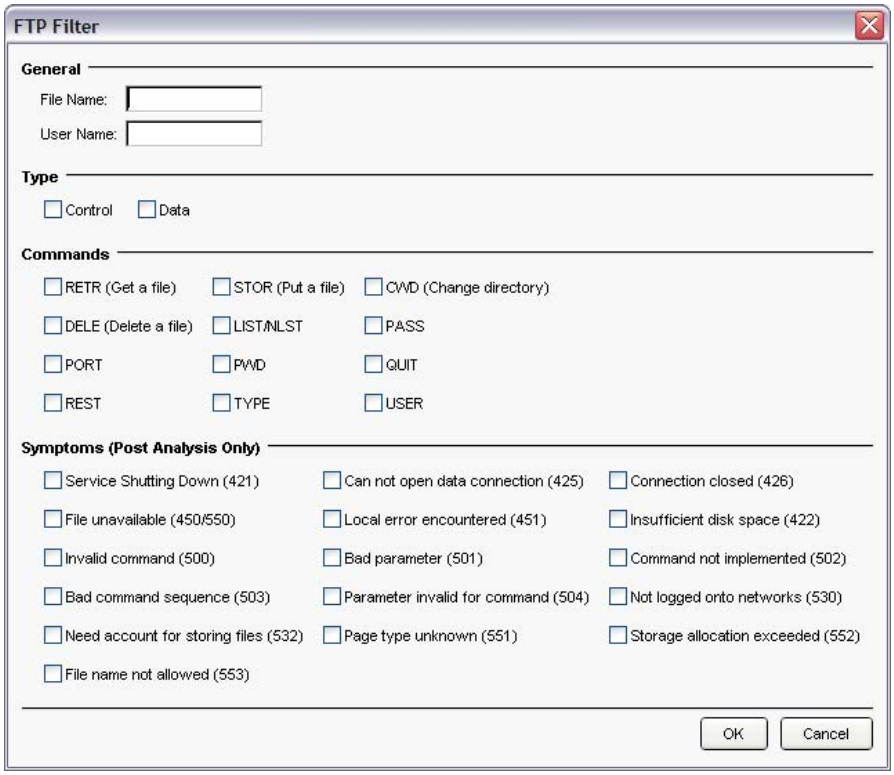


Figure 9-7: Filtering Criteria for FTP

Setting HTTP Filters

Click the **HTTP** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **HTTP Filter** dialog box. Here you can specify various types of HTTP traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-8, you can filter on the following criteria for HTTP traffic:

Resource	Specify a particular URL to use as a filtering criterion. Traffic including the specified URL will be included as part of this filter. You can specify up to five different URLs. **TIP:** This filter is useful when troubleshooting problems relating to a particular resource on an HTTP server.
Commands	Select different HTTP command types to include as part of this filter.
HTTP Applications	Use the drop-down lists to select different HTTP server and browser types as part of this filter. Frames including HTTP fields referencing the specified server or browser type will be included as part of this filter.
Symptoms	Select different HTTP error message types to be included as part of this filter.

IMPORTANT: Symptoms filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including Symptoms criteria will not be available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

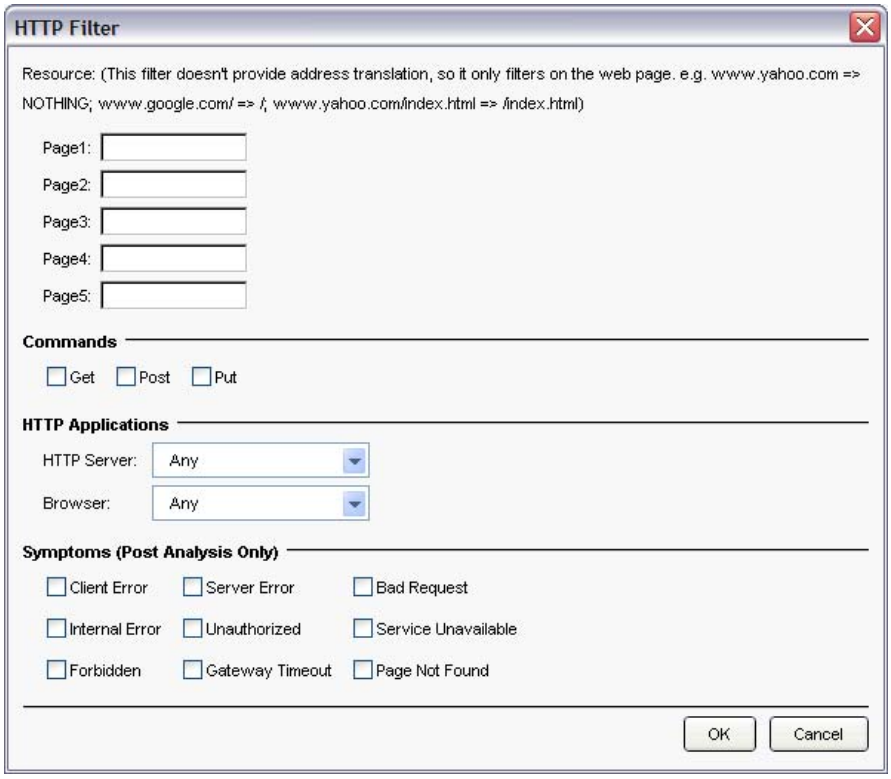


Figure 9-8: Filtering Criteria for HTTP

Setting POP Filters

Click the **POP** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **POP Filter** dialog box. Here you can specify various types of POP traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-9, you can filter on the following criteria for POP traffic:

General	Specify values for different fields in an POP email message to be included as part of this filter (**From Address**, **To Address**, **Subject**, and **Message**). Traffic including the specified fields will be included as part of this filter.
Commands	Select different POP command types to include as part of this filter.
Symptoms	Select different POP error message types to be included as part of this filter.

IMPORTANT: Symptoms filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including **Symptoms** criteria is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

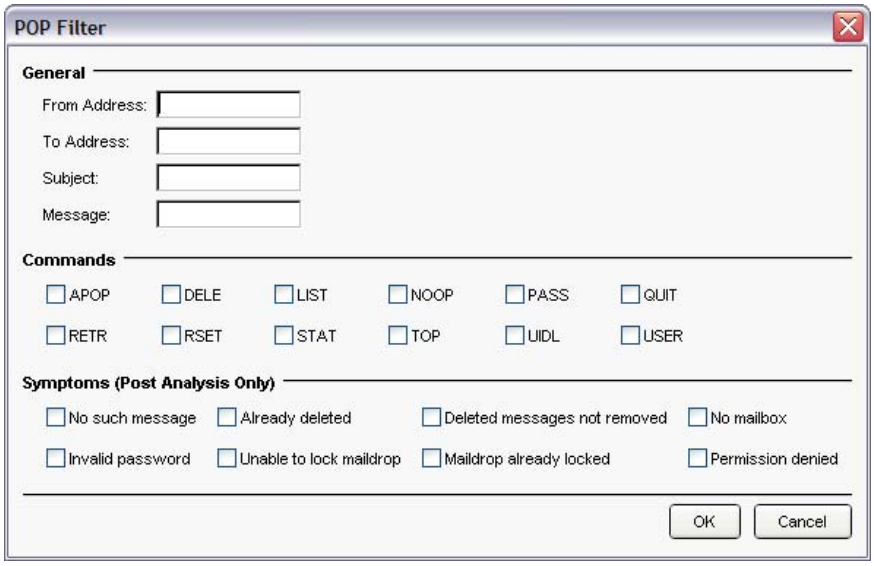


Figure 9-9: Filtering Criteria for POP

Setting SMTP Filters

Click the **SMTP** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **SMTP Filter** dialog box. Here you can specify various types of SMTP traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-10, you can filter on the following criteria for SMTP traffic:

General	Specify values for different fields in an SMTP email message to be included as part of this filter (**From Address**, **To Address**, **Subject**, and **Message**). Traffic including the specified fields will be included as part of this filter.
Commands	Select different SMTP command types to include as part of this filter.
Status	Select different SMTP status flags to include as part of this filter.
Symptoms	Select different SMTP error message types to be included as part of this filter.

IMPORTANT: Status and **Symptoms** filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including criteria from these groups is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

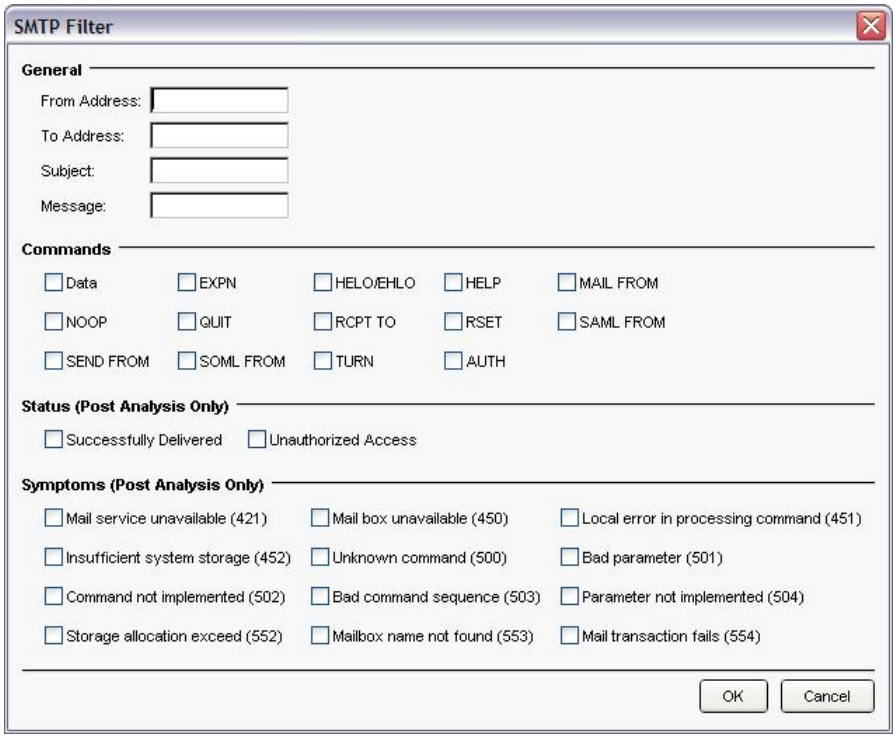


Figure 9-10: Filtering Criteria for SMTP

Setting MSN Filters

Click the **MSN** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **MSN Filter** dialog box. Here you can specify various types of MSN traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-11, you can filter on the following criteria for MSN traffic:

General	Specify a values for either **Email Address** or **Screen Name**. Traffic matching either of these will be included as part of this filter.
Servers	Specify which types of servers to include. Traffic to/from any of the checked server types will be included.

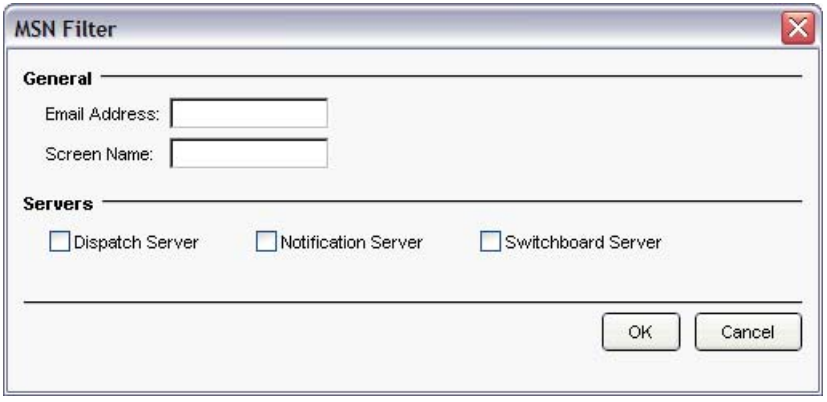


Figure 9-11: Filtering Criteria for MSN

Setting Voice-H.323 Filters

Click the **Voice-H.323** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **Voice-H.323 Filter** dialog box. Here you can specify various types of H.323 traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-12, you can filter on the following criteria for H.323 traffic:

General	Specify values for different general identifiers for a H.323 call, including the **Phone Number**, **User Name**, or **Call ID**. Traffic including the specified fields will be included as part of this filter.
Media Protocols	Select different session layer protocols used for end-to-end delivery of audio on an H.323 call (RTP, RTCP, or both) to include as part of this filter. In the case of RTP, you can also select a particular Codec.
Call Control	Select different call control messages to include as part of this filter.
Commands	Select different H.323 command types to include as part of this filter.
Status	Select different protocols in the H.323 family to include as part of this filter.
Symptoms	Select different H.323 error message types to be included as part of this filter.

IMPORTANT: Symptoms, **H.245**, and **Media Protocols** filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including criteria from these groups is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

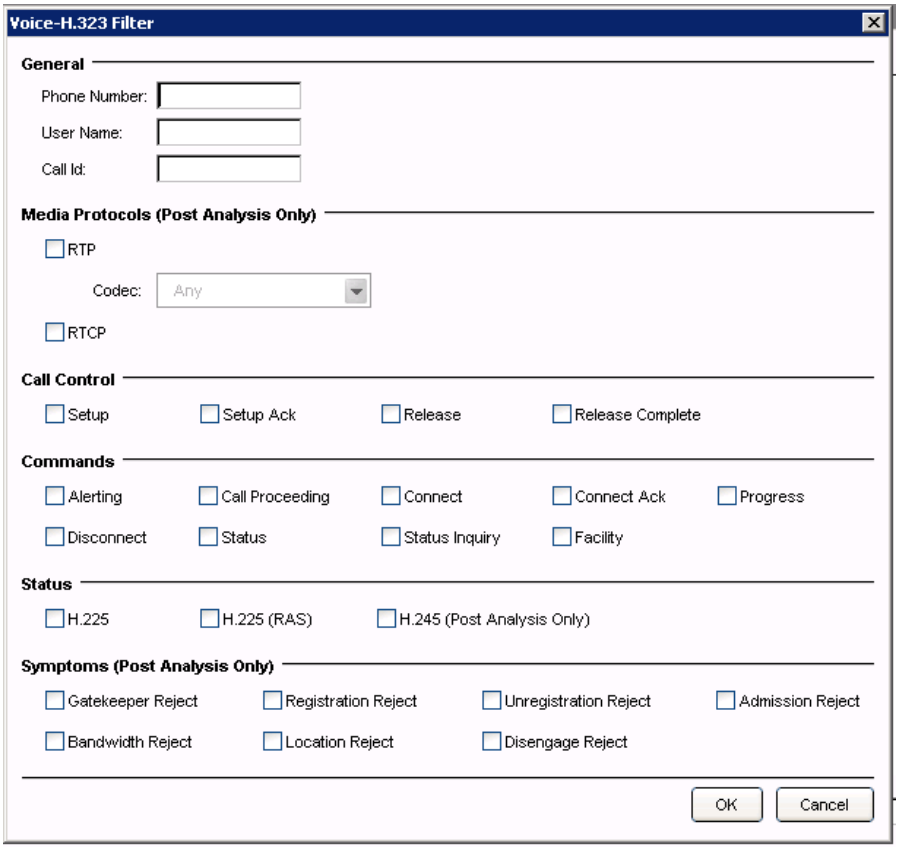


Figure 9-12: Filtering Criteria for H.323

Setting Voice-SIP Filters

Click the **Voice-SIP** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **Voice-SIP Filter** dialog box. Here you can specify various types of SIP traffic that interest you. As shown in Figure 9-13, you can filter on the following criteria for SIP traffic:

General	Specify values for different general identifiers for a SIP call, including the **Phone Number**, **User Name**, or **Call ID**. Traffic including the specified fields will be included as part of this filter.
Media Protocols	Select different session layer protocols used for end-to-end delivery of audio on a SIP call (RTP, RTCP, and/or T.38) to include as part of this filter. In the case of RTP, you can also select a particular Codec.
Phone and RTP	Select a **Phone Number** and related RTP flows to include as part of this filter.
Call Control	Select different call control messages to include as part of this filter.
Commands	Select different SIP command types to include as part of this filter.
Status	Select different SIP status flags to include as part of this filter.
Symptoms	Select different SIP error message types to be included as part of this filter.

IMPORTANT: Status, Symptoms, and Media Protocols filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including criteria from these groups is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

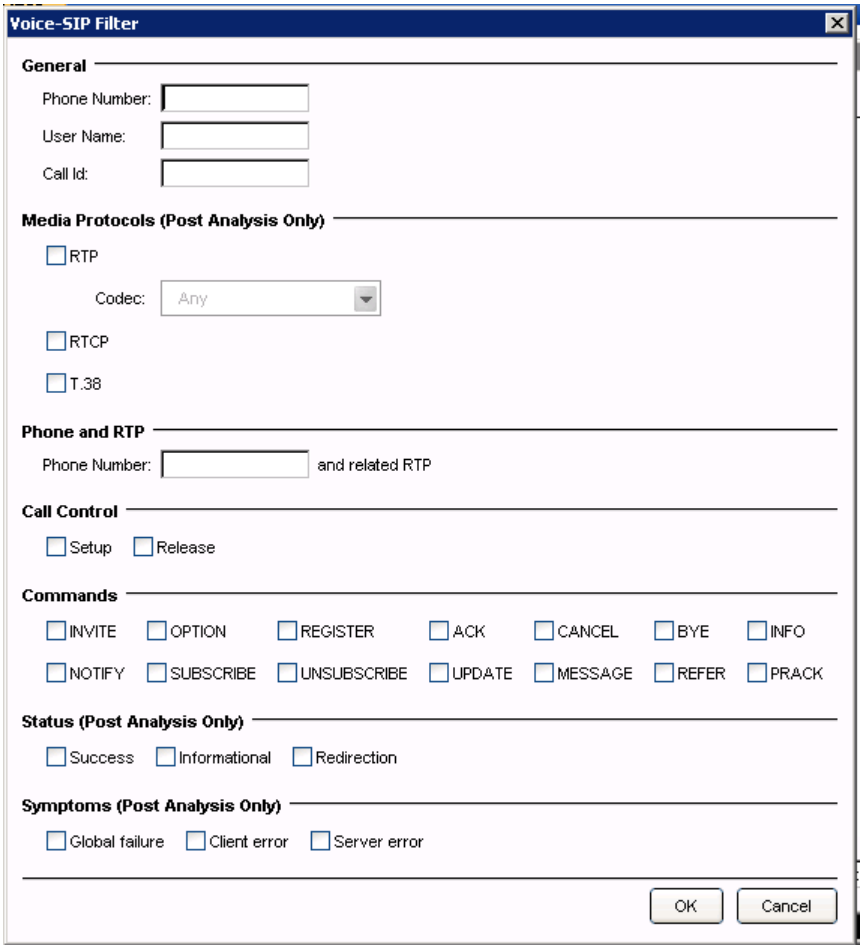


Figure 9-13: Filtering Criteria for SIP

Setting Voice-Skinny Filters

Click the **Voice-Skinny** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **Voice-Skinny Filter** dialog box. Here you can specify various types of Skinny traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-14, you can filter on the following criteria for Skinny traffic:

General — Specify values for different general identifiers for a Skinny call, including the **Phone Number**, **User Name**, or **Call ID**. Traffic including the specified fields will be included as part of this filter.

Media Protocols — Select different session layer protocols used for end-to-end delivery of audio on a Skinny call (RTP, RTCP, or both) to include as part of this filter. In the case of RTP, you can also select a particular Codec.

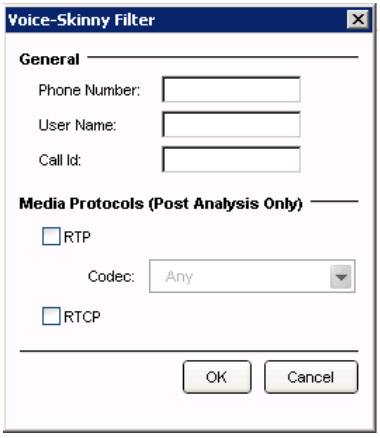


Figure 9-14: Filtering Criteria for Skinny

IMPORTANT: Media Protocols filtering criteria can only be applied during postcapture analysis as a display filter. Any filter including criteria from this group is not available during capture.

Setting Voice-MGCP Filters

Click the **Voice-MGCP** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **Voice-MGCP Filter** dialog box. Here you can specify various types of MGCP traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-15, you can filter on the following criteria for MGCP traffic:

General	Specify values for different general identifiers for a MGCP call, including the **Phone Number**, or **Connection ID**. Traffic including the specified fields will be included as part of this filter.
Media Protocols	Select different session layer protocols used for end-to-end delivery of audio on a MGCP call (RTP, RTCP, or both) to include as part of this filter. In the case of RTP, you can also select a particular Codec.
Call Control	Select different call control messages to include as part of this filter.
Symptoms	Select different MGCP error message types to be included as part of this filter.

IMPORTANT: Symptoms and **Media Protocols** filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including criteria from these groups is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters on page 271* for information on the differences between packet-based and flow-based filters.

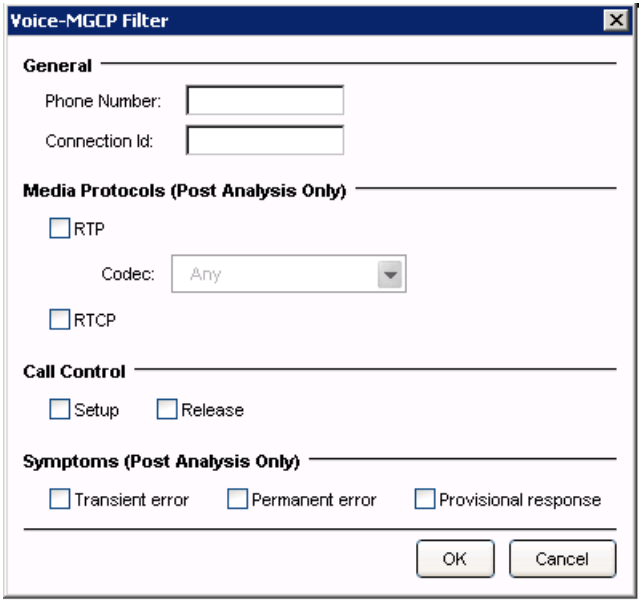


Figure 9-15: Filtering Criteria for MGCP

Setting Voice-Megaco Filters

Click the **Voice-Megaco** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **Voice-Megaco Filter** dialog box. Here you can specify various types of Megaco traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-16, you can filter on the following criteria for Megaco traffic:

General — Specify values for different general identifiers for a Megaco call, including the **Media Gateway ID** or **Termination ID**. Traffic including the specified fields will be included as part of this filter.

Media Protocols — Select different session layer protocols used for end-to-end delivery of audio on a Megaco call (RTP, RTCP, or both) to include as part of this filter. In the case of RTP, you can also select a particular Codec.

Commands — Select different Megaco command types to include as part of this filter.

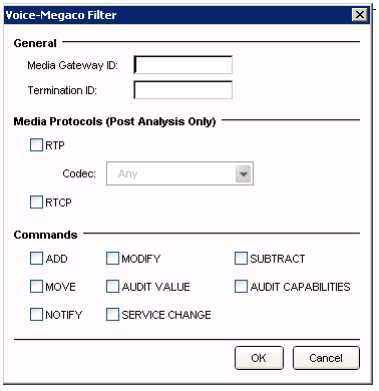


Figure 9-16: Filtering Criteria for Megaco

IMPORTANT: Media Protocols filtering criteria can only be applied during postcapture analysis as a display filter. Any filter including criteria from this group is not available during capture.

Setting ISAKMP Filters

Click the **ISAKMP** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **ISAKMP Filter** dialog box. Here you can specify various types of ISAKMP traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-17, you can filter on the following criteria for ISAKMP traffic:

Exchange Types — Select different ISAKMP exchange types to include as part of this filter.

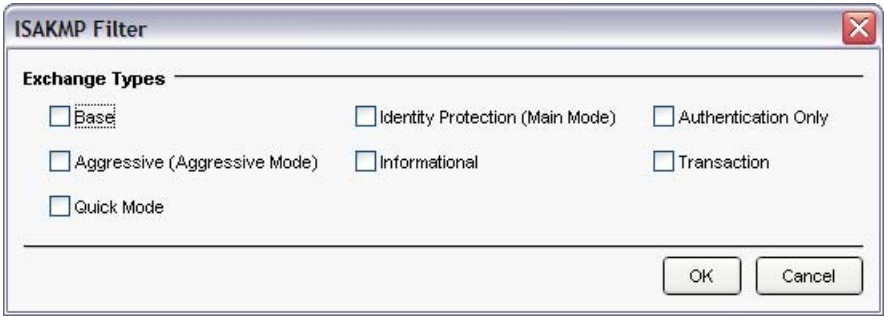


Figure 9-17: Filtering Criteria for ISAKMP

Setting Kerberos Filters

Click the **Kerberos** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **Kerberos Filter** dialog box. Here you can specify various types of Kerberos traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-18, you can filter on the following criteria for Kerberos traffic:

General	Specify values for different general identifiers for a Kerberos transaction, including the **Principal names**, **Server Realm**, and **Client Realm**. Traffic including the specified fields will be included as part of this filter.
Sub-Protocol	Select different sub-protocols: **AS Exchange**, **TGS Exchange**, and/or **CS Exchange**.
Symptoms	Select different Kerberos error message types to be included as part of this filter.

