Trademark Notices

©2013 Network Instruments,® LLC. All rights reserved. Network Instruments, Observer®, Gen2™, Link Analyst, and Observer Infrastructure and all associated logos are trademarks or registered trademarks of Network Instruments, LLC.

Open Source Copyright Notices

Portions of this product include software written by the University of Cambridge, Copyright © 1997-2012 University of Cambridge All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Portions of this product include software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/), Copyright © 1998-2013 The OpenSSL Project. All rights reserved.

Portions of this product include software written by the University of Cambridge, Copyright © 1997-2013 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Limited Warranty—Hardware

Network Instruments, LLC. (Network Instruments) warrants this hardware product against defects in materials and workmanship for a period of 90 days (1 year for nTAPs) from the date of shipment of the product from Network Instruments, LLC. Warranty is for depot service at Network Instruments corporate headquarters in Minneapolis, MN or London, England. Warranties and licenses may give you more coverage in certain local jurisdictions; Network Instruments also offers extended warranties as part of its maintenance agreement program.

If a defect exists during the initial warranty period or prior to expiration of a pre-paid maintenance program, at its option Network Instruments will (1) repair the product at no charge, using new or refurbished replacement parts, or (2) exchange the product with a product that is new or which has been manufactured from new or serviceable used parts and is at least functionally equivalent to the original product. A replacement product assumes the remaining warranty of the original product or 60 days, whichever provides longer coverage for you. When a product or part is exchanged, any replaced item becomes your property and the replaced item becomes Network Instruments’ property.

The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Network Instruments, LLC. Network Instruments, LLC assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual. Network Instruments, LLC does not warrant that the hardware will meet your requirements or that the operation of the hardware will be uninterrupted or that the hardware will be error-free.

Network Instruments, LLC SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL Network Instruments, LLC BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGE, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

Network Instruments, LLC makes no other warranty, expressed or implied.

Limited Warranty—Software

Network Instruments, LLC (DEVELOPER) warrants that for a period of sixty (60) days from the date of shipment from DEVELOPER: (i) the media on which the SOFTWARE is furnished will be free of defects in materials and workmanship under normal use; and (ii) the SOFTWARE substantially conforms to its published specifications. Except for the foregoing, the SOFTWARE is provided AS IS. This limited warranty extends only to END-USER as the original licensee. END-USER’s exclusive
remedy and the entire liability of DEVELOPER and its suppliers under this limited warranty will be, at DEVELOPER or its service center’s option, repair, replacement, or refund of the SOFTWARE if reported (or, upon request, returned) to the party supplying the SOFTWARE to END-USER. DEVELOPER does not warrant that the software will meet END-USER requirements, and in no event does DEVELOPER warrant that the SOFTWARE is error free or that END-USER will be able to operate the SOFTWARE without problems or interruptions.

Should DEVELOPER release a newer version of the SOFTWARE within 60 days of shipment of the product, DEVELOPER will update the copy of the SOFTWARE upon request, provided request is made by the licensed END-USER within the 60 day period of shipment of the new version. This update may consist of a CD or a manual or both at the discretion of DEVELOPER. END-USER may be charged a shipping fee for updates.

The information in the SOFTWARE manuals is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by DEVELOPER. DEVELOPER assumes no responsibility or liability for any errors or inaccuracies that may appear in any SOFTWARE manual.

This warranty does not apply if the software (a) has been altered, except by DEVELOPER, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by DEVELOPER, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultrahazardous activities.

DISCLAIMER. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

The above warranty DOES NOT apply to any beta software, any software made available for testing or demonstration purposes, any temporary software modules or any software for which DEVELOPER does not receive a license fee. All such software products are provided AS IS without any warranty whatsoever. This License is effective until terminated. END-USER may terminate this License at any time by destroying all copies of SOFTWARE including any documentation. This License will terminate immediately without notice from DEVELOPER if END-USER fails to comply with any provision of this License. Upon termination, END-USER must destroy all copies of SOFTWARE. DEVELOPER makes no other warranty, express or implied.

**Liability**

IN NO EVENT WILL DEVELOPER OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE EVEN IF DEVELOPER OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

DEVELOPER SHALL NOT BE LIABLE FOR MATERIAL, EQUIPMENT, DATA, OR TIME LOSS CAUSED DIRECTLY OR INDIRECTLY BY PROPER OR IMPROPER USE OF THE SOFTWARE. IN CASES OF LOSS, DESTRUCTION, OR CORRUPTION OF DATA, DEVELOPER SHALL NOT BE LIABLE. DEVELOPER DOES NOT TAKE ANY OTHER RESPONSIBILITY.

In no event shall DEVELOPER’s or its suppliers’ liability to END-USER, whether in contract, tort (including negligence), or otherwise, exceed the price paid by END-USER. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose.

DEVELOPER SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL DEVELOPER BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGE, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

DEVELOPER’S liability to the END-USER under this agreement shall be limited to the amount actually paid to DEVELOPER by END-USER for the SOFTWARE giving rise to the liability.

**Ownership and Confidentiality**

END-USER agrees that Network Instruments, LLC owns all relevant copyrights, trade secrets and all intellectual property related to the SOFTWARE.

**Technical Support**

Network Instruments provides technical support by phone (depending on where you are located):

US & countries outside Europe at (952) 358-3800

UK and Europe at +44 (0) 1959 569880

By fax (depending on where you are located):
Network Instruments provides technical support for a period of 90 days after the purchase of the product at no charge. After the 90-day initial support period (1 year for nTAPs), support will only be provided to those customers who have purchased a maintenance agreement.

Telephone technical support hours are between 9:00 am and 5:00 pm (local time for each office).

Suggestions are welcomed. Many of the improvements made to our products have originated as end user suggestions. Please submit detailed suggestions in writing to: support@networkinstruments.com or by fax at: (952) 358-3801. Please submit any corrections to or criticism of Network Instruments’ publications to: pubs@networkinstruments.com or by fax at (952) 358-3801.
Table of Contents

Chapter 1: Getting Started............................................................................................................................. 1

  Which version of Observer is right for you?.............................................................................................................. 1
  Observer Standard.............................................................................................................................................. 4
  Observer Expert............................................................................................................................................... 4
  Observer Suite................................................................................................................................................ 4

  System requirements and installing or upgrading the software........................................................................ 4
  FAQ: Licensing and updating............................................................................................................................ 6
  Capture card driver requirements..................................................................................................................... 7

  Overview of Observer....................................................................................................................................... 9

  User interface................................................................................................................................................... 9
  The dashboard.................................................................................................................................................. 10
  Customizing toolbars........................................................................................................................................ 11
  Ports used by Network Instruments products................................................................................................. 12

  Configuring Observer’s general settings........................................................................................................ 12

    General tab................................................................................................................................................ 12
    Security tab................................................................................................................................................. 13
    Folders tab.................................................................................................................................................. 15
    SNMP tab................................................................................................................................................... 15
    IPv6 tab..................................................................................................................................................... 16
    Third Party Decoder tab............................................................................................................................... 17
    GeoIP Settings.......................................................................................................................................... 17

Chapter 2: Real-Time Statistics......................................................................................................................... 19

  Monitoring connection statistics.................................................................................................................... 19

    Discovering conversations between local devices and the Internet............................................................... 19
    Configuring the IP application list................................................................................................................ 20
    Discovering conversations between local devices......................................................................................... 21

    Viewing real-time statistics per device.......................................................................................................... 21
    Viewing a list of protocols seen on the network............................................................................................ 22
    Viewing wireless access point statistics....................................................................................................... 22

  Monitoring network load............................................................................................................................... 23

    Viewing router utilization statistics............................................................................................................ 23
    Viewing bandwidth utilization....................................................................................................................... 24
    Viewing bandwidth utilization with a filter.................................................................................................... 24
    Wireless Access Point Load Monitor........................................................................................................... 24
    Viewing the distribution of packet sizes by station....................................................................................... 25
    Discovering current top talkers on the network............................................................................................. 25
    Load testing the network............................................................................................................................. 26
    Configuring your load test settings............................................................................................................... 26

  Viewing utilization history.............................................................................................................................. 27

    Tell me more about the Utilization History tool.......................................................................................... 27
    Viewing real-time utilization........................................................................................................................ 27
    Viewing a summary of network activity......................................................................................................... 28

  Checking the health of your network............................................................................................................... 28

    Viewing network errors............................................................................................................................. 28
Chapter 3: Discovery

Building and saving an address book ......................................................... 36
Configuring a discovery method (optional) ............................................... 36
Building an address book automatically .................................................. 36
Adding entries to the address book manually ......................................... 37
Resolving DNS names ............................................................................. 38
Saving the address book ........................................................................ 38
Editing address book entries ................................................................. 38
Importing a previously saved address book ............................................. 38
 Tell me more about importing a previously saved address book .......... 38
Using multiple address books ................................................................. 39
Discovery ......................................................................................... 39
Discovering server applications on the network ..................................... 39
Discovering SNMP devices .................................................................... 40
Discovering which devices are connected to a switch ............................ 41
Calculating subnet masks ...................................................................... 43
Performing ping and trace route ........................................................... 43
How to add application definitions ....................................................... 44
 How to associate non-standard ports with an application ..................... 44
 How to import application definitions ................................................... 45
 How to export application definitions .................................................. 46
 Adding derived application definitions ................................................... 46
Enabling or disabling applications that use dynamic ports ................. 47
Defining applications differently per IP address .................................... 47
Restoring the default application list ...................................................... 48
 How to restore TCP application definitions ......................................... 48
 How to restore UDP application definitions ......................................... 49
Sharing application definitions with others .......................................... 49
 How to export application definitions .................................................. 49
 How to import application definitions .................................................. 49

Chapter 4: Captures ............................................................................. 51
Configuring the capture buffer settings .................................................. 51
Fine-tuning the statistical buffer ......................................................... 52
 Tell me more about the statistical memory allocations ....................... 53
Configuring the packet capture options ................................................ 57
Excluding non-native packets from capture ......................................... 57
<table>
<thead>
<tr>
<th>Chapter 8: Logs</th>
<th>112</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing log file behavior</td>
<td>112</td>
</tr>
<tr>
<td>Disabling logging of certain event types</td>
<td>113</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9: Alarms</th>
<th>115</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring and using alarms</td>
<td>115</td>
</tr>
<tr>
<td>Enabling probe instance alarms</td>
<td>115</td>
</tr>
<tr>
<td>Enabling individual alarms</td>
<td>116</td>
</tr>
<tr>
<td>Creating filter-based alarms</td>
<td>117</td>
</tr>
<tr>
<td>Resetting statistical alarms</td>
<td>118</td>
</tr>
<tr>
<td>Customizing triggers and actions</td>
<td>118</td>
</tr>
<tr>
<td>Customizing alarm triggers</td>
<td>119</td>
</tr>
<tr>
<td>Customizing alarm actions</td>
<td>119</td>
</tr>
<tr>
<td>Sharing alarms with others</td>
<td>120</td>
</tr>
<tr>
<td>How to export alarms</td>
<td>120</td>
</tr>
<tr>
<td>How to import alarms</td>
<td>120</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10: Reports</th>
<th>122</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administering Observer reports</td>
<td>122</td>
</tr>
<tr>
<td>Configuring the Observer web server</td>
<td>122</td>
</tr>
<tr>
<td>Viewing reports in a web browser</td>
<td>122</td>
</tr>
</tbody>
</table>
### Chapter 13: VoIP and Videoconferencing

- Collecting VoIP or video conferencing trending data: 166
- Importing and exporting VoIP or video conferencing settings: 167
- Analyzing VoIP or video conferencing traffic: 167
- How to extract VoIP and video calls from your GigaStor: 168
- Configuring network trending settings for VoIP or video conferencing:
  - General tab: 171
  - MOS tab: 171
  - Device IP Addresses tab: 173
  - Caller ID Determination tab: 174
  - IP Range Filters tab: 174
- Enabling VoIP alarms: 175
- VoIP Top 10 best practices: 176
  - Network Jitter and Delay: 177
  - Packet Loss: 178
  - Managing VoIP Quality: 178
  - VoIP terminology: 179

### Chapter 14: SNMP Management Console

- Introduction to SNMP: 182
- Enabling SNMP CPU and Memory usage stats on Windows servers: 183
- Configuring Observer Suite for SNMP devices: 184
- What can Observer’s SNMP console tell me about a problem switch?: 184
- Long-term trending using the SNMP console: 185
- Resetting SNMP device alarm counters: 185
- About MIBs: 185
- Introduction to SNMP Management Console: 187
- Who should use SNMP Management Console?: 187
- SNMP Management Console main components: 187
- Preparing to use SNMP Management Console: 188
- Configuring SNMP agents:
  - OIDs: 189
  - SNMP Management Station: 189
- Using SNMP Management Console: 190
- Using the MIB editor: 191
- Adding triggers based on SNMP chart values: 192
- Adding, modifying, and deleting SNMP agents: 192
- Using agent information windows: 194
- Collecting SNMP agent information:
  - Collecting chart information: 195
  - Customizing charts: 195
  - Collecting list information: 195

Choosing your network trending types: 158
Scheduling your network trending data collection: 163
Adding specific servers to network trending: 163
Enabling NetLive trending collection: 163

**Customizing charts:** 195
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a probe instance</td>
<td>235</td>
</tr>
<tr>
<td>Creating GigaStor active and passive probe instances</td>
<td>236</td>
</tr>
<tr>
<td>Creating and configuring an MPLS probe instance</td>
<td>236</td>
</tr>
<tr>
<td>Using additional storage volumes for your GigaStor active instance</td>
<td>237</td>
</tr>
<tr>
<td>Changing the monitored network adapter</td>
<td>237</td>
</tr>
<tr>
<td>Connecting to a probe for the first time from the Observer analyzer</td>
<td>237</td>
</tr>
<tr>
<td>Connecting the Multi Probe or Expert Probe to an Observer analyzer</td>
<td>238</td>
</tr>
<tr>
<td>Connecting to a probe instance from an Observer analyzer</td>
<td>238</td>
</tr>
<tr>
<td>Connecting the probe to an Observer analyzer</td>
<td>239</td>
</tr>
<tr>
<td>Configuring a probe’s name and other probe options</td>
<td>239</td>
</tr>
<tr>
<td>Customizing statistics and capture buffers for probe instances</td>
<td>241</td>
</tr>
<tr>
<td>Configuring probes to collect data even when not connected to an analyzer</td>
<td>242</td>
</tr>
<tr>
<td>Setting the probe’s time clock synchronization settings</td>
<td>242</td>
</tr>
<tr>
<td>Configuring connections to multiple NICs or Observer analyzers</td>
<td>242</td>
</tr>
<tr>
<td>Setting the total system memory reserved for probes</td>
<td>242</td>
</tr>
<tr>
<td>Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling</td>
<td>243</td>
</tr>
<tr>
<td>Probe Properties field-level descriptions</td>
<td>244</td>
</tr>
<tr>
<td>Security and Encryption</td>
<td>249</td>
</tr>
<tr>
<td>Restricting access to probes with user accounts</td>
<td>249</td>
</tr>
<tr>
<td>Configuring access permissions for probe instances</td>
<td>249</td>
</tr>
<tr>
<td>Forcing users to authenticate before connecting to a probe</td>
<td>250</td>
</tr>
<tr>
<td>How to encrypt captured data</td>
<td>251</td>
</tr>
<tr>
<td>Encrypting the data sent between the probe and analyzer</td>
<td>253</td>
</tr>
<tr>
<td>Using the Probe</td>
<td>255</td>
</tr>
<tr>
<td>Using the Expert Probe software</td>
<td>255</td>
</tr>
<tr>
<td>VoIP Expert, Application Performance Analysis, and Application Transaction Analysis</td>
<td>255</td>
</tr>
<tr>
<td>Switching between the probe and analyzer user interfaces</td>
<td>256</td>
</tr>
<tr>
<td>Enabling Network Trending and setting which statistics are collected</td>
<td>256</td>
</tr>
<tr>
<td>Monitoring a wireless access point</td>
<td>256</td>
</tr>
<tr>
<td>Using the probe as a virtual TAP</td>
<td>257</td>
</tr>
<tr>
<td>When to use a virtual TAP</td>
<td>258</td>
</tr>
<tr>
<td>Configuring VMware ESX Server</td>
<td>262</td>
</tr>
<tr>
<td>Bonding probe instances to specific ports on the Gen2 card through virtual adapters</td>
<td>265</td>
</tr>
<tr>
<td>Capturing full-duplex traffic</td>
<td>265</td>
</tr>
<tr>
<td>Using the NetFlow features in Observer</td>
<td>265</td>
</tr>
<tr>
<td>Creating a NetFlow collector or NetFlow Trending collector</td>
<td>265</td>
</tr>
<tr>
<td>Create card driver requirements</td>
<td>228</td>
</tr>
<tr>
<td>Installing the wireless NIC driver on Windows 7/Vista</td>
<td>229</td>
</tr>
<tr>
<td>Installing a third-party USB wireless adapter</td>
<td>230</td>
</tr>
<tr>
<td>Installing Windows updates and updating virus protection</td>
<td>231</td>
</tr>
<tr>
<td>Upgrading the probe software</td>
<td>231</td>
</tr>
<tr>
<td>Upgrading the probe software directly</td>
<td>231</td>
</tr>
<tr>
<td>Remotely upgrading the probe software from within the Observer analyzer</td>
<td>231</td>
</tr>
<tr>
<td>FAQ: Licensing and updating</td>
<td>232</td>
</tr>
<tr>
<td>Backing up your Observer</td>
<td>233</td>
</tr>
<tr>
<td>Creating a probe instance</td>
<td>235</td>
</tr>
<tr>
<td>Capturing full-duplex traffic</td>
<td>265</td>
</tr>
<tr>
<td>Configuring VMware ESX Server</td>
<td>262</td>
</tr>
<tr>
<td>Bonding probe instances to specific ports on the Gen2 card through virtual adapters</td>
<td>265</td>
</tr>
<tr>
<td>Capturing full-duplex traffic</td>
<td>265</td>
</tr>
<tr>
<td>Using the NetFlow features in Observer</td>
<td>265</td>
</tr>
<tr>
<td>Creating a NetFlow collector or NetFlow Trending collector</td>
<td>265</td>
</tr>
<tr>
<td>Capture card driver requirements</td>
<td>228</td>
</tr>
<tr>
<td>Installing the wireless NIC driver on Windows 7/Vista</td>
<td>229</td>
</tr>
<tr>
<td>Installing a third-party USB wireless adapter</td>
<td>230</td>
</tr>
<tr>
<td>Installing Windows updates and updating virus protection</td>
<td>231</td>
</tr>
<tr>
<td>Upgrading the probe software</td>
<td>231</td>
</tr>
<tr>
<td>Upgrading the probe software directly</td>
<td>231</td>
</tr>
<tr>
<td>Remotely upgrading the probe software from within the Observer analyzer</td>
<td>231</td>
</tr>
<tr>
<td>FAQ: Licensing and updating</td>
<td>232</td>
</tr>
<tr>
<td>Backing up your Observer</td>
<td>233</td>
</tr>
<tr>
<td>Creating a probe instance</td>
<td>235</td>
</tr>
<tr>
<td>Capturing full-duplex traffic</td>
<td>265</td>
</tr>
<tr>
<td>Configuring VMware ESX Server</td>
<td>262</td>
</tr>
<tr>
<td>Bonding probe instances to specific ports on the Gen2 card through virtual adapters</td>
<td>265</td>
</tr>
<tr>
<td>Capturing full-duplex traffic</td>
<td>265</td>
</tr>
<tr>
<td>Using the NetFlow features in Observer</td>
<td>265</td>
</tr>
<tr>
<td>Creating a NetFlow collector or NetFlow Trending collector</td>
<td>265</td>
</tr>
</tbody>
</table>
Chapter 18: Using Your GigaStor ...............................................................................................................................282

Getting started using your GigaStor......................................................................................................................................................282

What is the GigaStor?...............................................................................................................................................................................284

Using the GigaStor Control Panel........................................................................................................................................................284

Non-GigaStor-specific settings............................................................................................................................................................285

Setting GigaStor's basic options........................................................................................................................................................286

GigaStor reports.....................................................................................................................................................................................................288

Understanding GigaStor protocol and port settings........................................................................................................................289

Capturing packets with the GigaStor........................................................................................................................................................289

Setting a schedule for when data captures should occur...............................................................................................................290

Trimming data from your captures for space or privacy..................................................................................................................290

Password protecting the ability to change partial packet capture size.........................................................................................291

Differences between statistics and packets.....................................................................................................................................291

Understanding GigaStor indexing........................................................................................................................................................292

Exporting GigaStor data for archiving................................................................................................................................................293

Configuring your GigaStor........................................................................................................................................................................294

Defining your subnets in GigaStor.......................................................................................................................................................294

Tracking individual analysis ports.........................................................................................................................................................294

Configuring the packet capture and GigaStor buffer size..................................................................................................................294

Generating NetFlow records from the GigaStor's NetFlow Agent.................................................................................................295

Configuring options for the GigaStor charts, graphs, and reports.................................................................................................296

Creating an sFlow collector....................................................................................................................................................................267

How a probe uses RAM........................................................................................................................................................................267

Packet capture buffer and statistics buffer........................................................................................................................................268

Running Observer without reserved memory.....................................................................................................................................269

Running Observer with reserved memory..........................................................................................................................................270

How packet capture affects RAM........................................................................................................................................................271

How to allocate the reserved RAM........................................................................................................................................................273

Recommendations for the Gen2 capture cards..................................................................................................................................273

Tweaking the statistics memory configuration......................................................................................................................................274

Troubleshooting common issues..............................................................................................................................................................274

Troubleshooting a slow probe system................................................................................................................................................275

A probe is not connecting to the analyzer or vice versa.....................................................................................................................276

No network adapter available..............................................................................................................................................................276

Integrated adapters report all sent packets with bad TCP checksum...............................................................................................277

“No VLAN” shown while using a Gigabit NIC.......................................................................................................................................277

VLAN Statistics tool is not working.....................................................................................................................................................277

Using Discover Network Names on a Layer 3 switch that uses VLANS........................................................................................279

Suspected NAT or VPN issues..............................................................................................................................................................279

Running Observer passively affects NetFlow......................................................................................................................................279

Daylight Savings Time...........................................................................................................................................................................280

Configuring Cisco 6xxx switches using a SPAN port to a full-duplex Gigabit Probe.........................................................................280

Cisco CatOS switches...........................................................................................................................................................................280

Cisco IOS switches.................................................................................................................................................................................280

Ports used by Network Instruments products...................................................................................................................................281
Chapter 19: Backup and Restoration

Configuring a FIX profile ........................................................................................................................................... 329
Sharing alarms with others .......................................................................................................................................... 330
How to import alarms .................................................................................................................................................... 330
How to export alarms .................................................................................................................................................... 330
Sharing application definitions with others .................................................................................................................. 331
How to export application definitions ........................................................................................................................ 331
How to import application definitions ........................................................................................................................ 331
How to export report data to XML .............................................................................................................................. 332
Private key locations per server ................................................................................................................................ 333
Importing and exporting VoIP or video conferencing settings ..................................................................................... 335
Restoring the default application list .......................................................................................................................... 335
How to restore TCP application definitions ............................................................................................................... 335
How to restore UDP application definitions....................................................................................................................................335
Importing and exporting Observer Alias (.adr) files...........................................................................................................................336
Importing or exporting a server profile..................................................................................................................................................336
Creating a Forensic Settings profile.........................................................................................................................................................336
Importing Snort rules.....................................................................................................................................................................................341

Chapter 20: Supported Protocols.........................................................................................................................................................342
Protocols supported by Observer.............................................................................................................................................................342

Chapter 21: Change Log...............................................................................................................................................................356
Recent Documentation Changes...........................................................................................................................................................356
Recent documentation changes..........................................................................................................................................................356
Recent Product Changes...............................................................................................................................................................................357

Index..........................................................................................................................................................................................358
Chapter 1: Getting Started

Which version of Observer is right for you?