IMPORTANT: Symptoms filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including criteria from these groups is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

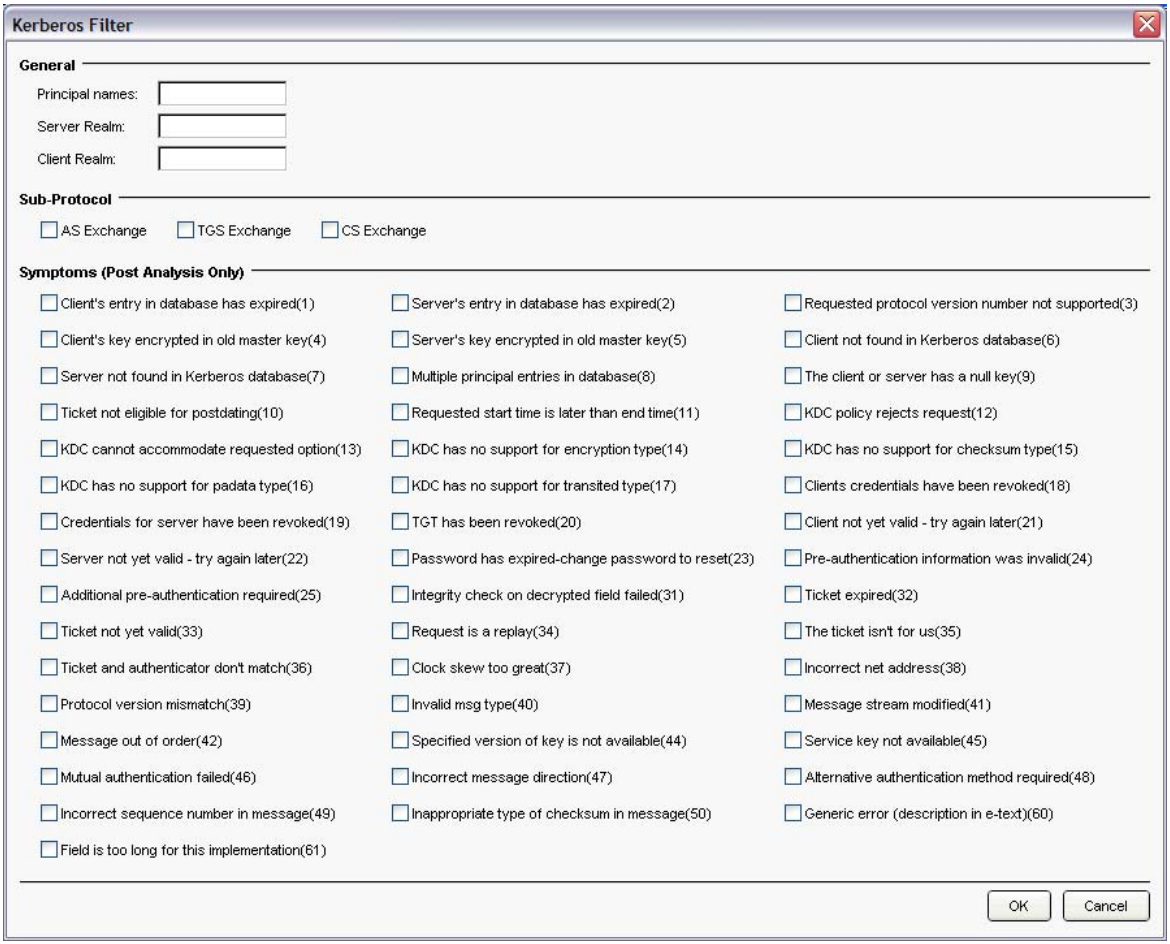


Figure 9-18: Filtering Criteria for Kerberos

Setting RTSP Filters

Click the **RTSP** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **RTSP Filter** dialog box. Here you can specify various types of RTSP traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-19, you can filter on the following criteria for RTSP traffic:

General	Specify values for different general identifiers for an RTSP stream, including **Server URL** and **Presentation**. Traffic including the specified fields will be included as part of this filter.
Methods	Check the methods that interest you. Traffic containing the specified methods will be included as part of this filter.
Symptoms	Select different RTSP error message types to be included as part of this filter.

IMPORTANT: Symptoms filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including criteria from these groups is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

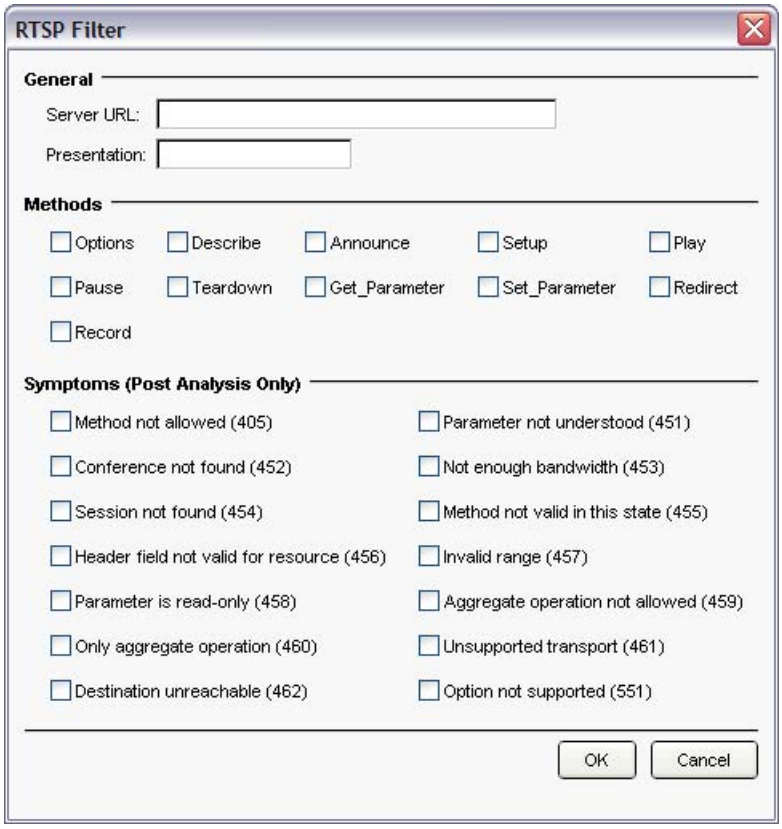


Figure 9-19: Filtering Criteria for RTSP

Setting IPTV Filters

Click the **IPTV** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **IPTV Filter** dialog box. Here you can specify various types of IPTV traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-20, you can filter on the following criteria for IPTV traffic:

General	Select **PID** frames and/or **PAT** frames. In the case of **PID** frames, you can specify a range. Traffic including the specified fields will be included as part of this filter.
Symptom	Select different IPTV error message types to be included as part of this filter.

IMPORTANT: General and **Symptoms** filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including criteria from these groups is not available during capture. See *Packet-Based Filters vs. Flow-Based Filters* on page 271 for information on the differences between packet-based and flow-based filters.

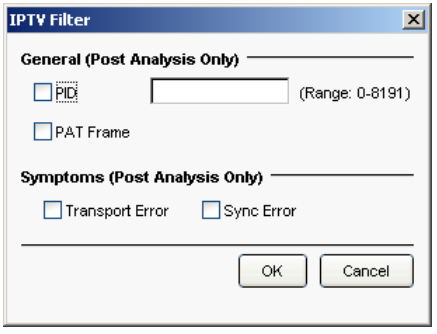


Figure 9-20: Filtering Criteria for IPTV

Setting SMB Filters

Click the **SMB** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **SMB Filter** dialog box. Here you can specify various types of SMB traffic that interest you. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-21, you can filter on the following criteria for SMB traffic:

Message Type — Check the message types that interest you. Traffic containing the specified message types will be included as part of this filter.

Errors — Check the error types that interest you. Traffic containing the specified error types will be included as part of this filter.

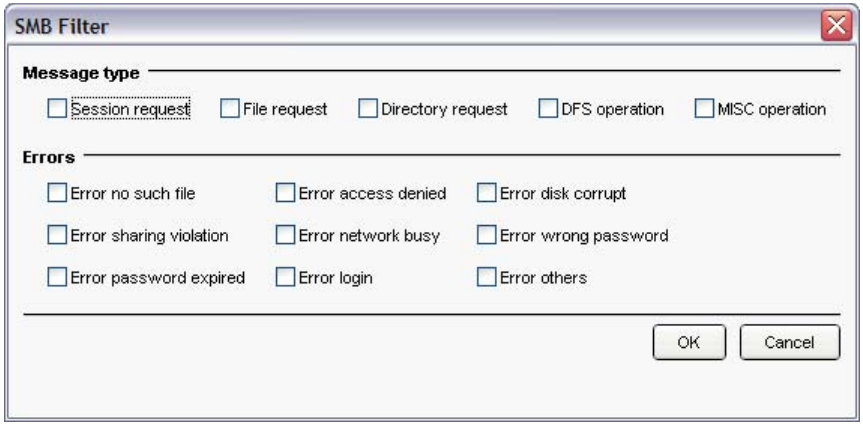


Figure 9-21: Filtering Criteria for SMB

Setting Flow Filters

Use Flow filters to include certain types of traffic between a communicating pair of IP hosts. You can specify a traffic direction to include, as well as a port number.

Click the **Flow** entry in the **New Filter** dialog box's **New Filter Items** menu and set the following options for a flow filter:

IP Address Type	Specify IPv4 or IPv6 addresses.
Source Address	The first address for this pair of hosts. Do not all 0s.
Port	The port on which to filter traffic to/ from the source address.
Dir	The direction in which traffic will be included for this pair of stations. Use the drop-down list to select a direction.
Destination Address	The second address for this pair of hosts. Do not enter all 0s.
Port	The port on which to filter traffic to/ from the destination address.

NOTE: Leaving a port number blank includes traffic on any port. Leaving an address blank includes traffic for all addresses.

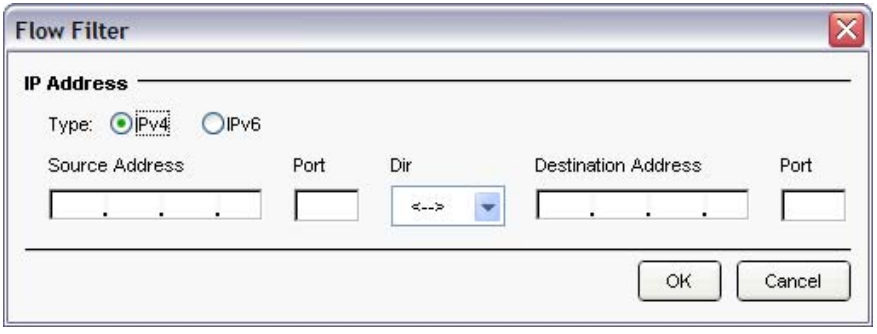


Figure 9-22: Flow Filtering Criteria

Setting Pattern Filters

Use Pattern filters to include frames that contain certain patterns.

Click the **Pattern** entry in the **New Filter** dialog box's **New Filter Items** menu and set the following options for a pattern filter (see Figure 9-23):

Match starting from:	Use the drop-down list to choose whether you want ClearSight to look for the pattern starting at the beginning of the frame, the beginning of the IP layer, or the beginning of the application layer. Alternatively, you can have ClearSight match the pattern at a specific **Offset** (in bytes) from the starting point that you choose from the drop-down list.
Offset	Choose **Text** or **Hex**, and enter the amount of the offset.
Pattern	Choose **Text** or **Hex**, and enter the pattern you want to match.

NOTE: You must enter hex data as pairs of characters separated by spaces — for example, 02 AA 03 BC.

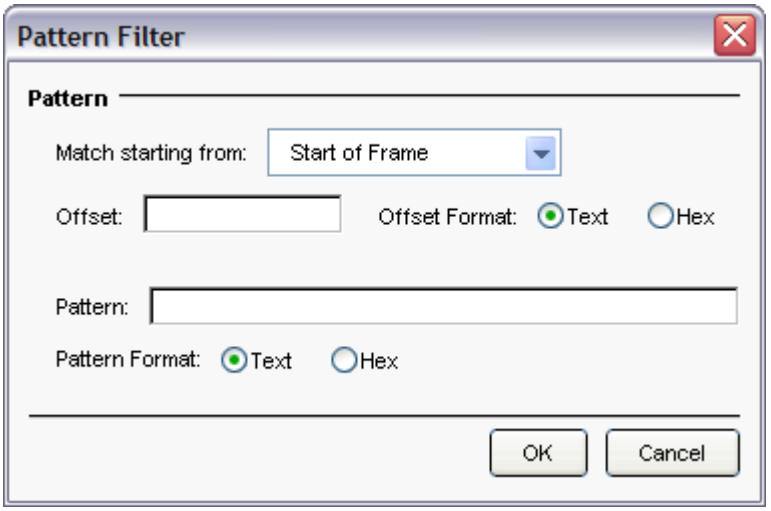


Figure 9-23: Pattern Filtering Criteria

Setting IP Subnet Filters

Use IP Subnet Filtering to include all traffic belonging to a particular IP subnet. Specify the subnet address and mask to include as part of the filter (see Figure 9-24). Use the drop-down list to select a direction.

NOTE: If you enter or 0.0.0.0 for both IP Addresses, ClearSight will ignore your input.

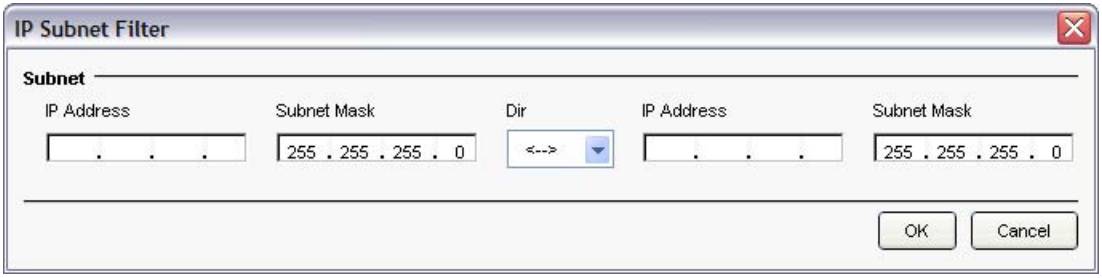


Figure 9-24: IP Subnet Filtering Criteria

Setting Protocol Filters

Use protocol filters to include packets including a particular protocol type, protocol flag, or aspect. You can set "parent" protocol filters for **IP**, **ARP**, and **IPv6** using the main **Protocol** entry in the **New Filter Items** menu. You can also configure more specific protocol filters using the dialog boxes for **IP**, **TCP**, and **UDP**. The options for each of these protocols are described below.

Setting Parent Protocol Filters

Click the **Protocol** entry in the **New Filter** dialog box's **New Filter Items** menu to bring up the **Protocols Filter** dialog box (Figure 9-25). Here you can select the parent protocols (**IP**, **ARP**, and/or **IPv6**) that interest you. Frames from any of the selected protocols will be included as part of this filter.

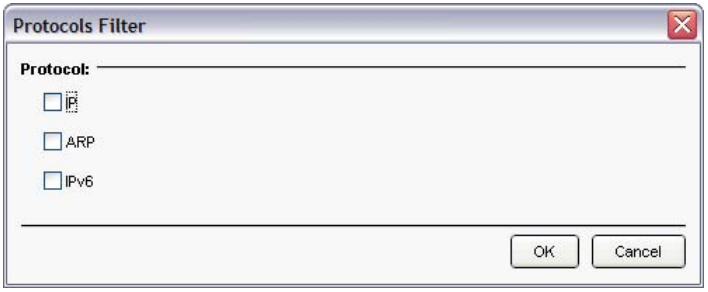


Figure 9-25: Protocols Filtering Criteria

Setting IP Filters

Click the **IP** entry in the **New Filter** dialog box's **New Filter Items** menu to specify various types of IP traffic you want to include as part of this filter. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-26, you can filter on the following criteria for IP traffic:

Service Type	Headers in IP packets can indicate different Quality of Service levels using the Service Type field. The Service Type field includes both the **Precedence** and **Transport Type** indicators. You can filter on both of these fields using the options in the **Service Type** area. Packets including a specified QoS indicator will be included as part of this filter.
Control	Select different IP control flags to include as part of this filter. Check the **Fragment** box if you want to include IP packets with the Fragment control flag set to May Fragment. Specify a value for **Hop Limit** if you want to include IP packets with a certain value in the Hop Limit field of the IP header.
Protocols	Select different TCP/IP suite protocols to include as part of this filter. If a protocol is not listed, you can type it in manually in the **Other Protocols** field. If ClearSight detects the specified protocol in the IP header's Protocol field, it will include the frame.
Frame	Check **Broadcast** to include Broadcast frames as part of this filter.

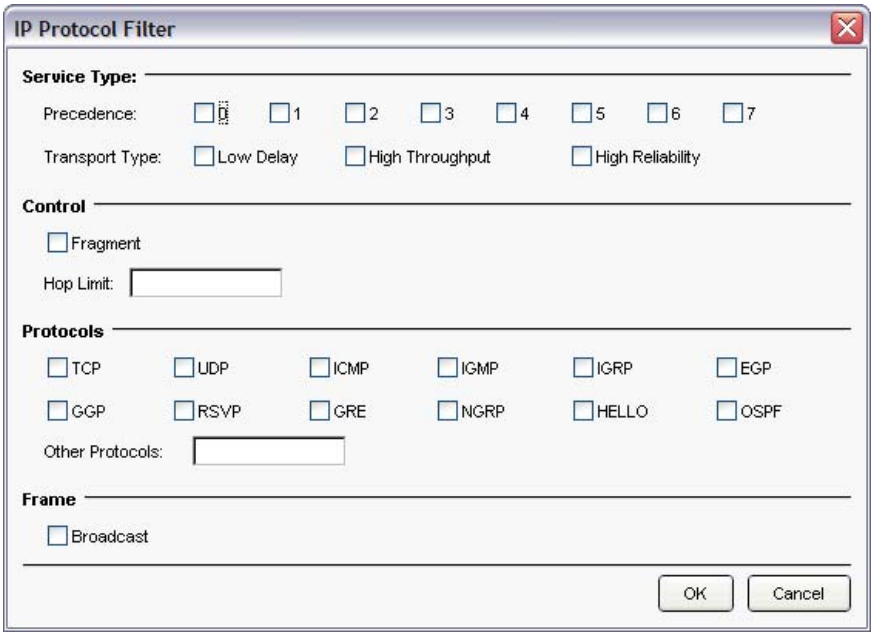


Figure 9-26: Filtering Criteria for IP

Setting TCP Filters

Click the **TCP** entry in the **New Filter** dialog box's **New Filter Items** menu to specify various types of TCP traffic you want to include as part of this filter. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-27, you can filter on the following criteria for TCP traffic:

TCP Flags	You can set filters to include packets with each of the six possible control flags in a TCP header. Packets including checked flags will be included as part of this filter.
Window	You can set filters to include packets with a specific value in the Window portion of their TCP header. Enter the value in the **Sliding Window Size:** field.
Protocols	Select different upper layer protocols to include as part of this filter. If ClearSight detects the well-known port number associated with a selected protocol in a packet's TCP header, it will include the packet. If a particular protocol is not listed, you can also specify its port number in the **Other Protocols** field to filter on it.
Symptoms	Select different TCP problem types to be included as part of this filter. You can set thresholds for the **Slow Response** and **Slow Connection** problem types. See *Setting IP Thresholds* on page 358 for information on these thresholds.

IMPORTANT: Symptoms filtering criteria are flow-based and can only be applied during postcapture analysis as a display filter. Any filter including **Symptoms** criteria will not be available during capture. See

Packet-Based Filters vs. Flow-Based Filters on page 271 for information on the differences between packet-based and flow-based filters.

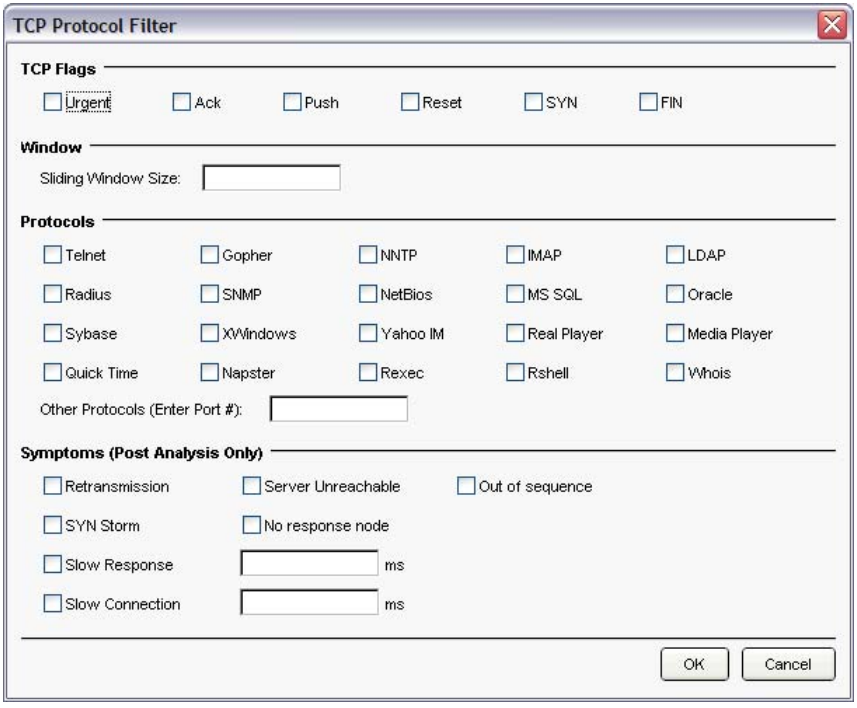


Figure 9-27: Filtering Criteria for TCP

Setting UDP Filters

Click the **UDP** entry in the **New Filter** dialog box's **New Filter Items** menu to specify various types of UDP traffic you want to include as part of this filter. Frames including any of the selected criteria will be included as part of this filter. As shown in Figure 9-28, you can filter on the following criteria for UDP traffic:

Protocols — Select different upper layer protocols to include as part of this filter. If ClearSight detects the well-known port number associated with a selected protocol in a packet's UDP header, it will include the packet.

If a particular protocol is not listed, you can also specify its port number in the **Other Protocols** field to filter on it.

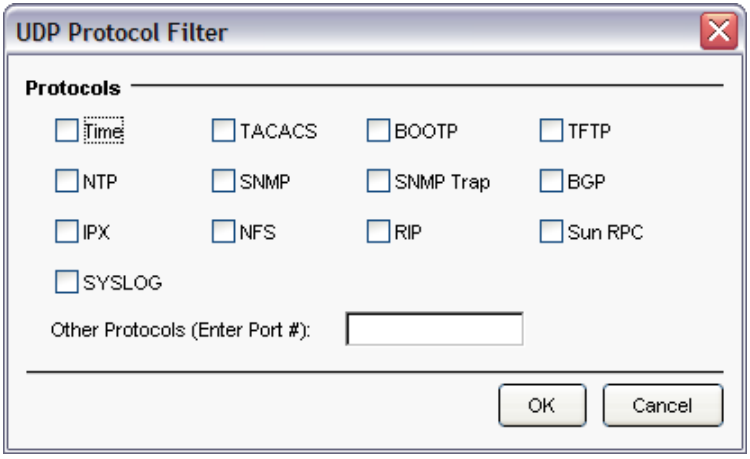


Figure 9-28: Filtering Criteria for UDP

Setting MAC Address Filters

MAC Address filters (Figure 9-29) let you include certain types of traffic between a communicating pair of MAC addresses. If desired, you can specify a traffic direction to include. Click the **MAC Address** entry in the **New Filter** dialog box's **New Filter Items** menu and set the following options for a MAC Address filter:

Source MAC	The first address for this communicating pair of nodes.
Dir	The direction in which traffic will be included for this pair of stations. Use the drop-down list to select a direction.
Destination MAC	The second address for this communicating pair of nodes.



Figure 9-29: MAC Address Filtering Criteria

Setting Physical Layer Filters

Physical layer filters (Figure 9-30) let you include traffic belonging to a particular VLAN. If you are using a full-duplex Ethernet card, you can also include traffic seen on either channel on the card, or on both channels.

Click the **Physical** entry in the **New Filter** dialog box's **New Filter Items** menu and set the following options for a Physical layer filter:

VLAN ID	Specify the ID for a VLAN whose traffic you want to include.
Channel	Full-Duplex Adapters Only. Specify the channels on the card whose traffic you want to include.
Auto-Negotiation	Specify whether to include auto-negotiation frames, non-autonegotiation frames, or both.
Filter	Specify which of these types of frames to include.
Size	From the drop down list, choose >=, ==, or <= and enter the number of bytes in the box to its right to include frames that contain >=, ==, or <= that number of bytes. If you choose <= or ==, the lower box will be grayed out. If you choose >=, you can enter the minimum number of bytes in the upper box, and the maximum number of bytes in the lower box.

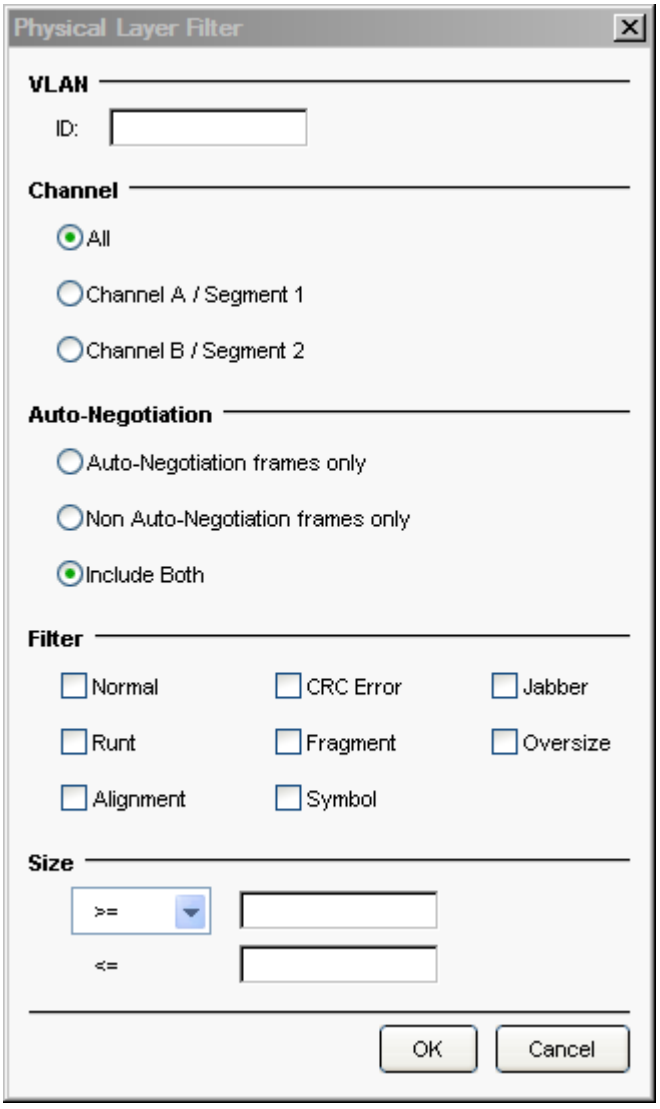


Figure 9-30: Physical Layer Filtering Criteria

The Filter List

You can view the Filter List by either of the following two methods:

- In the Capture workspace, click on the **Set** button in the **Filter** area of the **Settings** tab (if a filter is active, you must first click on the **Remove** button).
- In the Postcapture Analysis workspace, click on the **Apply Filter** icon in the status bar of the **Decode** tab.

In the Filter List, you can manage all of your defined filters. It lists each defined filter with its name, a summary description, and any restrictions that apply to the filter (for example, whether the filter is restricted to postcapture analysis use only).

From the Filter List, you can create new filters, as well as edit and delete existing filters. Figure 9-31 shows the Filter List.

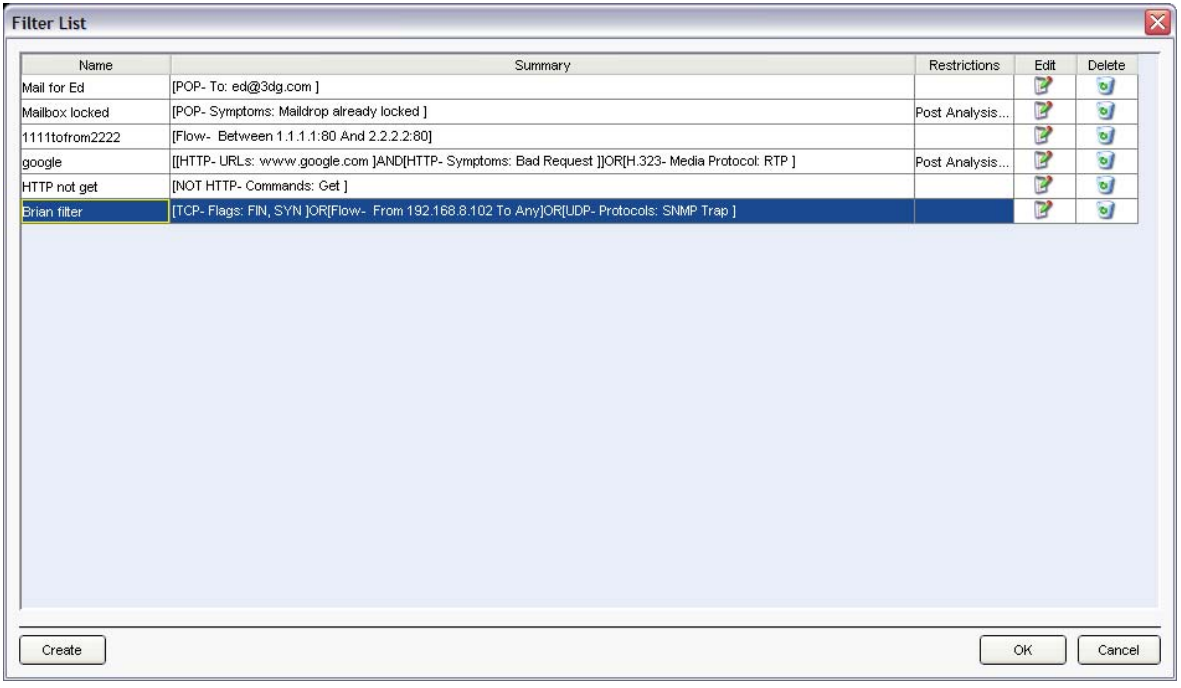


Figure 9-31: The Filter List Dialog Box

Chapter 10

Working with Alerts

This chapter describes how to work with ClearSight's **Alerts** features. ClearSight provides comprehensive alert reporting capabilities in the Alert Display, letting you keep track of issues and problems on your network in real time. You can set up different actions for different types of alarms, instructing ClearSight to send an email, dial a pager, or execute a script whenever a particular alarm severity is detected. You can also set thresholds that specify how ClearSight reports different types of alerts.

This chapter includes the following major topics:

- *About Alerts*
- *Working with the Alert Display*
- *Defining Severities and Actions*
- *Setting Thresholds for Problem Reporting*

About Alerts

ClearSight reports *alerts* to call your attention to error conditions it has detected on the network. ClearSight reports two types of alerts — *issues* and *problems*:

- **Issue** — An *issue* is a minor error condition detected on the network. A single issue does not necessarily need to be investigated on its own merits, but multiple recurrences of an issue would warrant further investigation. In addition, issues can be useful when troubleshooting a **Problem** detected by ClearSight for the same server, flow, connection, or node.

  A typical issue might be something as simple as a **404 - Not Found** error received by an HTTP client.

- **Problem** — A *problem* is a serious error condition that merits immediate investigation. An example of a problem on the network is a duplicate IP address — a condition that can cause degraded or unpredictable network performance.

  You can set thresholds for most of the problems ClearSight reports. This chapter describes how to set thresholds in *Setting Thresholds for Problem Reporting* on page 334.

Working with the Alert Display

You view the Alert Display by clicking the **Alerts** button in the ClearSight toolbar. The Alert Display lists detected problems and issues in separate tabs. Figure 10-1 shows an example of the Alert Display.

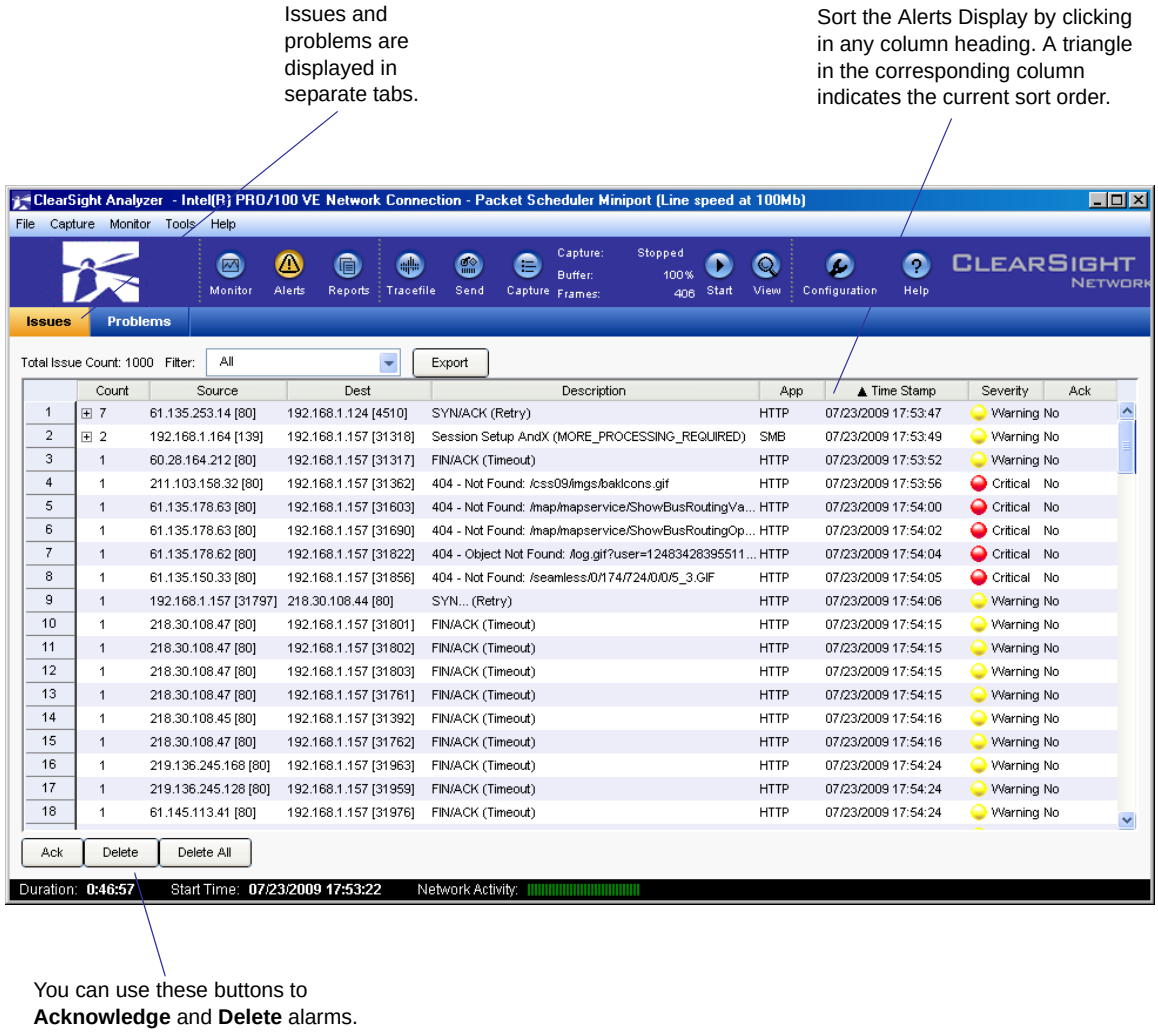


Figure 10-1: The Alerts Display

Issues Tab Information in the Alert Display

The **Issues** tab in the Alert Display lists all detected issues. Issues are listed with the following statistics:

Count	The number of similar type issues grouped together.
Source	The IP address of the source station for this issue.
Destination	The IP address of the destination station for this issue.
Description	A short description of the issue.
Application	The offending application.
Time Stamp	The time the issue was detected.
Severity	A color-coded icon indicating the severity of the issue.
Ack	Whether or not this issue has been acknowledged. You can acknowledge alerts you have already dealt with by selecting them and clicking the **Ack** button. This way, you can sort the Alert Log quickly to view only those alarms you have not yet dealt with.

You can sort the **Issues** tab by each statistic type by clicking in the corresponding column heading; click again to reverse the order. A triangle icon appears in the column heading of the statistic by which the pane is currently sorted.

Use the **Ack** button to acknowledge Issues; use the **Delete** button to delete them.

Problems Tab Information in the Alert Display

The **Problems** tab lists all detected problems. Problems are listed with the following statistics:

Count	The number of similar type problems grouped together.
Source	The IP address of the source station for this problem.
Destination	The IP address of the destination station for this problem.
Description	A short description of the problem.
Group	The offending application type.
Time Stamp	The time the problem was detected.
Severity	A color-coded icon indicating the severity of the problem.
Ack	Whether or not this problem has been acknowledged. You can acknowledge alerts you have already dealt with by selecting them and clicking the **Ack** button. This way, you can sort the Alert Log quickly to view only those alarms you have not yet dealt with.

You can sort the **Problems** tab by each statistic type by clicking in the corresponding column heading; click again to reverse the order. A triangle icon appears in the column heading of the statistic by which the pane is currently sorted.

Use the **Ack** button to acknowledge problems; use the **Delete** button to delete them.

Defining Severities and Actions

ClearSight can take different actions when an alert of a particular severity is detected. Set up severities and actions in the **Configuration > Preferences** tab (Figure 10-7 on page 334).

If you are working with a ClearSight Distributed Agent, you also use the **Central Problem Manager > Configure** option in the **Configuration > Problem Settings** tab to specify the hostname or IP address of a ClearSight Distributed Agent Manager to which you want to send problem reports for centralized collection. See *Using the Central Problem Manager* on page 101 for details.

Defining Severities

You can set severities for each of the problems ClearSight generates. Available severities range from **Critical** (the most severe) to **Major**, **Minor**, **Warning**, and **Informational** (the least severe).

To set an alarm severity:

1. Click the **Configuration** button in the ClearSight toolbar.
2. Click on the **Preferences** tab.
3. Click on **Problem > Thresholds** in the list on the left.
4. Click on an application (or other problem group) in the **Problems** list.
5. Alerts for the selected application are listed in the main pane. Select an alert by checking its box in the **Selected** column. Set the threshold by editing the value in the **Threshold** column. Use the drop-down list to set the severity.

Defining Actions

You set up actions and associate them with different alert severities by selecting **Problem > Actions** options at the left of the **Configuration > Preferences** tab. You can set up the following types of actions:

- **Email Actions** (see page 326)
- **Pager Actions** (see page 328)
- **Script Actions** (see page 330)
- **SNMP Actions** (see page 332)

The following sections describe how to set up each of these actions. When you have finished setting up actions, you can use the **Action List** option to see a quick overview of which actions you have assigned to which alert severities. The Action List is described in *Viewing the Action List* on page 333.

Configuring Email Actions

An Email action sends an email to one or more addresses when a particular alarm severity is detected. Set up an email action by clicking the **Create Email Action** button in **Configuration > Preferences > Problem > Actions**. Then set the options shown in Figure 10-2 and described in Table 10-1.

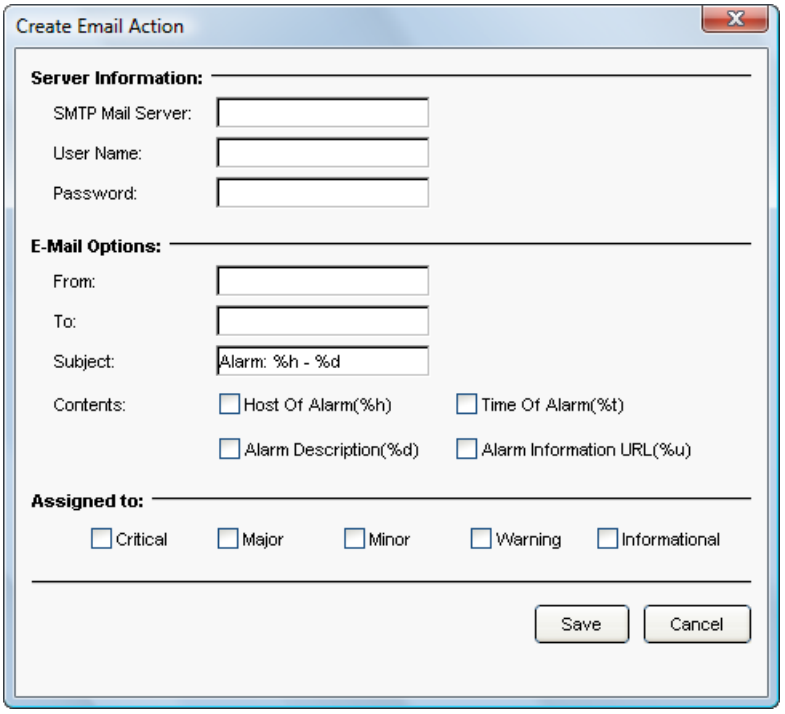


Figure 10-2: Configuring an Email Action

Table 10-1: Email Action Options

Option	Description
SMTP Mail Server	The address of the SMTP server used to send this email.
User Name	The sender's user name on this SMTP server
Password	The sender's password on this SMTP server

Table 10-1: Email Action Options

Option	Description
From	The address that appears in the **From** line of this email
To	The address to which this email will be sent.
Subject	The text for the **Subject** line in this email. By default, the subject line includes both the alarm host and a description of the alarm. You can change this to a different value. You can also use the same variables described below for the Contents option.
Contents	The text for the contents of this email. You set up the contents of the email by checking the boxes for the following variables: • **%h** — This variable includes the alarm host in the email contents. • **%t** — This variable includes the timestamp for the alarm in the email contents. • **%d** — This variable includes a description of the alarm in the email contents. • **%u** — This variable includes a URL where a user can get more information on the alarm in the email contents.
Assigned to	Specify which alarm severities are associated with this action. Check the boxes of each alarm severity for which you would like this action to take place. When an alarm of a checked severity is detected, ClearSight takes the specified action. For example, if you enable only the **Critical** severity, ClearSight will only send this particular email when a Critical alert is detected.

TIP: You can set up different email actions for different alarm severities, making sure that the proper people are notified when alarms of a particular severity are detected. For example, when a **Minor** alert is detected, you may just want to send an email to the helpdesk. However, when a **Critical** alert is detected, an email (or page) to a network manager may be more appropriate.

Configuring Pager Actions

A Pager action sends an alphanumeric page when a particular alarm severity is detected. Set up a pager action by clicking the **Create Pager Action** button in **Configuration > Preferences > Problem > Actions**. Then set the options shown in Figure 10-3 and described in Table 10-2.

NOTE: You must have a functioning modem attached to the ClearSight PC to dial out and send alphanumeric pages.

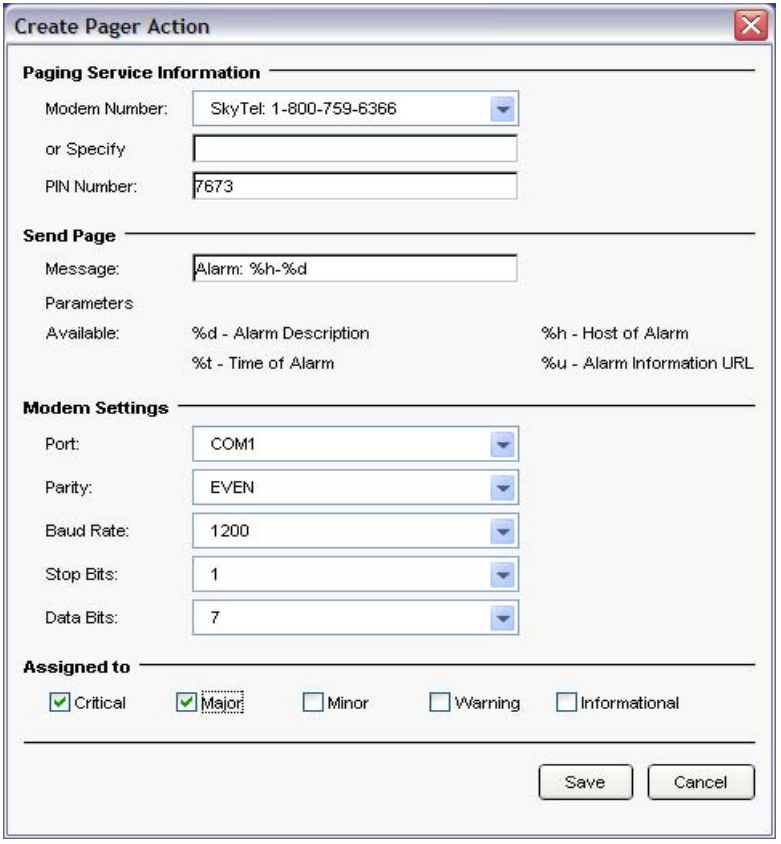


Figure 10-3: Configuring a Pager Action

Table 10-2: Pager Action Options

Option	Description
Modem Number	You can either select a commonly used pager access number from the drop-down list (SkyTel, Airtouch, and so on), or type a number in the **Specify** field.
PIN Number	Enter the PIN used to dial this pager.
Message	The text for this alphanumeric page. You set up the message using the following variables: • **%h** — This variable includes the alarm host in the page. • **%t** — This variable includes the timestamp for the alarm in the page. • **%d** — This variable includes a description of the alarm in the page. • **%u** — This variable includes a URL where a user can get more information on the alarm in the page.
Modem Settings	Specify the standard modem settings to be used for this page — port, parity, baud rate, and so on.
Assigned to	Specify which alarm severities are associated with this action. Check the boxes of each alarm severity for which you would like this action to take place. When an alarm of a checked severity is detected, ClearSight will take the specified action. For example, if you enable only the **Critical** severity, ClearSight will only send this particular page when a Critical alert is detected.

Configuring Script Actions

A Script action executes a custom JavaScript script when a particular alarm severity is detected. Set up a script action by clicking the **Create Script Action** button in **Configuration > Preferences > Problem > Actions**. Then set the options shown in Figure 10-4 and described in Table 10-3.

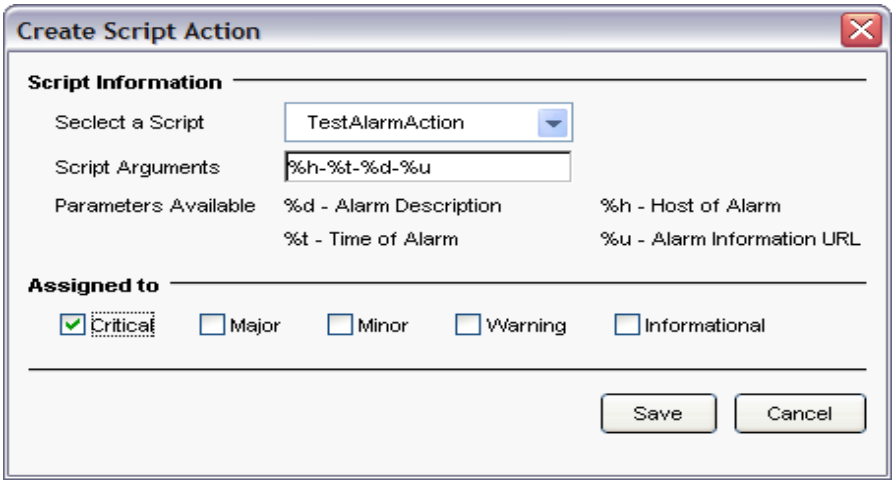


Figure 10-4: Configuring a Script Action

You can create your own scripts, using the sample program **TestAlarmAction.js** (that is provided in the **jsfiles\actions** subdirectory) as a model.

Copy your new .js file into the **jsfiles\actions** subdirectory, and it will automatically show up in the **Select a Script:** drop-down list.

Table 10-3: Script Action Options

Option	Description
Select a Script	Select a script from the drop-down list. The list includes all of the scripts stored in **\Program Files\ClearSight\jsfiles\actions**.
Script Arguments	Specify which of the following arguments to pass to the selected script: • **%h** — This variable includes the alarm host in the page. • **%t** — This variable includes the timestamp for the alarm in the page. • **%d** — This variable includes a description of the alarm in the page. • **%u** — This variable includes a URL where a user can get more information on the alarm in the page.
Assigned to	Specify which alarm severities are associated with this action. Check the boxes of each alarm severity for which you want this action to take place. When an alarm of a checked severity is detected, ClearSight takes the specified action. For example, if you enable only the **Critical** severity, ClearSight will only execute this particular script when a Critical alert is detected.

Configuring SNMP Actions

An SNMP action sends an SNMP trap to a specified host when a particular alarm severity is detected. Set up an SNMP action by clicking the **Create SNMP Action** button in **Configuration > Preferences > Problem > Actions**. Then set the options shown in Figure 10-5 and described in Table 10-4.

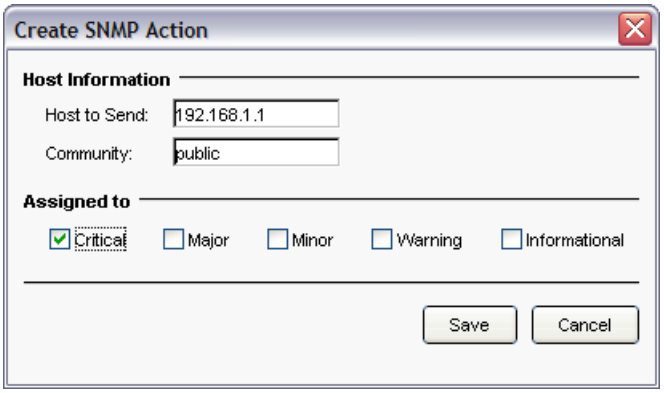


Figure 10-5: Configuring an SNMP Action

Table 10-4: SNMP Action Options

Option	Description
Host to Send	The IP address of the host to which this SNMP trap will be sent (presumably an NMS or SNMP active monitor).
Community	The community name to be included with the trap.
Assigned to	Specify which alarm severities are associated with this action. Check the boxes of each alarm severity for which you want this action to take place. When an alarm of a checked severity is detected, ClearSight takes the specified action. For example, if you enable only the **Critical** severity, ClearSight will only send this particular SNMP trap when a Critical alert is detected.

Viewing the Action List

You can review your currently defined actions in the Action List. Display the Action List by selecting **Problem > Actions** in the **Configuration > Preferences** tab.

The Action List includes each currently defined action along with an indication of the alarm severities to which it is currently assigned. From the Action List, you can quickly see which actions are assigned to which severities. You can edit any action in the list by clicking its **Edit** icon, or delete an action by clicking its **Delete** icon. You can also test the alert by clicking in the **Test** column for the alert you want to test. This will simulate the alert and perform the designated action.

Figure 10-6 shows an example of the Action List.

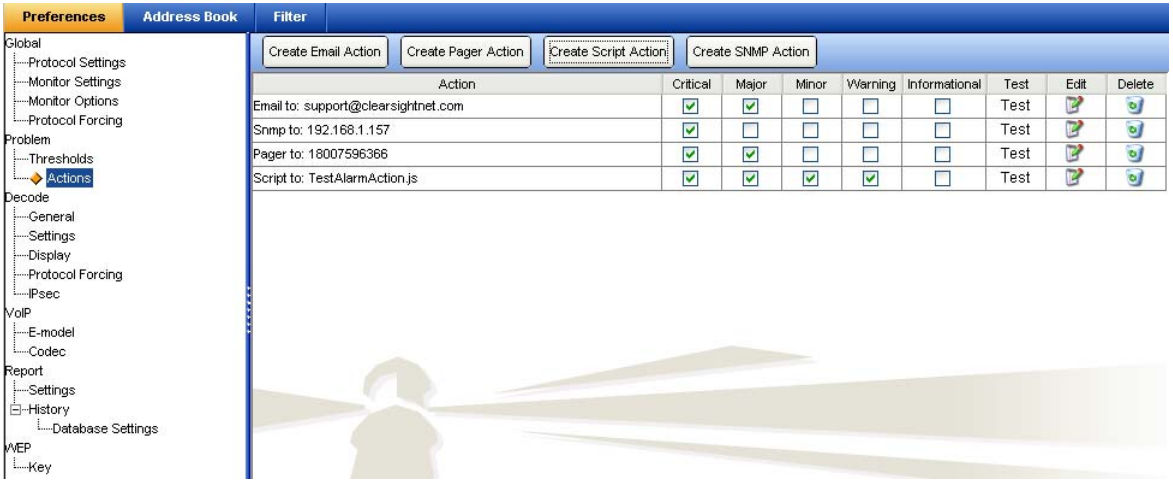


Figure 10-6: The Action List

Setting Thresholds for Problem Reporting

This section describes how to set the thresholds that control how (and when) ClearSight reports different types of problems in the Alert Display. You set thresholds for problem generation in the **Configuration > Preferences** tab. Within this tab, problem thresholds are organized by application (or other problem group) in the **Problem > Thresholds** section; click a particular selection to set the problem thresholds available for that selection.

Figure 10-7 shows an example of a **Problem > Thresholds** view; in this case, for HTTP. Following the figure, separate descriptions are provided for the thresholds available for each protocol.

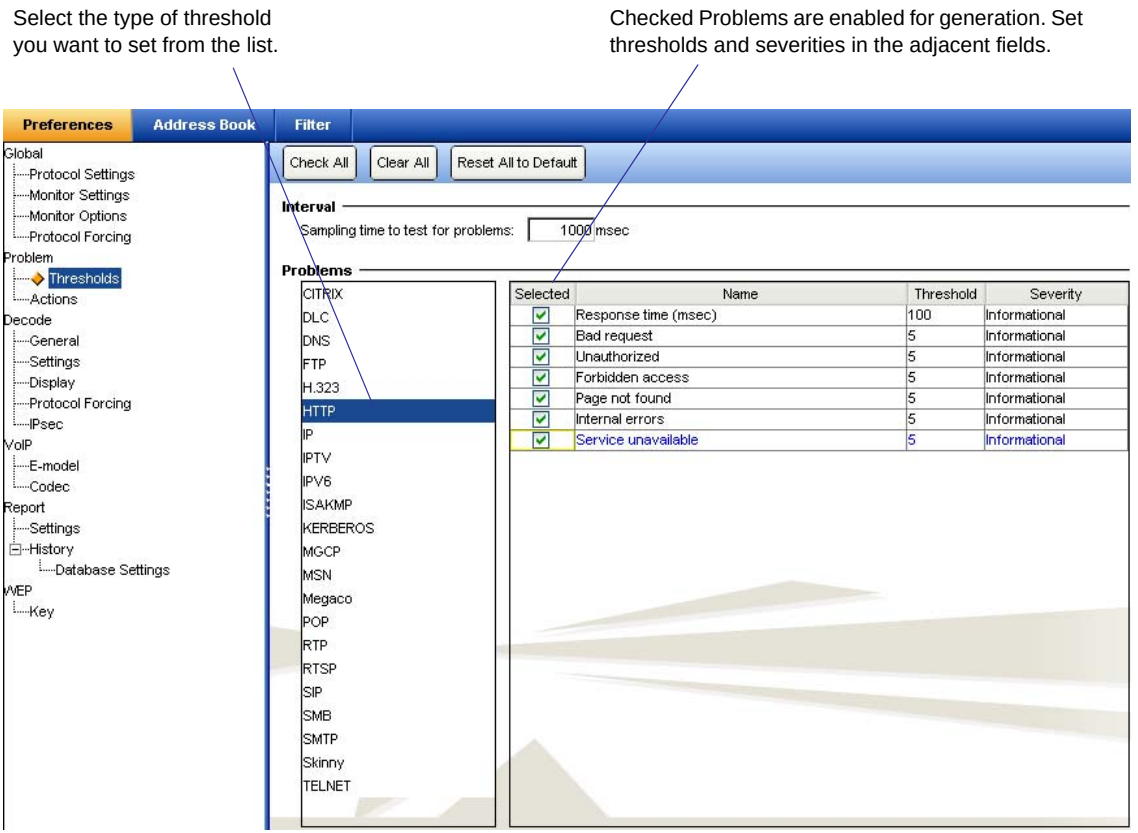


Figure 10-7: Setting Problem Thresholds

Setting DNS Thresholds

Table 10-5 lists and describes the problems and thresholds available for DNS.