Observer is available in three versions: Standard, Expert, and Suite. This section lists what features are available in each one.

Note: Because the functionality of Observer versions is additive, all features of Observer Standard are in Observer Expert. Similarly, Observer Suite includes the features of both Observer Standard and Observer Expert.

Observer Standard allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve problems within networks and network applications.

Observer Expert allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve network problems. Observer Expert is also the first offering of Observer to include advanced analysis tools for graphically viewing network conversations, analyzing server response time, VoIP, and much more.

Observer Suite allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve network problems. Observer Suite also includes advanced analysis tools for graphically viewing network conversations, analyzing server response time, and VoIP. Suite is also the first offering of Observer to include SNMP device management, support for RMON, and advanced reporting options.

Table 1: Comparing Observer versions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Standard</th>
<th>Expert</th>
<th>Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Capture on page 59</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Packet Decode</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Real-Time Packet Captures &amp; Decode</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Automated Packet Captures</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Nanosecond Resolution</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Financial Protocol Support</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Feature</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Filters on page 66</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Find Virus and Hack Signatures</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Statistical Drill Down</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarms on page 115</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Custom Alarm Triggers</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Error Tracking</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Real-Time Statistics</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Top Talkers on page 25</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Bandwidth Utilization on page 24</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VLAN Analysis</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Internet Activity on page 19</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wireless Analysis</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IP Pair Statistics</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Protocol Distribution on page 22</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>64 &amp; 32-bit applications on page 4</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Network Trending/Reporting</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Comparison Reports</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ready-Made Reports on page 122</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Custom Reports</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Report Scheduler</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>I Pv6 Support on page 16</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trace File Aggregation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SRTP Support</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Application Analysis Trending on page 149</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Stream Reconstruction</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Web pages</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Email</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Instant messages</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VoIP</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>HTTP-transferred files</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Expert Analysis on page 94</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Over 600 Experts</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Expert Summary</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Feature</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Network Delay</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection Dynamics on page 98</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MultiHop Analysis on page 105</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;What-If&quot; Analysis on page 102</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Analysis</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citrix</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIX</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Exchange</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Networking (SMB)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP Analysis</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Detail Records</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregate Call Summaries</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over 70 VoIP metrics</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over 50 VoIP Experts</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS Metrics</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOS, R-Factor</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRTP support</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP Systems Supported</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitel</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Observer Standard</td>
<td>Observer Expert</td>
<td>Observer Suite</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Nortel</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Siemens</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ShoreTel</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>MPLS Monitoring</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SSL decryption</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NetFlow Collector</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Video monitoring</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Video metrics</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>End-user experience monitoring</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Third-party decode and analysis on page 17</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>LTE Support</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SNMP Device Management on page 182</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RMON Support</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Station Locator on page 41</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Web Publishing Service</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated Report Delivery</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baselining with Alarms</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Observer Standard**

Observer Standard allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve problems within networks and network applications.

**Observer Expert**

Observer Expert allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve network problems. Observer Expert is also the first offering of Observer to include advanced analysis tools for graphically viewing network conversations, analyzing server response time, VoIP, and much more.

**Observer Suite**

Observer Suite allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve network problems. Observer Suite also includes advanced analysis tools for graphically viewing network conversations, analyzing server response time, and VoIP. Observer Suite is also the first offering of Observer to include SNMP device management, support for RMON, and advanced reporting options.

**System requirements and installing or upgrading the software**

Prerequisite(s):
The user running the probe software or Observer—as well as the user installing the software—must have local Administrator rights on the Windows system.

Standard network cards do not support “raw” wireless packets, nor do they enable “promiscuous” mode by default. Promiscuous mode captures all packets for the analyzer, not just those addressed to the network card. Both “raw” wireless packets and promiscuous mode are required by Observer. ErrorTrak drivers were needed in earlier versions of Observer. They are no longer necessary.

If you do not meet the minimum requirements, the system may seem to operate in the short term, but be aware that even if a sub-minimum installation works momentarily, a later, heavier load on the system can cause it to fail. Network Instruments sells hardware probes that are guaranteed to keep up with heavy loads. See the Network Instruments website for details.

You may install the probe software on a virtual machine so long as it meets the system requirements. The installation process is the same. You may also want to consider using a virtual TAP. See Using the probe as a virtual TAP on page 257.

This section describes the installation process and minimum requirements if you are installing the Observer analyzer or probe on your system. This applies to physical and virtualized servers. If you virtualize the server, each server must meet these specifications.

<table>
<thead>
<tr>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Quad core Pentium</td>
</tr>
<tr>
<td>RAM1</td>
<td>8 GB</td>
</tr>
<tr>
<td>Operating system2</td>
<td>Any Windows 64-bit</td>
</tr>
<tr>
<td>Network Card</td>
<td>Intel server-class</td>
</tr>
<tr>
<td>Capture Card3</td>
<td>Intel server-class</td>
</tr>
</tbody>
</table>

1) If your system has 4 GB of RAM, you cannot reserve any memory for Observer. This is a limitation of Windows known as the BIOS memory hole. Either add more RAM or take some out.

2) Supported operating systems are: Windows XP (32-bit SP3, 64-bit SP2); Windows Vista (32-bit SP1 or higher, 64-bit SP1 or higher); Windows 7 (32-bit SP1 or higher, 64-bit SP1 or higher); Windows Server 2003 Enterprise, Standard, Web (32-bit SP3 or higher, 64-bit SP3 or higher); Windows Server 2008 Enterprise, Standard, Web (32-bit SP2 or higher, 64-bit SP2 or higher); Windows Server 2008 R2 Enterprise, Standard, Web (SP1 or higher)

3) A second network card that acts solely as a capture card is required (and must be in “promiscuous mode”). Alternatively, a dual-port NIC can be used. For further details, see Capture card driver requirements on page 7.

The installer program has two versions of Observer and the GigaStor /probe software: 64-bit and 32-bit. It chooses the one appropriate for your operating system. If the version of Observer or GigaStor that you are upgrading was installed on a 32-bit operating system and you have upgraded the operating system to 64-bit, the installer upgrades existing installation to 64-bit version keeping the same path.

To install or upgrade the Observer analyzer, follow these steps:

1. Insert the installation CD in your CD drive or use the latest installation image from our FTP site. If you copied the installation files from our web site, start the installation program.


2. When the setup program runs, follow the onscreen instructions.

3. Choose to install:

   # Observer.
Advanced Probe. Choose this for Single Probe or Multi Probe. Your license determines whether it is a Single Probe or Multi Probe.

Expert Probe

4. After the files have been installed on your system you must restart Windows. You will not be able to run the software until you restart your computer.

After completing this task:

- License your software. See FAQ: Licensing and updating on page 6.
- If you are using a wireless network adapter to capture traffic, see Installing the wireless NIC driver on Windows 7/Vista on page 229.
- If you are using a USB wireless network adapter to capture traffic, see Installing a third-party USB wireless adapter on page 230.

FAQ: Licensing and updating

Some customer concerns deal with licensing and updating issues. Explore this good resource for licensing and updating help, or call the Technical Support department for further assistance.

Network Instruments probes must be licensed before use. If your probe is not licensed, the licensing dialog appears the first time the program is run.

Probes require two unique numbers for licensing: an identification number and a license number.

Note: Your license number (for your product version) is based on your identification number, and your identification number is based on your real name and company name.

The license number determines whether the probe is a Single Probe (one probe instance) or a Multi Probe (capable of running multiple probe instances and allowing multiple Observer analyzers to connect simultaneously).

When you first open a probe, it prompts you for license information. These executable files, found in the Observer installation directory, are the probes and must be licensed.

- Single and Multi Probe: NiProbe.exe
- Expert Probe: observer.exe

If the software is already running, choose Help > License.

After the software is licensed, you can begin using it.

What type of license do I have?

The type of license you have is described in your license document. Each license document contains a license number, and the document describes which version of Observer the license number applies to. If it does not, or you notice any other error, please call our support team for assistance.

Why is my license number not working?

Each license number is case-sensitive, so be sure to type it in exactly the way it was given to you. Also, if you copy-pasted the license number into the activation prompt, be sure you did not introduce a leading or trailing space character—those are not part of your license number.
Also, ensure you are licensing the correct version of Observer. License numbers are version specific. Each license number works only within equal major version numbers of the product. For example, an Observer 16.0 license can be used to activate 16.0 and 16.1, but not 15.0, 15.1, etc.

If you are still unsuccessful, please call our support team so we may assist you, whether that entails sending a correct license number or to discuss the upgrade policy for that product.

**Could I have my license re-sent to me?**

Yes. If you lost the original information containing your license number, please contact us so we can resend your license document(s).

**Should I uninstall Observer before updating it?**

First, verify that you are licensed to use the Observer version you wish to update to.

If you wish to update your existing Observer software to a newly released version *within the same major release number*, you do not need to uninstall your existing version for the update process to succeed. Simply install the new version over the old.

As with all software, it is a best practice to back up your existing installation and settings before updating to a new version.

**Capture card driver requirements**

If you are going to use a third-party capture card in your probe, the capture card must meet certain requirements so that Observer can report statistics and errors. The network card used to monitor or capture network traffic must have all of the mandatory and optional NDIS functions. The Network Instruments Gen2 capture card has all of the necessary features.

Most NIC vendors provide solid, functional NDIS drivers for all cards available within the Ethernet, Token Ring, and FDDI marketplace.

Accessing a standard network with a “normal” network device is somewhat different from what a protocol analyzer requires. While both share a number of driver functions, a protocol analyzer requires a set of features and functions that the average network device will never need. Examples of these optional functions are promiscuous mode, error tracking, and network speed reporting. (Examples of mandatory functions would include functions to determine the maximum packet size, functions to verify the number of sent packets, and functions to specify or determine a packets’ protocol.)

Microsoft made a number of the less used (by “normal” network users) functions “optional”, as opposed to “mandatory” regarding driver requirements. The result has been that most vendors support all (or most) mandatory functions with the first release of the driver. As time passes, and the initial chaos of the first release of the card and driver passes, most manufacturers add some or all of the optional functions, as well as fix or complete all of the mandatory functions.

As part of the optional section of defined NDIS functions, Microsoft specified a number of counters that can be kept for Ethernet frame errors. These counters include CRC errors, Alignment errors, Packets Too Big (Jabbers), and Packets Too Small (Runts). Collisions are counted, but there are limitations of NDIS collision statistics. Four important points should be considered:

- These optional counts only provide a numerical value to the total number of errors on the segment (i.e. the number of CRC errors found), they do not specify where (which station) the error originated from.
After the error packet is identified and the proper error counter is incremented, the packet is discarded, and not sent to Windows (this is the reason it is impossible to determine the source of an Ethernet error packet with standard NDIS drivers).

A number of vendor’s NDIS drivers return a positive acknowledgment when the NDIS error function is queried for existence, but the error statistic is not actually kept.

A few vendors (3COM, for example) do not keep any error statistics whatsoever.

If a NIC driver both reports that the optional Ethernet error statistics are being kept, and actually keeps data on these errors, Observer reports these statistics in the Network Vital Sign Display.

**How collisions are counted**

How collisions are counted by NDIS is a bit different than other errors, and thus a brief explanation is in order. NDIS drivers only count the number of collisions that the actual station where the NDIS driver is running has encountered. For example, if you are running an NDIS driver on station A and there is a collision between stations B and C, A will not increment its collision counter. If a packet from station A collides with station C (or if C collides with A), then station A’s collision counter is incremented.

In an effort to provide a more realistic view of how many collisions are occurring on a LAN segment, Observer has an option (“on” by default when using the Vital Sign mode) to run the “Collision Test”. When turned on, this test sends packets onto the LAN at specific intervals, and records the number of collisions that the Observer station experiences. This test provides a good idea of what any station may see - with regards to collisions - during normal network usage. The collision statistic reported by Observer is an approximation of what any one station may be experiencing, as opposed to an aggregate statistic for the entire LAN segment (as is the case with CRC, Alignment, Jabbers and Runts).

Additionally, Observer includes the “Collision Expert” that both generates packets to approximate each station’s collision potential, and reports which stations are most likely to re-send directly after a collision and which stations were sending just prior to a collision. This information is then reported in an expert dialog and is key in helping to determine the station(s) that are causing the collisions on the segment.

**Observer’s NDIS drivers for Errors-by-Station**

While the aggregate errors that are kept by NDIS provide a general view on the health of a LAN segment, when a high level of segment errors are encountered, the immediate question becomes “Where are these errors coming from?”. This station specific error information has historically been only available from hardware based protocol analyzers. The reason was that hardware-based analyzers have not been limited by the aggregate statistics provided in NDIS. That is not a limitation of Observer.

Network Instruments has worked with a number of NIC vendors and chip manufacturers to extend the standard NDIS drivers to both collect statistics on the aggregate errors on a LAN segment, but also to move the actual error packet information up the NDIS stack for further examination by Observer’s error displays. This allows Observer to report both general error statistics and error source addresses to help pinpoint troubleshooting down to the specific station with a problem.

Using the extended NDIS drivers included with Observer, administrators and technicians can see complete network errors broken down by type and (source) station. This can be done from within the standard Windows environment, without the need to re-boot, without proprietary drivers, and without sacrificing any standard network functionality. This dual functionality is achieved because the Network Instruments NDIS driver is a highly optimized NDIS driver with the addition of a module to collect and process error packets – these drivers have all the functionality of a standard NDIS driver, plus the ability to pass error packets to Observer.
Overview of Observer

Observer is the network administrator’s ultimate toolbox. Deep packet inspection, network analysis, and network management tools are included at various depths.

All Observer versions use the same set of TCP ports to communicate with Network Instruments’ probes. For more details, see Ports used by Network Instruments products on page 12.

Observer Standard allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve network problems. For more details, see Which version of Observer is right for you? on page 1.

Observer Expert allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve network problems. Expert is also the first offering of Observer to include advanced analysis tools for graphically viewing network conversations, analyzing server response time, VoIP, and much more. For more details, see Which version of Observer is right for you? on page 1.

Observer Suite allows you to discover your network, capture and decode network traffic, and use real-time statistics to solve network problems. Suite also includes advanced analysis tools for graphically viewing network conversations, analyzing server response time, and VoIP. Suite is also the first offering of Observer to include SNMP device management, support for RMON, and advanced reporting options. For more details, see Which version of Observer is right for you? on page 1.

The depth of features in Observer depends on which product license you purchased. For information about Observer licenses, see FAQ: Licensing and updating on page 6.

User interface

Expert Probe, the software and its user interface, is described as the analyzer. The engine that makes traffic collection possible is the probe. The Expert Probe analyzer (i.e. the Expert Probe software) is the key to viewing, manipulating and controlling all of the data that a probe captures or sees flow through it. The analyzer communicates with remote probes throughout your network using TCP/IP, or the analyzer uses the local probe built into it.

The leftmost portion of the Expert Probe user interface is the probe window where local and remote probes, NetFlow, sFlow, and SNMP devices are listed.

The main portion of the interface is the tools window. It is here where statistics, trending, decode, expert, and all other tools are displayed. Most tools have its own Settings button used to configure it. Within the tool window you can select and drag separator lines between windows (for instance, you may want to reduce the size of the probes list or log window or even hide it), and you can customize which tools are shown from the View menu.

To use Expert Probe select the desired probe, then pick the desired tool from the main toolbar or from the main menu. You may have multiple tools running simultaneously for each probe. Each tool is in its own tab at the bottom of the tool window. Some tools have additional tabs along the top or bottom that provide even more functionality and display options.
Close any tool by right-clicking in the desired tab in tool tray and select **Close**. Close all active tools by choosing **Window > Close All Statistics Windows**.

**The dashboard**

If you are new to Observer (or need to train others in its use), the dashboard is a great place to begin. In fact, the dashboard provides easy access to features that could otherwise be difficult to find.

By design, the dashboard welcomes you the first time Observer is launched. If you close the dashboard, however, it does not return until you purposely reopen it from the View menu.

If you want to force the dashboard to always appear during Observer startup, choose **Options > Observer General Options**. Then, scroll down and enable the appropriate option in the Startup and Runtime Settings branch.
The dashboard also has a second tab (noticeable in the figure) which displays all configured probes and monitoring instances in a sortable list—a great way to stay organized. All versions of Observer include the dashboard.

The first dashboard tab, Navigate Observer Features, provides shortcuts to some of Observer's most used features. It also has a search option that allows you to quickly find an Observer feature. For instance, if you type the word “capture,” you will get results including several kinds of “packet capture,” the many different “expert analysis” options, and “packet capture buffer” allowing you to jump directly to any of those features.

The second dashboard tab, Observer Status Dashboard, displays your probes and monitoring instances in a sortable list. Click any column header to sort your list by that column. Sorting can serve as a simple ranking system for your probes, favoring a specific statistic. Note that some statistics, such as CPU load and memory statistics, only reflect the utilization on your local system. From this dashboard tab you can also use the right-click menu to start or stop a probe and change settings or administer the probe.

**Customizing toolbars**

You can customize your Observer toolbars, which allows you to quickly move between tools without the need to navigate the menu system. To start a configuration session, select **View > Toolbar Setup**. The Customize dialog appears, allowing you to customize which items are shown.

Also, to move buttons from the main Observer display, hold the Shift key and drag and drop a button to a desired location. To delete a button, drag the button from the toolbar while holding the Shift key and drop it anywhere except on a toolbar.
Ports used by Network Instruments products

Firewalls are necessary for any network. These specific ports must be open to allow Network Instruments products can communicate with each other.

Network Instruments generally recommends that you open inbound and outbound TCP/UDP 25901 through 25905 on your firewalls for its products. This table lists more specifically what ports are used by your product.

<table>
<thead>
<tr>
<th>Ports</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 25901</td>
<td>Observer expert and trending data</td>
</tr>
<tr>
<td></td>
<td>Observer Reporting Server to Observer/GigaStor/Probe</td>
</tr>
<tr>
<td>TCP 25903</td>
<td>Observer/GigaStor/Probe redirection/connection request</td>
</tr>
<tr>
<td></td>
<td>GigaStor/Probe administration</td>
</tr>
</tbody>
</table>

Configuring Observer’s general settings

The Observer General Options window allows you to configure the general settings for Observer. These include general configuration options, e-mail and pager options, folder settings, and more. To configure Observer’s general settings, select **Options > Observer General Options**.

General tab

This tab allows you to set how the analyzer functions. Preferences you can set on this tab include:

- Whether Observer asks for confirmation before doing certain things
- What application certain file extensions are association with
- Whether any features are disabled
- Several display and formatting options
- Several startup and runtime options

One option of note is: Enable port control via command line on Gen2 (xxxGig2010) capture cards. This option is only available for 1 Gb, 10 Gb, or 40 Gb Gen2 capture cards released with version 15 or later. It will not work for any Gen2 capture cards in probes purchased prior to version 15 and later upgraded to version 15. The command line usage and options are:

```
NiDecodeApi.exe -VIRTADAPTER=C;V;;P:
```

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Sets the ports for the Gen2 capture card to be on or off from a command line using NiDecodeApi.exe -VIRTADAPTER. Parameters must be separated by a semi-colon (;).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>C: Specifies that the Gen2 capture card is a either a 1, 10, or 40 Gb capture card. The options are:</td>
</tr>
<tr>
<td></td>
<td>C:oneGig2010</td>
</tr>
<tr>
<td></td>
<td>C:tenGig2010</td>
</tr>
<tr>
<td></td>
<td>C:fortyGig2010</td>
</tr>
<tr>
<td></td>
<td>V: Specifies the virtual port adapter number. The Gen2 card supports up to four virtual adapters. You may only specify one virtual adapter at a time.</td>
</tr>
<tr>
<td></td>
<td>V:1</td>
</tr>
</tbody>
</table>
V:2
V:3
V:4

P: Specifies whether a port is on or off for a given virtual adapter. The Gen2 card has up to 12 ports.
0=off
1=on

Ports can be partially filled. For instance:
P;; means all ports are off.
P:1; means port 1 is on and all others are off.
P:0001; means ports 1, 2, and 3 are off and port 4 is on. If the Gen2 card has more than four ports, any ports beyond 4 are also off.