Table 10-5: DNS Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Unauthorized access	ClearSight reports this problem when the number of **Unauthorized access** error response codes on a DNS flow exceeds the threshold. DNS servers report this error when an unauthorized client sends a lookup request.
Unresolved name	ClearSight reports this problem when the number of **Unresolved name** error response codes on a DNS flow exceeds the threshold. DNS servers report this error when they cannot locate an IP address for the name sent in a lookup request.
Query refused	ClearSight reports this problem when the number of **Query refused** error response codes on a DNS flow exceeds the threshold. DNS servers report this error when they refuse to carry out a request for policy reasons.

Setting FTP Thresholds

Table 10-6 lists and describes the problems and thresholds available for FTP.

Table 10-6: FTP Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Max concurrent users	ClearSight reports this problem when the number of **Max concurrent users** errors on an FTP flow exceeds the threshold. FTP servers report this error when the number of simultaneous client connections has already been reached.
Unauthorized access	ClearSight reports this problem when the number of **Unauthorized access** errors on an FTP flow exceeds the threshold. FTP servers report this error when a client requests a file for which a user name and password is required
File unavailable	ClearSight reports this problem when the number of **File unavailable** errors on an FTP flow exceeds the threshold. FTP servers report this error when a client requests a file which is currently busy (for example, because someone else is retrieving it).
Invalid command	ClearSight reports this problem when the number of **Invalid command** errors on an FTP flow exceeds the threshold. FTP servers report this error when they do not recognize a client command.
Bad parameter	ClearSight reports this problem when the number of **Bad parameter** errors on an FTP flow exceeds the threshold. FTP servers report this error when there is a syntax error in parameters in a client command.

Table 10-6: FTP Problem Thresholds

Threshold	Description
Command not implemented	ClearSight reports this problem when the number of **Command not implemented** errors on an FTP flow exceeds the threshold. FTP servers report this error when a client sends a command which the server recognizes but does not support.
Bad command sequence	ClearSight reports this problem when the number of **Bad command sequence** errors on an FTP flow exceeds the threshold. FTP servers report this error when it receives an illegal sequence of commands from a client.
Parameter invalid for command	ClearSight reports this problem when the number of **Parameter invalid for command** errors on an FTP flow exceeds the threshold. FTP servers report this error when they receive a client command containing an inappropriate parameter.
Page type unknown	ClearSight reports this problem when the number of **Page type unknown** errors on an FTP flow exceeds the threshold. FTP servers report this error when a client makes a page request which the server does not understand.
Filename not allowed	ClearSight reports this problem when the number of **Filename not allowed** errors on an FTP flow exceeds the threshold. FTP servers report this error when a client attempts to store a file with an illegal filename.
Insufficient disk space	ClearSight reports this problem when the number of **Insufficient disk space** errors on an FTP flow exceeds the threshold. FTP servers report this error when a client attempts to store a file that is too large for the available disk space.

Table 10-6: FTP Problem Thresholds

Threshold	Description
Storage allocation exceeded	ClearSight reports this problem when the number of **Storage allocation exceeded** errors on an FTP flow exceeds the threshold. FTP servers report this error when a client attempts to store a file that is too large for the current directory's allocation.
Local error encountered	ClearSight reports this problem when the number of **Local error encountered** errors on an FTP flow exceeds the threshold. FTP servers report this error when they experience a local error that prevents them from completing a client request.

Setting Telnet Thresholds

Table 10-7 lists and describes the problems and thresholds available for Telnet.

Table 10-7: Telnet Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Login incorrect	ClearSight reports this problem when the number of **Login incorrect** errors on a Telnet flow exceeds the threshold. Telnet servers report this error in response to a client connection attempt using an incorrect user name or password.
Max concurrent users	ClearSight reports this problem when the number of **Max concurrent users** errors on a Telnet flow exceeds the threshold. Telnet servers report this error in response to a connect request when the number of simultaneous client connections has already been reached.

Setting Citrix Thresholds

Table 10-8 lists and describes the problems and thresholds available for Citrix.

Table 10-8: Citrix Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).

Setting HTTP Thresholds

Table 10-9 lists and describes the problems and thresholds available for HTTP.

Table 10-9: HTTP Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Bad request	ClearSight reports this problem when the number of **Bad Request** errors (code 400) on an HTTP flow exceeds the threshold. HTTP servers report **Bad Request** errors when they do not understand a client request.
Unauthorized	ClearSight reports this problem when the number of **Unauthorized** errors (code 401) on an HTTP flow exceeds the threshold. HTTP servers report **Unauthorized** errors when a client requests a page for which a user name and password is required.
Forbidden access	ClearSight reports this problem when the number of **Forbidden** errors (code 403) on an HTTP flow exceeds the threshold. HTTP servers report **Forbidden** errors when access to a requested page is forbidden.
Page not found	ClearSight reports this problem when the number of **Page Not Found** errors (code 404) on an HTTP flow exceeds the threshold. HTTP servers report Page Not Found errors when they cannot locate a requested page.
Internal errors	ClearSight reports this problem when the number of **Internal Server Errors** (code 500) on an HTTP flow exceeds the threshold. HTTP servers report this error when they experience an unexpected error condition.
Service unavailable	ClearSight reports this problem when the number of **Bad Request** errors (code 503) on an HTTP flow exceeds the threshold. HTTP servers report this error when they cannot complete a request because they are either overloaded or temporarily down.

Setting POP Thresholds

Table 10-10 lists and describes the problems and thresholds available for POP.

Table 10-10: POP Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Mail received	ClearSight reports this problem when the number of **Mail received** errors on a POP flow exceeds the threshold.
No such message	ClearSight reports this problem when the number of **No such message** errors on a POP flow exceeds the threshold. POP servers respond with this error message when a client attempts to retrieve a message that the server does not have.
No such mailbox	ClearSight reports this problem when the number of **No such mailbox** errors on a POP flow exceeds the threshold. POP servers respond with this error message when a client attempts to access a mailbox not on the server.
Invalid password	ClearSight reports this problem when the number of **Invalid password** errors on a POP flow exceeds the threshold. POP servers respond with this error message when a client attempts to access a mailbox using the wrong password.
Permission deny	ClearSight reports this problem when the number of **Permission deny** errors on a POP flow exceeds the threshold. POP servers respond with this error message to deny a particular POP request.

Table 10-10: POP Problem Thresholds

Threshold	Description
Maildrop locked	ClearSight reports this problem when the number of **Maildrop locked** errors on a POP flow exceeds the threshold. POP servers respond with this error message when a client attempts to access a mailbox that is already locked.
Unable to lock mailbox	ClearSight reports this problem when the number of **Unable to lock mailbox** errors on a POP flow exceeds the threshold. POP servers respond with this error message when they are unable to lock a specified mailbox.

Setting SMTP Thresholds

Table 10-11 lists and describes the problem thresholds available for SMTP.

Table 10-11: SMTP Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Unauthorized access	ClearSight reports this problem when the number of **Unauthorized access** errors returned by a server to a client on a flow exceeds the threshold. SMTP servers send Unauthorized access error messages when clients request services for which they are not authorized.
Out of resources	ClearSight reports this problem when the number of **Out of resources** errors returned by a server to a client on a flow exceeds the threshold. SMTP servers send Out of resources error messages when they lack the resources to carry out a client request.

Setting MSN Thresholds

Table 10-12 lists and describes the problem thresholds available for MSN.

Table 10-12: MSN Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Error	ClearSight reports the **Error** problem when the number of errors returned by a server to a client on a flow exceeds the threshold.

Setting H.323 Thresholds

Table 10-13 lists and describes the problems and thresholds available for H.323.

Table 10-13: H.323 Problem Thresholds

Threshold	Description
Call setup time (usec)	ClearSight reports this problem when the time it takes to set up an H.323 VoIP call exceeds the threshold (in microseconds). Call setup time is measured as the time between the initial **Setup** message and the corresponding **Alerting** message from the called party.
Call failure	ClearSight reports this problem when the number of call failures for a given flow exceeds the threshold. Call failures are reported in the H.225 signaling messages.
Gatekeeper reject	ClearSight reports this problem when the number of Gatekeeper Reject messages exceeds the threshold. RAS Gatekeepers send Reject messages to deny Gatekeeper Requests from H.225 terminals.
Registration reject	ClearSight reports this problem when the number of Registration Reject messages exceeds the threshold. RAS Gatekeepers send Registration Reject messages to deny registration requests from H.225 terminals.
Unregistration reject	ClearSight reports this problem when the number of Unregistration Reject messages exceeds the threshold. RAS Gatekeepers send Unregistration Reject messages to deny unregistration requests from H.225 terminals.
Admission reject	ClearSight reports this problem when the number of Admission Reject messages exceeds the threshold. RAS Gatekeepers send Admission Reject messages to deny admission requests from H.225 terminals.
Bandwidth reject	ClearSight reports this problem when the number of Bandwidth Reject messages exceeds the threshold. RAS Gatekeepers send Bandwidth Reject messages to deny bandwidth requests from H.225 terminals.

Table 10-13: H.323 Problem Thresholds

Threshold	Description
Location reject	ClearSight reports this problem when the number of Location Reject messages exceeds the threshold. RAS Gatekeepers send Location Reject messages to deny location requests from H.225 terminals.
Disengage reject	ClearSight reports this problem when the number of Disengage Reject messages exceeds the threshold. RAS Gatekeepers send Disengage Reject messages to deny disengage requests from H.225 terminals.

Setting SIP Thresholds

Table 10-14 lists and describes the problem thresholds available for SIP.

Table 10-14: SIP Problem Thresholds

Threshold	Description
Call setup time (usec)	ClearSight reports this problem when the time it takes to set up a SIP VoIP call exceeds the threshold (in microseconds).
Call failure	ClearSight reports this problem when the number of call failures for a given flow exceeds the threshold. Call failures are reported in the SIP signaling messages.
Client error	ClearSight reports this problem when the number of client errors for a given flow exceeds the threshold.
Server error	ClearSight reports this problem when the number of server errors for a given flow exceeds the threshold.
Global error	ClearSight reports this problem when the number of global errors for a given flow exceeds the threshold.

Setting Skinny Thresholds

Table 10-15 lists and describes the problem thresholds available for Skinny.

Table 10-15: Skinny Problem Thresholds

Threshold	Description
Call setup time (usec)	ClearSight reports this problem when the time it takes to set up a Skinny VoIP call exceeds the threshold (in microseconds).
Call failure	ClearSight reports this problem when the number of call failures for a given flow exceeds the threshold. Call failures are reported in the Skinny signaling messages.
Release time (msec)	ClearSight reports the **Release Time** problem when a server fails to release a Skinny VoIP call within the time specified by the threshold (in milliseconds).

Setting MGCP Thresholds

Table 10-16 lists and describes the problem thresholds available for MGCP.

Table 10-16: MGCP Problem Thresholds

Threshold	Description
Call setup time (usec)	ClearSight reports this problem when the time it takes to set up an MGCP VoIP call exceeds the threshold (in microseconds).
Call failure	ClearSight reports this problem when the number of call failures for a given flow exceeds the threshold. Call failures are reported in the MGCP signaling messages.
Transient error	ClearSight reports this problem when the number of transient errors for a given flow exceeds the threshold.
Permanent error	ClearSight reports this problem when the number of permanent errors for a given flow exceeds the threshold.

Setting Megaco Thresholds

Table 10-17 lists and describes the problem thresholds available for Megaco.

Table 10-17: Megaco Problem Thresholds

Threshold	Description
Call setup time (usec)	ClearSight reports this problem when the time it takes to set up a Megaco VoIP call exceeds the threshold (in microseconds).
Call failure	ClearSight reports this problem when the number of call failures for a given flow exceeds the threshold. Call failures are reported in the Megaco signaling messages.
Errors	ClearSight reports this problem when the number of errors for a given flow exceeds the threshold.

Setting RTP Thresholds

Table 10-18 lists and describes the problems and thresholds available for RTP.

Table 10-18: RTP Problem Thresholds

Threshold	Description
Silent Packet Gap (msec)	ClearSight reports this problem when the length of a silent packet gap exceeds the threshold. The silent packet gap is the number of milliseconds between the end of one RTP packet and the beginning of the next. In normal RTP traffic this will be a small number of milliseconds, not likely to trigger this problem. However, RTP endpoints can be configured to stop sending RTP packets when there is no actual audio to send. This is called Silence Suppression or Voice Activity Detection (VAD). A receiver can recognize this by looking at the timestamp of each RTP packet, and checking whether this is shortly after the end of the previous packet. If it is not a short amount of time, and yet the RTP sequence number has increased by only one, then the receiver recognizes that a silent packet gap has occurred.
RTP jitter	ClearSight reports this problem when the RTP jitter on a given flow exceeds the threshold.
Mean delay (sec)	ClearSight reports this problem when the mean delay for packets on a given flow exceeds the threshold.
Dropped frames	ClearSight reports this problem when the number of dropped frames on a given flow exceeds the threshold.
Out of sequence	ClearSight reports this problem when the number of out of sequence frames on a given flow exceeds the threshold.
Mean Opinion Score	ClearSight reports this problem when the Mean Opinion Score for a given flow is lower than the threshold.

Table 10-18: RTP Problem Thresholds

Threshold	Description
Japan Mean Opinion Score	ClearSight reports this problem when the Japan Mean Opinion Score for a given flow is lower than the threshold.
Dropped frames/Total RTP frames (%)	ClearSight reports this problem when the percentage of RTP frames dropped exceeds the threshold.
IPv6 RTP Fragments Lost/Total IPv6 RTP Fragments (%)	ClearSight reports this problem when the percentage of IPv6 RTP fragments lost exceeds the threshold.
IPv6 RTP Checksum errors/Total IPv6 RTP frames (%)	ClearSight reports this problem when the percentage of IPv6 RTP frames with checksum errors exceeds the threshold.
IPv6 RTP Fragment Packet Loss (per sample interval per flow)	ClearSight reports this problem when the number of IPv6 RTP fragments lost (per sample interval per flow) exceeds the threshold.
VQFactor	ClearSight reports this problem when the Video Quality Factor for a given flow is lower than the threshold.
R Value	ClearSight reports this problem when the R Value quality rating for a given flow is lower than the threshold.
MDI Average DF Value (msec)	ClearSight reports this problem when the average MDI Delay Factor exceeds the threshold.
MDI MLR Value	ClearSight reports this problem when the average MDI Media Loss Rate exceeds the threshold.

Setting RTSP Thresholds

Table 10-19 lists and describes the problems and thresholds available for RTSP.

Table 10-19: RTSP Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Method not allowed	ClearSight reports this problem when the number of **Method not allowed** errors exceeds the threshold.
Parameter not understood	ClearSight reports this problem when the number of **Parameter not understood** errors exceeds the threshold.
Conference not found	ClearSight reports this problem when the number of **Conference not found** errors exceeds the threshold.
Not enough bandwidth	ClearSight reports this problem when the number of **Not enough bandwidth** errors exceeds the threshold.
Session not found	ClearSight reports this problem when the number of **Session not found** errors exceeds the threshold.
Method not valid in this state	ClearSight reports this problem when the number of **Method not valid in this state** errors exceeds the threshold.
Header field not valid for resource	ClearSight reports this problem when the number of **Header field not valid for resource** errors exceeds the threshold.
Invalid range	ClearSight reports this problem when the number of **Invalid range** errors exceeds the threshold.
Parameter is read-only	ClearSight reports this problem when the number of **Parameter is read-only** errors exceeds the threshold.
Aggregate operation not allowed	ClearSight reports this problem when the number of **Aggregate operation not allowed** errors exceeds the threshold.

Table 10-19: RTSP Problem Thresholds

Threshold	Description
Only aggregate operation	ClearSight reports this problem when the number of **Only aggregate operation** errors exceeds the threshold.
Unsupported transport	ClearSight reports this problem when the number of **Unsupported transport** errors exceeds the threshold.
Destination Unreachable	ClearSight reports this problem when the number of **Destination Unreachable** errors exceeds the threshold.
Option not supported	ClearSight reports this problem when the number of **Option not supported** errors exceeds the threshold.

Setting IPTV Thresholds

Table 10-20 lists and describes the problems and thresholds available for IPTV.

Table 10-20: IPTV Problem Thresholds

Threshold	Description
Dropped frames	ClearSight reports this problem when the number of dropped frames on a given flow exceeds the threshold.
Out of sequence	ClearSight reports this problem when the number of out of sequence frames on a given flow exceeds the threshold.
Dropped frames/Total Media frames (%)	ClearSight reports this problem when the percentage of Media frames dropped exceeds the threshold.
MDI Average DF Value (msec)	ClearSight reports this problem when the average MDI Delay Factor exceeds the threshold.
MDI MLR Value	ClearSight reports this problem when the average MDI Media Loss Rate exceeds the threshold.
VQFactor	ClearSight reports this problem when the Video Quality Factor for a given flow is lower than the threshold.

Setting ISAKMP Thresholds

Table 10-21 lists and describes the problem thresholds available for ISAKMP.

Table 10-21: ISAKMP Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Phase 1 failure	ClearSight reports this problem when the number of Phase 1 failures for a given flow exceeds the threshold.

Setting Kerberos Thresholds

Table 10-22 lists and describes the problem thresholds available for Kerberos.

Table 10-22: Kerberos Problem Thresholds

Threshold	Description
No response Kerberos server	ClearSight reports the **No response Kerberos server** problem when the number of consecutive retries to a server without any response exceeds the threshold.
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Error	ClearSight reports this problem when the number of errors for a given flow exceeds the threshold.

Setting SMB Thresholds

Table 10-23 lists and describes the problem thresholds available for SMB.

Table 10-23: SMB Problem Thresholds

Threshold	Description
Response time (msec)	ClearSight reports the **Response Time** problem when a server fails to respond to a request within the time specified by the threshold (in milliseconds).
Error no such file	ClearSight reports this problem when the number of **No such file** errors exceeds the threshold.
Error access denied	ClearSight reports this problem when the number of **Access denied** errors exceeds the threshold.
Error disk corrupt	ClearSight reports this problem when the number of **Disk corrupt** errors exceeds the threshold.
Error sharing violation	ClearSight reports this problem when the number of **Sharing violation** errors exceeds the threshold.
Error network busy	ClearSight reports this problem when the number of **Network busy** errors exceeds the threshold.
Error wrong password	ClearSight reports this problem when the number of **Wrong password** errors exceeds the threshold.
Error password expired	ClearSight reports this problem when the number of **Password expired** errors exceeds the threshold.
Error login	ClearSight reports this problem when the number of **Login** errors exceeds the threshold.
Error others	ClearSight reports this problem when the number of other errors exceeds the threshold.

Setting IP Thresholds

Table 10-24 lists and describes the problems and thresholds available for IP.

Table 10-24: IP Problem Thresholds

Threshold	Description
Ping Storm	ClearSight reports this problem when the number of ping messages seen per second exceeds the threshold.
Syn Storm	ClearSight reports this problem when the number of TCP SYN messages seen per second exceeds the threshold.
Retransmission	ClearSight reports this problem when it sees a frame with a TCP sequence number less than or equal to an earlier value seen on the same connection, indicating that it has already been transmitted.
Timeout	ClearSight reports this problem when one end of a connection fails to respond to the other within the time limit specified by the threshold.
Slow TCP Connection (msec)	ClearSight reports this problem when it detects a TCP connection with average response times exceeding the threshold.
Slow Response (msec)	ClearSight reports this problem when the time it takes one end of a TCP connection to respond to the other end exceeds the threshold.
Very Slow Response (msec)	ClearSight reports this problem when the time it takes one end of a TCP connection to respond to the other end exceeds the threshold. **NOTE:** The Slow Response and Very Slow Response problems work together so you can identify slow responses that are somewhat trivial and slow responses that are truly problematic. You should set the thresholds accordingly.
No Response Host (retrans)	ClearSight reports this problem when it detects that a host has not responded to the same request retransmitted multiple times.

Table 10-24: IP Problem Thresholds

Threshold	Description
Duplicated IP Address	ClearSight reports this problem when it detects a duplicate IP address on the network.
Port Scan (Socket Port Number)	ClearSight reports this problem when it detects a packet using the specified port number. You can set this to an unused port number; if ClearSight sees a SYN made to the specified port number, it will report this problem. SYNs made to an unused port number are one signature of a port scan in progress.

Setting IPv6 Thresholds

Table 10-25 lists and describes the problems and thresholds available for IPv6.

Table 10-25: IPv6 Problem Thresholds

Threshold	Description
IPv6 fragment packets lost (per sample interval per flow)	ClearSight reports this problem when the number of IPv6 fragments lost (per sample interval per flow) exceeds the threshold.
IPv6 checksum error (per sample interval per flow)	ClearSight reports this problem when the number of IPv6 checksum errors (per sample interval per flow) exceeds the threshold.
IPv6 fragment packets lost (cumulative per flow)	ClearSight reports this problem when the number of IPv6 fragments lost (cumulative per flow) exceeds the threshold.
IPv6 checksum error (cumulative per flow)	ClearSight reports this problem when the number of IPv6 checksum errors (cumulative per flow) exceeds the threshold.

Setting DLC Thresholds

Table 10-26 lists and describes the problems and thresholds available at the DLC layer.

Table 10-26: DLC Problem Thresholds

Threshold	Description
Utilization (%)	ClearSight reports this problem when percentage network utilization exceeds the threshold during any one minute interval.
Broadcast Storm	ClearSight reports this problem when the number of broadcast frames per second from a single DLC station exceeds the threshold.
Multicast Storm	ClearSight reports this problem when the number of multicast frames per second from a single DLC station exceeds the threshold.
High physical error rate	ClearSight reports this problem when the number of physical errors per second from a single DLC station exceeds the threshold. Physical errors include CRC errors, runts, fragments, oversize errors, jabbers, collisions, and alignment errors.
Gigabit Link	ClearSight reports this problem when the gigabit link is down at a Gigabit Ethernet adapter.

Chapter 11

Using the Address Book

This chapter describes how to use ClearSight's Address Book. The chapter includes the following topics:

- *About the Address Book*
- *Working with the Address Book*

About the Address Book

ClearSight's *Address Book* lets you substitute easily recognizable names for IP, IPv6, or MAC addresses in the postcapture analysis workspace's **Decode** tab. Since most people find it easier to remember names than IP addresses, the Address Book can be an invaluable aid when troubleshooting network data.

For example, instead of trying to remember that the IP address **192.168.1.1** is used on an interface on a router in Seattle in your corporate network, you can use the Address Book to refer to this address simply as **Seattle Router**. Careful maintenance of Address Book entries can help make network troubleshooting much more intuitive.

Working with the Address Book

Display the Address Book by clicking the **Configuration** button in the ClearSight toolbar and then clicking on the **Address Book** tab. Figure 11-1 shows the Address Book and explains how to add and delete entries.

NOTE: If the **Overwrite existing address book entries** option is checked, ClearSight will automatically update an address book entry when it detects an NDS packet containing the same Name or IP address.

Click the **Add** button to add a new entry to the Address Book.

You can **Edit** and **Delete** existing Address book entries using the corresponding icons adjacent to each entry.

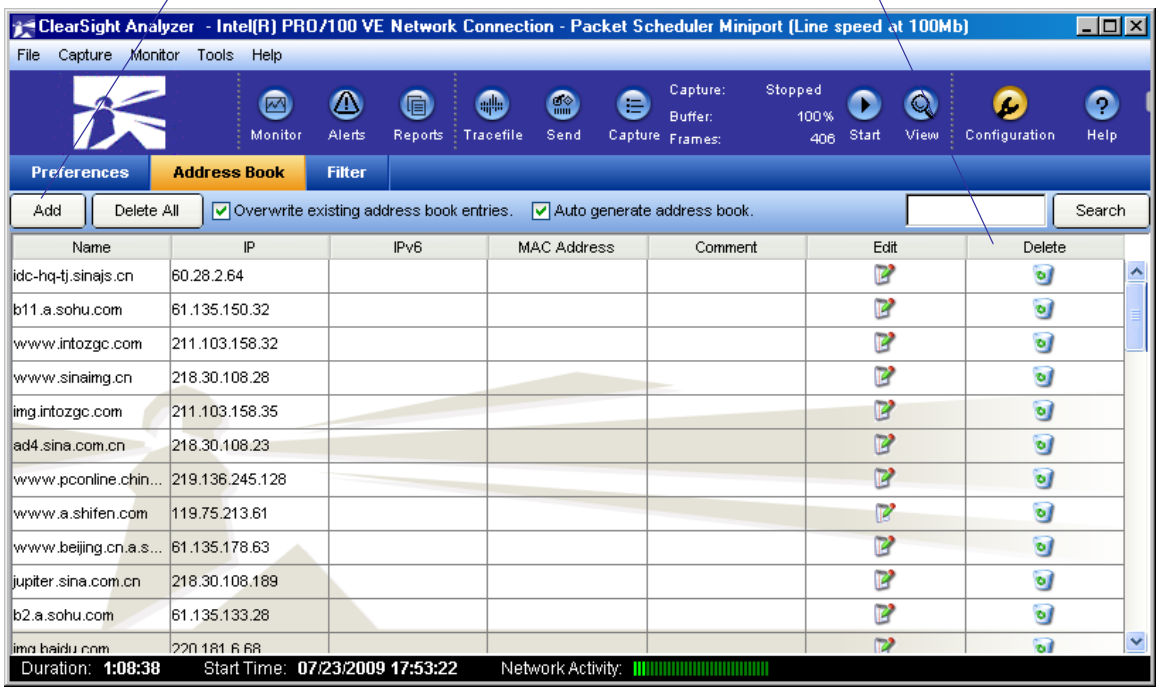


Figure 11-1: The Address Book

Clicking the Add button brings up the Host dialog box (Figure 11-2).

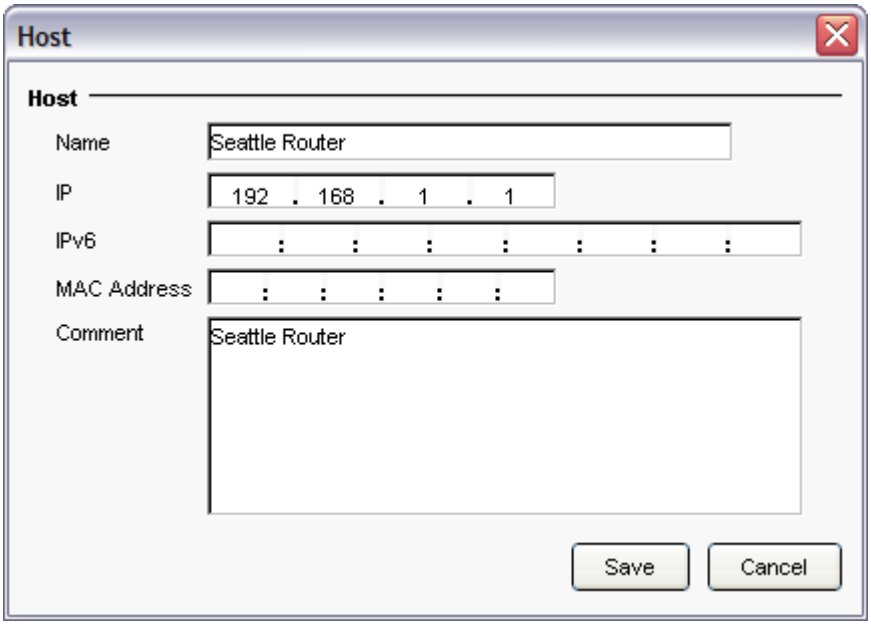


Figure 11-2: Adding a New Address Book Entry

You can add names to substitute for IP, IPv6, and MAC addresses on your network. The names you enter here will be substituted for the corresponding addresses in the **Decode** tab in ClearSight's postcapture analysis workspace.

Enabling Automatic Address Book Entries

To enable address book entries to be generated automatically as ClearSight discovers them, simply check the **Auto generate address book** check box (see Figure 11-1 on page 364).

If you also check **Overwrite existing address book entries**, a newly discovered address will automatically overwrite an existing address book entry that has the same Name or IP address.

Chapter 12

Using Reports

This chapter describes how to use ClearSight's integrated reports for network data. The chapter includes the following major topics:

- *About Reports*
- *Using Application Reports*
- *Using Network Reports*
- *Using DLC Reports*
- *Creating a User-Defined Report*
- *Using the History Reporter*

About Reports

ClearSight provides a wide variety of reports charting various network statistics, including:

- Most frequently accessed servers for a wide variety of applications.
- Jitter analysis and packet loss statistics for VoIP applications.
- Most active IP connections, and hosts by frames and bytes.

- Most active DLC nodes by frames and bytes.
- Most active VLANs by frames and bytes.
- Numerous VoIP performance reports.
- History Reports showing network statistics for previously monitored traffic.

NOTE: You must have the **History Reporter** option on your ClearSight Analyzer in order to generate the History Reports. See *Using the History Reporter* on page 391.

ClearSight provides both *real-time reports* and *postcapture reports*.

- Real-time reports are based on the data ClearSight has seen during the current monitoring session. You can display real-time reports by clicking the **Reports** button in the ClearSight toolbar, and then clicking the **Real Time** tab. In response, the Real-time Report workspace appears, providing you with access to numerous types of real-time reports.
- Postcapture reports are based on the data in the current capture buffer or trace file. You can display postcapture reports by clicking the **Tracefile** button in the ClearSight toolbar**,** and then clicking the **Report** tab. In response, the Postcapture Report workspace appears, providing you with access to numerous types of postcapture reports.

  NOTE: The postcapture reports are exactly the same as those available during real-time monitoring, except that the real-time reports include a Utilization Distribution report (see page 388).

Generating Reports in Windows XP

If you are using Windows XP and have not disabled the Windows Firewall, you will see the dialog box shown in Figure 12-1 when you click the **Reports** button for the first time after installing ClearSight.

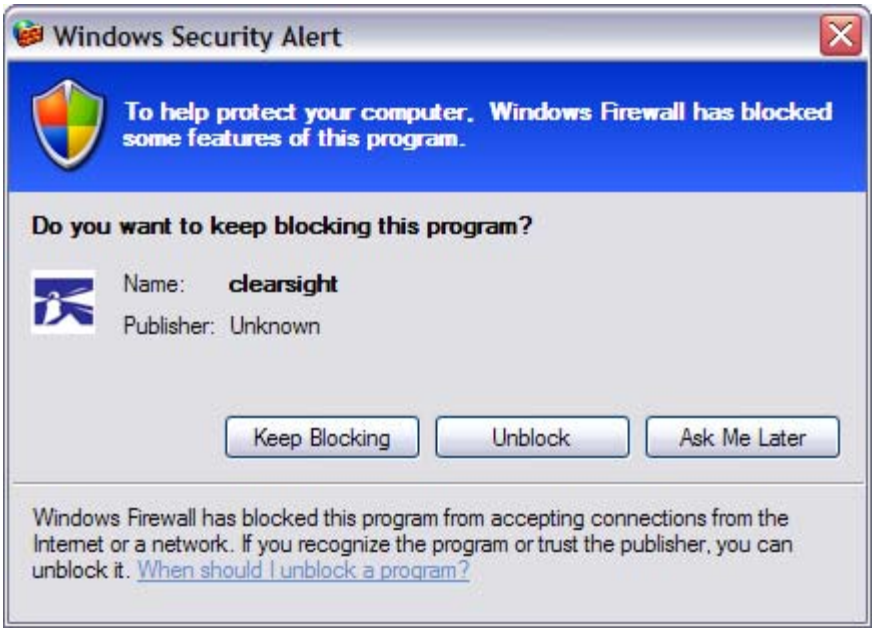


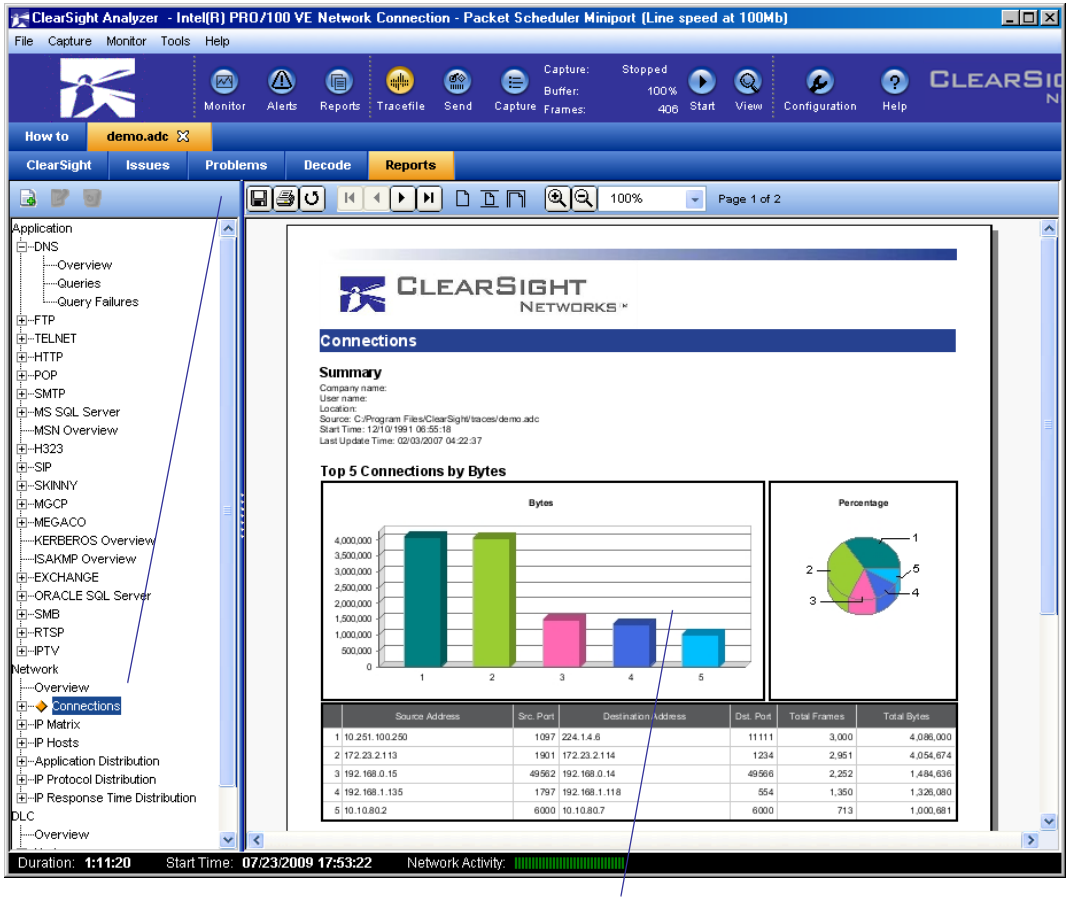
Figure 12-1: The Windows Security Alert Dialog Box in Windows XP

Simply click **Unblock** to enable the reports.

The Report Workspace

Figure 12-2 shows a typical report workspace, in this case showing a Network Connections report based on a trace file.

The **Report** menu at the left of the workspace gives you access to the individual reports available. Click an entry to see the corresponding report. In this example, the Network Connections Report is selected.



Most reports provide at least a single chart illustrating the selected statistic, followed by a table presenting the same information in tabular format.

Figure 12-2: The Report Workspace

Once a report has displayed in the Report Workspace, you can view, save, or print the report using the controls in the right hand pane just above the report. You can save the report in html, pdf, or rtf format.

You can make some choices as to the format of these reports by going to **Configuration > Preferences > Report > Settings**, as shown in Figure 12-6.

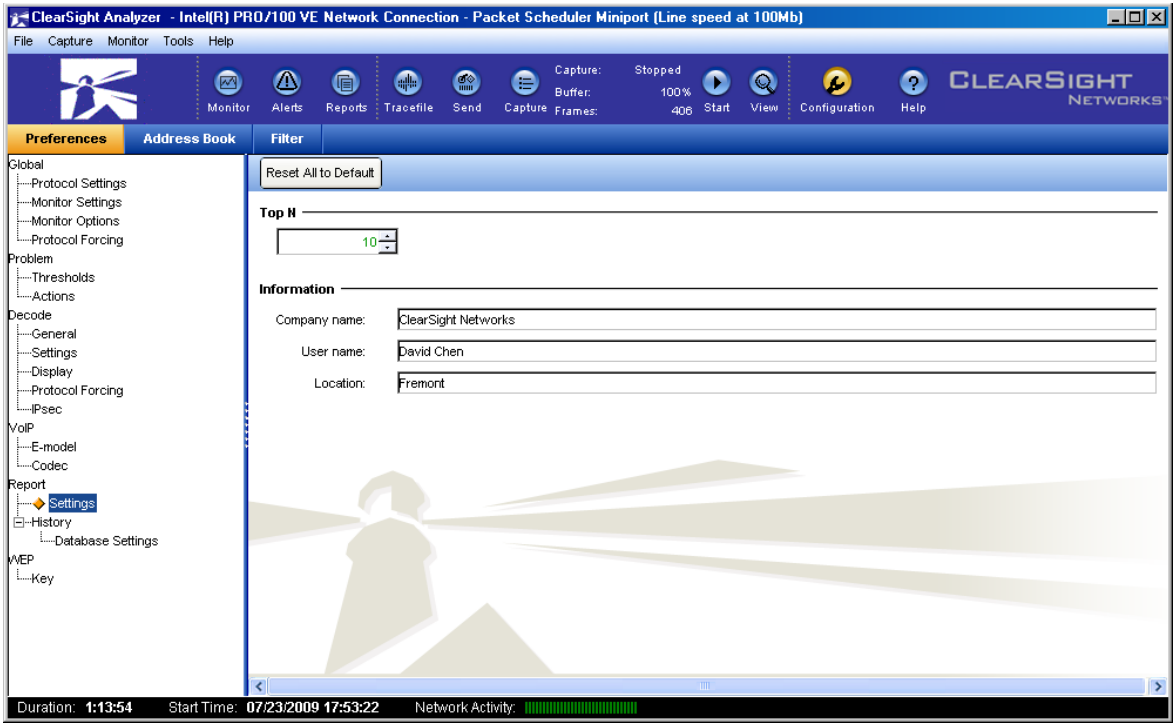


Figure 12-3: Controlling the Report Format

The **Top N** setting lets you choose how many objects are shown on the bar graphs in a report —for example, if you select **Top N** equal to 10, an HTTP Hits report will show a bar graph of the top 10 web sites, ranked according to the number of hits. You can choose **Top N** values of 5, 10, 15, or 20.

The **Information** section lets you enter identifying information that will be displayed in a **Summary** section at the beginning of the report.

Using Application Reports

ClearSight provides reports for a wide variety of applications. All applications include an **Overview** report showing traffic statistics for the selected application type. However, some applications have additional reports. The available reports are described below by application. Most of the reports are constructed similarly to the example shown in Figure 12-2 on page 370.

- *DNS Reports* on page 373
- *FTP Reports* on page 374
- *Telnet Reports* on page 374
- *HTTP Reports* on page 375
- *POP Reports* on page 376
- *SMTP Reports* on page 377
- *MS SQL Server Reports* on page 377
- *Oracle SQL Server Reports* on page 378
- *VoIP Reports* on page 380
- *IPTV Quality Reports* on page 382
- *Kerberos Reports* on page 382
- *ISAKMP Reports* on page 382
- *Exchange Reports* on page 383
- *MSN Reports* on page 383
- *SMB Reports* on page 384
- *RTSP Reports* on page 384

DNS Reports

ClearSight provides the following reports for DNS application flows:

DNS Overview	This report provides DNS traffic statistics, including number of servers, total frames, total bytes, average throughput, number of queries, and number of query failures.
DNS Top N Queries	This report provides a bar chart showing the number of DNS queries for each of the Top N lookups. In addition, a table breaks out details for each bar, showing the requested hostname, the associated IP address, the server used to perform the lookup, the number of queries and failures, and the type of lookup.
DNS Top N Query Failures	This report provides a bar chart showing the number of DNS query failures for each of the N DNS lookups having the highest number of query failures. In addition, a table breaks out details for each bar, showing the requested address, the DNS server reporting the failed lookup, the number of queries and failures, and the type of lookup.

FTP Reports

ClearSight provides the following reports for FTP application flows:

FTP Overview	This report provides FTP traffic statistics, including number of servers, total frames, total bytes, average throughput, downloaded files, downloaded frames, downloaded bytes, uploaded files, uploaded frames, and uploaded bytes.
FTP Top N Download Files	This report provides a bar chart showing the number of files downloaded from each of the N FTP servers having the most downloaded files. In addition, a table breaks out details for each bar.
FTP Top N Upload Files	This report provides a bar chart showing the number of files downloaded from each of the N FTP servers having the most downloaded files. In addition, a table breaks out details for each bar.

Telnet Reports

ClearSight provides the following reports for Telnet application flows:

TELNET Overview	This report provides Telnet traffic statistics, including number of servers, total frames, total bytes, average throughput, number of current sessions, number of logins, and number of login failures.

TELNET Top N Login Sessions	This report provides a bar chart the number of login sessions for each of the N TELNET servers having the most login sessions. In addition, a table breaks out details for each bar, showing the TELNET server address, number of login sessions, number of failed logins, and the number of frames and bytes transferred.
TELNET Top N Failed Logins	The **Failed Logins** report provides a bar chart the number of login sessions for each of the N TELNET servers having the most failed logins. In addition, a table breaks out details for each bar, showing the TELNET server address, number of login sessions, number of failed logins, and the number of frames and bytes transferred

HTTP Reports

ClearSight provides the following reports for HTTP application flows:

HTTP Overview	This report provides HTTP traffic statistics, including number of servers, total frames, total bytes, average throughput, number of hits, number of browsing pages, client errors, and server errors.

HTTP Top N Hits	This report provides a bar chart showing the N web servers receiving the most hits. In addition, a table breaks out details for each bar, showing the HTTP server address, number of hits, number of frames transferred, and the number of bytes transferred.
HTTP Top N Traffic	This report provides a bar chart showing the N web servers transferring the most bytes of traffic. In addition, a table breaks out details for each bar, showing the HTTP server address, number of hits, number of frames transferred, and the number of bytes transferred.

POP Reports

ClearSight provides the following reports for POP application flows:

POP Overview	This report provides POP traffic statistics, including number of servers, total frames, total bytes, average throughput, number of messages received, frames received, and bytes received.
POP Top N Mails Received	This report provides a bar chart showing the N POP servers from which the greatest number of messages were received. In addition, a table breaks out details for each bar, showing the POP server address, number of messages received, number of frames transferred, and the number of bytes transferred.

SMTP Reports

ClearSight provides the following reports for SMTP application flows:

SMTP Overview	This report provides SMTP traffic statistics, including number of servers, total frames, total bytes, average throughput, number of messages sent, frames sent, and bytes sent.
SMTP Top N Mails Sent	This report provides a bar chart showing the N SMTP servers to which the greatest number of messages were sent. In addition, a table breaks out details for each bar, showing the SMTP server address, number of messages sent, number of frames transferred, and the number of bytes transferred.

MS SQL Server Reports

ClearSight provides the following reports for MS SQL application flows:

MSSQL Overview	This report provides MS SQL Server traffic statistics, including number of servers, total frames, total bytes, and average throughput.
MSSQL SQL Command	This report provides a bar chart showing the relative frequency of each of ten SQL commands (Commit, Delete, Insert, and so on). The same information is presented in the table at the bottom of the report.

MSSQL Top N Avg. Transaction Time	This report provides a bar chart showing the N MS SQL servers with the highest average transaction time. Transaction time is measured as the interval between when ClearSight sees a request from an MS SQL client and when it sees the corresponding response from the server. In addition, a table breaks out details for each bar, showing the MS SQL server address, average transaction time, average TCP connection time, and average first byte download time.

Oracle SQL Server Reports

ClearSight provides the following reports for Oracle SQL application flows:

ORACLE Overview	This report provides Oracle SQL server traffic statistics, including number of servers, total frames, total bytes, and average throughput.
ORACLE SQL Command	This report provides a bar chart showing the relative frequency of each of ten SQL commands (Commit, Delete, Insert, and so on). The same information is presented in the table at the bottom of the report.

ORACLE Top N Avg. Transaction Time

This report provides a bar chart showing the N ORACLE SQL servers with the highest average transaction time. Transaction time is measured as the interval between when ClearSight sees a request from an MS SQL client and when it sees the corresponding response from the server.

In addition, a table breaks out details for each bar, showing the MS SQL server address, average transaction time, average TCP connection time, and average first byte download time.

VoIP Reports

ClearSight provides the following reports for VoIP application flows:

VoIP Overview	This report provides VoIP traffic statistics, including number of servers, total frames, total bytes, and average throughput. It also provides signaling and error statistics that vary as a function of the particular VoIP protocol (H.323, SIP, Skinny, MGCP, and Megaco)
VoIP Call Status	This report provides a bar chart and a pie chart showing the number of instances observed for each possible call status. The same information is presented in the table at the bottom of the report.
VoIP Call Distribution	This report provides a bar chart and a pie chart showing the number of calls and the corresponding total duration observed for each possible call type. The same information is presented in the table at the bottom of the report.
VoIP Top N Callers	This report provides a bar chart and a pie chart showing the number of calls and the corresponding total duration observed for each of the top N callers. The same information is presented in the table at the bottom of the report.

VoIP MOS Reports

These reports provide:

- 0 (PCMU) Call Quality Overview: A table showing the number of calls, the average Mean Opinion Score (MOS), and the overall call quality on a scale of 1 to 3. The quality rating relates to the Mean Opinion Score as follows:

Quality Rating	MOS Range
1 (Good)	MOS > 4.34
2 (Acceptable)	3.60 < MOS ≤ 4.34
3 (Poor)	MOS ≤ 3.60

- 0 (PCMU) Call Quality Distribution: a bar chart and a pie chart showing the number of calls having each of the 3 possible quality values. The same information is presented in the table at the bottom of the report.
- Factors Affecting Call Quality based on 0 (PCMU): a bar chart and a pie chart showing the relative importance of four factors (delay, jitter, lost data, and codec) as they contribute to the degradation of call quality. The same information is presented in the table at the bottom of the report.

Additional VoIP Reports are available at the flow level in the application detail displays. See *Viewing VoIP QoS Reports* on page 153.

IPTV Quality Reports

ClearSight provides the following reports for IPTV application flows:

Video Quality Overview	This report provides IPTV traffic statistics, including number of video streams, and average values for MDI DF, MDI MLR, VQFactor, and Quality Rating.
Video Quality Distribution	This report provides a bar chart and a pie chart showing the percentages of IPTV streams that fall into each of the five Quality Rating values.

Kerberos Reports

ClearSight provides the following report for Kerberos application flows:

KERBEROS Overview	This report provides Kerberos traffic statistics, including number of servers, total frames, total bytes, average throughput, number of ticket granting tickets, service principal names, AS exchange count, TGS exchange count, CS exchange count, and errors.

ISAKMP Reports

ClearSight provides the following report for ISAKMP application flows:

ISAKMP Overview	This report provides ISAKMP traffic statistics, including number of servers, total frames, total bytes, average throughput, number of sessions, successes, Phase 1 successes, Phase 1 failures, Phase 2 negotiations, quick modes, and quick mode successes.

Exchange Reports

ClearSight provides the following reports for Exchange application flows:

Exchange Overview This report provides Exchange traffic statistics, including number of servers, total frames, total bytes, average throughput, number of messages, mail frames, mail bytes, and faults.

Exchange Top N Mail This report provides a bar chart showing the N Exchange servers handling the greatest number of messages. In addition, a table breaks out details for each bar, showing the Exchange server address, number of messages handled, number of frames transferred, and the number of bytes transferred.

MSN Reports

ClearSight provides the following report for MSN application flows:

MSN Overview This report provides MSN traffic statistics, including number of servers, total frames, total bytes, average throughput, client and server average response times, logins, and failed logins. It also shows the number of file transfers, voice conversations, video conversations, IM (instant messaging) conversations, and the associated number of bytes transferred.

SMB Reports

ClearSight provides the following reports for SMB application flows:

SMB Overview	This report provides SMB traffic statistics, including number of servers, total frames, total bytes, average throughput, number of sessions requests, file requests, directory requests, DFS operations, and MISC operations.
SMB Requests	This report provides a bar chart showing the relative frequency of each of five SMB requests. The same information is presented in the table at the bottom of the report.
SMB Errors	This report provides a bar chart showing the relative frequency of each of nine SMB errors. The same information is presented in the table at the bottom of the report.

RTSP Reports

ClearSight provides the following reports for RTSP application flows:

RTSP Overview	This report provides RTSP traffic statistics, including number of servers, total frames, total bytes, average throughput, total number of methods used, and total number of client errors.
RTSP Method Distribution	This report provides a bar chart showing the relative frequency of each RTSP method used. The same information is presented in the table at the bottom of the report.

RTSP Client Errors Distribution	This report provides a bar chart showing the relative frequency of each RTSP client error type observed. The same information is presented in the table at the bottom of the report.

Using Network Reports

ClearSight provides reports for network layer flows, connections, and hosts. The available reports are described below. Most of the reports are constructed similarly to the example shown in Figure 12-2 on page 370.

- *Network Overview Reports* on page 386
- *Connections Reports* on page 386
- *IP Matrix Reports* on page 386
- *IP Hosts Reports* on page 387
- *Application Distribution Reports* on page 387
- *IP Protocol Distribution Reports* on page 387
- *IP Response Time Distribution Reports* on page 387

Network Overview Reports

A **Network Overview** report contains statistics for all observed IPv4 and IPv6 traffic. This report provides counts for a wide variety of IP frame types. You can see the composition of your IP traffic at a glance — how much is multicast, how much is broadcast, how much uses TCP and how much uses UDP, and so on.

Connections Reports

A **Connections** report tracks the top N most active connections on the network by both **Bytes** and **Frames**. Flows are shown in bar chart and pie chart form, as well as in a table. The table lists the source and destination IP addresses and ports, as well as total frames and bytes counters for the flow as a whole.

IP Matrix Reports

An **IP Matrix** report tracks the top N most active IP connections on the network by both **Bytes** and **Frames**. Connections are shown in bar chart and pie chart form, as well as in a table. The table lists the

source and destination IP addresses, as well as total frames and bytes counters for the connection as a whole.

NOTE: In contrast to **IP Flows** reports, the **IP Matrix** reports are concerned with total traffic between two addresses rather than total traffic between two addresses on a specific pair of ports.

IP Hosts Reports

An **IP Hosts** report tracks the top N most active IP hosts on the network by both **Bytes** and **Frames**. Hosts are shown in bar chart and pie chart form, as well as in a table. The table lists each host with total frames and bytes counters.

Application Distribution Reports

An **Application Distribution** report breaks down traffic into common application protocols by both **Bytes** and **Frames**. Application protocol composition is shown in bar chart and pie chart form, as well as in a table. The table lists protocols in order of usage with both total frames and bytes counters.

IP Protocol Distribution Reports

An **IP Protocol Distribution** report breaks down traffic into common transport layer protocols (UDP, TCP, ICMP, and so on) by both **Bytes** and **Frames**. Transport layer protocol composition is shown in bar chart and pie chart form, as well as in a table. The table lists protocols in order of usage with both total frames and bytes counters.

IP Response Time Distribution Reports

An **IP Response Time Distribution** report shows the number of responses that fell into each of ten different time windows. Responses are listed from quickest (0-25 µs) to slowest (over 2000 µs). The table at the bottom of the report tallies the exact number of responses in each response time window.

Using DLC Reports

ClearSight provides reports for physical layer nodes, VLANs, and general traffic statistics. The available reports are described below.

- *DLC Overview Reports* on page 388
- *Nodes Reports* on page 388
- *VLAN Reports* on page 388
- *Utilization Distribution Reports* on page 388

DLC Overview Reports

A **DLC Overview** report contains statistics for all observed traffic. The report includes counts for utilization, total bytes, total frames, multicast frames, broadcast frames, and various types of frame errors.

Nodes Reports

A **Nodes** report shows the top N most active DLC layer nodes on the network by both **Bytes** and **Frames**. Nodes are shown in both a bar chart and a table. The table lists each node by address along with total frames and bytes counters.

VLAN Reports

A **VLAN** report shows the top N most active VLANs on the network by both **Bytes** and **Frames**. VLANs are shown in both a bar chart and a table. The table lists each VLAN by VLAN ID along with total frames and byte counters.

Utilization Distribution Reports

ClearSight measures network utilization over each second as a percentage of available network bandwidth. The value for each one-second sample is sorted into one of ten possible utilization ranges (for example, 20 - 30% utilization). The occurrences are

counted and displayed in the **Utilization Distribution** report, as both a bar chart and a pie chart. The table at the bottom of the report tallies the exact number of occurrences within each percentage utilization window.

Creating a User-Defined Report

You can create composite reports consisting of any combination of the predefined reports listed in the Report Workspace.

To create a user-defined report, click on the **Create new user-defined report** button at the upper left. The Create User-Defined Report dialog box (Figure 12-4) appears.