Use
NiDecodeApi.exe -VIRTADAPTER=C:oneGig2010;V:1;P:1111
NiDecodeApi.exe -VIRTADAPTER=C:tenGig2010;V:3;P:01010101
NiDecodeApi.exe -VIRTADAPTER=C:fortyGig2010;V:2;P:11110101

Security tab

There are several options available to you to tighten access to the Observer analyzer. Many of the options are used in conjunction with NIMS, but some can be used by the Observer analyzer by itself.

To view and change the security settings for an Observer analyzer, in the Observer analyzer choose Options > Observer General Options > Security tab. Use the information in Table 2 on page 13 to configure the analyzer’s security and NIMS options.

Table 2: Security options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Observer Login</td>
<td>When enabled, this option forces a user to provide a user name and password to open the Observer analyzer. The user name can be stored locally if you are not using NIMS, or maintained by NIMS if the “Authenticate Observer login with NIMS” option is enabled. This option is not visible unless you have a special license enabling it. <strong>Caution:</strong> Do not lose this password! There is no way to recover a lost administrative password. Observer Login Credentials—Type a user name and password. This information is encrypted and stored locally. Only one user account is allowed per system. If you want numerous people to have access to the Observer analyzer with different user accounts, you must use NIMS. Administrative Credentials—A local administrative user account that allows you to create a non-administrator account and to set security options for NIMS.</td>
</tr>
<tr>
<td>Use Observer Encryption Key file for secure connections</td>
<td>Strong encryption is available for Observer Expert and Suite users. Observer Encryption Key (.OEK) files let you use private encryption keys to ensure that unauthorized persons do not have access to the data flowing between Observer analyzers and probes. To use Observer Encryption Key files, you must copy the encryption key file into the installation directory (usually C:\Program Files\Observer) of each probe or analyzer that you want to authorize. To generate a key file, click the</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>“Launch Encryption Key Generator” button. Its online help explains its use and how to set up the keys it generates. Each analyzer and each probe must have the .oek file. Observer encryption keys are required if you want to use NIMS.</td>
<td>Authenticate users (for redirected Probe instances)</td>
</tr>
<tr>
<td>Forces users to authenticate with NIMS before using remote probes. User accounts belong to user groups in NIMS and through the user group’s access to probe instances can be granted or restricted. Only probe instances to which the user has access will be visible in the analyzer. This option does not control whether users can open Observer. That is done through the “Authenticate Observer login with NIMS” option.</td>
<td>Manage Observer /Probe license with NIMS</td>
</tr>
<tr>
<td>An Observer or probe license can be stored and managed locally at each analyzer or probe, or it can be managed centrally by NIMS. If unchecked, it is managed locally and you must provide a license for each analyzer/probe. If selected, then you can provide a pool of licenses in NIMS and the analyzer or probe will take an available license when the analyzer or probe starts.</td>
<td>Get list of Probe Instances available for redirection from NIMS</td>
</tr>
<tr>
<td>When selected all probe instances to which you the user has access to through group permissions set in NIMS are available when connecting to a probe. When unchecked only the local probe instances are available and no probe instances are listed when connecting to a remote probe.</td>
<td>Share filters with NIMS</td>
</tr>
<tr>
<td>When selected you may create filters and share them with others. You may also get any filters created by others. Whenever a filter is updated, other users can be informed and update their local version. The list is maintained by NIMS.</td>
<td>Synchronize user protocol definitions through NIMS</td>
</tr>
<tr>
<td>When selected you synchronize protocol definitions, including any derived applications definitions, automatically through NIMS. If any protocol definitions are updated in another analyzer, you automatically receive those. If a protocol definition is updated in one analyzer, it is published to NIMS and NIMS pushes that new definition to all analyzers that choose to synchronize their protocol definitions. Extra caution should be used with this setting because definitions are automatically propagated to all analyzers (assuming the setting is selected in Observer). If two users are updating the same protocol definition, the last user to save and close the window is whose definition is used. Only one user (or a small select group of users) should be responsible for maintaining the list of protocol definitions. This ensures that no inadvertent changes are made.</td>
<td>Primary/Secondary server</td>
</tr>
<tr>
<td>Provide the IP address of the primary NIMS server. If you are also using a failover NIMS server, type its IP address in the Secondary server box.</td>
<td>Allowed to modify shared filters</td>
</tr>
<tr>
<td>When selected, you can get a shared filter from someone else, modify it locally, then upload your modified version to NIMS thereby making your new version available to everyone else. When disabled, you can only get filters from NIMS and upload your own. You cannot modify any filters you get from NIMS. This option requires that you have the ability to share filters with NIMS.</td>
<td>Authenticate Observer login with NIMS</td>
</tr>
<tr>
<td>This option works in conjunction with the “Require Observer Login” option. This forces Observer to use NIMS to authenticate users rather than Observer’s local user list. A user list is maintained in NIMS.</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Require a password to change partial packet capture size</td>
<td>Select this option if you want to require someone to provide a password before they may change the partial packet capture size. This is a central password and all users must use the same password.</td>
</tr>
<tr>
<td>Launch Encryption Key Generator</td>
<td>Click this button to open the Network Instruments encryption key generator. If you want the GigaStor payload to be encrypted using 256 bit AES encryption before it is stored, select the “Encrypt GigaStor network traffic…” option. An encryption key is needed on the GigaStor (or a location accessible by the GigaStor) to encrypt and decrypt the data. The AES key is not needed on workstations, probes, or other collection points. A special license is required for this feature. Contact Network Instruments for this license.</td>
</tr>
</tbody>
</table>

**Folders tab**

This tab allows you set the directories that hold Observer data. In most cases, the defaults are fine. We do not recommend pointing to networked directories or mapped drives.

<table>
<thead>
<tr>
<th>Network Trending Folder</th>
<th>The location for Observer to store Network Trending data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Trending viewer data size</td>
<td>The maximum amount of memory to use when loading trending data in the network trending viewer. If the data exceeds the specified memory limit, an error message is displayed.</td>
</tr>
<tr>
<td>Folder for saving network packets to a file while capturing</td>
<td>The location for packet captures. Automatically generated files will be stored here; this will also be the default directory for manual packet capture saves.</td>
</tr>
<tr>
<td>SNMP Trending Folder</td>
<td>The location for Observer Suite to store SNMP Trending data.</td>
</tr>
<tr>
<td>Write SNMP Trending data to disk every x minutes</td>
<td>Allows you to set the number of minutes the system will wait before writing trended SNMP data to disk.</td>
</tr>
<tr>
<td>Compiled SNMP MIB folder</td>
<td>The location for Observer to store and access compiled SNMP Management Information Base (MIB) files. The default is C:\Program Files\Observer\SNMP. We do not recommend changing this unless you have a specific reason to do so. When you change the MIBs or requests directory, any currently installed MIBs (or requests) will become inaccessible to the SNMP Management Console and its supporting utilities. If you change these directories, you will need to move the files in the existing directories to the new location. All executable files in the SNMP Management Console package use these definitions to find installed MIBs and requests.</td>
</tr>
<tr>
<td>SNMP Requests folder</td>
<td>Allows you to define the path to the directory where SNMP Management Console should look for compiled request files. The default is C:\Program Files\Observer\SNMP.</td>
</tr>
</tbody>
</table>

**SNMP tab**

This tab will not be active unless you have purchased a licensed copy of Observer Suite. After installation, the SNMP Management Console will generally require little, if any, configuration before it can be used.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop MIB compilation upon error in MIB source file</td>
<td>If you want Observer to complete the compilation even though the source file contains errors, leave the box unchecked.</td>
</tr>
<tr>
<td>Use as MIB source editor</td>
<td>Allows you to enter the program you wish to use to edit MIB source files. The default is Microsoft Windows Notepad, although any editor capable of saving a plain text file will do.</td>
</tr>
<tr>
<td>Default SNMP version</td>
<td>Allows you to select the default version of SNMP to use for new agents. You may also override this in the Agent Properties dialog.</td>
</tr>
<tr>
<td>Request time-out period (sec)</td>
<td>Allows you to set the number of seconds that SNMP Management Console will wait for an agent to respond before resending a request.</td>
</tr>
<tr>
<td>Request retry count</td>
<td>Allows you to define how many times SNMP Management Console will re-send a request to an agent before timing out.</td>
</tr>
<tr>
<td>Max data buffer (x100K) for running charts</td>
<td>Allows you to define how much memory will be made available for SNMP Management Console’s chart display. The more memory made available, the more data points the chart display will be able to show. Memory saved for the SNMP Management Console’s chart display; however, will not be available for other programs or purposes.</td>
</tr>
<tr>
<td>Max allowed RMON objects in MIB Walk</td>
<td>Allows you to set the maximum number of RMON objects to appear and/or be processed during a MIB Walk. The default value is 9999.</td>
</tr>
<tr>
<td>Repeat alarm notifications</td>
<td>Allows you to select the number of times that Observer should send out SNMP-related alarms when the alarm has been triggered.</td>
</tr>
<tr>
<td>Repeat trap notifications</td>
<td>Allows you to select how many times to repeat trap notifications. While, in practice, the vast majority of notifications sent via UDP will reach their destination, the UDP protocol, which is specified by the SNMP RFC for trap notification, does not require or permit packets being acknowledged by the receiving station. It is simply a matter of sound practice to repeat trap notifications several times.</td>
</tr>
</tbody>
</table>

**IPv6 tab**

IPv6 is fully and natively supported in Observer.

This tab configures Observer to display actual IPv6 addresses when sensed, rather than their IPv4-compatible representation. This affects all statistical displays that show IP addresses in an IPv6 environment. You can also choose how to represent these addresses.

- **Compressed hexadecimal** represents the address as native IPv6 (i.e. each of the eight 16-bit portions of the address are specified), but with the 0000 portions of the address replaced by double colons (:). For example: FE80::254E:F35D:7DB4:11

- **Not compressed hexadecimal** represents the address as native IPv6 (i.e. each of the eight 16-bit portions of the address are specified), including the 0000 portions. For example: FE80:0000:0000:0000:254E:F35D:7DB4:0011

- **The IPv4 compatible formats** represent the address as x:x:x:x:x:d.d.d.d, where the x’s are the 16-bit left-most portions of the IPv6 address, and the d’s are four 8-bit (IPv4-style) decimal values derived from the last two portions of the 16-bit IPv6 address. An example of the **compressed form** is FE80::254E:F35D:125.180.0.17. In uncompressed format, it would be FE80:0000:0000:0000:254E:F35D:125.180.0.17
Third Party Decoder tab

**Prerequisite:** Observer Expert or Observer Suite

This tab allows you to specify a third party decoder, which can be installed anywhere on the same system as Observer, to use when loading saved packet captures. By enabling this option, a new menu option is available: File > Decode Capture File using Wireshark. Some third party packet analyzers can decode some things that Observer cannot. You can use Observer to capture the traffic and use the third party decoder to analyze it. Additionally, if you want to use a third party decoder to look at the same packet capture and compare the results side-by-side, you can now launch the decoder from within Observer.

<table>
<thead>
<tr>
<th>Assign menu name</th>
<th>Defines the menu option that appears under the File menu. It defaults to “Decode Capture File using Wireshark,” but this menu item can be anything you want.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executable name</td>
<td>Provide the full path to the third party application you want to use to decode capture files. The decoder must be installed on the same system as the Observer analyzer, not the probe.</td>
</tr>
<tr>
<td>Command line</td>
<td>Provide any command line options you want to pass to the third party decoder when you are opening the application.</td>
</tr>
<tr>
<td>Capture buffer format</td>
<td>Choose which file format to export your capture to: Observer’s native BFR format or PCAP. See Saving packet captures on page 63.</td>
</tr>
</tbody>
</table>

**GeoIP Settings**

There may be times when you want to know more about an IP address you are seeing in Observer. Using an external geolocation service, you can more easily find out information such as the IP’s carrier or service provider and the city, state, and country where the IP address is located in the world. This information could be valuable in identifying the source of a security threat, malicious communication, or a simply misconfigured system somewhere in the world impacting your organization.

This tab allows you to define a URL that is called and opened in a web browser. By default the geolocation service of the GeoIP website is used, but you may change this to any geolocation service you wish.

You can look up the geolocation information for an IP address when you are on the Decode and Analysis tab in Observer or when you are on the IP Stations tab in the GigaStor Control Panel. For instance, click the Top Talkers tab, select an IP address, right-click and choose **Connect to the Selected Station via > GeoIP Lookup**.

**Related Topics**

- Building and saving an address book on page 36
- Configuring and using alarms on page 115
- Viewing bandwidth utilization on page 24
- Discovering current top talkers on the network on page 25
- Discovering conversations between local devices and the Internet on page 19
- Viewing a list of protocols seen on the network on page 22
- Viewing router utilization statistics on page 23
- Viewing network errors on page 28
- Viewing network errors by device on page 29
- Capturing network traffic on page 59
- Pre-filtering your packet captures on page 66
- Preparing expert decoding techniques on page 93
Using the Expert Analysis feature on page 94
Using Connection Dynamics on page 98
Using Server Analysis on page 101
Using “What-if” modeling on page 102
Using MultiHop Analysis on page 105
Analyzing VoIP or video conferencing traffic on page 167
Introduction to SNMP on page 182
Administrating Observer reports on page 122
Configuring SNMP agents on page 188
Using the MIB editor on page 191
Using the MIB Walker on page 208
Discovering which devices are connected to a switch on page 41
Viewing reports in a web browser on page 122
Creating or modifying Observer and GigaStor reports on page 129
Using the probe as a virtual TAP on page 257
Installing the wireless NIC driver on Windows 7/Vista on page 229
Upgrading the probe software directly on page 231
Chapter 2: Real-Time Statistics

Monitoring connection statistics

Real-time statistics can aid you in more ways than just determining network health—they can provide information about the connections seen on the network. This section describes several Observer tools to help you oversee how devices are communicating over the network.

Discovering conversations between local devices and the Internet

To discover conversations between local network devices and the Internet, use the Internet Observer tool. To reveal it, choose Statistics > Internet Observer.

The Internet Observer tool has three distinct tabs:

- Internet Patrol—Internet Patrol permits you to examine established connections between local devices (e.g. stations) and the greater Internet.
- IP Pairs (Matrix)—Similar to Internet Patrol, the IP Pairs (Matrix) permits you to examine established connections between local devices (e.g. stations) and the greater Internet.
- IP Subprotocols—IP Subprotocols displays network traffic flow categorized by subprotocol, such as HTTP or SMTP.

Each tab of the Internet Observer tool can be customized. Specifically, you can change the layout of the in-focus tab by clicking View and selecting another. To make further customizations to each view, click the Settings button and a window appears.
The Statistics Settings tab of the Internet Observer Settings window is its most important tab. Notably, you can specify a specific TCP or UDP port to observe if desirable, and you can also configure which subprotocols are recognized by clicking Configure IP Application List.

Changes made to the Statistics Settings tab are saved and shared by all modes (tabs) of the Internet Observer tool; however, changes made to any layout view (list, pair circle, etc.) are saved and used independently.

**Internet Patrol tab**

Internet Patrol displays MAC address to layer 3 IP address traffic. If the MAC address has an alias assigned, this text will be displayed instead of the true MAC address. Additionally, the IP addresses of the destination sites will be resolved using DNS. This view of your Internet traffic is most appropriate for local network traffic to and from the Internet, and for sites that use DHCP. Since DHCP changes IP addresses frequently, source IP addresses are not useful on DHCP sites for identification.

**IP Subprotocols tab**

IP Subprotocols display layer 3 IP addresses traffic flow broken-down by subprotocol. Subprotocols are defined in the setup dialog. Twenty-four (24) user-defined subprotocols can be created. Other indicates a protocol that did not match the criteria of the twenty-four user-defined protocols.

**Configuring the IP application list**

Clicking the Configure IP Application List buttons displays the subprotocols and allows you to add a new one, change an existing one, or remove an existing one.

1. To edit or add a protocol, click the Edit or New button.
2. The Configure IP Application Ports dialog is displayed.
3. If you are editing a protocol, the protocol you selected on the List of IP SubProtocols will be displayed in the IP Application box. The information in this box is editable.
4. If you are adding a protocol, enter the desired name of the SubProtocol in the box. You can have a total of 24 subprotocols in your list of IP SubProtocols.

5. Choose either Add TCP or Add UDP, and another dialog is displayed that lets you define a port or range of ports for the IP application. The maximum is five ports. A range of ports counts as two ports. In other words, you can define one range and three ports, or two ranges and one port. You cannot assign three ranges.

6. Click OK to display the List of IP SubProtocols dialog.

Discovering conversations between local devices

To discover conversations between local network devices, choose Statistics > Pair Statistics. This reveals the Pair Statistics tool, which tracks established connection between local devices. Observer recognizes each of these conversations to be a **station pair**.

Click the Start button to activate the tool, or click Settings for more configuration options. To view a different layout, click the View button and select another.

Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.

Many statistics are kept for each pair, including the packets and bytes in each direction, and the latency for each direction. Latency can further be configured to be ignored after a certain number of milliseconds. Latency configuration will make Observer only track packets that are part of a true conversation flow.

Over a few hours, you will find that almost every station on your segment will have some sort of conversation with every other station. This is why Observer provides the ability to zoom in on a specific conversation on the top of your display. This will make watching one conversation amongst many hundreds much easier. To zoom in, highlight the pair you are interested in and it will be displayed on the top of the Pair dialog.

In Pair Circle view, the thickness of each line represents the amount of data flowing between the stations, and the thickness grows in a logarithmic pattern.

**Viewing real-time statistics per device**

To view real-time statistics of individual stations, choose **Statistics > Web Observer**. This reveals the Web Observer tool, which focuses on HTTP traffic (port 80)—or all traffic if desired—to and from an individual station.

At least one station must be configured before Web Observer can be activated. To configure a station, click the Settings button and select an address to monitor. Click OK, and click Start to activate. As always, you can change your layout by clicking View and selecting something else.

Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.

Web Observer can be configured to show additional individual stations—you are not limited to viewing one station at a time. To view the real-time statistics of individual stations in bulk, simply configure more stations in Web Observer.

To do this, right-click the row of empty tabs near the lower, leftmost portion of the Web Observer window, and select Create Web Observer Window.

**Figure 4:** Right-click and create more windows
Viewing a list of protocols seen on the network

The Protocol Distribution tool tracks how data is being distributed across the network. Viewing protocols can give you an idea of which servers and applications are being used and if there are any unknown or misconfigured protocols on your network.

To view a list of protocols seen on the network, choose **Statistics > Protocol Distribution**.

Click the Start button to activate the tool, or click Settings for more configuration options. Right-click results to navigate to a list of stations using a particular protocol.

You can have a maximum number of the following for each: 512 for UDP and TCP subprotocols, and 512 for major protocols.

To view a different layout, click the View button and select another.

Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.

Viewing wireless access point statistics

To view wireless access point statistics, choose **Statistics > Wireless Access Point Statistics**. This reveals the Wireless Access Point Statistics tool, which shows network traffic passing through any access points visible to the Observer wireless NIC.

Wireless Access Point Statistics is only available using a supported Network Instruments wireless driver.

The Access Point Statistics mode shows traffic passing through any Access Points (APs) visible to the Observer wireless NIC.

This mode is an all-purpose tool for maintaining performance and security on a WLAN that uses APs, showing you:

- Wireless stations that are connected to an AP
- Non-wired stations that they communicate with
- Levels of signal strength, quality, data/non-data transfer rates for each station on the access point
- AP traffic totals

For example, you can immediately see if there is a station connected to the wrong AP, or if an unauthorized AP has been installed. AP statistics will display whether a station has a problem with quality or range of connection based on the number of reassociations and retransmissions, or whether a station is misconfigured based on station poll totals.

There are two Access Point Statistics tabs. The Cumulative tab shows running totals of statistics collected since the mode was started; the Latest/Min/Max tab shows the most recent, the minimum, and the maximum values for access point statistics.

1. Choose **Statistics > Wireless Access Point Statistics**.
2. Click the Settings button.

After completing this task:

Click the tab that you want to use to configure how the pair circle or list appears.
Monitoring network load

Network congestion can be caused by numerous factors, and many can affect the network simultaneously. The greatest contributing factor of network congestion is sustained high network load—times when bandwidth is fully allotted.

This section describes several Observer tools for monitoring network load, which may help you find bottlenecks in your network.

Viewing router utilization statistics

To view real-time router utilization statistics, choose Statistics > Router Observer. This reveals the Router Observer tool, which allows you to monitor one or more routers’ utilization rates. Observation is done passively; the router is not performing extra work.

Router Observer is suitable for searching for failing or over-stressed routers, and it can determine whether the source of demanding packets is incoming or outgoing (or both).

At least one router must be configured before Router Observer can be activated. To configure a router, click the Settings button and select an address to monitor.

Be sure to select the address of a port, on your router, that is visible to the Observer analyzer. For example, no results are seen by selecting an outside interface, as the MAC address is not visible.

You must specify the router speed before continuing. Type the speed and click OK. Now click Start to activate. As always, you can change your layout by clicking View and selecting something else.

Results can be saved in a comma delimited file using File > Save > Save Data in Comma Delimited Format.

Figure 5: Setting the known speed of a router

The top status bar shows router speed and IP address. In Graph view, dials show packets per second, bytes per second, and the current utilization. When you receive user complaints that the network is slow, check the 1 minute, 1 hour, and total bandwidth utilization averages. You can tell whether a bandwidth problem is temporary or persistent. Each listing also shows values by direction (in or out of the router).

After completing this task:

Router Observer can be configured to show additional routers—you are not limited to viewing just one router. So, to view the real-time statistics of routers in bulk, simply configure more routers in Router Observer.

To do this, right-click the row of empty tabs near the lower, leftmost portion of the Router Observer window, and click Create Router Observer Window.

Figure 6: Right-click and create more windows
**Viewing bandwidth utilization**

To view real-time bandwidth utilization as seen by a probe instance, choose **Statistics > Bandwidth Utilization**. This reveals the Bandwidth Utilization tool, which calculates utilization by how many bytes are seen over a one-second interval. If you are monitoring multiple ports (which the tool displays if true), the results are averaged.

The Bandwidth Utilization tool automatically activates. Click the View button to choose a different layout, or click Settings to further customize said layouts.

The Bandwidth Utilization tool is only accurate when the network adapter speed is set correctly in Observer. To do this, choose Options > Selected Probe or SNMP Device Properties, and click the Adapter Speed tab.

Adapter speed is automatically determined by Observer. If necessary, you can manually set the network adapter speed—choose Options > Selected Probe or SNMP Device Properties, and click the Adapter Speed tab.

Changing the network adapter speed only affects Observer’s understanding of the adapter on that probe instance; no actual changes are made to the speed of your network adapter.

Bandwidth utilization is calculated by recording the number of bytes seen by the Observer (or probe) station. By running the mode at different times under typical network load, you can get an idea of what “normal” utilization is for your network. Knowing what is normal for your network is key to understanding any analyzer statistical modes and putting them in context. After you understand and recognize what is normal for your network, you can easily spot the anomalies if and when they occur.

**Viewing bandwidth utilization with a filter**

Bandwidth Utilization with Filter offers the same features and functionality as the Bandwidth Utilization tool; however, only filtered data appears. If you have multiple filters applied, they are applied with a logical OR expression.

To view real-time bandwidth utilization as seen by a probe instance and with one or more filters applied, choose **Statistics > Bandwidth Utilization with Filter**.

Bandwidth utilization is calculated by recording the number of bytes seen by the Observer (or probe) station. By running the mode at different times under typical network load, you can get an idea of what “normal” utilization is for your network. Knowing what is normal for your network is key to understanding any analyzer statistical modes and putting them in context. After you understand and recognize what is normal for your network, you can easily spot the anomalies if and when they occur.

**Wireless Access Point Load Monitor**

Shows wireless Access Points utilization rates. Available only when the current probe (or probe instance) is capturing packets from a wireless network interface. Note that for Observer to accurately assess utilization rates, you must enter the correct bandwidth speed in the Settings dialog.

The Wireless Access Points Load Monitor lets you look at an access point in real-time to see its utilization rate. You can create a tab for each access point, allowing you to easily click between them. You can quickly find out if an access point is acting as a bottleneck and, if so, whether the source of the packets clogging the AP are incoming or outgoing (or both). By examining historical information you can tell whether this is a chronic problem, which might indicate the need for a faster connection, or an acute problem, which might indicate a failure of some sort. Observer does this passively; therefore, the Access Point is not affected.

**Tip!** Right-click any tab at the bottom of the Load Monitor window to select an access point to set up and monitor. You can then view any access point by simply clicking on its tab.

2. Click the Settings button to configure the wireless access point.

3. Select an AP from the list. This list is read from your address/alias list. If no routers are displayed, use Discover Network Names to scan your network and populate the list. See Building an address book automatically for more details.

4. In the Access Point speed (Bits/second), type the throughput speed for the wireless device. Typically, assuming theoretical maximums, this will be 300000000 for 802.11n (two-streams), 54000000 for 802.11a/g access points or 11000000 for 802.11b access points.

Dials provide a heads-up immediate display of packets/second, bits/second, and interface utilization.

### Viewing the distribution of packet sizes by station

Observer makes it easy to see what protocols are being used on your network, and what devices are using them. For example, you can see if printers are sending packets out to non-existent devices or routers are broadcasting in protocols that no other devices understand; these are just two examples of misconfigured devices that could be wasting bandwidth on your network.

To view the distribution of packet sizes by station, choose **Statistics > Size Distribution Statistics**. This reveals the Size Distribution Statistics tool, which shows stations’ traffic patterns (subject to filter criteria) sortable by packet size.

You can collapse or expand the tree’s subprotocol branches. The statistics are derived from the raw bytes and utilization percentages for each protocol and subprotocol. Search for any protocols that should not be running on your network, or discover if an expected protocol is generating an unexpected amount of traffic, which may indicate a hardware or configuration problem.

By right-clicking the display, you can jump immediately to a list of stations generating the selected protocol.

### Discovering current top talkers on the network

Observer’s Top Talkers tool lets you see who is using the most network bandwidth, which can show whether a particular user, station, or application is consuming excessive network bandwidth. View LAN use patterns, detect faulty network hardware, and determine what percentage of the network’s bandwidth potential each system is using, all from one comprehensive window.

If you are considering implementing a switch, the information gathered by the Top Talkers tool can help divide stations effectively for your switch.

To discover current top talkers on the network, choose **Statistics > Top Talkers Statistics**, and click Start to begin to tool. Observer then displays a tree of protocols and subprotocols seen on your network.

In Observer, top talkers are defined as stations or devices that process more packets per second than others during an observed period of time.

Top talker statistics are relative; for example, an active station may appear especially “chatty” during times when other stations are idle.

To immediately identify the stations using the most bandwidth, sort by %Bytes, which is done by clicking that column heading. You can determine whether systems generating the most traffic are servers (which probably means everything is OK) or user workstations (which could indicate a hardware problem or unauthorized use of a computer).

You can start a packet capture on any of the listed addresses by right-clicking that entry. The right-click menu also allows you to list the protocols generated by the selected station.
Load testing the network

Sometimes network problems only appear under peak load conditions. Instead of waiting for those conditions to occur naturally, create them yourself by using the traffic generator tool at Tools > Traffic Generator. Doing so helps reveal problems in your network.

Specifically, the traffic generator tool allows you to load test (stress) your network by generating packets of a certain type and size, at the frequency you specify, sent toward a specific device or device group.

When generating traffic it is best to view the generated traffic, including results, from a station separate from the Observer station generating the traffic.

The network adapter must be capable of generating sufficient traffic to heavily load the network. For example, a 100 megabit NIC cannot use more than 10% of a 1 Gb network’s bandwidth.

Be careful when generating traffic. Generating too much traffic can slow down the network. This is especially true using the broadcast destination (default), as packets are sent to every switch port of every switch in the broadcast domain. Be aware of what you are doing, and perhaps notify your users of possible downtime.

Configuring your load test settings

The traffic generator tool is located at Tools > Traffic Generator. Several noteworthy settings can be configured directly in the tool, and they are described in Table 3 on page 26.

The Network Instruments Gen2 capture cards do not allow the generation of network traffic using this tool.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet size</td>
<td>Allows you to define the size of the packets to be generated.</td>
</tr>
<tr>
<td>Allow jumbo frames</td>
<td>Allows packet sizes to be set greater than the conventional maximum of your network type. This change is reflected in the packet size setting. Ensure the network card driver generating the traffic is also configured to support jumbo frames.</td>
</tr>
<tr>
<td>Requested utilization</td>
<td>If selected, the traffic generator attempts to generate packets at a fast enough rate to meet the requested bandwidth utilization. An error is displayed if the requested utilization cannot be fulfilled.</td>
</tr>
<tr>
<td>Generate sequential source MACs</td>
<td>If selected, the tool generates packets with MAC source addresses in a sequence, up to the number of addresses specified. If generating more packets than the number of addresses in the sequence, the traffic generator restarts the address sequence from the beginning. The start of the sequence is defined in the Edit Header dialog’s Source MAC Address field.</td>
</tr>
<tr>
<td>Generate sequential destination MACs</td>
<td>If selected, the tool generates packets with MAC destination addresses in a sequence, up to the number of addresses specified. If generating more packets than the number of addresses in the sequence, the traffic generator restarts the address sequence from the beginning. The start of the sequence is defined in the Edit Header dialog’s Destination MAC Address field.</td>
</tr>
</tbody>
</table>

You can also right-click anywhere in the Generated Packet Header area to reveal the following options:
Load Packet From File—displays the Load Packet dialog, letting you load a particular packet number from a particular buffer file.

Save Packet to File—lets you save the currently configured packet to a standard Observer capture file.

Open Packet in Decode—shows currently formed packet in Observer’s packet capture decode window.

Viewing utilization history

The Utilization History tool ignores any filters applied to the probe instance. This means the utilization shown is not affected by filters, which ensures the utilization history you see is always accurate.

**Note:** Bandwidth Utilization—a separate Observer tool—may serve as a substitute if you need to see utilization that adheres to your probe instance’s filters. For details, see Viewing bandwidth utilization with a filter on page 24.

To view short-term utilization history of the network, choose **Statistics > Utilization History**. For viewing utilization history over a longer period, we recommend using network trending features instead; see Network Trending on page 146.

Click the View button to choose a different layout, or click Settings to further customize said layouts. Most importantly, changes can be made to the update interval of the graph view. Regardless of the graph view’s update interval, sampling is done each second.

Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.

Tell me more about the Utilization History tool

Utilization History displays (and allows for export) longer term information about your bandwidth utilization. The graph shows high, low and average utilization over time—the amount of time is only limited by your computer’s RAM. Sampling is still once a second, but the display can be configured to report at various time intervals.

After the Utilization History graph is displayed, it automatically begins capturing data. The display of the data will depend on how you have setup each item in the Settings dialog. There are three statistics that the display will keep track of: maximum, average, and minimum. Although data points are only shown for the period set in the Settings dialog, data is collected and processed every second, and then averages the data over the configured period (seconds/interval).

Viewing real-time utilization

Utilization Thermometer can be activated from the main window by choosing **Statistics > Utilization Thermometer**. There are no configuration options for the Utilization Thermometer.

The Utilization Thermometer tool displays the current network bandwidth utilization as a percentage of the total theoretical network speed. Additionally, the thermometer shows a running one minute and five minute average. These averages are shown on the right of the bandwidth scale as round blue (1 minute) and red (5 minute) balls.

The Utilization Thermometer auto-scales as the utilization percent rises above its own maximum. For example, when the percentage reaches above 100%, it increases its scale. The thermometer will not scale down; you must close and re-launch the tool to return to the default scale.
Viewing a summary of network activity

To view a simple summary of current network activity, choose Statistics > Summary. This reveals the Network Summary tool, which lists packet size distribution, error count, seen protocols, and other general network information.

Click the Start button to activate the tool, or click Settings for more configuration options. Since this tool is basic, the only configurable option is to enable or disable the use of your current filter.

Results can be saved in a comma delimited file using File > Save > Save Data in Comma Delimited Format.

Checking the health of your network

Network health is difficult to measure and usually relies on your judgment as a network administrator. This section describes several Observer tools to help you make meaningful measurements.

Viewing network errors

Observer’s Network Vital Signs tool informs you at a glance as to network error conditions and their severity, with respect to traffic conditions, by combining graphical shapes with specific color codes.

To view network vital signs—i.e. error occurrences—choose Statistics > Vital Signs. This reveals the Vital Signs tool, which gives you a complete snapshot of errors witnessed during current network activity.

Click the View button to choose a different layout, or click Settings to further customize said layouts. Most importantly, changes can be made to the update interval of the graph view and to thresholds of the plot view.

Results can be saved in a comma delimited file using File > Save > Save Data in Comma Delimited Format.

If you are using an Ethernet network and are worried that errors may be traversing the network, yet this tool has not detected any, ensure that your NIC’s NDIS driver can indeed recognize errors. To check driver error support, choose Options > Selected Probe or SNMP Device Properties, and click the Parameters tab.

After you are familiar with your network's “signature,” you will be able to immediately notice spikes in utilization and error activity as they occur. If you see an unusual divergence from the typical Vital Signs signature for your network, you can then use Network Errors by Station to pinpoint the source of the anomaly.

Color codes

- Yellow lines anywhere in the display represent an idle condition. In other words, no matter what your display is telling you, activity is so low that the errors are not statistically important.
- Green lines show normal network activity and error counts.
- Red lines indicate error counts out of normal range.
- Red lines are displayed when the following default error counts are encountered. Whenever a red line (i.e. a critical condition) is displayed, all of the formerly green lines turn blue to highlight the network state.
  - Utilization goes over 35%.
  - CRC & packets too small represent more than 25% of the total traffic.
  - Packets too big represent over 1% of total traffic.
- Gray “shadows” show you an image of the reading taken immediately before the current reading.

About Vital Signs’ broadcasting LLC Exploratory packets

Vital Signs sends exploratory LLC packets when running the collision test. When the collision test option is on, Observer bursts 100 exploratory LLC packets per second, addressed to 00:00:FF:FF:FF, and listens for packet collisions. On a 1 Gb network this uses 0.004% of the network’s bandwidth and significantly less on a 10 Gb
Collision testing is generally only run when a collision problem is suspected, although it can be run routinely at your discretion. If you turn off Vital Signs, then Observer will be completely passive and not send any LLC packets.

**Viewing network errors by device**

Network errors can be caused by many factors; hardware failure, slightly incompatible drivers, and even poorly shielded cables may be the culprit.

To discover network errors and their originating source, choose **Statistics > Errors by Station**. Click the Start button to activate the tool, or click Settings for more configuration options. Finally, click View to select a different layout. Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.

**Searching for wireless interference**

The Wireless Site Survey tool displays activity by channels on your wireless network, detailed activity on the WLAN by channel, and allows you to search for wireless (Wi-Fi) interference, including its potential sources.

Wireless Site Survey is only available using a supported Network Instruments wireless driver.

To use the Wireless Site Survey tool—and search for wireless interference—choose **Statistics > Wireless Site Survey**. See Table 4 on page 29 for a list of noteworthy settings.

If you want to scan multiple channels:

- You must set the channels to scan in the Probe or Device Properties dialog, 802.11a/b/g/n Settings.
- When Observer is scanning wireless channels, the other modes (such as Top Talkers, Access Point Statistics) will no longer be able to present a complete view of the network, as Observer’s data sample is limited to the current channel being scanned. Therefore, you should only use the Site Survey by itself.

**Table 4: Wireless interference**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information Tab</td>
<td>This table summarizes essential information about what access points and stations are currently visible to wireless Observer. The status line at the bottom of the display shows all channels currently being scanned, highlighting each channel as it is looked at. Click Scan Setup to change the list of channels to scan.</td>
</tr>
<tr>
<td>Frame Type Tab</td>
<td>This table summarizes frame type totals for wireless data, management, and control packets.</td>
</tr>
<tr>
<td>Control Frames Tab</td>
<td>This table details control frames analyzed, including Power Save Polls, Requests to Send (RTS), Clear to Send (CTS), acknowledge (ACK), and CF (Contention Free) End packets.</td>
</tr>
<tr>
<td>Management Frames Tab</td>
<td>Displays detailed information about wireless management frames, including association requests and responses, reassociation requests and responses, ATIMs (Announcement Traffic Indication Message), and authentication/de-authentications.</td>
</tr>
<tr>
<td>Data Frames Tab</td>
<td>Displays detailed information about data frames on the wireless network.</td>
</tr>
<tr>
<td>Speeds Tab</td>
<td>Shows what stations are either transmitting (or receiving) wireless data at the various supported rates. To switch between transmitting and receiving speeds, click the down arrow next to the Tx (or Rx) and select the desired setting.</td>
</tr>
<tr>
<td>Signal Tab</td>
<td>Displays detailed statistics on wireless signal strength, quality, and data rates being used by stations and APs.</td>
</tr>
</tbody>
</table>
Channel Scan Tab  Shows the channel being tracked along with many statistics.

How Observer calculates wireless signal strength

A few of Observer’s wireless analysis modes display a metric labeled “signal strength,” expressed as percentage of the optimum signal strength. Table 5 on page 30 shows how dB measurements are calculated into signal strength percentage.

Table 5: Wireless signal strength

<table>
<thead>
<tr>
<th>Sensed (dB)</th>
<th>Reported (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3 dB</td>
<td>0%</td>
</tr>
<tr>
<td>4-22 dB</td>
<td>1%</td>
</tr>
<tr>
<td>23 dB</td>
<td>5%</td>
</tr>
<tr>
<td>24 dB</td>
<td>10%</td>
</tr>
<tr>
<td>25 dB</td>
<td>12%</td>
</tr>
<tr>
<td>26 dB</td>
<td>14%</td>
</tr>
<tr>
<td>27 dB</td>
<td>16%</td>
</tr>
<tr>
<td>28 dB</td>
<td>18%</td>
</tr>
<tr>
<td>29 dB</td>
<td>20%</td>
</tr>
<tr>
<td>30 dB</td>
<td>22%</td>
</tr>
<tr>
<td>31 dB</td>
<td>24%</td>
</tr>
<tr>
<td>32 dB</td>
<td>26%</td>
</tr>
<tr>
<td>33 dB</td>
<td>28%</td>
</tr>
<tr>
<td>34 dB</td>
<td>30%</td>
</tr>
<tr>
<td>35 dB</td>
<td>34%</td>
</tr>
<tr>
<td>36 dB</td>
<td>38%</td>
</tr>
<tr>
<td>37 dB</td>
<td>42%</td>
</tr>
<tr>
<td>38 dB</td>
<td>46%</td>
</tr>
<tr>
<td>39 dB</td>
<td>50%</td>
</tr>
<tr>
<td>40 dB</td>
<td>52%</td>
</tr>
<tr>
<td>41 dB</td>
<td>54%</td>
</tr>
<tr>
<td>42 dB</td>
<td>56%</td>
</tr>
<tr>
<td>43 dB</td>
<td>58%</td>
</tr>
<tr>
<td>44 dB</td>
<td>60%</td>
</tr>
<tr>
<td>45 dB</td>
<td>62%</td>
</tr>
<tr>
<td>46 dB</td>
<td>64%</td>
</tr>
<tr>
<td>47 dB</td>
<td>66%</td>
</tr>
<tr>
<td>Sensed (dB)</td>
<td>Reported (%)</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>48 dB</td>
<td>68%</td>
</tr>
<tr>
<td>49 dB</td>
<td>70%</td>
</tr>
<tr>
<td>50 dB</td>
<td>73%</td>
</tr>
<tr>
<td>51 dB</td>
<td>75%</td>
</tr>
<tr>
<td>52 dB</td>
<td>78%</td>
</tr>
<tr>
<td>53 dB</td>
<td>80%</td>
</tr>
<tr>
<td>54 dB</td>
<td>83%</td>
</tr>
<tr>
<td>55 dB</td>
<td>85%</td>
</tr>
<tr>
<td>56 dB</td>
<td>88%</td>
</tr>
<tr>
<td>57 dB</td>
<td>90%</td>
</tr>
<tr>
<td>58 dB</td>
<td>92%</td>
</tr>
<tr>
<td>59 dB</td>
<td>93%</td>
</tr>
<tr>
<td>60 dB</td>
<td>95%</td>
</tr>
<tr>
<td>61 dB</td>
<td>97%</td>
</tr>
<tr>
<td>62 dB</td>
<td>98%</td>
</tr>
<tr>
<td>63 dB</td>
<td>99%</td>
</tr>
<tr>
<td>64-257 dB</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Ethernet errors tracked by Observer**

Observer tracks many Ethernet errors, including alignment errors, CRC errors, collisions, runts, and jabbers.

**Alignment Errors**

Ethernet Alignment errors are detected when a packet is not “aligned” on a phase boundary. For timing purposes, the network adapter card assembles and sends a “preamble” for Ethernet packets. Then timers on both Ethernet adapters (sending and receiving) synchronize (agree) on phase timing, and calculate a phase position to begin the actual packet. This phase position is used so that the receiving adapter can know when the packet begins, and how the packet should correspond to the actual signal wave.

Alignment errors can be caused by a number of factors. Typically, they are caused by a previous collision. When a collision occurs, either a CRC error or an Alignment error almost always results. In the case of an Alignment error, if the collision occurs during a transmission after the preamble, the position of the resulting signal with respect to the phase of the wave is incorrect. The receiving adapter acknowledges this, and the packet is discarded.

**MAC Frame CRC Errors**

These CRC errors are the most common, and are what most devices and analyzers are referring to when they claim a CRC error has occurred. Ethernet packets are encapsulated in a MAC frame that contains a preamble, and a post-envelope CRC check. The Ethernet adapter on the sending station is responsible for creation of
the preamble, the insertion of the packet data (addressing, protocol, data, etc.) and then calculating a CRC checksum and inserting this at the end of the packet. The receiving station uses the checksum to make a quick judgment if the packet was received intact. If the checksum is not correct, the packet is assumed to be bogus and is discarded.

MAC frame CRC errors can be caused by a number of factors. Typically they are caused by either faulty cabling, or as the result of a collision. If the cabling connecting an Ethernet Adapter or hub is faulty the electric connection may be on and off many times during a transmission. This “on and off” state can interrupt parts of a transmission, and “damage” the signal.

If a collision happens during packet transmission, the signal for the specific packet will be interrupted, and the resulting received packet will be damaged.

If the signal is interrupted partially during transmission, the CRC checksum that was calculated by the network adapter will no longer be valid and the packet will be flagged as a CRC error and discarded.

CRC errors are common on a busy network, and a small percentage does not reflect a network problem. When the percentage is large, or when a single station shows a larger percent CRC errors there is probably a problem that needs to be addressed.

**Protocol CRC Checksums**

Some protocols (TCP/IP for example), have a second (in addition to the MAC frame CRC checksum) checksum for data integrity purposes. This checksum is calculated on only a portion of the internal data of each packet, and can give a second and independent check for the validity of the packet’s contents. Observer calculates this checksum independent of the MAC layer CRC and displays the results in the decode display.

These CRC errors are very rare and can be caused by malfunctioning software or protocol drivers.

**Collisions**

Collisions happen when two Ethernet adapters send a signal on the Ethernet simultaneously. Ethernet networks operate under a principle known as Carrier Sense, Multiple Access with Collision Detection (CSMA/CD). In a nutshell, this means that a station (prior to sending a packet) listens to the wire for any other traffic (it senses the wire for a carrier), if no other stations are sending, the station may proceed with sending the packet. Otherwise it must wait and repeat the carrier sensing later. During periods of heavy traffic, several stations may be waiting to send data. If two (or more) of these stations carrier sense at the same time, they may each decide that it is O.K. to send. If this occurs, a collision will result. Depending on the timing this may also cause an Alignment error, a CRC error, both or neither. Collisions also become self-perpetuating. As they begin to occur, bandwidth is wasted, and more stations must wait to use the wire, thus causing more collisions.

Collisions are a natural (at reasonable levels) and acceptable part of any Ethernet network and the busier the network, the more collisions you may see. Collisions are acceptable to a point, but after that collisions can bring your network to a virtual standstill.

Collisions are caused by either a faulty network adapter (the “sensor” is failing), or a congested network segment. If the adapter is faulty, replacement is the only option. For a congested network, segmentation is usually the best option.