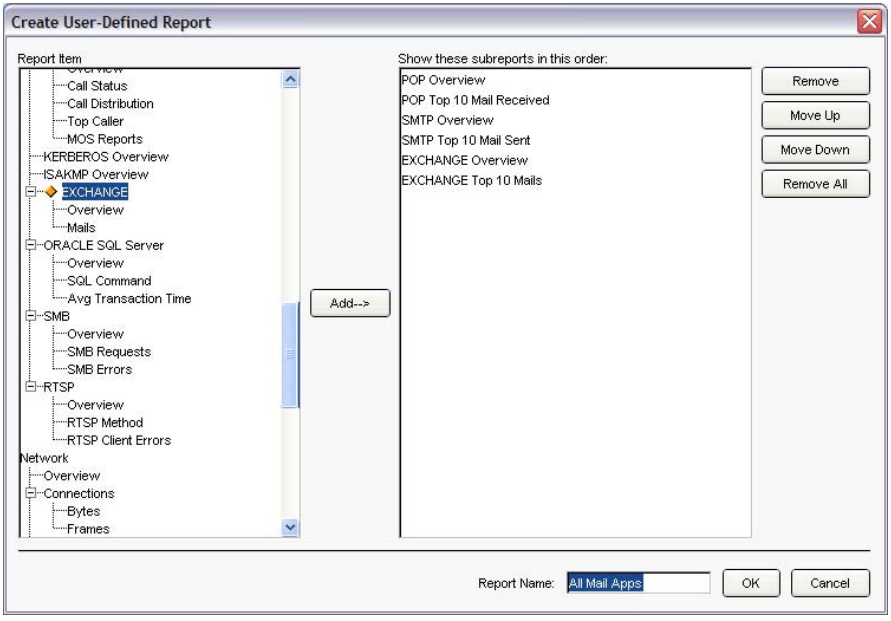


Figure 12-4: The User-Defined Report Dialog Box

The example shown in Figure 12-4 creates a composite report (AllMailApps) showing all available reports for the three mail applications — POP, SMTP, and Exchange — in a single document.

When you click OK, the new user-defined report will be added to the list at the bottom of the Report workspace, as shown in Figure 12-5.

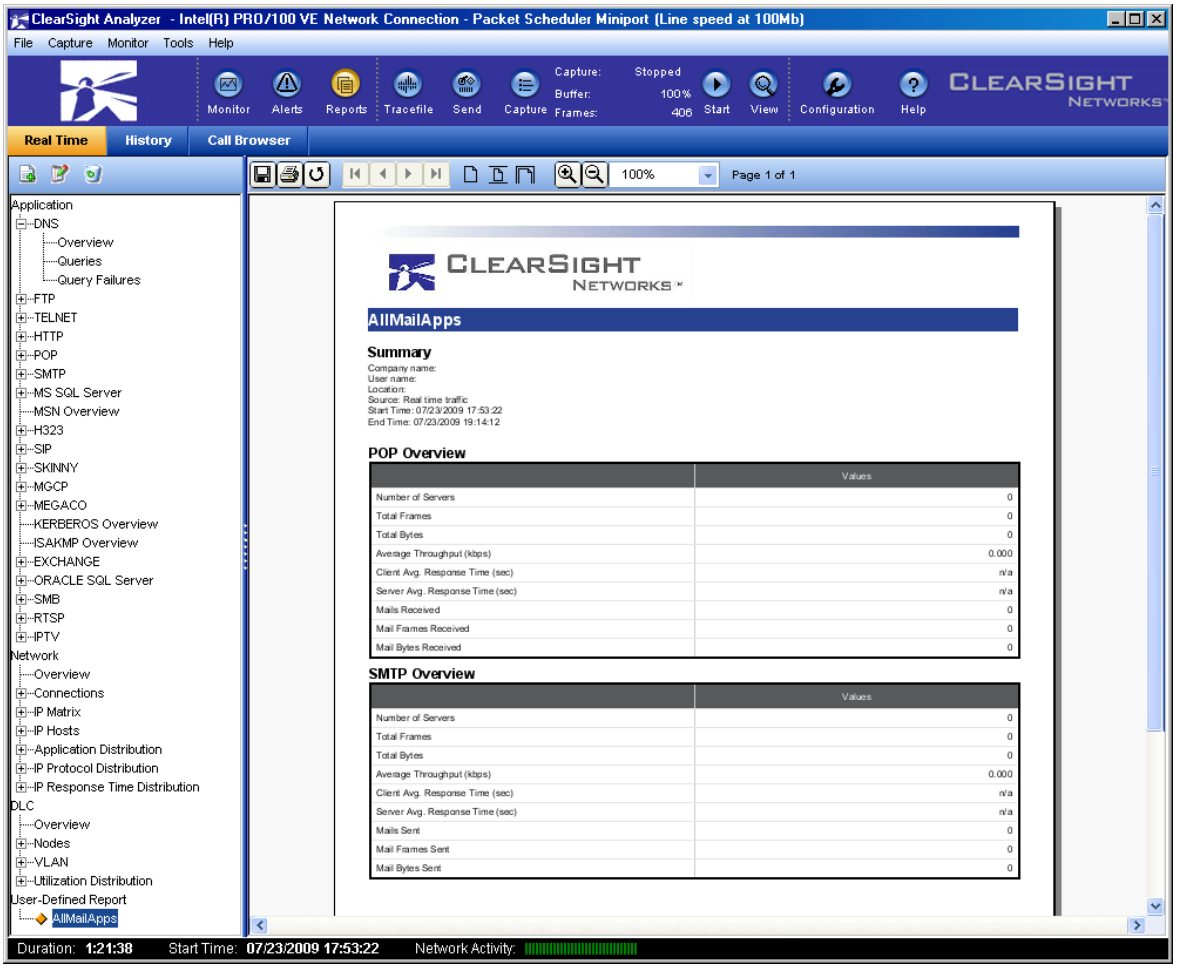


Figure 12-5: A User-Defined Report

You can edit the composition of an existing user-defined report by selecting it in the Report Workspace, and then clicking on the **Edit selected user-defined report** button.

You can delete an existing user-defined report by selecting it in the Report Workspace, and then clicking on the **Delete selected user-defined report** button.

Using the History Reporter

The **History Reporter** is an optional feature that you can add to your ClearSight Analyzer. When this feature is present, you can periodically save application, network, and DLC layer statistics as you monitor traffic on your network. These statistics are saved in CSV files and accumulated in databases that you can access later. There is a separate database for each network adapter.

You can generate reports based on the information in these databases. You can make some choices as to the format of these reports by going to **Configuration > Preferences > Report > Settings**, as shown in Figure 12-6.

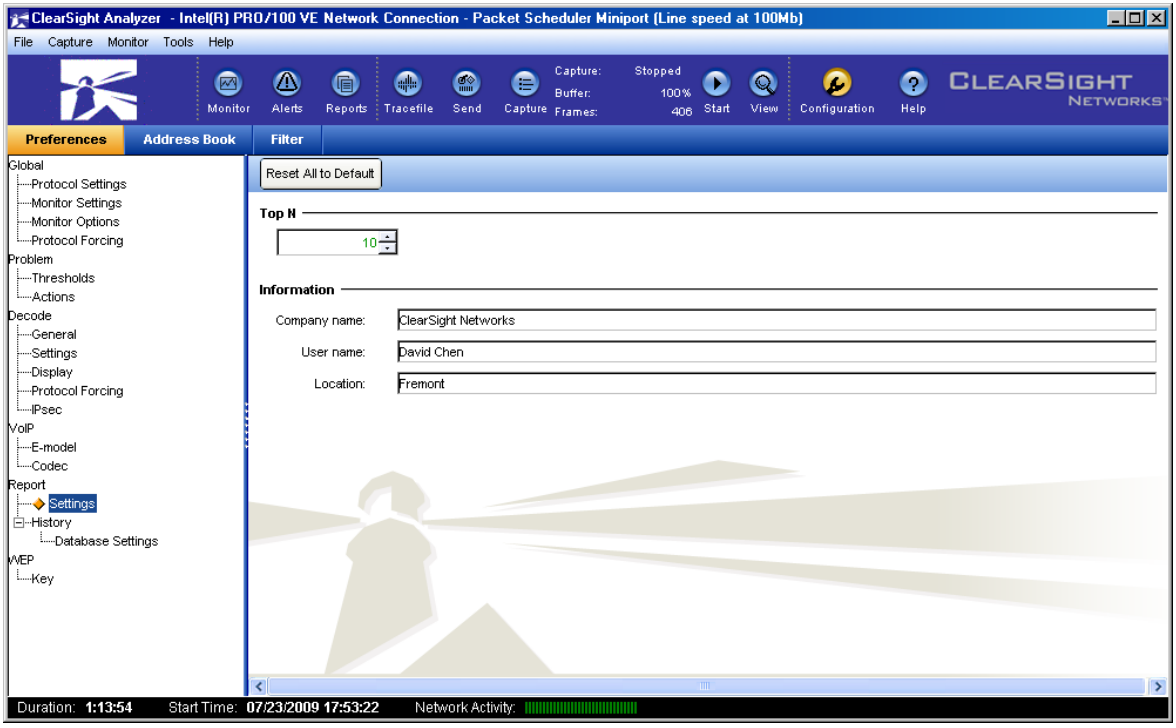


Figure 12-6: Controlling the Report Format

The **Top N** setting lets you choose how many objects are shown on the bar graphs in a report —for example, if you select **Top N** equal to 10, an HTTP Hits report will show a bar graph of the top 10 web sites,

ranked according to the number of hits. You can choose **Top N** values of 5, 10, 15, or 20.

The **Information** section lets you enter identifying information that will be displayed in a **Summary** section at the beginning of the report.

NOTE: The **Report > Settings** screen is not unique to History Reports. It affects all of the reports discussed in this chapter.

Controlling the Accumulation of Data

You can specify what data will be accumulated for the History reports by selecting **Configuration > Preferences > Report > History > Database Settings**. This takes you to the History Reporter's Database Settings screen, shown in Figure 12-7.

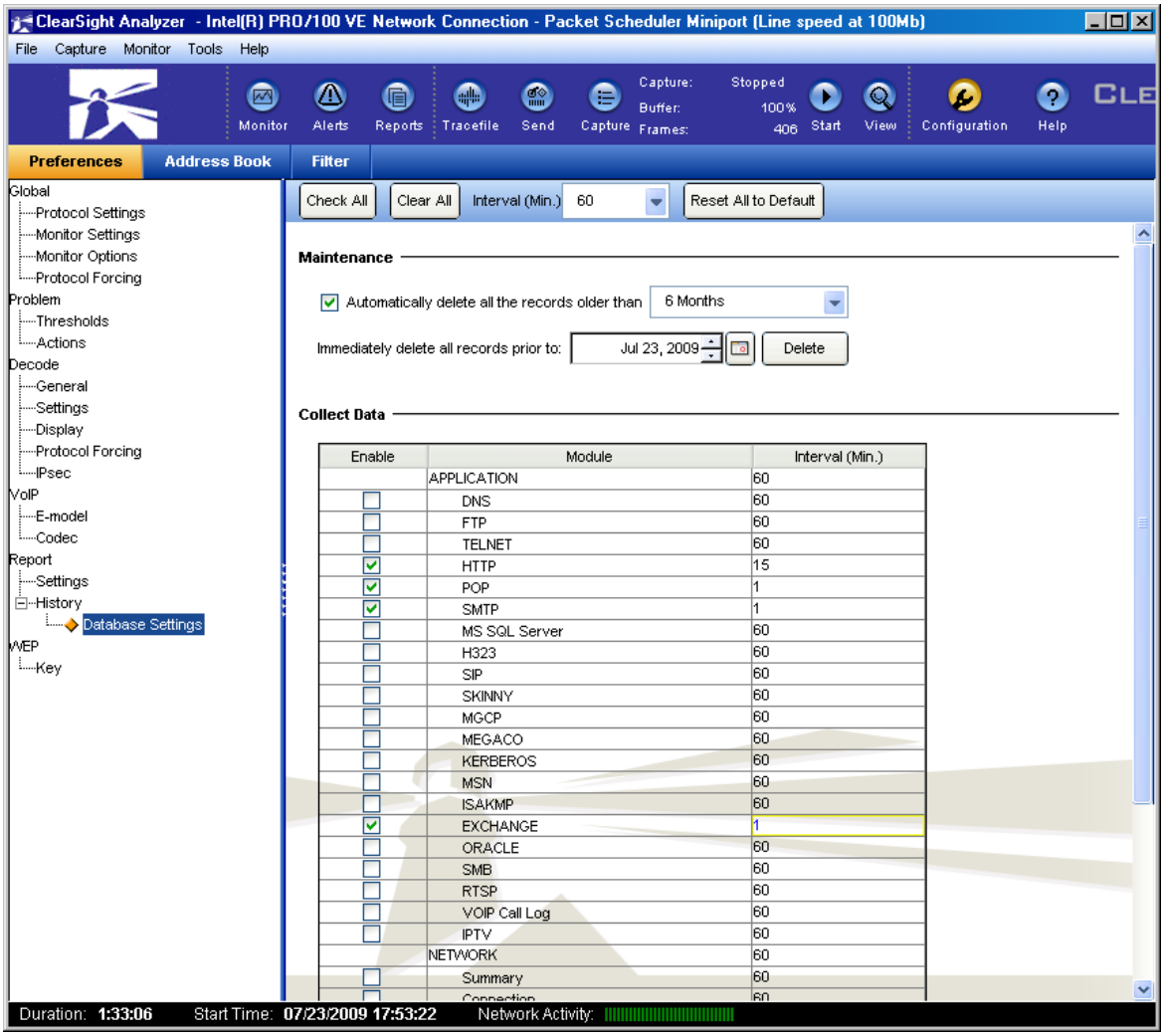


Figure 12-7: Database Settings for the History Reporter

The **Maintenance** section at the top of the screen lets you control the size of the database by deleting records that you no longer need. You can set this control to automatically delete records that are older than the selected age — possible selections range from 1 month to 2 years. In addition, you can immediately delete all of the records prior to a given date, which you can select using the calendar tool provided.

NOTE: The **Immediately delete** function will affect only the database for the current network adapter. All the other functions on this screen will affect the databases for all network adapters.

The **Collect Data** section lets you choose the particular application, network, and DLC layer statistics that you want to save into the databases. The **Enable** column contains checkboxes for making these selections. To save time, you can also use the **Check All**, **Clear All**, and **Reset all to default** buttons at the top.

For each selected set of statistics, the corresponding data will be saved in a CSV file. You can then use the **Interval** column to specify how often the data in the CSV file should be saved to the database. For example, if you check **HTTP** and set **Interval** to 15 minutes, then every 15 minutes the data currently in the CSV file for HTTP will be saved in the database, and deleted from the CSV file.

Creating a History Report

You can create reports based on the information in the database. To do this go to **Reports > History** and select the report you want to create. As shown in Figure 12-9, the selection is made in the left pane, and the report appears in the right pane.

You can select the time interval for which the report will display data by clicking on the  button. This brings up the Report Time Configuration dialog box, shown in Figure 12-8.

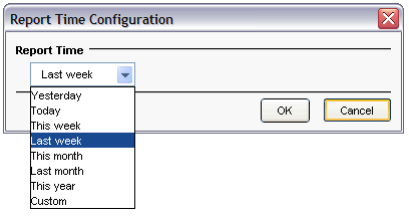


Figure 12-8: Report Time Configuration Dialog Box

Select the time interval you want (or create a **Custom** time interval) and click **OK**. The report then appears, as shown in Figure 12-9.

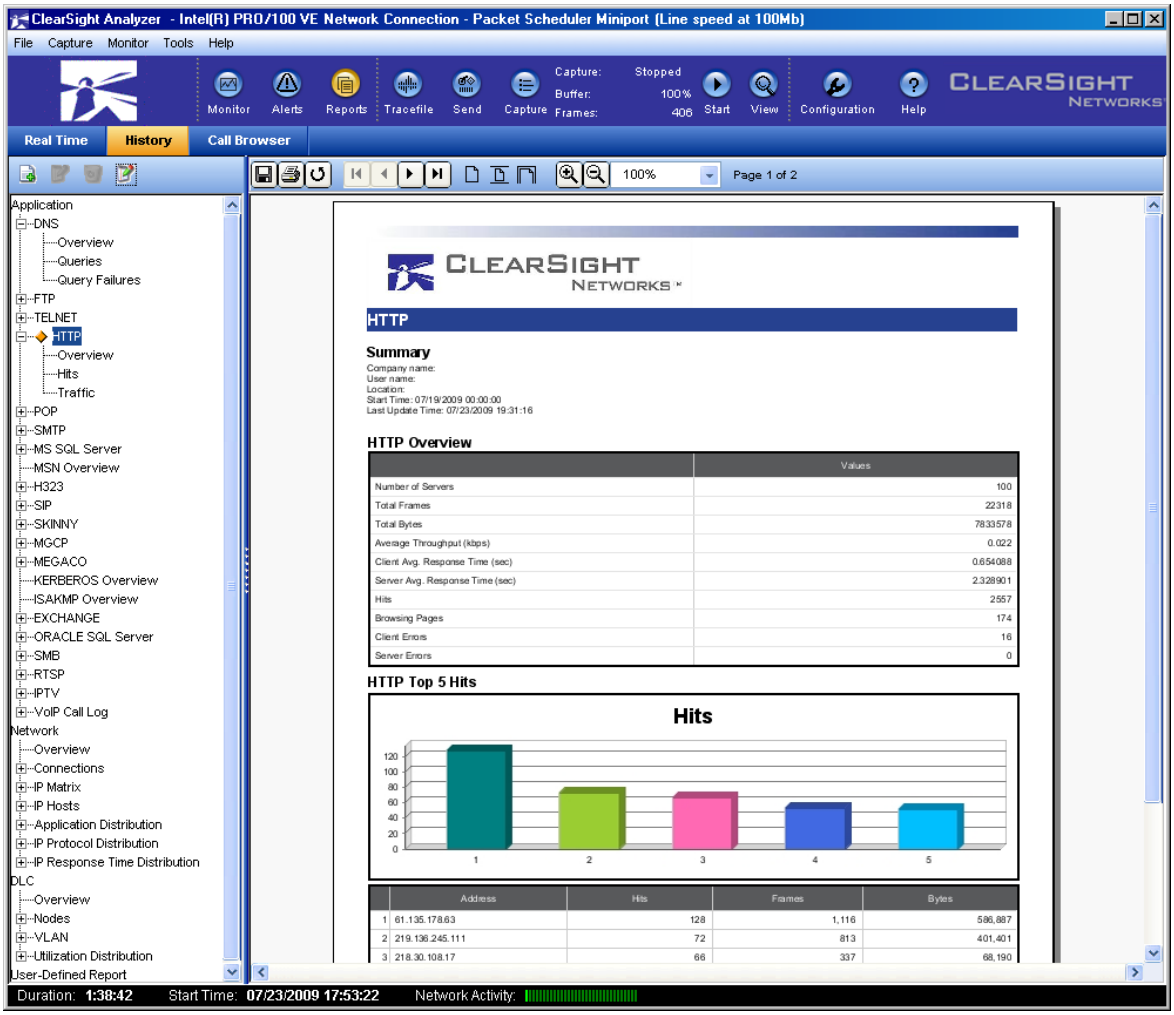


Figure 12-9: Example of an HTTP History Report

You can view, save, or print the report using the controls in the right hand pane just above the report. You can save the report in html, rtf, or pdf format.

Trending Charts

Within any table in the report, you can click on a specific line to generate a chart showing how that statistic varies over the time span selected for that report.

You can also generate multiple trending charts by clicking on the title of a particular table. In that case you will see a dialog box similar to the one shown in Figure 12-10.

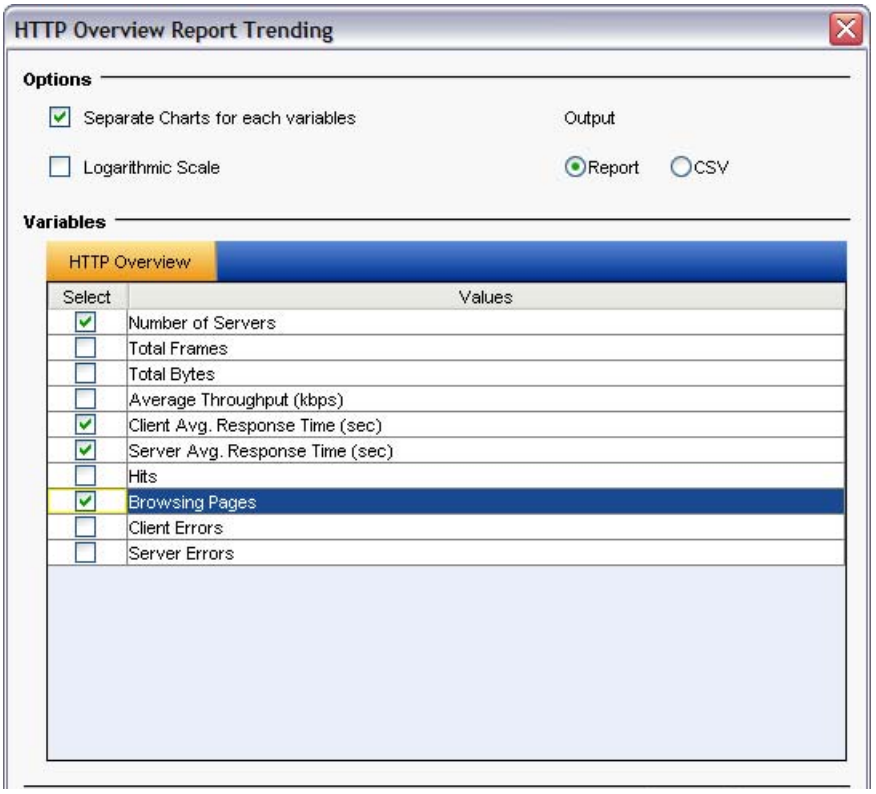


Figure 12-10: Selecting Multiple Trending Charts

In addition to selecting any combination of statistics to display, you have the option to display them as separate charts or superimposed. You can also select either linear or logarithmic scale for the vertical axis of the chart. You can choose to output the data in report format or as CSV data.

Creating a VoIP Call Log

A VoIP Call Log is a particular kind of history report that lets you see compile information about the performance of VoIP traffic on your network. Figure 12-11 shows the first of many available VoIP Call Log reports.

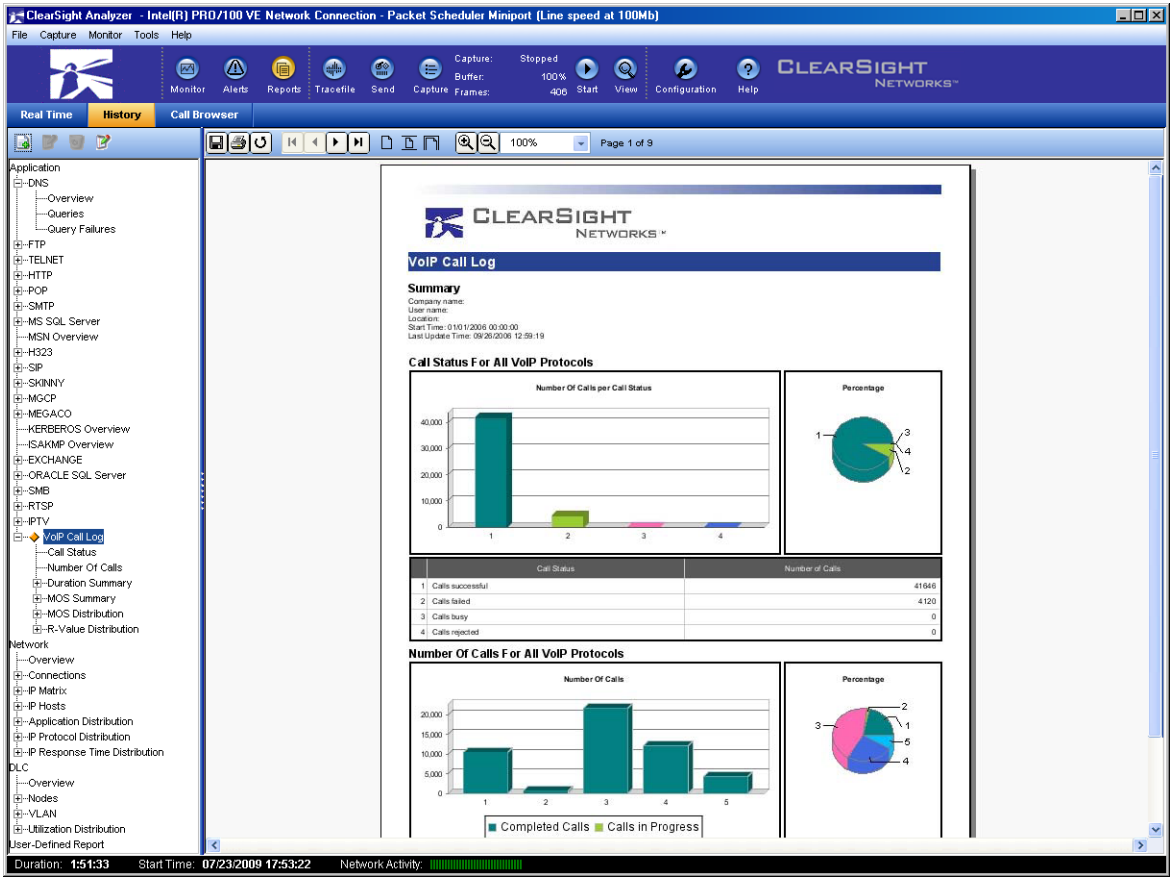


Figure 12-11: VoIP Call Log

Using the Call Browser

You can access basic information about calls on your network by using the Call Browser. Figure 12-12 shows the Call Browser screen.

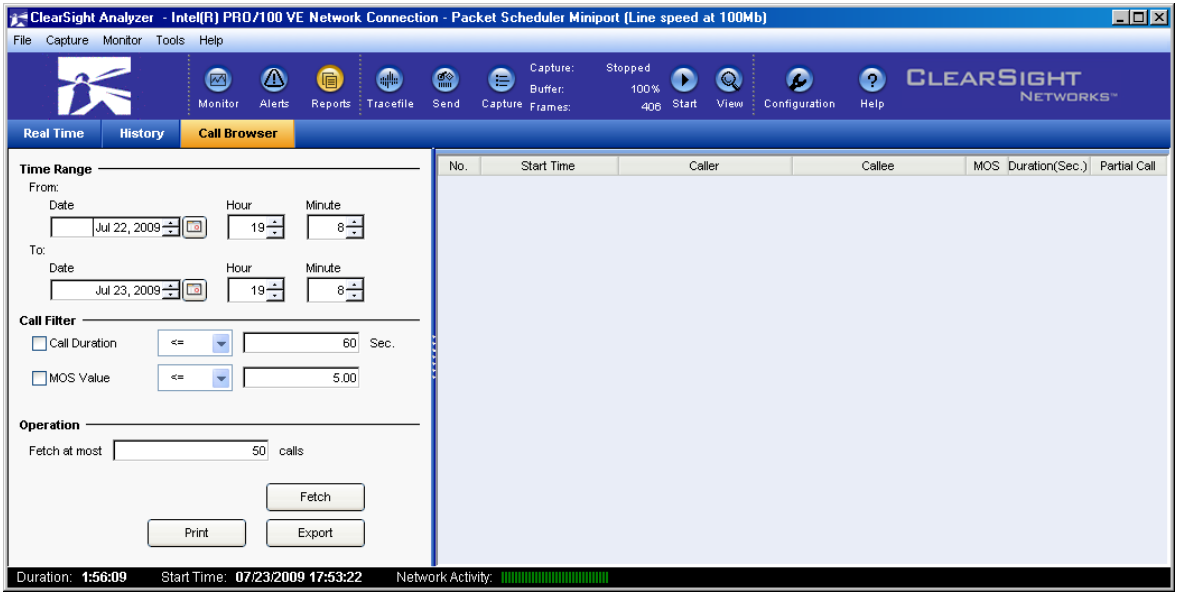


Figure 12-12: The Call Browser

As the figure shows, you can limit your investigation to a particular **Time Range**. In the **Call Filter** area you can specify criteria for **Call Duration** and **MOS Value**. You can also limit the maximum number of calls listed.

For calls that satisfy your criteria, the list will show **Start Time**, **Caller**, **Callee**, **MOS** score, and **Duration**, and indicate whether only a **Partial Call** is included.

Chapter 13

Using the Packet Generator

This chapter covers the following major topics:

- *The Packet Generator Option*
- *ClearSight Packet Generator Features*
- *Using the Packet Generator*

The Packet Generator Option

The ClearSight Packet Generator is an option that you can elect to buy when you order the ClearSight Analyzer. If you have bought this optional functionality, there will be a **Send** button on the ClearSight toolbar. Clicking the **Send** button starts the packet generator.

ClearSight Packet Generator Features

The ClearSight Packet Generator can generate network traffic based either on a single packet or on the contents of a trace file. Features of the packet generator include:

- The user can configure either a delay time (interval between packets) or utilization (percentage of network bandwidth used for packet generator traffic).
- As the packets are transmitted, the MAC addresses, IP addresses, and application port numbers can be incremented sequentially or randomized.
- The length of the packets can be randomized.
- The user can edit packet content.
- Both IPv4 and IPv6 protocols are supported.
- The user can save and replay packet generator settings.
- Scripts can be written to perform any of the functions on the graphical user interface.
- Multiple trace files can be opened and played sequentially, with delay options, changing addresses, and changing port numbers all programmable.

NOTE: The ClearSight Packet Generator does not support 10/100 Full Duplex Ethernet or Gigabit Ethernet adapters.

Using the Packet Generator

Start the packet generator by clicking the **Send** button in the toolbar.

As shown in Figure 13-1, the packet generator user interface has the following components:

- *The Statistics Table*
- *Traffic Graphs*
- *Traffic Control Buttons*
- *The Profile List*

Each of these are discussed in detail later in this chapter.

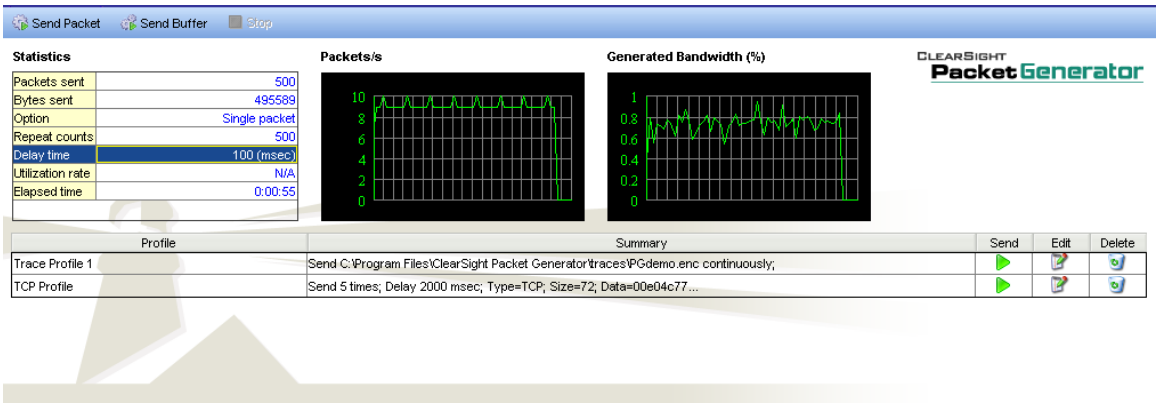


Figure 13-1: ClearSight Packet Generator User Interface

The Statistics Table

The Statistics Table shows the progress of the packet generation, and lists some of the controlling parameters. The user specifies these parameters in the Send Packet and Send Buffer dialog boxes, described later in this chapter.

The fields in the Statistics Table are as follows:

Packets sent	The number of packets sent since this packet generation session started.
Bytes sent	The number of bytes sent since this packet generation session started.
Option	Initially shows **N/A**, then **Single packet** if the **Send Packet** option has been selected, or the full path and file name of a trace file if **Send Buffer** has been selected.
Repeat counts	If the **Send Packet** option has been selected, this field shows how many packets are being sent. If the **Send Buffer** option has been selected, this field shows how many times the trace file is being sent. If you have chosen to send traffic continuously, then this field shows **Continue**.
Delay time	The gap (in milliseconds) between the end of each packet and the start of the next packet, if a delay time is specified. Otherwise this field shows **N/A**. **NOTE: Delay time** and **Utilization rate** apply to the **Send Packet** option only, and are mutually exclusive. One will show a value and the other will show **N/A**. For the **Send Buffer** option, both will show **N/A**.
Utilization rate	The percent of available network bandwidth being used by the packet generator, if a Network Utilization value is specified. Otherwise this field shows **N/A**.
Elapsed time	The time (hours:minutes:seconds) since this packet generation session started.

Traffic Graphs

The Traffic Graphs show the progress of the Packet Generation in real time. The **Packets/s** graph on the left shows the number of packets per second being sent by the packet generator; the **Generated Bandwidth** graph on the right shows the bandwidth being utilized by the packet generator, as a percent of the nominal network bandwidth.

Traffic Control Buttons

The Traffic Control Buttons function as follows:



opens the Send Packet dialog box



opens the Send Buffer dialog box.



stops the current packet generation session.

The Send Packet Dialog Box

The Send Packet dialog box (Figure 13-2) controls the **Single packet** mode of transmission. It lets you specify what type of packet is to be sent, and to set various parameters to control the transmission.

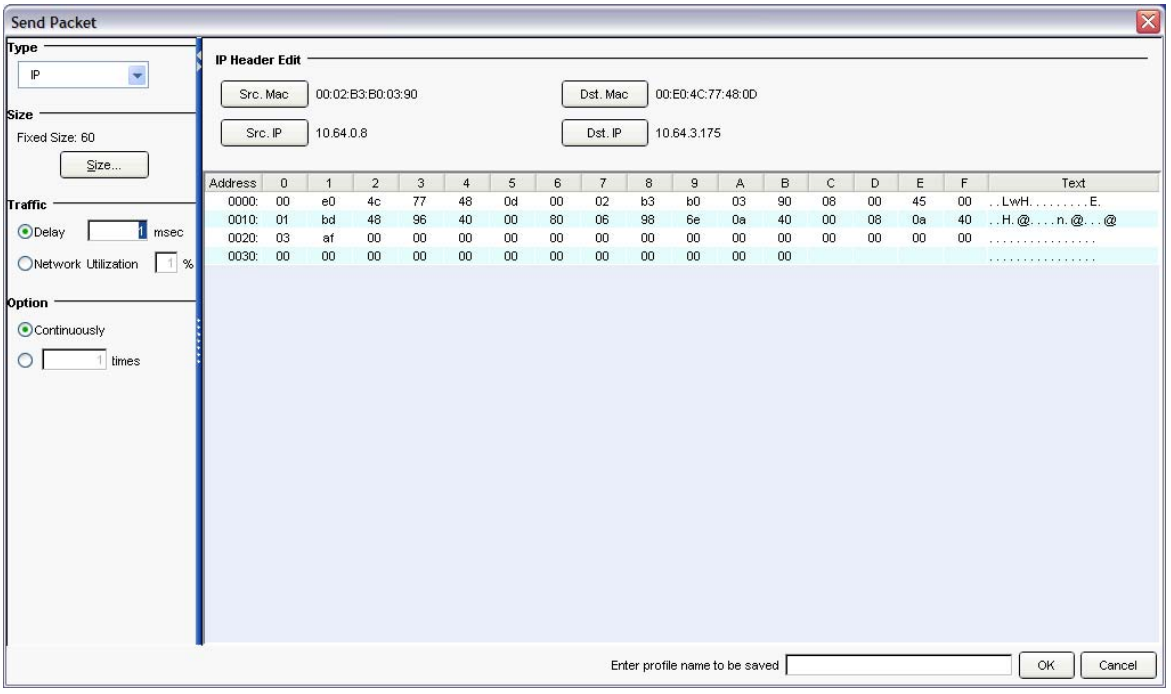


Figure 13-2: The Send Packet Dialog Box

The following paragraphs explain how to set the controls in each pane of this dialog box.

Type

The Type pane lets you choose from the following packet types: IP, TCP, UDP, ICMP, IPv6, TCPv6, UDPv6, ICMPv6, or Custom. What you select from this drop-down list affects the contents of the Size, Header Edit, and Hex Values panes.

Size

The Size pane lets you specify the size of the packets to be sent. Except for the Custom type, the default value in **Fixed size** is the smallest packet that can be sent for the specific packet type chosen. For example, for a TCP packet the default value size is 72 bytes, not including the CRC. For the Custom packet type, the default size is the most recent fixed size specified, regardless of the packet type.

When you click on the Size button, the Size dialog box (Figure 13-3) appears.

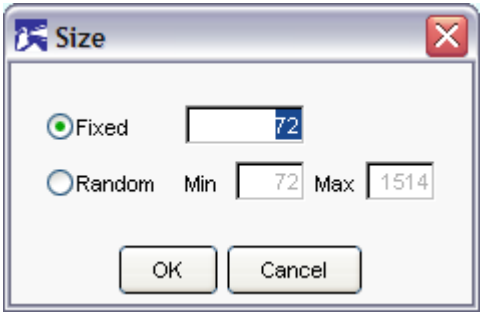


Figure 13-3: The Size Dialog Box

If you want a fixed size packet, click the **Fixed** radio button, enter the number of bytes, not including the CRC, and click **OK**. If you enter a value smaller than the minimum number of bytes for this packet type, or a value greater than 1514, you will get an error message.

If you want the packet generator to send random length packets, click the **Random** radio button, enter the minimum and maximum values you want, and click **OK**. If you enter a **Min** value smaller than the minimum number of bytes for this packet type, or a **Max** value greater than 1514, you will get an error message.

The following table shows the minimum and maximum packet sizes for the various packet types:

Packet Type	Minimum Size	Maximum Size
IP, UDP, ICMP	60 bytes	1514 bytes
TCP, IPv6, ICMPv6	72 bytes	1514 bytes
UDPv6	80 bytes	1514 bytes
TCPv6	92 bytes	1514 bytes

Traffic

The Traffic pane lets you control how frequently packets are transmitted onto your network. There are two ways you can do this:

- Click the **Delay** radio button and enter the number of milliseconds delay to be inserted between the end of each packet and the start of the next packet. The allowable range is 1 ms to 1,000,000 ms (1000 sec).
- Click the **Network Utilization** radio button and enter the percent of the available network bandwidth that you want the packet generator to use. the allowable range is 1% to 100%.

Option

The Option pane lets you control how many times the packets will be sent.

- To send the packet a defined number of times, click the **times** radio button and enter the number of repetitions you want. The allowable range is 1 to 1,000,000,000.
- If you click the **Continuously** radio button, the packet generator will send packets continuously, until you click the **Stop** button.

Header Edit

The Header Edit pane gives you an easy way to edit the source and destination MAC addresses and the source and destination IP (or IPv6) addresses of the packet(s) to be sent. In the case of TCP, UDP,

TCPv6, and UDPv6 packets, it also gives you an easy way to edit the application port numbers.

Whether you want to edit a MAC address, an IP address, or a port number, the process is the same. As an example, suppose you want to edit the source IP address in a TCP packet. Click on **Src. IP** to bring up the IPv4 Edit dialog box (Figure 13-4).

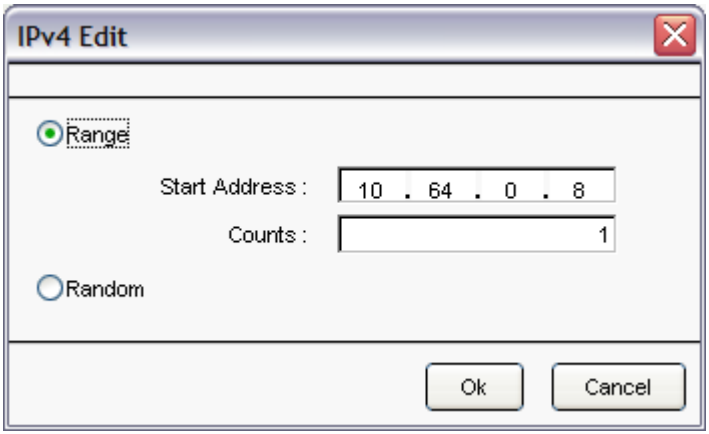


Figure 13-4: IPv4 Edit Dialog Box

If you want all the packets to have the same address, just click the **Range** button, enter that address in the **Start Address** box, and leave the **Counts** field set to **1**. Alternatively, you can have the address increment by 1 for each successive packet. In that case, enter the number of successive addresses you want to use in the **Counts** field. For example, if **Start Address** is 10.64.0.8, and **Counts** is set to 8, then the address will increment through the values 10.64.0.8, 10.64.0.9, ... 10.64.0.15. Then the address will return to 10.64.0.8 and start over. If **Counts** is set to a value high enough to increment beyond 255 in the rightmost column, then the second-from-rightmost column increments by one and the rightmost column goes to 0 and continues counting upward.

Allowable values in the **Counts** field are 1 to 65536. Allowable values in the **Start Port** field are 0 to 65536.

If you want the packet generator to use random IP addresses, click the **Random** button.

Hex Values

The hex values pane lets you edit the actual contents of the packet manually. Simply type over the hex values shown to edit the packet. Use the cursor keys to move the cursor within this array of hex values. For packet types other than Custom, the CRC will be recalculated automatically.

NOTE: If you have chosen the Custom packet type, you can feel free to edit any of these hex values. If you have chosen any of the others, you must avoid changing any of the fields that actually define that packet type. In the IP type, for example, if you change position 001D to something other than 08, it won't be an IP packet anymore.

Saving a Profile

After you have made all your edits, you can save these settings as a profile, so that you can use these settings in the future without having to make all those entries again. To save the settings, simply type a profile name (1 to 40 characters) in the **Enter profile name to be saved** box and click **OK**. for details on managing your saved profiles, see *The Profile List* on page 413.

The Send Buffer Dialog Box

The Send Buffer dialog box (Figure 13-6) controls the transmission of trace files. It lets you specify what trace file is to be sent, and to set various parameters to control the transmission.

On the way to the Send Buffer dialog box you must specify the desired trace file in the Open dialog box, as shown in Figure 13-5.

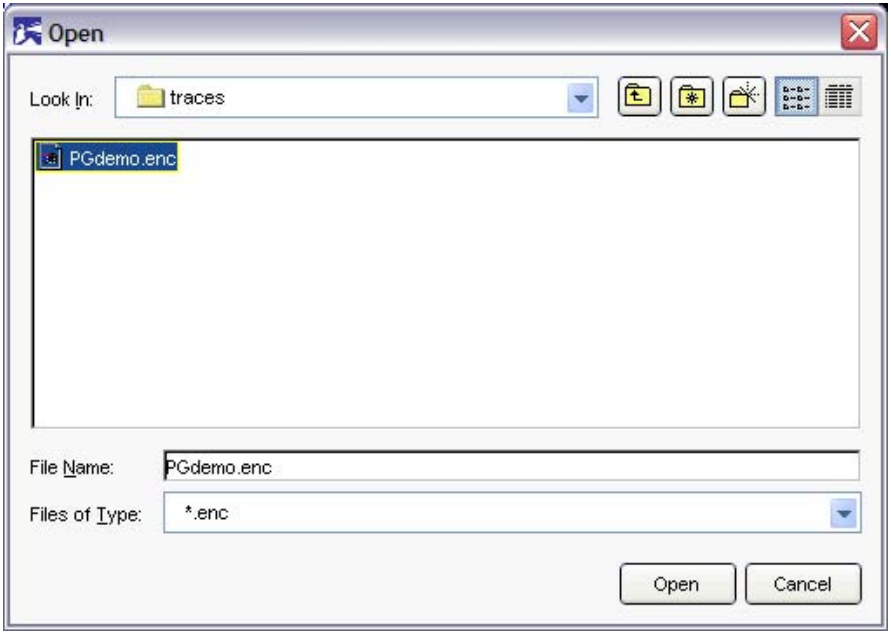


Figure 13-5: Specifying a Trace File to Send

When you click **Open**, the Send Buffer dialog box (Figure 13-6) will appear.

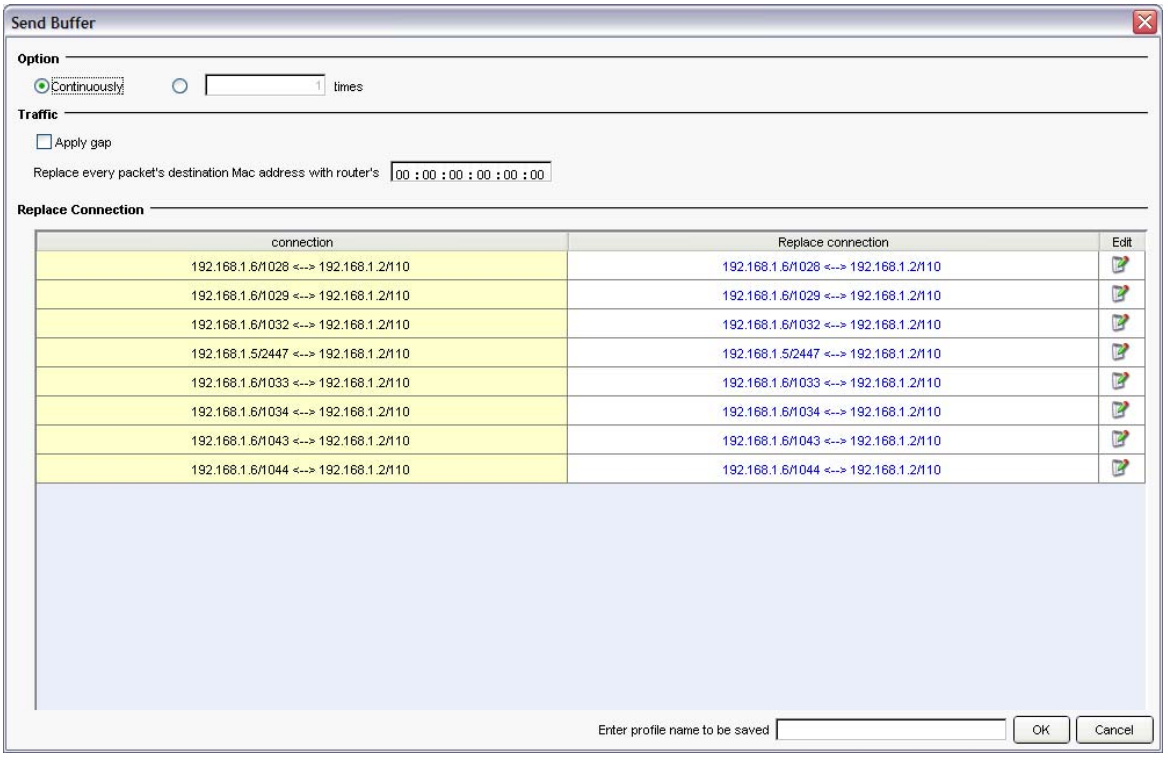


Figure 13-6: The Send Buffer Dialog Box

The following paragraphs explain how to set the controls in each pane of this dialog box.

Option

The Option pane lets you control how many times the trace file will be sent.

- To send the trace file a defined number of times, click the **times** radio button and enter the number of repetitions you want. The allowable range is 1 to 1,000,000,000.
- If you click the **Continuously** radio button, the packet generator will send trace file over and over, until you click the **Stop** button.

Traffic

The Traffic pane controls the time interval between the end of each packet and the beginning of the next packet.

- If you check the **Apply gap** box, the packet generator will attempt to reproduce the original delay time stored in the trace file. This delay time may not be reproduced exactly, because the Microsoft OS timer has a minimum granularity of 1 millisecond. Additionally, the delay time may be affected by other applications you are running concurrently. For optimum performance, close all other active programs.
- If you leave the **Apply Gap** box unchecked, the packet generator will leave a gap of about 1 millisecond between packets.

The Traffic pane also lets you specify the Mac address of a router on your local network segment. Specifying a router address lets you send packets beyond your local network segment.

If you leave this address at 00:00:00:00:00:00, the destination Mac addresses will remain unchanged.

Replace Connection

After the trace file is opened, the Replace Connection pane lists all of the known connections. You can send the packets as they are in the trace file, or with the connection addresses and ports changed. To replace these parameters for a given connection, click on the **Edit** symbol to the right of that connection. This will bring up the Replace Connection dialog box, shown in Figure 13-7.

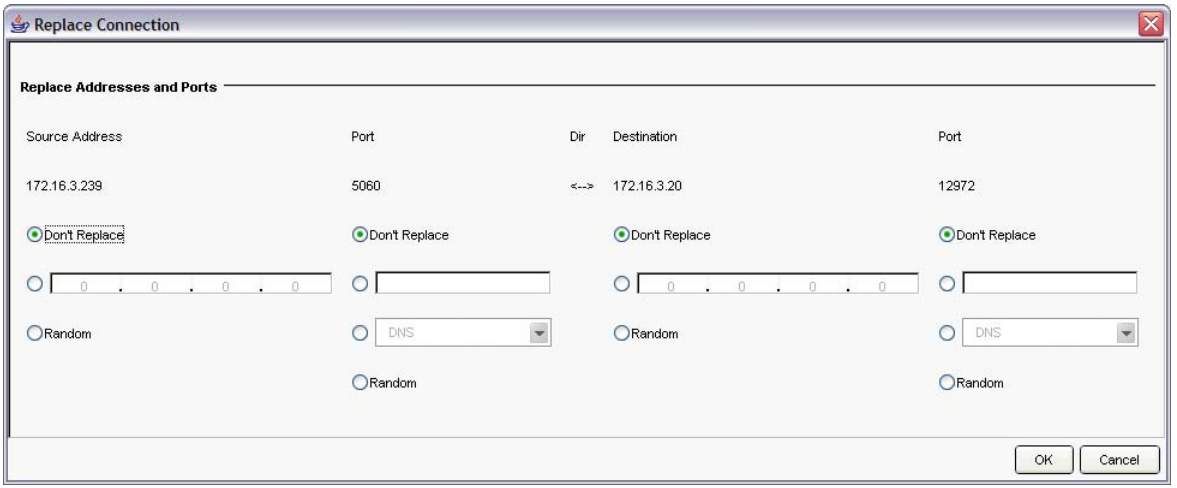


Figure 13-7: The Replace Connection Dialog Box

For each address (source or destination) you can choose not to replace it, replace it with another address that you specify, or have the packet generator use a random address.

Similarly, for each port number, you can choose not to replace it, replace it with another port number that you specify, or have the packet generator use a random port number. If you want to specify the port number, you can either type it in (0 to 65536) or choose a well-known application port number from the drop-down list.

Saving a Profile

After you have made all your edits, you can save these settings as a profile, so that you can use these settings in the future without having to make all those entries again. To save the settings, simply type a profile name (1 to 40 characters) in the **Enter profile name to be saved** box and click **OK**. for details on managing your saved profiles, see *The Profile List* on page 413.

The Profile List

The Profile List shows the profiles that have been saved. A profile is a collection of settings that have been entered via the Send Packet or Send Buffer dialog box. *Main Packet Generator Screen Showing the Profile List* shows the profile list at the bottom of the main packet generator screen.

The columns in the Profile List are as follows:

Profile	The name given to a profile.
Summary	A short list of the settings.
Send	Clicking this box sends traffic based on this profile.
Edit	Clicking this box lets you edit this profile.
Delete	Clicking this box deletes this profile from the Profile List.

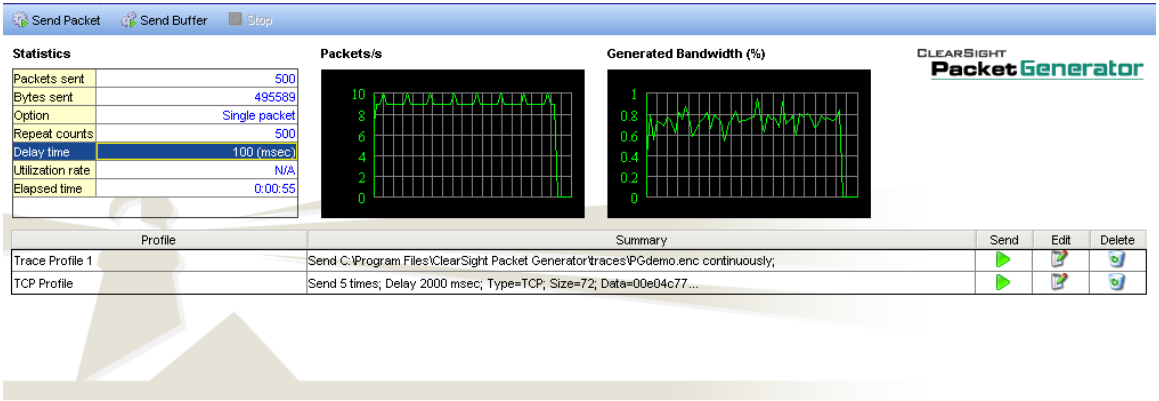


Figure 13-8: Main Packet Generator Screen Showing the Profile List

Chapter 14

Linking to ClearSight Apex

ClearSight Apex is a license option that is offered as an add-on to CSA, beginning with CSA 6.6.

This chapter describes how CSA can link to the ClearSight Apex product.

For a full description of ClearSight Apex, see the *ClearSight Apex User Guide*.

What Apex Provides

ClearSight Apex is provided to help ClearSight customers better understand the problems and issues that can be recognized on networks being monitored by ClearSight products.

Where CSA identifies a problem or an issue, the user who has the Apex option enabled can right-click on the item and be taken to a knowledge base that gives a description of the problem or issue and suggests possible causes and recommended actions to help improve the situation.

Where to Find the Links

Within CSA there are numerous lists of both problems and issues. Within a problems list, you can right-click on a individual problem, as shown in Figure 14-1. When you select **Apex Analysis**, you will immediately jump to a knowledge base article giving expert information about that problem.

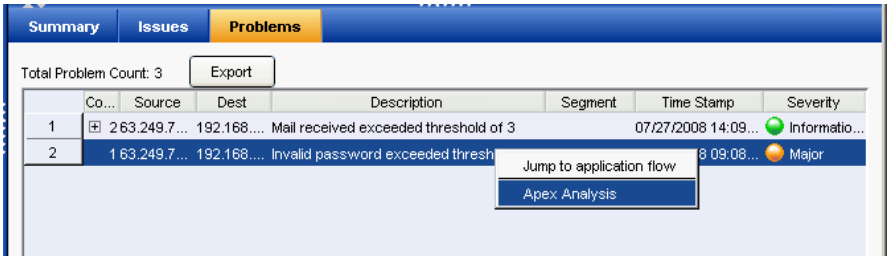


Figure 14-1: Invoking the Knowledge Base from a Problem Listing

Similarly, within an issues list, you can right-click on a individual issue, as shown in Figure 14-2. When you select **Apex Analysis**, you will immediately jump to a knowledge base article giving expert information about that issue, if it is available within the current knowledge base. If that issue is not yet available, you will jump to the top level of the knowledge base.