**Packets Too Small (Runts)**

The Ethernet specification requires that all packets be at least 64 bytes long. 64 bytes is the total length, including checksum. Any packet on the wire that is less than 64 bytes is considered a “Packet Too Small”. Unfortunately, not all vendors adhere to this rule, and many send valid packets smaller than 64 bytes.
Packets Too Big (Jabbers)

The Ethernet specification requires that no packets be larger than 1518 bytes (including checksum). Any packet that is larger than this is flagged as an error and discarded. These packets are also sometimes referred to as “Jabbers”.

Packets too big are almost always caused by faulty hardware. The network adapter card in a station showing a high rate of packets too big should be replaced.

Watching for packet storms

Broadcast and multicast storms can greatly slow the network. To watch for impending broadcast or multicast storms, choose **Statistics > Activity Display**. This reveals the Activity Display tool, which tracks occurrences of broadcast/multicast packets.

Click the View button to choose a different layout, or click Settings to further customize said layouts. Most importantly, changes can be made to the update interval of the graph view and to thresholds of the plot view.

Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.

The indicator lines change color for easy viewing of specific network conditions. If an indicator line is yellow, the Activity Display is showing a network condition that is essentially idle (total net utilization is under 5%). Here, the percentage of broadcast or multicast packets may be high compared to actual traffic. However, because the traffic is so low, this condition is not statistically important.

If an indicator line segment is green, the Activity Display is displaying a normal network condition. If an indicator line segment displays red, the Activity Display is letting you know that a load condition exists. This is not necessarily a problem, but indicates that you should be aware of this condition.

Load conditions can mean different things depending on where the red, blue, or green lines appear. Typically, a red line means that a threshold has been overcome. Blue lines display on the side where the threshold may be an indication of trouble. By default, red lines are displayed if broadcast or multicast packets are representing more than 10% of total network utilization or if utilization goes over 35%.

Understanding Real-time Statistics

In Observer, real-time statistics are gathered by viewing—not capturing or trending—network traffic and incrementing a statistic counter. Statistics are particularly useful for determining network health. For example, real-time statistics can display the number of errors occurring on your network, the number of established connections, and the bandwidth utilization across the network.

Real-time statistics are fundamentally different from packet captures and network trending.

If you are connected to a GigaStor, you may view statistics in the GigaStor Control Panel.

To discover current top talkers on the network, choose **Statistics > Top Talkers Statistics** (or any tool of interest), and click **Start** to start the tool. The tool begins to show the relevant statistics. For Top Talkers, it is a tree of protocols and subprotocols seen on your network.

There are **Start**, **Stop**, and **Settings** buttons for the statistics tool (top). Notice that there are three separate statistics tools running, each with its own tab in the tool tray (bottom). Select the tab of the desired tool to display that statistics window. Recall that by dragging the vertical line between the probe and tool window, the window sizes can be adjusted. Right-click a row to show even more options, like filters or start a packet capture on that station.
VLAN Statistics  Shows the VLANs operating on your network.

Top Talkers Statistics  Lets you see who is using the most network bandwidth.

Protocol Distribution Statistics  Displays all protocols running on the network.

Internet Observer  Show what websites users are visiting and how much time was spent on a website.

Internet Patrol  Allows you to view MAC to IP communication as a list, pairs circle, or charts.

Wireless environments  There are several statistics tailored to provide information that is characteristic or unique to wireless networks. Wireless Site Survey and Wireless Access Point Statistics are available only for wireless interfaces and common statistics such as Top Talkers and Vital Signs contain wireless tabs that are only available when monitoring a wireless interface.

Monitoring your VLAN

VLANs can be used to contain broadcast traffic, act as a load balancing tool, and enhance data security, but there are some maintenance and troubleshooting challenges. Observer makes it easy to see a breakdown of total traffic (or each station’s traffic) by VLANs.

Being able to see VLAN information within the context of other metrics makes it much easier to separate VLAN configuration problems from general network problems, and thus keep your network running smoothly.

The VLAN Summary tab lets you focus on VLAN-level statistics by omitting station-level statistics. For example, you can quickly determine if traffic levels on your VLAN have become extraordinarily high and it allows you to assess your overall network performance health.
**VLAN Stations** shows what stations comprise each VLAN, what VLAN(s) a station belongs to, and traffic totals by station or by VLAN. You can think of it as a “top talkers” for VLANs.

If you want to limit packet captures to particular VLANs (or to exclude particular VLANs), you may filter by VLAN header fields for 802.1Q and ISL VLANs when troubleshooting a network on which VLANs are implemented.

Knowing which VLAN has been assigned to a switch port can be indispensable in troubleshooting connection problems. Although you could theoretically keep up-to-date records of VLAN port assignments, in the real world no one ever has time for this housekeeping task. You could also look up the information through the switch’s administrative interface when necessary, but it is much more convenient to have this information available directly from your analyzer. Using an SNMP form query, you can query your switch for VLAN port assignments.

### Viewing optional VLAN statistics

Depending on your network infrastructure, virtual LANs (VLANs) may exist on your network. If VLANs exist, the VLAN Statistics tool is useful to you.

To view optional VLAN statistics, including a list of seen VLANs and the traffic passing through them, choose **Statistics > VLAN Statistics**.

Click the Start button to activate the tool, or click Settings for more configuration options. To view a different layout, click the View button and select another.

Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.

**Related Topics**
- Installing the wireless NIC driver on Windows 7/Vista on page 229
- Load testing the network on page 26
- Pre-filtering your packet captures on page 66
- Installing the wireless NIC driver on Windows 7/Vista on page 229
- Network Trending on page 146
- Packet Captures on page 59
- Pre-filtering your packet captures on page 66
- Collecting forms information on page 196
- A probe is not connecting to the analyzer or vice versa on page 276
- “No VLAN” shown while using a Gigabit NIC on page 277
- Viewing optional VLAN statistics on page 35
Chapter 3: Discovery

Building and saving an address book

After your probe instance has adequate visibility of the network, you should take time to discover the devices on your network. Start by building an address book or importing a previously saved one.

To build and save an address book in Observer, choose Tools > Discover Network Names. This reveals the Discover Network Names tool, which records all seen network addresses on the segment, stores them in the table, and assigns them names (aliases).

Configuring a discovery method (optional)

Observer discovers network names using two separate methods—IP or Microsoft Network Discovery. Both of these methods have specific configuration options, which can be set by clicking Settings.

The default discovery method, IP, places some additional load on your network during the discovery process. If you want to passively discover the names instead, click the Settings button and choose “Passively discover IP addresses.” Passive discovery may take longer than active, but it requires the least amount of network resources.

Building an address book automatically

Typically, you can use the Discover Network Names tool successfully without additional setup. The default method of discovery is IP. In this method, Observer attempts to use ARP to discover all of the addresses in the IP address range given in the IP configuration, and listens for any additional addresses that may show up over time.

We recommend running the discovery process long enough to ensure the resulting address book is complete —this process can take several hours on larger networks; you may consider running the discovery process overnight when network load is typically lowest.

To build an address book automatically, complete the following steps:

2. Click Start to begin the discovery process.
3. Click Stop to end the discovery process.
4. Click Save Aliases to save your results.
You successfully built an address book, which will help you throughout numerous portions of Observer in the future because other modes and tools rely on it.

**Adding entries to the address book manually**

If necessary, you can manually add entries to your address book. Here are some common reasons for doing so, followed by instructions:

To build an address book to only contain specific network addresses:
- May help you stay organized (smaller list)
- Only solicits the stations you specify (good neighbor)

To add stations to an existing address book:
- Add network addresses without running another discovery

If the automatic discovery process is prohibited:
- Due to security policies, applicable laws, etc.
- Avoid introducing potential interference to devices within a mission critical environment

To manually add entries to the address book:

1. Choose **Tools > Discover Network Names.**
2. Click Add Entry. The Add Alias dialog box appears.

![Figure 7: Manually adding an address book entry](image)

3. Select the network address type of the station, and type information into the fields; the first field is always required.
4. Click OK to save your entry in the address book.

You successfully added an address book entry without having to run a full discovery. Remember, you can manually add more entries by repeating this process.

After completing this task:

Typically, DNS names are more meaningful to end-users than IP addresses, so you should resolve them. To do this, click the Resolve IP button. Observer then attempts to resolve the DNS name of each entry in the address book.
Resolving DNS names

After building an address book, consider resolving the DNS names of the collected IP addresses. Typically, DNS names are more meaningful to end-users than IP addresses, so you should resolve them. To do this, click the Resolve IP button. Observer then attempts to resolve the DNS name of each entry in the address book.

Having trouble resolving DNS names in other portions of the Observer software? Check any of the following:

- Save your address book after resolving DNS names as described above, and see if this resolves your problem.
- Ensure the option for resolving DNS names is enabled in Observer’s general options. Choose Options > General Observer Options. Then, in the General tab, ensure Disable IP Address DNS Resolution is not enabled.

Saving the address book

To save the address book, choose Tools > Discover Network Names, and click the Save Aliases button. This saves all address book entries in an internal file, which Observer references frequently in the application.

Because the address book is used internally by Observer, you cannot specify a custom file name from this location. Instead, choose Actions > Select Address Table for Local Observer and create a new, empty address book that you can name and switch between at any time (local Observer only).

Editing address book entries

Prerequisite(s):
You have completed Building and saving an address book on page 36.

To edit address book entries in Observer:
2. Select an entry from the list, and click Edit Entry.
3. Edit the address book entry.
4. Click Save Aliases to save your changes.

Importing a previously saved address book

If you have access to a previously saved address book (file extensions *.ADR; *.ADR11; *.ALI) and would like to import it as your address book, complete the following steps:

2. Click the Import Aliases button.
3. Follow the on-screen instructions that appear.

After completing this task:
If you own multiple Observer licenses/installations, consider building an address book on one machine and then securely distribute it to other machines for importing. This can save you time and effort.

Tell me more about importing a previously saved address book

The format of address entries in an .ali file is:
MACaddress, IP, alias
where MACaddress is the MAC address, IP is the Internet Protocol dot address, and alias is the alias by which you want the system to be known. Note that entries are separated by commas. If you want to specify a MAC Address/Alias pair without an IP, the format is:

MACaddress, , alias

Note the two commas separated by a space. You can specify the MAC address with or without colons, as long as the format is consistent within the .ali file. Leading zeros are allowed but not required. For example

00:00:C0:87:49:45, 168.0.0.1, router
100:00:C0:13:4B:33, 223.188.11.3, Sue’s Accounting PC

-or-

0000C08B4194, 175.203.57. 8, JohnC0134B33 Roman

The alias can be no longer than 17 characters.

The Replace aliases with newly discovered name option will replace any existing MAC address/alias pairs in the Address Table with the entry found in the .ali file. If this option is left unchecked, any pair of existing MAC address/alias entries are not overwritten. Existing IP address and comment fields are never overwritten by the Import Aliases action.

Using multiple address books

Multiple address books are supported to allow the saving and reuse of different address/alias lists (e.g., for multiple sites). The default address table, LocalAddressTable.adr, is stored in the LocalAddressTable directory under the Observer installation directory.

To switch to a different address book, complete the following steps:

1. Choose Actions > Select Address Table for Local Observer. The Select Local Observer Address Table dialog appears.
2. Select the address book you want to use, and click OK.

You are now using the selected address book, and you can repeat the process to switch again.

Discovery

Mapping your network is important, and it should be completed as thoroughly as possible to ensure Observer has visibility of the full network (or your chosen portion of it). This section describes discovery tools for mapping your network.

Discovering server applications on the network

Typically, the Server Application Discovery tool is used only when needed; running the discovery continuously provides little benefit over running it on demand. For example, many users run the Server Application Discovery tool only long enough to discover a set of applications that they want to interact with using the right-click menu.

To fully understand Observer's application discovery method, and how to modify it, we recommend you review this entire section.

Using the Server Application Discovery tool, Observer can automatically analyze network traffic and identify servers and applications, along with the ports being used. Observer then reports how confident it feels each discovery is using a color legend seen along the bottom of the window.

To discover server applications running on the network, complete the following steps:
To save time, you can import and export your protocol definitions. Choose Options > Protocol Definitions and Server Application Discovery > Tools and select the option you want.

**Tip!** If you use NIMS, you can have NIMS collect and publish your protocol definitions. The setting to enable is at Options > Observer General Options > Security > Synchronize user protocol definitions through NIMS.

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. (Optional) If you have applications that use non-standard ports or you want to specify a range of IP addresses, click Settings to modify the settings before starting the server discovery process.
3. Click the Server Application Discovery tab. This screen is where the discovery occurs.
4. Click the Start button to begin discovering applications. Clicking any of the Protocol or Application Definitions tabs cause the search to automatically stop. You will need to restart the search.

   Wait patiently for the discovery process to begin showing results; this may take some time because the tool acts passively—results are collected and not “grabbed”. Results appear in the manner shown in Figure 8 on page 40.

![Figure 8: Server applications being discovered](image)

You successfully discovered server applications seen on the network. Right-click any result to perform additional functions such as adding the server directly to the Network Trending tool. Remember, you can repeat the server application discovery process at any time for any reason.

**Discovering SNMP devices**

Some SNMP devices on your network may not adhere to RFC1213, causing them to remain undiscoverable even when your other settings are configured correctly.

**Note:** If you suspect this is occurring—or you want to discover SNMP devices that react to a very specific MIB—change the assigned device type to something more fitting (option seen in the lower-right of Figure 9 on page 41). You may need to experiment with this setting if you are unsure of what to choose. Remember that RFC1213 is default.

Before SNMP devices can be discovered, the IP discovery ranges must be configured. An error message is shown if you try discovering before the discovery ranges are configured.

We highly recommend allowing Observer to communicate with Simple Network Management Protocol (SNMP) enabled devices on your network. To do so, you must attempt to discover those devices automatically or add them manually. Observer SNMP functionality is only available with an Observer Suite license.

This section only describes the process for automatic SNMP device discovery; to add SNMP devices manually (and perhaps with greater success than automatically) see Introduction to SNMP on page 182.
Set the IP address discovery ranges by completing the following:

1. Choose **Tools > Discover SNMP Devices.**
2. Click the Settings button. The SNMP Device Discovery window appears.

**Figure 9: Configure SNMP IP discovery ranges**

3. In the IP Ranges area, click Add to specify the IP discovery range. Repeat as necessary until all your IP discovery ranges are set.
4. In the SNMP Credentials area, click Add to configure an SNMP credential. Repeat as necessary until all of your possible SNMP credentials are listed.

   The purpose of 4 on page 41 is to ensure the SNMP devices return a discovery handshake. Without providing credentials, SNMP devices may not react to your discovery attempts—overlooking devices that might otherwise have been discovered.
5. Click OK to save your changes. SNMP device discovery is now configured and discovery can be attempted.
6. Click Start to begin the discovery process.
7. As SNMP devices are discovered, select one from the list and click Add to SNMP Devices.

The SNMP devices you add are now recognized by Observer.

**Discovering which devices are connected to a switch**

**Prerequisite:** Observer Suite

Use the Switch Station Locator tool to show the MAC addresses of devices connected to switches on the network; in this way, you can determine which stations are connected to a network switch. This tool strictly uses SNMP queries to function, and requires an Observer Suite license.

This tool is well-suited for responding to complaints about network slowdowns, as you can use the Switch Station Locator to immediately narrow down the problem to a particular switch. You can then query the switch to find out if a particular port is generating a lot of errors. This in turn might cause you to be suspicious of a server connected to that port, in which case you can retrieve the server’s SNMP statistics to see if there is a problem with that system.
During 3 on page 42, you can optionally associate your new switch with a probe instance, allowing the Switch Station Locator tool to use its corresponding address book. Do this by choosing a probe instance from the list.

**Note:** See Building and saving an address book on page 36 for more information about address books in general.

1. From the main menu, choose Tools > Switch Station Locator. The Switch Station Locator window appears.

2. Do one of the following:
   - If your switch station list is empty—click New Switch, and proceed directly to 3 on page 42 of these instructions.
   - If your switch station list is populated—proceed directly to 5 on page 43 of these instructions.

3. The Edit Switch window appears. Type the details of your switch, or choose an existing SNMP device.

   **Figure 10: Creating a new switch**

4. Click OK to save your new switch.
5. Double-click the switch you want to query. The tool polls the switch and populates the list with connected stations.

6. (Optional) Click the Settings button. If you want all seen stations to be indefinitely remembered, choose that option.

   Otherwise, if you only want currently connected stations to appear in the list (default behavior) keep that option enabled.

7. (Optional) Save your populated list by choosing **File > Save > Save Data in Comma Delimited Format**.

### Calculating subnet masks

This IP Subnet Mask Calculator tool calculates the network address, the host address and the broadcast address for a given TCP/IP address and subnet mask. It will also tell you the number of available addresses in the network, displaying the first, last, and next addresses given the parameters entered.

This tool is located at Tools > IP Subnet Mask Calculator.

Only the top of the dialog is editable; the rest of the fields are determined by what you select in the first three controls. After making any changes, click Calculate to see the results. Click close when you are done.

- **IP Address**: Enter the IP address for which you want to calculate subnet parameters.

- **Subnet Mask**: Select the subnet mask for the network you are calculating parameters for. Depending on whether you have selected Show all masks or Show class-specific masks, the number of masks available on the drop-down menu will change.

- **Show class-specific masks**: This choice lets you limit the mask selection drop-down menu to show only those masks valid for the current class of address. The first octet of the IP address defines the address class.

- **Show all masks**: This choice expands the mask selection drop-down menu to include all subnet masks, including those masks that are not compatible with the current class. Address class is defined by the first octet of the IP address.

### Performing ping and trace route

A flexible Ping/Trace Route tool is located at Tools > Ping/Trace Route, giving you quick, robust access to this common task.

Observer’s Ping/Trace Route tool permits the user to see if specific stations on an IP network are active and to trace a route from the Observer (or probe) PC to a selected station. To open Ping/Trace Route, select Tools > Ping/Trace Route. See **Table 6 on page 43** for more information.

**Table 6: Ping/Trace Route options**

<table>
<thead>
<tr>
<th>Internet Address</th>
<th>Allows you to specify the Internet address to ping, or the address to which the route will be traced.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save button</td>
<td>Allows you to save the present Internet address.</td>
</tr>
<tr>
<td>Delete button</td>
<td>Selecting an address in the saved addresses box and clicking this button allows you to delete the address from the saved addresses.</td>
</tr>
<tr>
<td>Ping</td>
<td>Allows you to select the Internet address to ping and the results to be displayed in the main Ping/Trace Route display area. To ping an address is to send out an ICMP echo request to that address. If the station is operating normally, it will respond, unless it is behind a firewall that prevents such response.</td>
</tr>
<tr>
<td>Trace Route</td>
<td>Allows you to select a route from the Observer personal computer to the specified Internet address to be traced.</td>
</tr>
</tbody>
</table>
### Timeout (sec)
Allows you to specify the number of seconds that Observer will wait for a response before assuming that the packet Observer sent was either not received or not responded to.

### Packets
If the Ping option is selected, this box specifies the number of ping packets or ICMP echo requests that will be sent. When the Trace Route option is selected, this option has no effect and will be grayed out.

### Packet size
If the Ping option is selected, this edit box selects the number of ping packets or ICMP echo requests that will be sent. When the Trace Route option is selected, this option will not be activated.

### Display Window
Displays the results of the ping or trace.

---

## How to add application definitions

The Server Application Discovery tool is pre-loaded with popular application definitions, ensuring most of the server applications you discover are recognized by Observer. There are cases, however, when adding more application definitions to the stock set is desirable.

To add more application definitions for the Server Application Discovery tool to use, complete the following steps or see Adding derived application definitions on page 46 for details about creating definitions for applications that are subsets of another application:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click **Add Application**. The Add Application window appears.

![Add Application Window](image)

Your new application now appears in the list of application definitions.

## How to associate non-standard ports with an application

Some applications running on the network may be using a non-standard port. If you are aware of these exceptions and want to add the port to an application’s definition, you can do so.

The benefit of is that you do not need to wait for the Server Application Discovery tool to see something that you already know exists.
For example, the standard server port for MySQL is 3306. But you configured your MySQL server to use 63245 instead—a non-standard port. You must therefore associate port 63245 with the MySQL application definition so that it can be reported with greater ease in Server Application Discovery.

To associate non-standard ports with an application definition, complete the following steps:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click an applications definitions tab that interests you (seen below the Start and Stop buttons).
3. Scroll through the list of application definitions, and find one that you want to associate non-standard ports with.
4. Click the application definition to select it.
5. Click **Add Ports**.
   
   The Add Application Definition dialog appears.
6. Type the port number to be associated with the selected application. Here, port ranges can also be set.
7. Click **OK** to confirm your changes.
8. Click **Apply Changes**.

You successfully associated a non-standard port with an application. You can repeat this process for any application definition at any time.

Observer is intelligent enough to not require you to complete these steps—it will discover items regardless—but your manual entry adds meaningful intelligence to your tool set and may aid you in the future.

Using the MySQL example, you would select the TCP Application Definitions tab, scroll down the list, select MySQL, click Add Ports, type 63245, click OK, and finally click Apply Changes. The software now recognizes activity on port 63245 as potentially being MySQL.

**How to import application definitions**

Prerequisite(s):

To import application definitions, you need access to an exported *.protodefs file. See **Exporting app definitions on page 46** for details.

To import application definitions, follow the import process:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click any one of the applications definitions tabs (not the Server Application Discovery tab itself) to ensure one of these tabs has focus.
3. Click **Tools**, and click **Import Application Definitions**.
   
   The Open file dialog appears.
4. Locate and select the *.protodefs file that you want to import, and click **Open**. The Import Application Definitions dialog appears.
5. Select the protocols to import and the importing behavior.

You successfully imported application definitions. The definitions you import are now part of your local collection.

How to export application definitions

To share application definitions with other users, you must first save them to a file. Create your file by following this export process:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click any one of the applications definitions tabs (not the Server Application Discovery tab itself) to ensure one of these tabs has focus.
3. Click **Tools**, and click **Export Current Application Definitions**. The Export Application Definitions dialog appears.
4. Select the groups of definitions you want to export, and click **Export**.
5. Type a name for your file, and click **Save**.

You successfully exported your application definitions to a *.protodefs file.

You can now share this file with other users and installations, or keep it as a backup copy.

Adding derived application definitions

Creating a derived application definition allows Observer to take one large application that may have many sub-applications within it and identify each of the sub-applications.

For instance, Java traffic can be identified within HTTP. After Observer identifies the derived application, it appears on your reports and elsewhere within Observer as its own application. The Decode tab is unaffected though. The derived application decodes as part of its parent’s application type. In our Java example, all Java traffic is viewable on the Decode tab as part of HTTP.

To add a derived application definition for the Server Application Discovery tool to use, complete the following steps:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click the applications definitions tab you want to add to (below the Start and Stop buttons).
3. Click **Add Derived Application**. The Add Derived Application window appears.
4. Type a name for the derived application (this name will appear in reports and throughout Observer) and choose from which application it stems. The Add Application Definition window appears.
5. Specify the port or port range and IP address or range on which the application is found and click OK. Your new derived application now appears in the list of application definitions. Most importantly, the new application is discoverable using the Server Application Discovery tool and, if the application is seen, it is recognized correctly by Observer.

### Enabling or disabling applications that use dynamic ports

When run, the Server Application Discovery tool automatically recognizes applications (if any are seen) that are known to use dynamic ports; they appear light blue in your discovery results. These applications are flagged by the Observer software as being dynamic, and this designation cannot be changed.

You can, however, enable or disable dynamic port discovery for each application known by Observer to use dynamic ports by completing the following steps:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click a protocol/applications definitions tab that interests you (seen below the Start and Stop buttons).
3. Scroll through the list of application definitions, and find a dynamic port application.
   - Dynamic port applications always display the string *(dynamic - enabled)* or *(dynamic - disabled)* in the ports column of the table.
4. Right-click a dynamic port application, and click Enable/Disable Dynamic Discovery.

**Figure 13: Enabling or disabling a dynamic port application**

### Defining applications differently per IP address

Sometimes, you may want to treat server application definitions differently depending on the IP address that is discovered in tandem with the port(s).

For example, if you know an FTP server is hosted on 192.168.0.90 on port 63245 (a non-standard port), you could force Server Application Discovery to report all server application discoveries that use port 63245 as FTP—but only if it is destined to 192.168.0.90. This specific rule does not apply to other IP addresses; meaning, the standard port of 21 is recognized as FTP for all other IP addresses.

To define application definitions differently depending on the IP address seen, complete the following steps:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click an applications definitions tab that interests you.
   Application definition tabs are located below Start and Stop.

3. Scroll through the list of application definitions, and find one that you want to associate non-standard ports with per IP address.

4. Click an application definition to select it.

5. Click Add Ports.

6. Type the port number or port range to be associated with the selected application.

7. Select Use Specific IP Address, and type the IP address you want to treat differently.

8. Click OK.

9. Click Apply Changes.

Now, as server applications are discovered, those matching an IP address and port combination are correctly recognized by the Server Application Discovery tool.

Figure 14: A completed example of FTP ports being recognized differently per IP address

---

Restoring the default application list

Under certain circumstances, it may be beneficial for you to restore the default application list. Doing so removes all of your custom or modified application definitions and returns your applications to default—exactly how the default installation would behave.

How to restore TCP application definitions

To restore the default TCP applications, complete the following steps:

1. Choose Options > Protocol Definitions and Server Application Discovery.

2. Click the TCP Application Definitions tab to ensure it has focus.

3. Click the Tools button, and click Restore Predefined TCP Applications. A confirmation prompt appears.

4. Click OK to confirm.

5. (Optional) Select Apply Changes Across All Probe Instances if you want to apply these changes to all probe instances.

6. Click OK to apply and save your changes.
Your TCP application definitions list is now restored.

How to restore UDP application definitions
To restore the default UDP applications, complete the following steps:
1. Choose Options > Protocol Definitions and Server Application Discovery.
2. Click the UDP Application Definitions tab to ensure it has focus.
3. Click the Tools button, and click Restore Predefined UDP Applications. A confirmation prompt appears. Click OK to confirm.
4. (Optional) Select Apply Changes Across All Probe Instances if you want to apply these changes to all probe instances.
5. Click OK to apply and save your changes. Your list is restored.

Sharing application definitions with others
Application definitions can be shared using the included import and export functions. Sharing is useful for making your application definitions uniform across multiple installations, and it can even be used as a backup tool. This section describes the exporting and importing processes.

How to export application definitions
To share application definitions with other users, you must first save them to a file. Create your file by following this export process:
1. Choose Options > Protocol Definitions and Server Application Discovery.
2. Click any one of the applications definitions tabs (not the Server Application Discovery tab itself) to ensure one of these tabs has focus.
3. Click Tools, and click Export Current Application Definitions. The Export Application Definitions dialog appears.
4. Select the groups of definitions you want to export, and click Export.
5. Type a name for your file, and click Save.
   You successfully exported your application definitions to a *.protodefs file.
You can now share this file with other users and installations, or keep it as a backup copy.

How to import application definitions
Prerequisite(s):
To import application definitions, you need access to an exported *.protodefs file. See Exporting app definitions on page 46 for details.
To import application definitions, follow the import process:
1. Choose Options > Protocol Definitions and Server Application Discovery.
2. Click any one of the applications definitions tabs (not the Server Application Discovery tab itself) to ensure one of these tabs has focus.
3. Click Tools, and click Import Application Definitions.
   The Open file dialog appears.
4. Locate and select the *.protodefs file that you want to import, and click **Open**. The Import Application Definitions dialog appears.

**Figure 15: The final importing dialog**

5. Select the protocols to import and the importing behavior.

You successfully imported application definitions. The definitions you import are now part of your local collection.

**Related Topics**

- Building and saving an address book on page 36
- Saving the address book on page 38
Chapter 4: Captures

Configuring the capture buffer settings

Experimenting with buffer sizes is encouraged; it may take some time to find a balance between how large or small your buffer sizes should be for a probe instance, and it depends greatly on how the probe instance is used.

**Note:** Try finding the best balance between what the probe instance needs to operate efficiently and how much RAM a fully-maxed buffer would leave for other services to use.

Observer can perform packet captures without additional setup. However, to maximize Observer performance, you should consider configuring your capture settings manually. This section describes several areas of Observer that can be manually configured.

During the creation of your probe instance(s), you set the size of your buffers. The capture buffer is used to store raw data captured from the network, and the statistical buffer stores statistical data entries (example buffer change shown in Figure 16 on page 51).

Figure 16: Changing your buffer sizes
If you are pushing the limits of the PC system on which the probe is installed by creating many instances, you may be able to avoid some performance problems by fine-tuning the memory allocation for each instance.

For example, the default settings for the statistical buffer work perfectly well for most installations—change them if they do not. The packet capture buffer, however, typically needs increasing or decreasing to best reflect your system.

To change the buffer sizes of probe instances, complete the following:

1. Choose Options > Selected Probe or Local Observer Instance, Memory and Security Configuration.
   The Observer Memory and Security Configuration window appears, listing all configured probe instances.
2. Double-click the probe instance you want to configure. The Edit Probe Instance window appears.
3. Change the buffer sizes to better match the needs of your chosen probe instance. Generally, more is better, but not always.
4. (Optional) Select a predefined statistics memory configuration from the drop-down list. Your configuration choices are small, medium, and large.
   The choices in 4 on page 52 affect the maximum number of entries per statistic. All of these allocated statistical entries combined determine the amount of memory used by statistics.
5. Click OK twice to confirm and save your changes.

You successfully changed the buffer sizes of a chosen probe instance. In the future, you may need to reevaluate your buffer sizes using the same process; this is especially true after adding or removing memory from your system or after adding new probe instances.

Fine-tuning the statistical buffer

There are two kinds of buffers that a probe instance uses to store data in real-time: a capture buffer and a statistical buffer. The capture buffer stores raw data captured from the network; the statistical buffer stores statistical entries and nothing more. This section is only concerned with statistical buffers.

The default statistics configuration is sufficient for most users and does not need to be changed. The memory settings are preconfigured based on network size and network type. Choose the type of network you are monitoring with this probe instance.

Each statistic is collected in its own section of RAM, where the processed data is stored. Alias List Entries is the first entry. It is used in the Discover Network Names portion of Observer. It has 800 allocated entries (stations), which consumes 114.4 kilobytes of RAM. When Discover Network Names is running, the captured packet is passed to the statistics queue buffer. After the data is processed, it is passed to the statistical memory buffer and to each relevant Observer statistic for that particular network type.

Observer collects statistics for numerous types of applications and trending, some of which may not apply to your network. You may increase or decrease the allocated entries as necessary.

For instance, if you are using Discover Network Names it will run until it fills the 800 stations. After it reaches 800 entries it cannot add any more because there is no memory space available. Any stations beyond 800 are not included in the list. You must increase the number of stations that may be allocated. This increases the memory requirements though. If you have 8,500 stations on your network, you will need at least 8,500 entries, which requires 1.2 MB of RAM.

Conversely, if you are not using statistics, such as VoIP, the RAM is still allocated to it. The default VoIP Trending is for 1,500 entries, which requires 12.6 MB of RAM. By reducing the allocated entries to 10 (the minimum) you need only 86.3 KB of RAM — saving nearly 12 MB to be used elsewhere.

By tweaking the statistics allocation, you can fine tune how Observer processes its data.
You cannot modify the default statistics memory configuration. You must create a new profile based on one of the existing profiles (Small, Medium, Large, 4G LTE) and modify it.

1. To view and manage memory allocation for probe instances, click the Memory Management tab to display the list of instances and their buffer sizes.

2. Right click any instance and select Configure Memory to access the memory allocation dialog. Right click any instance and select Configure Memory to access the memory allocation dialog.

Figure 17: Probe Instance Memory

3. Click View to see the different types of networks and the default memory configuration for them. The memory settings are preconfigured based on network size and network type.

When allocating memory for a probe instance with the Gen2 10 Gb or 40 Gb Ethernet adapter as the chosen adapter, at least 80 MB of memory must be allocated to both the capture buffer and statistics queue buffers. Failure to do so will result in the inability to capture data.

4. Choose the type of network you are monitoring with this probe instance. Click OK.

Tell me more about the statistical memory allocations

| Alias List | Used with Discover Network Names. 1 MAC address per entry. Each MAC Address can have 1 IP Address and an Alias. |
| Application Analysis | Used with Network Trending. 1 entry per server to be monitored for application analysis. If this is set to 50, then Network Trending can only be configured to monitor 50 stations for application analysis. |
| Global Station Statistics | Used by the following modes: Errors by Station, Protocol Distribution, Size Distribution Statistics, Summary, Top Talkers (MAC TAB ONLY) Each of these modes are MAC based, meaning they look only at the source and destination MAC address. They do not look at any IP data. The thing that is important to understand about this memory configuration is that each of these modes listed above are linked together. If you start Errors by Station, it actually starts Errors by Station, Protocol Distribution, Size Distribution Statistics, Summary and Top Talkers. When a packet is seen data from that packet is |
stored for each of these modes. It allows Observer the ability to do “drill down” navigation, such as right clicking on a MAC station in Top Talkers and choosing Display Protocol Distribution for Selected Station. Each MAC address seen uses 1 entry.

<table>
<thead>
<tr>
<th>Global Station Statistics Protocol Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is linked to the Global Stations Statistics as well. For each MAC seen we monitor the protocol used. We keep track of each level of the protocol stack for each MAC address seen. Assume we have a machine that has sent an HTTP packet to a server, we would use six entries for that one packet.</td>
</tr>
<tr>
<td>Source MAC</td>
</tr>
<tr>
<td>IP &gt; Entry 1</td>
</tr>
<tr>
<td>TCP &gt; Entry 2</td>
</tr>
<tr>
<td>TCP PORT # (OTHER) &gt; Entry 3</td>
</tr>
<tr>
<td>Destination MAC</td>
</tr>
<tr>
<td>IP &gt; Entry 4</td>
</tr>
<tr>
<td>TCP &gt; Entry 5</td>
</tr>
<tr>
<td>HTTP &gt; Entry 6</td>
</tr>
<tr>
<td>As you can see for just 1 packet 6 entries were used. We typically like to see 25 times the number of entries for Global Station Statistics Protocol Buffer as compared to Global Station Statistics. So if you have 100 for Global Station Statistics, we would like to see 2500 entries for the Protocol Buffer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Top Talkers</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is linked to the IP tab within the Top Talkers mode. Since it is an IP based mode it is not part of the Global Statistics memory configuration. Each individual IP seen uses one entry.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Trending Pairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is specific to Network Trending. Data collected by this can be seen within the Network Trending Viewer under the IP to IP Pairs Matrix and within the Web Based Reports under:</td>
</tr>
<tr>
<td>Drill Down (Classic Reports) - Internet Trending - IP to IP tab</td>
</tr>
<tr>
<td>It collects station pairs based on IP addresses. Using the example above you would see two entries</td>
</tr>
<tr>
<td>Station 1 IP Station 2 IP Total Packets Packets 1-&gt;2 Packets 2&lt;-1</td>
</tr>
<tr>
<td>192.168.1.1 192.168.1.2 1 1 0</td>
</tr>
<tr>
<td>192.168.1.2 192.168.1.1 1 0 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Trending Patrol</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is specific to Network Trending. Data collected by this can be seen from within the Network Trending Viewer under the Internet Patrol tab within the IP area of the viewer and within the Web Based Reports under:</td>
</tr>
<tr>
<td>Drill Down (Classic Reports) - Internet Trending - on the Internet Patrol tab</td>
</tr>
<tr>
<td>Trending Pairs creates entries with both MAC and IP Addresses. For each packet seen 2 entries are used. Example:</td>
</tr>
<tr>
<td>1 packet is sent from IP 192.168.1.1 to 192.168.1.2</td>
</tr>
<tr>
<td>Source MAC Address: 00:00:E4:56:AB:08</td>
</tr>
<tr>
<td>Source IP Address: 192.168.1.1</td>
</tr>
<tr>
<td>Destination MAC Address: 00:08:F9:01:BC:12</td>
</tr>
<tr>
<td>Destination IP Address: 192.168.1.2</td>
</tr>
<tr>
<td>Inside of Trending you would see the following entries:</td>
</tr>
<tr>
<td>Station 1 MAC Station 2 IP Total Packets Packets 1-&gt;2 Packets 2&lt;-1</td>
</tr>
</tbody>
</table>
Table showing memory allocations for different network protocols:

<table>
<thead>
<tr>
<th>Protocol Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Trending by Station</td>
<td>Collects a list of IP addresses seen. It is tied into the IP Trending Protocols by Station Buffer setting. It uses 1 entry per IP address seen.</td>
</tr>
<tr>
<td>IP Trending by Station Buffer</td>
<td>Collects protocol information on a per IP address basis. The protocols are only collected for those IP Addresses in the IP Trending Protocols by Station list. By default we have ten times the number of Station Buffer entries for every by Station entry. So if there are 100 by Station entries, there would be 1000 by Station Buffer entries by default.</td>
</tr>
<tr>
<td>Internet Observer - IP Pairs</td>
<td>Tracks IP to IP conversations. It acts exactly like the IP Trending Pairs memory configuration.</td>
</tr>
<tr>
<td>Internet Observer - IP Patrol</td>
<td>Tracks MAC to IP based conversations. It acts exactly like the IP Trending Patrol memory configuration.</td>
</tr>
<tr>
<td>Internet Observer - IP Protocols by Station</td>
<td>Creates a list of IP Addresses and provides information about which protocols were used by that IP address. It uses 1 entry per IP address seen.</td>
</tr>
<tr>
<td>Network Trending Protocols by Station Buffer</td>
<td>Collects data about which MAC address sent or received each protocol. It uses multiple entries for each level of the packet. However, unlike the IP Trending Protocols by Station Buffer, this keeps track of all protocols seen, not just IP based protocols. Example:</td>
</tr>
</tbody>
</table>
As you can see an individual MAC address can have a large number of entries used. By default we allocate 25 entries for each entry allocated in Network Trending Stations. So if you have 100 allocated Network Trending Stations, by default there would be 2500 entries allocated for Network Trending Protocols by Station Buffer.

This data can be viewed within the Network Trending Viewer under the MAC header on the Protocols tab. This data can also be viewed in the Web Based Reports under:
- Network Summary - Protocol Distribution
- Network Summary - Protocol Summary
- Network Summary - IP Subprotocol Distribution
- Network Summary - IP Group Protocol Distribution
- Network Summary - IP Application Distribution
- Network Summary - IPX Subprotocol Distribution
- Network Stations - Protocols

| Network Trending Station Display | This is specific to Network Trending. This memory configuration does NOT affect how data is collected within Network Trending. When looking at Network Trending, you will see a set of dials and a table which shows which statistics are being collected. This configuration adjusts how many stations are displayed within the Station/Pair column. If this entry is set to 100, then we will only show the statistics of the first 100 MAC addresses seen during the collection interval. If 1000 stations were seen, we will collect on all 1000 stations (if Network Trending Stations is set to 1000 or higher), but the number of stations along with packets and bytes will only reflect the first 100 stations seen during the collection interval. |
| Network Trending Stations | Specific to Network Trending. It collects information about individual MAC addresses seen. It uses 1 entry per MAC address seen, whether the MAC address is the Source or the Destination. This data can be viewed within any of the Web Based Reports under the headings Network Summary and Network Station. Also this data can be viewed within the Network Trending Viewer under the MAC section. |
| Pair Statistics (Matrix) | This is specific to the statistical mode Pairs Statistics (Matrix). This mode collects data based on MAC address pairs. For each MAC pair 1 entry is used. |
| Server Discovery | This is specific to the Application Analysis mode. It is used to limit the number of stations seen during discovery. The maximum number of servers that can actively be monitored is 32. For each server discovered 1 entry is used. |
| VLAN Statistics | This is specific to the VLAN Statistics mode. For each MAC address seen we monitor which VLAN it was seen from. 1 entry is used for each MAC address seen. |
| VLAN Trending Stations | This is specific to Network Trending and works in the same fashion as the VLAN Statistics memory configuration works, in that it uses 1 entry for each MAC address seen and keeps track of which VLAN it was seen on. This data can be viewed only from the Web Based Reports under: Report Library - VLAN |
Configuring the packet capture options

There are numerous ways to configure how your network traffic is captured. To alter the most basic of these settings, first choose one of the following tasks you want to complete:

- Excluding non-native packets from capture
- Configuring a circular capture buffer
- Configuring Observer to capture partial packets

All packets seen by the capture card interface are time stamped immediately, then are passed to the capture buffer. This ensures the most accurate timestamp.

Excluding non-native packets from capture

By default, non-native packets—called expert information packets—are automatically added to your captures by Observer. These packets serve as reference points, time-stamping important network events and utilization rates in your captures. These packets help network administrators understand the context of the captures they share.

If you do not find expert information packets useful, disable them by completing the following steps:

1. Choose Capture > Packet Capture.
2. Click the Settings button. The Packet Capture Settings window appears.
3. Ensure the Capture Options tab is selected.
4. Disable any or all settings in the Include Expert Information Packets area.

The disabled settings exclude the corresponding expert information packets from entering your future captures.

What are Expert Information Packets? Can I disable them? Do I need them?

When viewing a decode captured from an Expert Observer or Observer Suite, the capture contains Expert Information Packets.

What are Expert Information Packets?

Expert Information Packets are packets inserted into a capture to assist the Expert engine within Observer while processing packets. There are 3 types of Expert Information Packets:

- Expert Load Packets – These packets are inserted every second into the capture. They include information about the number of packets and bytes seen during the previous second, along with the utilization seen.
  These figures are used while drawing the graph seen on the Expert Events tab within the Expert screen.
- Start/Stop Packet Capture – These packets are inserted whenever you click Start or Stop from either the Packet Capture or Decode Screen. They are used to help expert know that there are gaps of time between packets.
- Wireless Channel Change – These packets are inserted when monitoring a wireless network adapter. They are inserted only if you are using the Channel Scan option. Each time Observer begins monitoring a new channel while in the Channel Scan mode, a new packet is inserted with the current channel being monitored.
Can I disable them?

Yes. These packets can each be disabled from within Packet Capture. From the Packet Capture screen, click Settings. (GigaStor users, can modify these settings from GigaStor Control Panel > Settings). Uncheck those boxes beside the Expert Information Packets you do not want to have generated.

Do I need them?

Expert Information packets are not required for the Expert to work. The following describes the behavior you will see if these packets are disabled:

(Disabling Expert Load Packets) – Disabling these packets will cause Expert to draw the Summary graph based solely on those packets within the capture buffer. As an example assume 20,000 packets were seen during a one second period, also that there was 10,240,000 bytes and 10% utilization. With these packets enabled Expert would graph 20,000 packets and 10% utilization.

Now assume during this one second you used a filter and captured only five packets during that second, with these packets Observer would graph 20,000 packets and 10% utilization. If you had disabled the Network Load Packets, Observer would graph five packets and 0% utilization.

(Disabling Start/Stop Packet Capture) – Disabling these packets can cause Observer to produce invalid response times to packets seen as Observer does not know that the capture was stopped. It only sees gaps within a sequence of the data stream and assumes that the data was not sent or dropped and will, in the case of VoIP packet loss within calls, register calls that have not actually occurred.

(Disabling Wireless Channel Change) – When Expert is processing Wireless data, we need to understand when the adapter is looking at a different channel then when a packet in a conversation was originally seen. This allows Observer to know that though Expert was looking at a conversation on Channel 5, that the next set of packets is now looking at channel 6 or 7 and so on. This prevents Observer from believing data is missing from a conversation due to packets not being captured. If you disable these packets while using the Channel Scan option, your response times and other calculations within the Expert System may not be accurate.

Configuring a circular capture buffer

Circular buffer is an optional buffer type that, as the packet capture buffer fills, writes new packets to the end of the buffer and discards packets from the start of the buffer (i.e. first in, first out). This allows you to continually run a packet capture, as the buffer recycles itself.