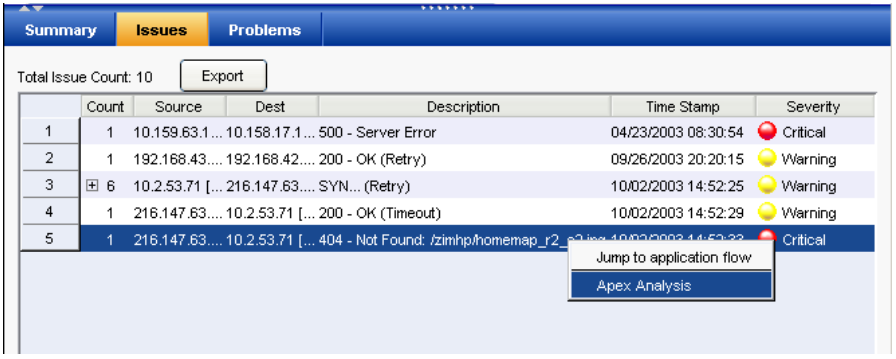


Figure 14-2: Invoking the Knowledge Base from an Issue Listing

You can also jump to the knowledge base when an issue is highlighted in a ladder diagram. Simply right-click on the highlighted issue and select **Apex Analysis**, as shown in Figure 14-3. You will immediately jump to a knowledge base article giving expert information about that issue, if it is available within the current knowledge base. If that issue is not yet available, you will jump to the top level of the knowledge base.

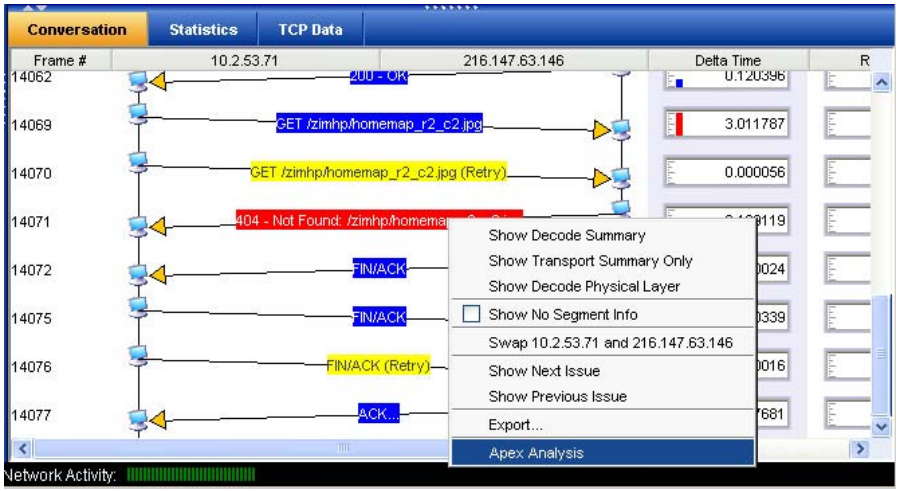


Figure 14-3: Invoking the Knowledge Base from a Ladder Diagram

Chapter 15

Sending Error Reports to ClearSight Networks

This chapter describes a feature that can send error reports to ClearSight Networks in the event of a malfunction of the ClearSight Analyzer itself.

Basic Operation of the Error Reporting Feature

This error reporting feature will be activated whenever the ClearSight Analyzer (CSA) detects an exception or shuts down abnormally.

This feature gives you a chance to report such an error situation to ClearSight Networks Technical Support. You can send relevant log files and trace files. ClearSight Networks Technical Support will study these and then contact you in an effort to resolve any problems.

When an error of this type occurs, the next time CSA is started, it will present the error reporting options dialog box shown in Figure 15-1.

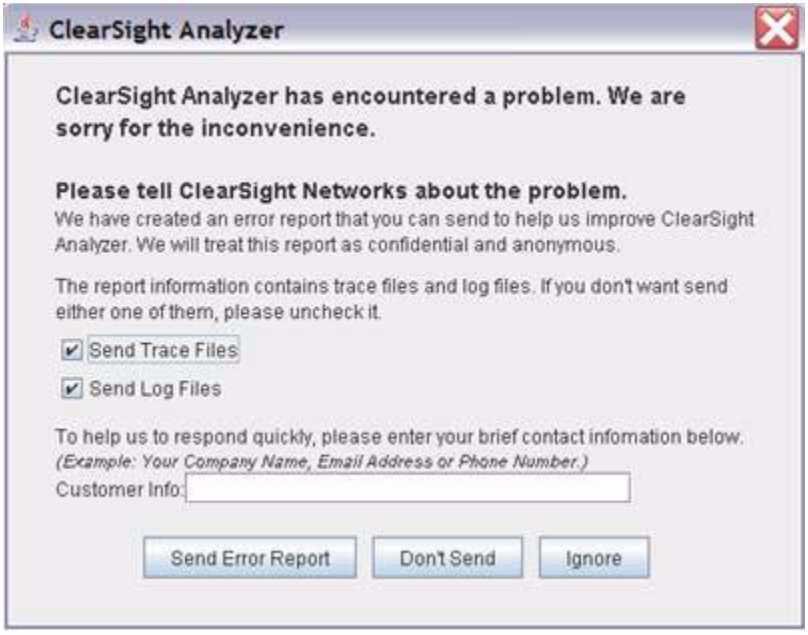


Figure 15-1: Error Reporting Options Dialog Box

You can choose whether CSA should send trace files, log files, or both. However, CSA cannot send trace files unless you have first enabled debug capture, as described below following Figure 15-4.

Be sure to enter some contact information so that ClearSight Networks can get back to you.

You can choose one of the three buttons at the bottom, with the following results:

- **Ignore** cancels this interaction, and does not save any settings.
- **Don't Send** saves your choices and contact information, but does not actually send a report.
- **Send Error Report** saves your choices and contact information, and also sends a report to ClearSight Networks. If **Send Log Files** is checked, CSA sends all the log files in the **C:\Program Files\Clearsight\log** directory. If **Send Trace Files** is checked,

CSA will send the trace files that have been saved in the **C:\Program Files\Clearsight\log** directory, provided that debug capture has been enabled, as explained below.

If you intend to select **Send Error Report**, be sure to have an active internet connection.

If you choose **Send Error Report**, and the reporting process is proceeding normally, you will see the progress bar shown in Figure 15-2.



Figure 15-2: Debug Information Progress Bar

If for any reason the report cannot be sent successfully, you will see the error message shown in Figure 15-3.

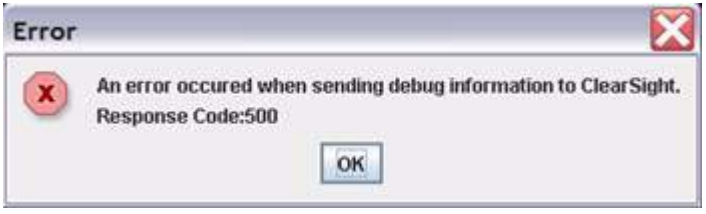


Figure 15-3: Debug Information Error Message

After the report has been sent, or if you choose **Don't Send**, the Enable Debug Capture dialog box (Figure 15-4) will appear. You will then be able to choose a debug capture buffer size (8 MB or 64 MB). Unless you uncheck the **Enable Debug Capture** box, then CSA will save the most recent portion of what it monitors for use in case of another crash. The contents of the debug capture buffer will be saved as a trace file in the **C:\Program Files\Clearsight\log** directory.

For example, if you choose 8 MB, then at any given time the most recent 8 MB of captured packets will exist in the debug capture buffer. If an exception occurs, the debug capture is stopped and the contents of the debug capture buffer are written to a special trace file of the form Deb*nnn*.adc, where *nnn* is a randomly assigned number. This trace file will contain the very last 8 MB of traffic monitored by CSA, including any packet that might have caused the exception.

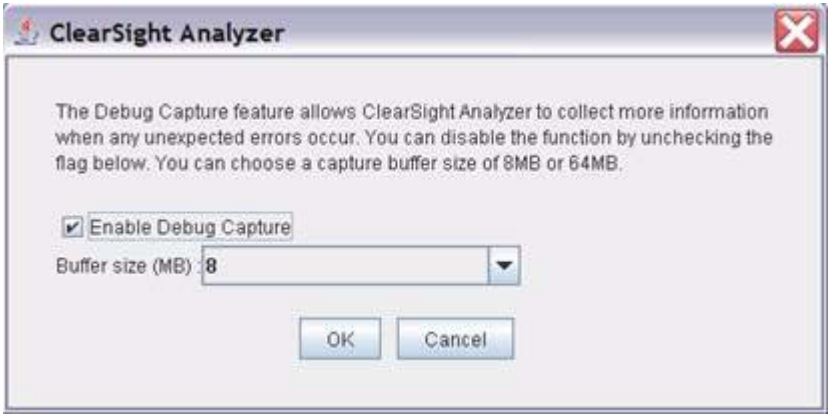


Figure 15-4: Enable Debug Capture Dialog Box

If debug capture is enabled, and you subsequently exit CSA, the Debug Capture Confirmation message (Figure 15-5) will remind you that it is still on and ask whether you want to keep it enabled.

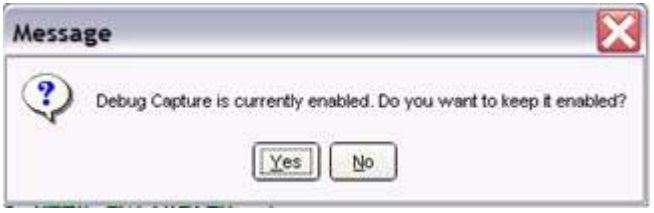


Figure 15-5: Debug Capture Confirmation

If you want CSA to continue the debug capture process the next time CSA is started, click **Yes**. Otherwise, click **No**.

Appendix A

Configuring Special Network Cards

This appendix provides connection instructions for optional ClearSight network cards:

- *Configuring the Gigabit-XD Ethernet Card*
- *Configuring the 10-Gigabit Ethernet Card*

In addition, the appendix also describes the special configuration options for these adapters found in the **Configuration > Preferences > Adapter Settings** screen.

NOTE: The **Adapter Settings** selection appears only when ClearSight is monitoring the 10/100 Full Duplex Ethernet card or a Gigabit Ethernet card.

Configuring the Gigabit-XD Ethernet Card

When using this card, you need to set the following options in the **Configuration > Preferences > Adapter Settings > Gigabit - XD** screen:

- **Mode** options specify how the Gigabit-XD Ethernet adapter card is connected to the network (page 424).

- **Physical Connection** options specify the particular type of hardware port device used (page 425).

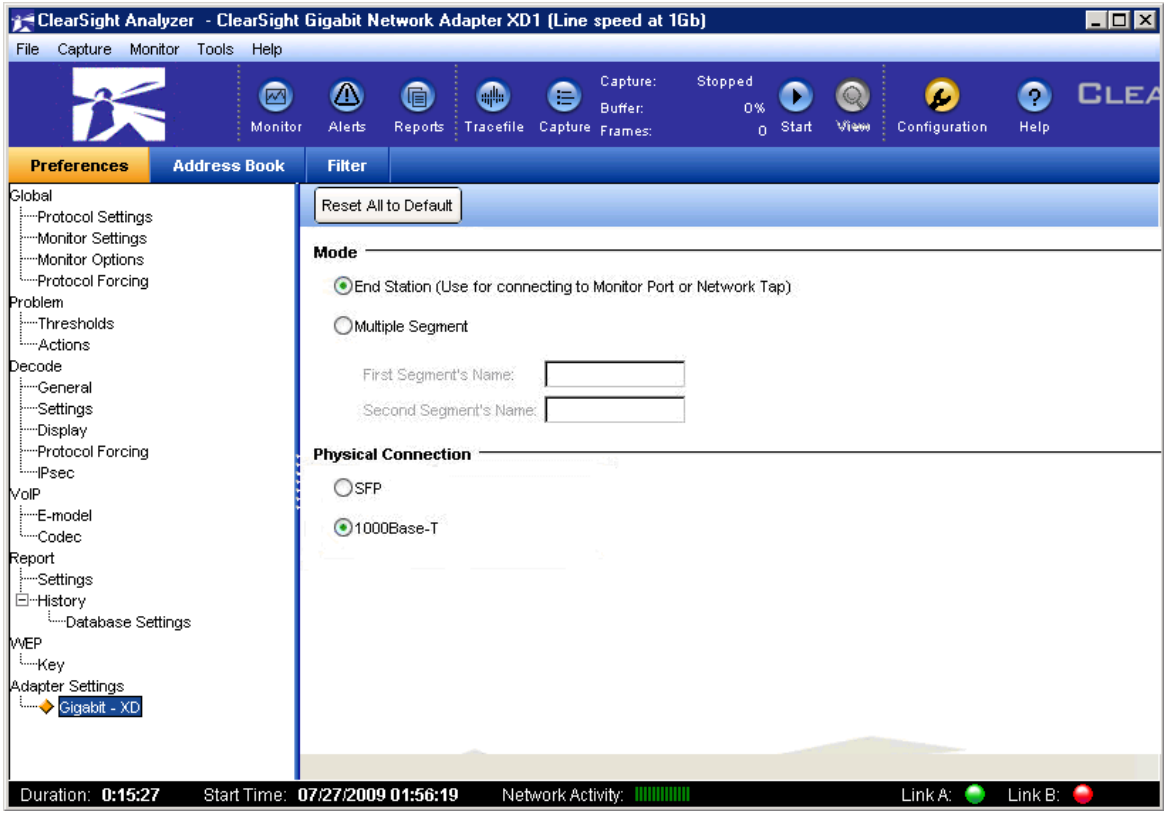


Figure A-2: Adapter Settings for the Gigabit-XD Ethernet Card

Mode Options

The **Mode** options specify how the card is connected to the network. You can select from the options listed below.

End Station

Use the **End Station** option:

- With one cable when attaching to a monitoring port on a switch. Use the switch's built in configuration software to set up port

mirroring so that traffic is sent to the port where the card is connected.

- With two cables when attaching to a network tap.

Multiple Segment Option

Use the **Multiple Segment** option when the two ports of the Gigabit-XD Ethernet card are connected to two independent network segments for use in multi-segment analysis (see *Multi-Segment Analysis* on page 253 for details). Enter names for the segments in the **First segment's Name** and **Second segment's Name** boxes.

You can also use the **Multiple Segment** option when connecting the two ports of the Gigabit Ethernet card to two SPAN ports on two different switches.

Use the switch's built in configuration software to set up port mirroring so that traffic is sent to the ports where the card is connected.

Physical Connection Options

Use the **Physical Connection** options to specify the physical port device being used.

- **SFP —** Either of two Small Form Pluggable fiber optic connectors:
  - single mode optical fiber
  - multi-mode optical fiber
- **1000Base-T —** 10/100/Gigabit Ethernet connection for 150 ohm twisted pair copper wire, using the hardwired Ethernet port(s).

Configuring the 10-Gigabit Ethernet Card

When using this card, you need to set the following options in the **Configuration > Preferences > Adapter Settings > Gigabit - 10G** screen:

- **Mode** options specify how the 10G NT20X Ethernet adapter card is connected to the network (page 427).
- **Capture Mode** options specify whether the 10G NT20X Ethernet card captures in **Streaming** mode to the analyzer's capture buffer or in **Wire speed** mode to the card's onboard buffer (page 427).

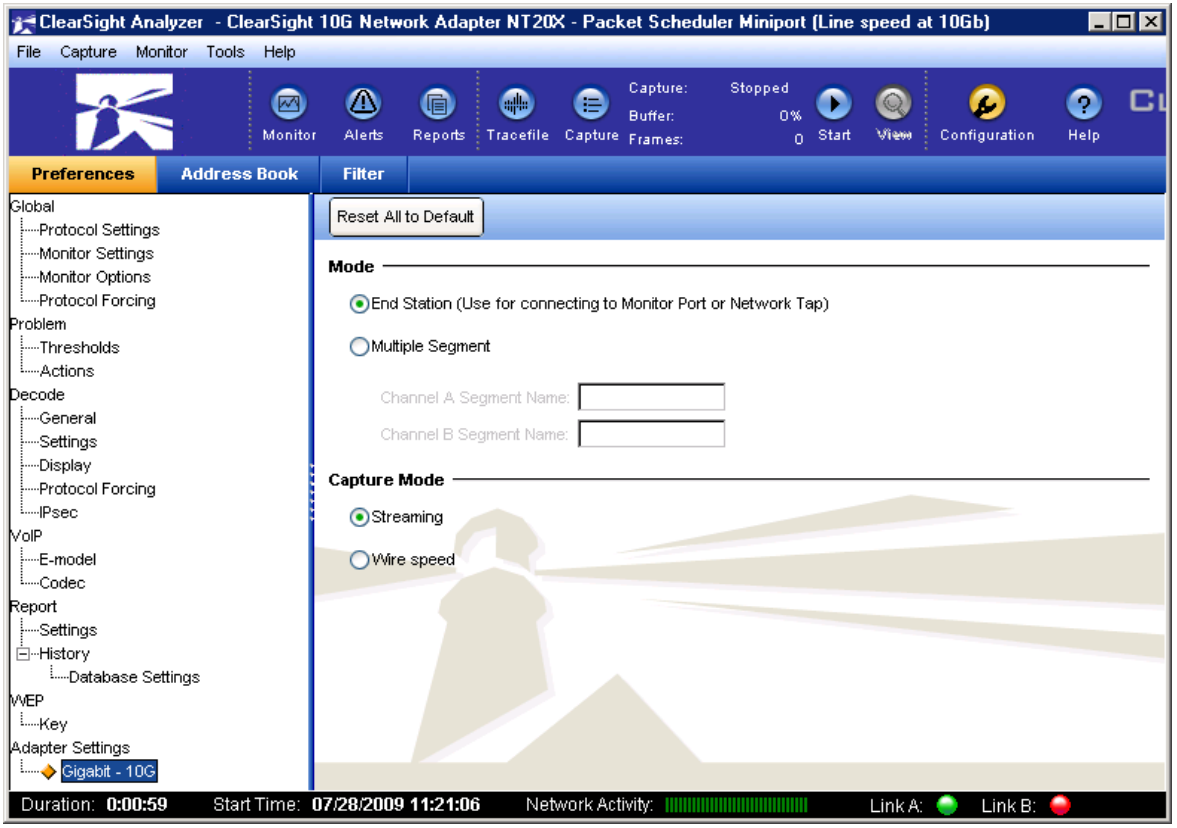


Figure A-3: Adapter Settings for the 10-Gigabit Ethernet Card

Mode Options

The **Mode** options specify how the card is connected to the network. You can select from the options listed below.

End Station

Use the **End Station** option when connecting to a monitor port on a switch or to a network tap.

Multiple Segment Option

Use the **Multiple Segment** option when the two ports of the 10-Gigabit Ethernet card are connected to two independent network segments for use in multi-segment analysis. Enter names for the segments in the **First Segment's Name** and **Second Segment's Name** boxes.

You can also use the **Multiple Segment** option when connecting the two ports of the 10-Gigabit Ethernet card to two SPAN ports on two different switches.

Use the switch's built in configuration software to set up port mirroring so that traffic is sent to the ports where the card is connected.

Capture Mode Options

Use the **Capture Mode** options to specify how the Gigabit Ethernet card captures data from the network.

- **Streaming —** In **Streaming** mode, data is passed from the card into the analyzer buffer in real time as the capture progresses.
- **Wire speed —** In **Wire speed** mode, captured data is stored in the 10 Gigabit Ethernet card's onboard buffers. After capture stops, data is transferred automatically from the card's buffer to the analyzer's buffer for postcapture analysis. The 10 Gigabit Ethernet card is able to view Utilization data while capturing data at **Wire speed**.

Use **Streaming** mode when you want to see real-time statistics. Use **Wire speed** mode when you want to capture a buffer full of data at line rate speeds. Capture performance will be higher when **Wire speed** mode is selected.

Index

Numerics

3G-324M
    replaying video 236
3G-324M frames
    decoding 235

A

actions
    associating with alert severities 325
    defining 325
    email 326
    pager 328
    script 330
    SNMP 332
    viewing list 333
Add Agent dialog box 60
address book
    described 363
    working with 364
addresses
    toggling 125
Agent Manager 91
Agent Viewer-Agent communications 59
Agents List 60, 89, 93
    connecting agents 97
alerts
    and actions 325
    and severities 324
    color coding 115
    described 320
    Issues tab 322
    Problems tab 323
    thresholds 334
    working with display 320
Apex
    how to link 416
    product 415
application layer
    described 117
    filters 277
    monitoring 119
    reports 372
application monitoring
    described 119
    detail displays 120, 131

summary screen 109
audience of this guide 18
Auto Save feature 209
auto-combine filters 261
automatic filters 226, 269
capture 272
display 273
smart navigation 222

B

Buffer Settings tab 206

C

call log
VoIP 397
calls
replaying 155
capture
buffer 201
described 201
observing 216
overview 79
Statistics tab 205
toolbar controls 202
triggers 213
workspace 202
Central Alarm configuration 104
Central Problem Manager 84, 86, 91, 101, 103
Charts tab
network layer 177
physical layer 186
Check Interval option 190
ClearSight
contact information 23
features 64
terminology 116
ClearSight Distributed Agent 84
connecting to 59
Manager 83
ClearSight kernel 86
ClearSight Server service 86
color
and alert levels 115
in ClearSight displays 115
in Decode tab 246
combined flows
non-VoIP 259
VoIP 254, 257
combining flows
automatically 261
manually 266
communications card 59
configuration
analyzer 188
decodes 237
thresholds 334
connecting
overview 52
using hubs 53
using port mirroring 57
using taps 55
Connections tab
network layer 170
contact information 23
conventions, notational 21
Conversation tab 129
custom protocols, adding 189
customer service 23

D

Decode tab
detail pane 230
Ethernet OAM frames 233
hex pane 232
panes 228
postcapture analysis 226
searching for frames 232
smart navigation from 224

Summary pane 228
default
password 66, 87
username 66, 87
defined filters 269, 274
detail displays
application monitoring 131
Detail pane (Decode tab) 230
disconnecting an Agent 98
display of capture frames 217
DOCSIS frames 240

E

Ethernet OAM frames 233

F

filter list 317
filters
application layer 277
auto-combine 261
automatic 226
automatic vs. defined 269
described 269
DNS 278
flow 304
FTP 280
H.323 289
HTTP 282
IP 309
IP subnet 307
IPTV 302
ISAKMP 297
Kerberos 298
list 317
MAC address 314
Megaco 296
MGCP 294
MSN 288
pattern 305
physical layer 315
POP 284
protocol 308
RTSP 300
SIP 291
Skinny 293
SMB 303
SMTP 286
TCP 311
UDP 313
Voice 289, 291, 293, 294, 296
flow
described 116
filters 304
font
in Decode tab 246
frames
searching for 232
slicing 209

H

Hex pane (Decode tab) 232
History Reporter 391
Hostname field 60
Hosts tab
network layer 175
HTTP
child flows option 193

I

indicators in this guide 22
IPsec
decode 250
issue
described 116
Issues tab
alerts 322
in real-time monitor displays 127

J

Java RMI over SSL 86
jumbo frames 193
Jump to a related page button 224

M

merging trace files 254
monitor card 59
monitoring
  application layer 119
  network layer 168
  physical layer 180
  user interface 109
MS SQL
  viewing MSSQL flow errors 146
MSN
  viewing MSN messages 151
Multicast tab
  network layer 178
Multi-Segment analysis 253
Multi-segment monitoring
  real-time 267
Multi-Tiered tab 264

N

NAT tab 265
navigation, smart 221
network adapters
  10-gigabit 426
  Gigabit-XD 423
network layer
  Charts tab 177
  Connections tab 170
  described 117
  Hosts tab 175
  monitoring 168
  Multicast tab 178
  Overview tab 169
  reports 386
Nodes tab
  physical layer 185
notational conventions 21

O

Open Adapter dialog box 61, 97
Oracle
  recreating a transaction 147
  viewing Oracle flow errors 149
Overview tab
  network layer 169
  physical layer 182

P

packet generator 400
panes
  in Decode tab 228
  monitoring interface 112
Password
  default 66, 87
phone numbers 23
physical layer
  Charts tab 186
  described 117
  filters 315
  monitoring 180
  Nodes tab 185
  Overview tab 182
  Subnet tab 184
  VLAN tab 183
POP
  viewing POP emails 140
ports
  adding 189
postcapture analysis 217
  ClearSight tab 222
  Decode tab 226
  external application launching 238
  overview 79

smart navigation 221
tabs 219
workspace 218
problem
described 116
Problem Interval option 197
problems
thresholds 334
Problems tab
in alerts display 323
in real-time monitor displays 128
protocol decodes 226
protocol forcing
decode 247
global configuration 195
protocol settings 189

R

real-time monitoring
application layer 119
network layer 168
overview 78
physical layer 180
user interface 109
reports
Application Distribution 387
application layer 372
Connections 386
described 367
DNS 373
Exchange 383
FTP 374
History 391
HTTP 375
IP Hosts 387
IP Matrix 386
IP Protocol Distribution 387
IP Response Time Distribution 387
IPTV 382
ISAKMP 382
Kerberos 382
MS SQL 377
MSN 383
network layer 386
Network Overview 386
Nodes 388
Oracle SQL 378
POP 376
real-time vs. postcapture 368
RTSP 384
SMB 384
SMTP 377
Telnet 374
Utilization Distribution 389
VLAN 388
VoIP 380
RTP
replaying streams 159

S

searching for frames (Decode tab) 232
Secure Socket Layer (SSL) 107
severities
defining 324
slicing (of frames) 209
smart navigation 221
from Decode tab 224
SMTP
viewing emails 142
Statistics pane 126
Statistics tab (Capture) 205
Subnet tab
physical layer 184
Summary pane (Decode tab) 228
support 23
system requirements 25

T

technical support 23

telephone numbers 23
terminology
ClearSight 116
thresholds 334
DNS 335
FTP 336
H.323 345
HTTP 340
IP 358
IPTV 355
IPv6 360
ISAKMP 356
Kerberos 356
Megaco 350
MGCP 349
MSN 344
POP 341
RTP 351
RTSP 353
SIP 347
Skinny 348
SMB 357
SMTP 343
Telnet 339
Throughput Interval option 190
toggling
address displays 125
toolbar buttons 74
trace files
formats 251
merging 254
using 251

U

User Configuration utility 67, 88
user interface
overview 72
User List 66, 69, 86, 89
Username
default 66, 87

V

video
replaying 157
VLAN tab
physical layer 183
Voice
filters 289, 291, 293, 294, 296
voice
replaying calls 155
VoIP
call log 397
combined flows 254, 257
replaying calls 155
replaying video 157
reports 380

W

Windows Security Manager 108