To configure a circular capture buffer, complete the following steps:

1. Choose Capture > Packet Capture.
2. Click the Settings button. The Packet Capture Settings window appears.
3. Ensure the Capture Options tab is selected.
4. Enable the Use Circular Packet Buffer setting.

A circular buffer also allows you to save the packet capture buffer to multiple, sequentially labeled files instead of overwriting a circular capture file. Some of the next steps describe how to enable that functionality.
5. (Optional) Enable the Save Captured Packets to a File setting; type the maximum amount of disk space to be used for this purpose.

   By design, as a circular capture buffer is filled/capped, the oldest packets are discarded to make room for the new, incoming packets. If, however, you want to save those oldest packets from being discarded, this option allows you to do so.

6. (Optional) Enable the Create Multiple Sequential Files setting; type the maximum number of files to create this way.

   This option causes Observer to write out a sequence of files rather than overwriting the file each time the buffer fills up.

7. Click OK to confirm and save your changes.

Configuring Observer to capture partial packets

By default, Observer captures each packet in its entirety. Under certain circumstances, however, you may want to configure Observer to capture a smaller portion of each packet. Such circumstances may include, but are not limited to:

- If you have trouble capturing or processing bandwidth spikes
- If you are interested in capturing packet headers only
- To extend the length of capture time before the buffer is full

To configure Observer to capture partial packets, instead of full packets, complete the following steps:

The partial packet capture setting affects all Observer consoles that connect to this probe instance. You cannot change this setting unless you have administrative privileges to do so. See Configuring user accounts for secure access on page 139.

1. Choose Capture > Packet Capture.
2. Click the Settings button. The Packet Capture Settings window appears.
3. Ensure the Capture Options tab is selected.
4. Enable the Capture Partial Packets setting. For now, leave the default number of bytes unchanged.
5. (Optional) Click Change Size to increase or decrease the number of bytes to be captured per packet—starting at the beginning of the header. Also, to password protect this field, see Password protecting the ability to change partial packet capture size.
6. Click OK to confirm and save your changes.

Packet Captures

The ability to capture network traffic as it flows through the network is invaluable. This section describes how to perform packet captures, including advanced pre-filtering techniques and other settings.

Packet captures are fundamentally different from real-time statistics and network trending.

Capturing network traffic

Capture packets so you can use Expert analysis to identify network problems and to help determine the best course of action.

Are you seeing duplicate packets collected during your capture? Do you want to ignore them? See Removing duplicate packets on page 78.
Using Observer, network traffic can be captured in real-time and examined immediately or later. This section describes several methods for capturing network traffic using Observer.

Observer makes capturing network traffic easy. The very simplest way to capture packets (i.e. create a packet capture) is to use the Packet Capture tool as described below:

1. **Choose Capture > Packet Capture.**
2. Click the Start button to begin your packet capture. If desired, filters can be defined before the capture from Actions > Filter Setup for Selected Probe.
   
   Capture options like buffer size and where to save packets is configured in Settings. At any time during the capture, click Decode to open the Decode tool and display the Expert Analysis.

3. Click Stop to complete the packet capture.

After completing this task:

After capturing is complete, you may want to:

- Save your capture—select File > Save to keep a shareable buffer file. For information about saving packet captures, see Saving packet captures on page 63.
- Analyze the capture—click Decode to examine the captured packets and how they interact over the network.

**Capturing from multiple probe instances**

Capturing from multiple probes allows you to collect multiple, synchronized packet captures from multiple points of visibility, which can be especially useful in Multi-Hop Analysis. Complete the following steps:

1. **Choose Capture > Packet Capture on Multiple Instances.** The Packet Capture on Multiple Instances Settings window appears.
2. Select the probe instances you want to capture from, and, if desired, set filters for any of the instances enabled for capture.
3. Click Start to begin the synchronized packet captures. Meanwhile, the Multiple Instance Packet Capture dialog appears.
4. (Optional) If you want any remote packet captures transferred and saved locally (and you should if you intend to run Multi-Hop Analysis), ensure the Transfer and Save Packet Captures setting is enabled.
5. (Optional) You can also choose to load Multi-Hop Analysis immediately upon completing the packet capture. To do this, ensure the Start MultiHop Analysis setting is enabled.
6. Click the Stop button after Observer collects enough packets for your purpose.

**Scheduling packet captures**

One way to ensure you always have timely packet captures is to schedule them. For example, you may want to automatically start a packet capture at the beginning of business hours each day; you can accomplish this by scheduling your packet captures accordingly.

Scheduled packet captures only tell Observer when to automatically begin and end a packet capture. The true length of capture time still depends on the size of your capture buffer; after it fills, you are no longer capturing packets. In effect, all scheduled packet captures automatically end in one of two ways: the capture buffer becomes full or the capture ends at the scheduled time.

**Note:** One way to prevent a premature end to scheduled captures is to use a circular capture buffer that writes to disk. See Configuring a circular capture buffer on page 58.
To schedule packet captures to begin at preset times, complete the following steps:

1. Choose **Capture > Packet Capture**.
2. Click the Settings button. The Packet Capture Settings window appears.
3. Click the Schedule tab.
4. Select one of the following scheduling types:
   - No scheduling—captures are never scheduled
   - Always—capture runs continuously unless explicitly stopped
   - Daily at specified times—capture runs at same time each day
   - By day of week at specified times—capture runs at specific times on specific days
     
     For Daily at specified times, you must specify a capture begin and end time by clicking the Add button. Multiple time intervals are configurable if the times do not conflict.
     
     For by day of week at specified times, you must specify a capture begin and end time by clicking the Add button for each day you select. Multiple time intervals are configurable, per day, if the times do not conflict.
   
5. Click OK to confirm and save your changes

**Transferring a packet capture to another probe instance**

If for any reason you want to transfer and view a packet capture from one probe instance to another, you can do that. The packet capture must be saved on the remote probe instance. By default the file is saved in `C:\Program Files\Observer\Data`.

1. Select the remote probe instance from which you want to transfer the packet capture.
2. Choose **File > Transfer or View Packet Capture From Remote Probe**. The Probe Packet Capture Files window opens. This option is disabled if you selected a local probe instance.
3. Select the files you want to transfer.
4. Choose whether you want to transfer the files or view them, and whether Expert Analysis should be included.
5. If you want to transfer the files to a different probe instance, select the probe instance to which to transfer the files. By choosing a probe-to-probe transfer you do not need to use an intermediary location. It is a direct transfer.
6. Choose whether to apply a filter to the data before the transfer is made.
7. (Optional) Choose whether to delete the files after the transfer is complete.

**Tell me more about the Packet Capture tool**

In Graph view, the cyan line shows the total number of packets; yellow shows the number of packets being captured. Unless there are filters in effect, the yellow line should cover the cyan line. This can be used to verify that you are capturing the percentage of traffic that you intend to capture.

The graph also shows any dropped packets as a red line (which is usually zero). Dropped packets mean that something is wrong with the system running Observer; either it is not fast enough to keep up with traffic, or it is incorrectly configured in some way. If you see dropped packets you should check your hardware for conflicts and make sure that system processing power meets the minimum requirements for Observer.
Why am I missing packets?

Assuming your Observer analyzer has the network visibility it needs—and packets are not being dropped due to hardware or driver issues—there are a few reasons Observer may not “see” packets that you, yourself, were expecting to see. Fortunately, this problem can typically be fixed by changing a simple setting in Observer, which is outlined in this section.

By default, Observer’s packet capture tool is configured to see (i.e. follow) only newly opened TCP connections. A newly opened TCP connection is any connection established after Expert Analysis was started. To change this behavior, complete the following steps:

1. Choose **Capture > Packet Capture**.
2. Click the Decode button. The Decode and Analysis tool opens.
3. Click Settings. The Expert Global Settings window appears.
4. Ensure the TCP/IP tab is selected.

![Expert Global Settings window - TCP/IP tab]

5. Clear the “Follow only newly opened TCP connections” check box; this changes Observer’s default behavior. A newly opened TCP connection is any connection established after Expert Analysis was started. If the conversation started before Expert Analysis was started, Observer cannot see it.
6. Click OK to confirm and save your changes. You may need to restart the Observer application for these changes to take effect.

This change should allow you to see connections that were established prior to opening the packet capture tool, along with the packets they contain. If you are still not seeing all packets, ensure you have all pre-filters deactivated. See **Activating and deactivating filters on page 71**.
Saving packet captures

A packet capture is most useful after saving it to disk. This is because a saved packet capture can be re-opened, shared, or even converted to other file formats for analysis in third-party applications.

After starting a packet capture—described in Capturing network traffic on page 59—save the packet capture by choosing File > Save > Save Capture Buffer. Alternatively, you can press CTRL+S.

The available file formats you can save to depend on the network topology of the captured traffic—although Observer’s native BFR format can be saved to regardless of topology. Observer can save packet captures to any of the formats listed in Table 7 on page 63.

### Table 7: Save Capture Buffer options

<table>
<thead>
<tr>
<th>File format</th>
<th>Supported topologies</th>
<th>Limitations and other information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFR</td>
<td>Any topology</td>
<td>BFR can only be read in Observer and Wireshark. Retains both nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>CAP</td>
<td>Ethernet, FDDI, Token Ring</td>
<td>CAP loses nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>ENC</td>
<td>Ethernet</td>
<td>ENC loses nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>FDC</td>
<td>FDDI</td>
<td>FDC loses nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>PCAP</td>
<td>Ethernet, FDDI, Token Ring</td>
<td>PCAP retains nanosecond resolution, but loses expert information packets.</td>
</tr>
<tr>
<td>TRC</td>
<td>Token Ring</td>
<td>TRC loses nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>XML</td>
<td>Any topology</td>
<td>XML loses nanosecond resolution, but retains expert information packets. Limited in usefulness.</td>
</tr>
</tbody>
</table>

1) Any topology refers to ATM, Ethernet, FDDI, Fibre Channel, SONET/SDH, Token Ring, WAN, and Wireless.
2) XML formatted packet captures cannot be re-opened by Observer.
3) Wireless topology is excluded from XML, but it does support all other topologies.

Saving to any format other than Observer’s native BFR format removes all expert information packets from the resulting saved packet capture. For more information about expert information packets, see Excluding non-native packets from capture on page 57. Saving to any format other than Observer’s native BFR format or the PCAP format removes all nanosecond resolution from the resulting saved packet capture. If you need to retain nanosecond resolution, ensure you save a packet capture to either the BFR or PCAP format. See the table for a full list of limitations per format.

Except for XML, Observer can load all of the files formats that it can save to, plus the DMP format. To load packet captures, see Decoding network traffic on page 77.

### Merging two packet captures

**Prerequisite:** Observer Expert or Observer Suite

If you have two packet capture files that captured the same data, but from different viewpoints, you can merge them to create a more comprehensive packet capture.
If you have many buffer files that you want to merge, you can do so by merging two files, saving them and then merging the newly joined file with yet another capture. Repeat until you have just two files to merge.

To merge two packet captures, complete the following steps:

1. Choose **File > Merge Two Packet Capture Buffers**. The Merge Two Packet Capture Buffers dialog appears.
2. Select two packet capture files to merge.
3. Type a file name for the resulting capture.
4. (Optional) Configure how duplicate packets are handled, and make time adjustments if necessary. See Table 8.
5. Click the Start Merge button. Depending on the size of the captures, this process may take a few minutes.

You successfully merged two packet captures. If you have additional capture files to merge with your new capture, do so by simply repeating the process indefinitely.

**Table 8: Merge Two Packet Capture Buffers**

<table>
<thead>
<tr>
<th>First packet capture file</th>
<th>Click the button to locate a saved capture buffer file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second packet capture file</td>
<td>Click the button to locate a saved capture buffer file.</td>
</tr>
<tr>
<td>Merged file name</td>
<td>Click the button and type a name for the merged buffer file you are creating.</td>
</tr>
<tr>
<td>Discard duplicate packets</td>
<td>Enable if you do not want duplicate packets in the merged buffer file.</td>
</tr>
<tr>
<td>When packet time is less than</td>
<td>Type of value (in milliseconds) if you want duplicate packets to be discarded that are less than X.</td>
</tr>
<tr>
<td>Ignore MAC or WAN address field</td>
<td>Enable if you want the MAC or WAN address field to be ignored when merging the buffer files.</td>
</tr>
<tr>
<td>Ignore IP TTL</td>
<td>Enable if you want the IP time to live field to be ignored when merging the buffer files.</td>
</tr>
<tr>
<td>Ignore TCP numbers</td>
<td>Enable if you want the TCP sequence and acknowledgment numbers to be ignored when merging the buffer files.</td>
</tr>
<tr>
<td>Time of first packet</td>
<td>Auto-filled by the first packet in the buffer files.</td>
</tr>
<tr>
<td>Time adjustment</td>
<td>If you want to create a time adjustment for the second buffer file (relative to the first file), select a time increment and type a new value or use the arrow buttons to create your time adjustment.</td>
</tr>
<tr>
<td>Launch a decode window</td>
<td>Enable this option if you want to view the merged buffer file immediately.</td>
</tr>
</tbody>
</table>

**Redirecting a probe instance**

Your local Observer analyzer may already have local probe instances defined, but you can add numerous remote probes, including GigaStor, too. You must first “redirect” the remote probe to your local Observer analyzer.

A probe may have multiple probe instances, which are useful if you need multiple users using the same probe simultaneously or if you have specific needs for each probe instance (for instance, packet capture, trending, and so on). When you connect to a probe, ensure you select the probe instance you need and not one being used by someone else.
Probe redirection can either be password protected or disabled, depending on the target probe.

To redirect a probe instance, complete the following steps:

1. Choose **Actions > Redirect Probe Instance(s)**. The Remote Probe Administration and Redirection window appears.
   
   If you have several remote probe instances already configured in your Observer software, this window lists them. If you see none, you currently have no remote probe instances configured.

2. Do one of the following:
   
   # If you see a remote probe instance you want to redirect, skip directly to 6 on page 65.
   
   # If your list is empty or missing the remote probe instance you want to redirect, proceed to 3 on page 65.

3. Click New. The Edit Remote Probe Entry dialog appears.

4. Type the IP address, or DNS address, of the remote probe. If you type a DNS name, it resolves to its IP address Observer connects.

5. If necessary for probe access, type a user name and password, and click OK.

6. Select the remote probe instance from the list, and click the Redirect Selected Probe Instance(s) button. The probe instances of the remote probe are then listed.

   Allow time for the remote probe to redirect. How long this operation can take is limited by a timeout countdown. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa for details.

7. Select a probe instance from the list, and click **Redirect Selected Instance**. The Redirecting Probe Instance dialog appears.

8. Select the “Redirect to this Observer” option, and click the Redirect button. Within 30 seconds the probe will connect with the analyzer.

9. (Optional) After the probe instance is connected, see configure the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.

10. Close the Probe Instance Redirection window.

If the operation succeeds, the remote probe instance is now redirected to the local Observer analyzer. Now you can use the remote probe instance just as you would if it was running on your local machine.

**Related Topics**

- How a probe uses RAM on page 267
- Fine-tuning the statistical buffer on page 52
- How a probe uses RAM on page 267
- Capturing network traffic on page 59
- Network Trending on page 146
- Understanding Real-time Statistics on page 33
- Connecting the probe to an Observer analyzer on page 239
- Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling on page 243
Pre-filtering your packet captures

By filtering your packet captures, you can extract and examine only network packets that meet certain criteria. You can introduce such a filter either before (pre-filter) or after (post-filter) you perform a packet capture.

Failing to click OK in 8 on page 66 causes Observer to discard any and all changes made since the Active Filters window first appeared in 1 on page 66, including all filters you may have created during that period of time.

This section describes pre-filters only; these filters affect what your future packet captures record. If you have an existing capture file and would like to post-filter it instead, see Post-filtering your packet captures on page 72.

To create and apply a pre-filter, complete the following steps:

1. Choose **Actions > Filter Setup for Selected Probe**. The Active Filters window appears.
3. Type a name for your new filter, and click OK. The Edit Filter window appears.
4. Use the editor to create a filter.
   
   See for a list of rules, types, and their usage.
5. Click OK to confirm your changes. Your new filter appears in the Active Filters window.
6. (Optional) To exclude, negate, or do the inverse of what you just defined, select the rule, right-click and choose “Toggle Include/Exclude on rule.” When you exclude a rule, a diagonal red line crosses through it.
7. (Optional) Activate your new filter by enabling it from the list.
8. Click OK to save your changes.

Tell me how to filter by protocol

Observer’s Protocol Data Field filter rule lets you search for specific values in selected protocol header fields. For example, you can filter for ICMP destination unreachable packets and wireless control, data, and management packets. You can also define your own custom protocol filter, either by port or search pattern.
Click Add and give the protocol filter a descriptive name and choose whether you want to define the protocol by a pattern filter or a port filter. After you click OK, the appropriate filter dialog is displayed allowing you to enter the pattern or port that defines the protocol.

**Tell me how to filter by pattern**

**Tip!** For hexadecimal patterns, you must enter the two-character representation of each byte in the hex pattern, with a SPACE between. For the example above, telnet is on port 23, which is represented as 00 17 in hex. Note the SPACE between the 00 and the 17. For binary patterns, you must enter each byte as two 8-position bit strings separated by a space (for example, 10011101 11001100).

When defining a Pattern rule, you can enter a specific offset from the beginning of a packet header (or from the beginning of a protocol’s header), and a specific pattern or data sequence to search for after that offset.

The offset is the decimal position to start looking for the sequence, in the byte order you specify (Big Endian or Little Endian, or most significant bit first or last, respectively). Enter the offset as a decimal value. If you select Search Using Range you can enter an ending offset beyond which the filter will not search for the pattern. You can also make the search case sensitive or insensitive.

The pattern itself is the actual ASCII, Regular Expression, Hex or Binary string that you are filtering for.

For example, to define an offset-sequencing filter to look for telnet packets (i.e., looking for TCP port 23) in one direction, the offset would be 34 (14 bytes of Ethernet header + 20 more bytes of IP header) and the hex pattern would be 00 17 (23 in hex).
To create a Hex Pattern rule for telnet in both directions, you could first tell Observer you want to start the offset at the IP-TCP protocol portion of the header (specify IP-TCP in the Protocol dialog), then tell Observer that you want the first offset to start immediately (port number is the first field after the TCP header) by entering 0 in the first offset field and 00 17 in the first Offset Filter area. This will filter for telnet packets in the direction of source to destination. To see the telnet response packets, you should enter a second offset (in the same dialog) for offset 2 and with a value of 00 17. The second offset specifies the destination port (this is the reason for the offset of 2).

### Table 9: Rules types

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address - IP Range/IP</td>
<td>Specify a hardware or IP address or range of addresses for source and destination. You can also limit the rule to apply only to packets from particular source or destination ports. For IPv4 packets, you can specify a subnet mask for inclusion/exclusion.</td>
</tr>
<tr>
<td>Packets with Comments</td>
<td>Filter for packets that have been commented by an Observer user and saved with a capture file. Comments are useful for annotating packets when two analysts are working on a problem together, perhaps sending each other captures from remote sites on a corporate network. There are no setup options. Available for post-filter only.</td>
</tr>
<tr>
<td>Error</td>
<td>Specify the categories of errors you want to filter for: CRC, Alignment, packet too small, and packet too large are available for all network types. You can also filter for Wireless WEP errors if you are analyzing a wireless network. If you are analyzing a WAN link, you can filter for WAN abort and RBIT errors. Observer also lets you filter for Token Ring error notifications when analyzing Token Ring networks.</td>
</tr>
<tr>
<td>Ethernet Physical Port</td>
<td>Allows you to filter on the physical port or link of the Ethernet capture card. When choosing to filter by link, you can also choose the direction (DCE or DTE).</td>
</tr>
<tr>
<td>Expert Packets</td>
<td>This rule lets you filter for Observer-generated Expert packets. These packets will only be generated if the Include Expert Load information packets box has been checked in Mode Commands Setup for Packet Capture. There are no setup options. Available for post-filter only.</td>
</tr>
<tr>
<td>Full Duplex Ethernet Port</td>
<td>Lets you filter for direction (DCE or DTE) on a selected full-duplex port.</td>
</tr>
<tr>
<td>Length (Bytes)</td>
<td>Specify a packet length, and whether you want to filter for packets that are less than, equal to, or greater than that length. You can also filter for packets that fall within a range of length values.</td>
</tr>
<tr>
<td>MPLS</td>
<td>The MPLS filter allows you to filter on any level of the MultiProtocol Label Switching protocol.</td>
</tr>
<tr>
<td>Numeric Value</td>
<td>This rule is useful when you need to filter for a numeric value (or range of values) that is embedded within a byte, word or double word.</td>
</tr>
<tr>
<td>Packet Time</td>
<td>Allows you to create a capture file with packets only before, after, or during a specific time. This filter is only available for pre- and post-filtering.</td>
</tr>
<tr>
<td>Partial Packet Payload for TCP/UDP</td>
<td>Allows you to capture (or not capture) specific payload data based on how the rule is configured. This is especially useful if you need to share packet captures. See Sharing packet captures with third-parties on page 141</td>
</tr>
<tr>
<td>Pattern</td>
<td>Use this rule to filter an ASCII, Regular Expression, hexadecimal, or binary string starting at specified offset or within a specified range. Hexadecimal and binary</td>
</tr>
<tr>
<td>Rule Type</td>
<td>Usage</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>Specify a port or range of ports for inclusion or exclusion.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select a protocol and field to filter on. For example, you can filter for ICMP Destination unreachable messages, or the presence of a VLAN tag.</td>
</tr>
<tr>
<td>VLAN 802.1Q</td>
<td>Match specific tag values for a Virtual Local Area Network (VLAN). You can filter on VLAN ID, priority (or a range of priorities) and the canonical format indicator. You can also filter for packets that contain any VLAN tag regardless of values.</td>
</tr>
<tr>
<td>VLAN ISL</td>
<td>VLAN ISL (Cisco proprietary VLAN). Beyond the VLAN ID, you can filter by user-defined bits.</td>
</tr>
<tr>
<td></td>
<td>Source address (MAC):</td>
</tr>
<tr>
<td></td>
<td>CDP and BPDU indicator:</td>
</tr>
<tr>
<td></td>
<td>High bits of source address:</td>
</tr>
<tr>
<td></td>
<td>Port index:</td>
</tr>
<tr>
<td></td>
<td>Reserved field:</td>
</tr>
<tr>
<td>VNTag</td>
<td>Allows you to define the direction, loop, DVIF, and SVIF for tags created by the vNIC in your virtual network.</td>
</tr>
<tr>
<td>WAN - DLCI Address</td>
<td>Specify a WAN DLCI by number.</td>
</tr>
<tr>
<td>WAN Port</td>
<td>Specify a WAN Port by number.</td>
</tr>
<tr>
<td>WAN Conditions</td>
<td>Lets you filter for direction (DCE or DTE or both), and logically chain tests for forward congestion packets, backward congestion packets, and discard eligibility.</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td>Enter or select a hardware address that corresponds to the wireless access point you want to capture traffic from.</td>
</tr>
<tr>
<td>Wireless Data Rate</td>
<td>Select a wireless data rate, and whether you want to filter for packets traveling at, under, or over that rate.</td>
</tr>
<tr>
<td>Wireless Channel</td>
<td>Select a wireless channel, and whether you want to filter for packets received from channels less than, greater than, or equal to that channel.</td>
</tr>
<tr>
<td>Wireless Channel Strength</td>
<td>Select a wireless signal strength, and whether you want to filter for packets received at, under, or over that signal strength.</td>
</tr>
</tbody>
</table>

**Tell me more about regular expressions**

Regular expressions provide a powerful method of building sophisticated search filters in which you can wildcard single characters, groups of characters, ranges of characters and numbers, and more. If you are familiar with Snort pattern-matching, you probably already have some familiarity with regular expressions.

The power of regular expressions comes from the ability to interpret meta-characters, which are a kind of programming code to specify search patterns. For example, in a regular expression, a period by itself means match any single character in this position. Suppose you want to find all references of the phone number 555-5155 in a large buffer filled with email traffic, for purposes of SOX audit. Depending on who typed the email,
the number could be separated with the dash, a space, or even a period. You could search separately for all these versions of the phone number, or you could use the regular expression (the forward slashes enclosing the string identify it as a regular expression; these are optional unless you use modifiers).

Rather than providing a comprehensive definition or tutorial, this section gives a few short examples which are intended to give you an idea of the kinds of things you can do with regular expressions.

```
/555.5155/
```

Which would match 555-5155, 555 5155,555.5155, etc. But it would also match 555X5155, 555BS155 etc. A more precise regular expression would be:

```
/555[-\.|\.]5155/
```

which demonstrates how to use the bracket and pipe (\[x|y|z\]) construct to search for any of a class of characters. This regular expression would only match 555-5155, 555 5155, and 555.5155. Note the slash in front of the period, which tells the filter to look for a literal period rather than interpreting the period as a meta-character. This use of the slash (interpret a meta-character as a literal character) is called slash-quoting.

Be careful with meta-characters. Consider the following regular expression:

```
/210.43.165.90/
```

This would match not only the IP address 210.43.165.90, but also any other string of digits that included the literal elements (i.e., non-meta-characters) in the string;

```
2105433165490
2107435165190
210x434165890
2103437165a90
```

would all match. As noted before, to specify a literal period match, you must slash-quote the meta-character: To match only the IP address 210.43.165.90, use the regular expression

```
/210\.43\.165\.90/
```

_Tell me more about modifiers_

The backslash not only turns meta-characters into literal characters, it is also used to give otherwise literal characters special meaning. In the Perl-compatible regular expressions supported by Observer, this includes modifiers or controls that affect the way the entire expression is interpreted. For example, regular expressions are case-sensitive unless you use the /i modifier:

```
/network instruments/i
```

Would match:

Network Instruments and NETWORK INSTRUMENTS and Network instruments

_Table 10 on page 70_ lists the modifiers supported by Observer’s regular expression filters. For more comprehensive definitions of all the meta-characters supported by Perl-compatible regular expressions, see [http://perldoc.perl.org/perlre.html](http://perldoc.perl.org/perlre.html).

**Table 10: Modifiers**

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>Make the search case insensitive.</td>
</tr>
<tr>
<td>s</td>
<td>Interpret the period (.) meta-character to include newlines.</td>
</tr>
<tr>
<td>m</td>
<td>By default, the string is treated as one big line of characters. <code>^</code> and <code>$</code> (two other meta-characters) match at the beginning and ending of the string. When <code>m</code> is set, <code>^</code> and <code>$</code> match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.</td>
</tr>
</tbody>
</table>

70 | Observer® (pub. 17.Sept.13)
<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>Whitespace data characters in the pattern are ignored unless escaped or inside a character class. This is useful for making long regular expressions more readable.</td>
</tr>
<tr>
<td>A</td>
<td>The pattern must match only at the start of the buffer (same as <code>^</code>)</td>
</tr>
<tr>
<td>E</td>
<td>Set $ to match only after the subject string. Without E, $ also matches immediately before the final character if it is a newline (but not before any other newlines).</td>
</tr>
<tr>
<td>G</td>
<td>Inverts the greediness of the quantifiers so that they are not greedy by default, but become greedy if followed by a question mark (<code>?</code>). Greediness refers to how many characters it will consider when trying to match strings of variable length.</td>
</tr>
</tbody>
</table>

**Activating and deactivating filters**

Typically, an active (activated) filter narrows the scope of your packet captures according to that filters' rules. For example, a filter that filters LDAP traffic—if active—causes only LDAP packets to be captured to the capture buffer. Furthermore, this effect is additive, meaning if you activate an additional filter, both filters' rules apply to future captures using a logical **OR** expression.

While enabling filters narrows the scope of your future packet captures, you can broaden that scope by enabling more filters. Alternatively, consider creating a “negative” filter to ignore packets you do not want to capture, and use that instead.

By activating more than one filter (if desired), all activated filters are linked together with a logical **OR** statement. Also, if you apply a rule that is not relevant to your pre-filter or post-filter scenario, that rule is ignored.

1. Choose **Actions > Filter Setup for Selected Probe**. The Active Filters window appears.
2. Browse the list of filters, and activate any filter by enabling it.
3. (Optional) Edit any filter by selecting it and clicking **Edit Filter**.
4. (Optional) If you want to deactivate all filters, activate the “Empty Filter” filter.
5. Click OK to save your changes.

All future packet captures now adhere to the rules of all active filters. When necessary, you can deactivate filters by disabling them during **2 on page 71**. To deactivate all active filters simultaneously, activate the Empty Filter filter.

**How to chain filter rules using logical operators**

Sometimes you need more sophisticated rules to capture packets from several addresses that meet complex criteria.

For these kinds of situations, you can chain multiple rules together into a single filter using the logical operators **AND**, **OR**, and **BRANCH**. The filter rule editor arranges the rules according to where they fall logically in the decision tree that you are building when using multiple rules. Each rule is represented by a rectangle, **ANDs** are represented by horizontal connecting lines, **ORs** and **BRANCHes** are represented by vertical lines.

**AND** and **OR** mean exactly what you would think. For example, the following rule would cause Observer to include only CRC error packets that originate from IP 255.0.0.1 (in other words, both the address rule **AND** the error rule must return positive for the packet to be captured).
If you want to capture traffic from 255.0.0.1 along with any error packets regardless of originating station, you would chain the rules with OR:

BRANCH is somewhat like an OR, but if the packet matches the first rule in the branch, it is matched only against the rules that follow on that branch.

When you chain multiple rules in a filter, packets are processed using the first match wins method: If a packet matches an exclude in the filter, further processing through that particular string stops. However, the packet is still processed through any subsequent OR or BRANCH rules in the filter.

**Post-filtering your packet captures**

By filtering your packet captures, you can extract and examine only network packets that meet certain criteria. You can introduce such a filter either before (pre-filter) or after (post-filter) you perform a packet capture.

This section describes post-filters only; these filters affect what you see in a loaded capture file. If you have an existing capture file and would like to pre-filter it instead, see Pre-filtering your packet captures on page 66.

To apply a post-filter, complete the following steps:

1. Choose **File > Select Probe Instance to Use for Packet Capture Files from Unknown Locations** and pick the probe instance with the settings you want to use to decode the buffer file. For more details about why this is important, see Opening files from unknown locations.
2. Choose **File > Prefilter and Analyze Capture Buffer**.
3. Navigate to the capture file you want to load, and select it.
4. Click Open. The Pre-Filtering window appears.
5. Enable the filters you want to apply to the capture file.
   
   If you do not see any pre-installed filters worth using, create your own.
6. Click OK. The capture file loads into Observer and you arrive at the Decode tab.

The Decode tab, of the Decode and Analysis window, displays each captured packet stored in the file matching the filter criteria. See Using the Decode pane on page 87 for more details.
Enabling command-line filtering

Command-line filtering is a method for post-filtering your packet captures via command line.

To enable command-line filtering:
1. Choose **Capture > Packet Capture**.
2. Click the Start button to begin your packet capture.
3. Click the Decode button.
4. Ensure the Decode tab is selected, and then click Settings.
5. Select “Enable type script filters” in the General tab.
6. Click OK to save your changes.

After command-line filtering is enabled, you can post-filter via command line as described in Post-filtering via command line on page 73.

Post-filtering via command line

As an alternative to traditional set-up of filters, it is possible to post-filter your packet captures via command line.

**Note:** Command-line filtering must be enabled before continuing. See Enabling command-line filtering on page 73.

Post-filtering via command line can save you time if you are comfortable building a filter using text. Some benefits of creating a command-line filter include:

- Ability to create a custom filters without losing focus of your capture window
- Ability to automatically convert to a traditional filter that is...
  - persistent, exportable, and shareable using NIMS or the network
  - suitable for more complex rules or later reconfiguration
- Familiarity with command-line interfaces may save you time

You can either type the text manually or use text building blocks to aid your syntax. To use this tool most efficiently, we highly recommend using saved packet captures.

This filtering process also works with an unsaved, real-time packet capture, but realize the data that appears after the filter is applied is static and unchanging. Your packet capture is still running, but new packets are not shown in the filtered view. Simply re-run your query from the active packet capture window to refresh your filtered data.

To post-filter via command line:
1. Choose **File > Load and Analyze Observer Capture Buffer**.
2. Navigate to the capture file you want to load, and select it.
3. Click Open. The capture file loads into Observer and you arrive at the Decode and Analysis tool.
4. Click the Type Script Filter button.
5. Build your filter, using the building blocks list as your guide.

Descriptions of each building block, including example usage, can be found in Table 11 on page 74.
6. Click Apply when finished.

   The packet capture is filtered according to the rules. If you encounter an error, or provide improper syntax, Observer alerts you that the filter must be fixed.

7. (Optional) To automatically convert your command-line filter to a traditional Observer filter, which can be kept forever, click Save Filter.

**Table 11: Building blocks**

<table>
<thead>
<tr>
<th>Building block</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-ip=</code></td>
<td><code>-ip=10.0.36.139</code></td>
<td>IPv4 Address—use this to filter for a single IP address (IPv4).</td>
</tr>
<tr>
<td></td>
<td><code>-ip=74.125.224.72</code></td>
<td></td>
</tr>
<tr>
<td><code>-ip_pair=</code></td>
<td><code>-ip_pair=10.0.36.139/10.0.36.154</code></td>
<td>IPv4 Pair—use this to filter for two IP addresses (IPv4) that have conversed with each other.</td>
</tr>
<tr>
<td></td>
<td><code>-ip_pair=10.0.36.139/74.125.224.72/</code></td>
<td></td>
</tr>
<tr>
<td><code>-ip_range=</code></td>
<td><code>-ip_range=10.0.36.1/10.0.36.255</code></td>
<td>IPv4 Range—use this to filter for any IP address (IPv4) within a set range. The IP addresses that form the beginning and the end of the range are included in the filter.</td>
</tr>
<tr>
<td></td>
<td><code>ip_range=192.168.0.20/192.168.0.100</code></td>
<td></td>
</tr>
<tr>
<td><code>-ipv6=</code></td>
<td><code>-ipv6=FE80::F544:9E0:9C81:9FB1</code></td>
<td>IPv6 Address—use this to filter for a single IP address (IPv6).</td>
</tr>
<tr>
<td></td>
<td><code>-ipv6=ff00::7f00:1</code></td>
<td></td>
</tr>
<tr>
<td><code>-ipv6_pair=</code></td>
<td><code>-ipv6_pair=FE80::F544:9E0:9C81:9FB1/2002::4A7D:E048</code></td>
<td>IPv6 Pair—use this to filter for two IP addresses (IPv6) that have conversed with each other.</td>
</tr>
<tr>
<td><code>-ipv6_range=</code></td>
<td><code>-ipv6_range=FE80::A00:2401/FE80::A00:24FF</code></td>
<td>IPv6 Range—use this to filter for any IP address (IPv6) within a set range. The IP addresses that form the beginning and the end of the range are included in the filter.</td>
</tr>
<tr>
<td><code>-mac=</code></td>
<td><code>-mac=00:0C:85:BD:08:80</code></td>
<td>MAC Address—use this to filter for a single MAC (hardware) address.</td>
</tr>
<tr>
<td></td>
<td><code>-mac=00:50:56:2E:AB:A0</code></td>
<td></td>
</tr>
<tr>
<td>Building block</td>
<td>Examples</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>- mac_pair=</td>
<td>mac_pair=00:50:56:2E:AB:A0/00:0C:85:1</td>
<td>MAC Address Pair—use this to filter for two MAC addresses that have conversed with each other.</td>
</tr>
<tr>
<td>- mac_range=</td>
<td>mac_range=01:00:5E:00:00:00/01:00:5E:00:00:00</td>
<td>MAC Address Range—use this to filter within a set range. The IP addresses that form the beginning and the end of the range are included in the filter.</td>
</tr>
<tr>
<td>- tcp=</td>
<td>tcp=22, tcp=80, tcp=25901, tcp=25903, tcp=63268</td>
<td>TCP Port—use this to filter for a single TCP port number. As with other building blocks, you can add more using an -and building block.</td>
</tr>
<tr>
<td>- tcp_pair=</td>
<td>tcp_pair=63268/25901, tcp_pair=25901/25903, tcp_pair=3389/3391</td>
<td>TCP Port Pair—use this to filter for any pair of TCP ports that have conversed with each other. Direction is a non-factor for this building block; the filter looks for a pair of ports regardless of source or destination.</td>
</tr>
<tr>
<td>- tcp_range=</td>
<td>tcp_range=0/5000, tcp_range=35/1023, tcp_range=60000/63500</td>
<td>TCP Port Range—use this to filter for communication on any TCP port between the specified range. The port numbers that form the beginning and the end of the range are included in the filter. Direction is a non-factor for this building block; the filter looks for a pair of ports regardless of source or destination.</td>
</tr>
<tr>
<td>- udp=</td>
<td>udp=53, udp=88, udp=26000, udp=61001</td>
<td>UDP Port—use this to filter for a single UDP port number. As with other building blocks, you can add more using an -and building block.</td>
</tr>
<tr>
<td>- udp_pair=</td>
<td>udp_pair=63240/27015, udp_pair=49501/42</td>
<td>UDP Port Pair—use this to filter for any pair of UDP ports that have conversed with each other. Direction is a non-factor for this building block; the filter looks for a pair of ports regardless of source or destination.</td>
</tr>
<tr>
<td>- udp_range=</td>
<td>udp_range=27901/27910, udp_range=27030/27000, udp_range=0/1023</td>
<td>UDP Port Range—use this to filter for communication on any UDP port between the specified range. The port numbers that form the beginning and the end of the range are included in the filter. Direction is a non-factor for this building block; the filter looks for a pair of ports regardless of source or destination.</td>
</tr>
<tr>
<td>Building block</td>
<td>Examples</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| -vlan= | -vlan=101  
-vlan=101 -and -vlan=102 | VLAN ID—use this to filter for a single VLAN ID. As with other building blocks, you can add more using an -and building block. |
| (space character) | -tcp=80 -tcp=8080  
(TCP port 80 -OR- TCP port 8080) | Use this to denote a logical OR statement. Use this to include more items and broaden the scope of your filter. |
| / (forward slash) | -ip_range=10.0.36.1/10.0.36.255  
(Any IPv4 address between 10.0.36.1 and 10.0.36.255) | Use this to denote a value range or any pairs. Do not add a leading or trailing space character to the forward slash. |
Chapter 6: Decodes

Decoding network traffic

The ability to decode and analyze network traffic is equally as important as the ability to collect it. This section describes how to decode and analyze packet captures, including advanced post-filtering techniques and other settings.

Observer can easily decode and analyze packet capture files, including multiple file formats. Even captures made using third-party tools can be analyzed in Observer, as long as they are based on Ethernet, Token Ring, or FDDI traffic. This section describes several methods for decoding network traffic using Observer.

The simplest method for decoding network traffic is to load a capture file—a saved file that is a complete, self-contained packet capture collected during an earlier time. If you do not have access to a capture file and need help creating one, see Capturing network traffic on page 59 before continuing. Also, that section describes how to decode a real-time packet capture, while this section does not.

If you are already comfortable loading capture files and decoding their contents, this section may not be useful to you. Advanced decoding methods are described in Preparing expert decoding techniques on page 93.

To decode network traffic stored in a capture file, complete the following steps:

1. Choose File > Load and Analyze Observer Capture Buffer.
2. Navigate to the capture file you want to load, and select it.
3. Click Open.

The capture file loads into Observer and you arrive at the Decode and Analysis tool. The Decode tab displays each captured packet that is stored in the file.

After completing this task:

See Using the Decode pane on page 87 for more details.

I have a packet capture to analyze. What file formats can Observer load?

Except for XML, Observer can load all of the files formats that it can save to, plus the DMP format. Simply, Observer can load any packet capture of these formats:

BFR
Removing duplicate packets

Duplicate packets are packets that are captured twice or multiple times by Observer. Typically, duplicates are a result of how data is sent to the Observer analyzer. For a switch, the use of a SPAN/mirror port and/or trunk is required to capture data. Knowing this, the following scenarios may produce duplicate packets—which are then seen by Observer:

- If a SPAN/mirror port is configured to send both ingress (in) and egress (out) data from multiple ports, any communication between any two ports being monitored results in a duplicate packet.
- If a trunk is monitoring multiple VLANS, data flowing between VLANS is seen as duplicate packets.
- If Observer is monitoring data pre- and post-route. Meaning, a single packet is seen at one location pre-route and again post-route. The post-route packet is considered by Observer as a duplicate packet.

While this is harmless as it pertains to your network working correctly, Observer identifies these as duplicate packets. There are two ways of dealing with this situation:

- Configure the SPAN/mirror port or trunk to show only ingress or egress traffic, but not both.
- Use Observer to remove duplicate packets from an existing capture file, as described in this section.

Observer includes a feature that removes the “noise” caused by duplicate packets without affecting the underlying packet capture data. This feature is a special version of the standard capture buffer file-loader. To remove duplicate packets (i.e. skip them) while loading a capture buffer file, complete the following steps:

1. Choose File > Load and Analyze Observer Capture Buffer (Skip Duplicates).
2. Type, or navigate to, the capture file you want to load.
3. Select your criteria for how duplicate packets are handled. We recommend using the default settings first.
4. Click Open. The capture file loads into Observer and you arrive at the Decode and Analysis tool. See Using the Decode pane for more details.
5. (Optional) If duplicate packets are still visible, repeat the process and select different duplicate packet handling criteria.

Duplicate packets should now be skipped/ignored in your capture file. No permanent changes are made to your loaded capture file, so if you want to make your changes permanent, save your results as a new capture file.

Opening files from unknown locations

You may not know where or how a packet capture was taken. This can cause some confusion when decoding a foreign buffer file, because probe instance settings that may be unique to that probe instance may be saved in the buffer file. When opening a capture buffer, Observer uses the probe instance settings of the first probe instance in its list unless you specify which probe instance to use.

You may want to use this option if you are:

- Unsure of the header, MPLS analysis, or ToS/QoS settings
Decrypting wireless data

Decoding protocols on non-standard ports (although user-defined protocols are not decoded for a NetFlow instance)

This option is not intended to allow you to open a capture from a different topology. For instance, it will not make sense to use an Ethernet Probe instance to open a WAN capture or a Wireless probe instance to open a Fibre Channel capture.

Create a probe instance just for analyzing packet captures that you load into the Observer analyzer. By using a dedicated probe instance, you can easily and temporarily change the probe instance settings. This allows you to view the buffer files using settings for the type of probe instance used to capture the file, and more importantly, you do not need to change any probe instance you use for monitoring.

Do this by choosing File > Select Probe Instance to Use for Packet Capture Files from Unknown Locations and selecting a probe instance with settings you think are similar to the capture adapter used to capture the file.

Private key locations per server

Microsoft Lync Server

Microsoft Lync Server encrypts all of its VoIP traffic, including the call set up process. To decrypt a Microsoft Lync server conversation, you must have the security certificate and Observer must see the telephone’s power up.

By default, the Lync Server key is not exportable. You must create an exportable key for Observer to use. Getting the Lync Server key is similar to that for the IIS Web Server. See Windows IIS Web Server on page 79.

Apache Web Server

Perform a search for the file with the name “server.key”. Check the format of the server.key file to ensure it is not an encrypted private key file. See Example of an encrypted private key file on page 80.

However, if the private key file is encrypted, the private key file must be decrypted using the openSSL command line tool and the password that was used to encrypt it. This utility can be obtained by following an appropriate link as follows:

- http://www.openssl.org
- For Windows compatible versions, use a search engine to search for the terms “Download,” “Win32,” and “OpenSSL”.

After obtaining the openSSL command line utility, the private key file can be decrypted using the following command (choose the appropriate locations for the input and output files):

openssl rsa -in server.key -out UnencryptedKey.key [enter passphrase]

You can now use the newly created output key, in Observer, to successfully decrypt and analyze encrypted network traffic.

Windows IIS Web Server

Windows does not contain a searchable private key file. The key file must be extracted from the website server certificate, and the server certificate must contain the private key file. Use the following Microsoft Support
document to export your server certificate and private key to a single .pfx file: [http://support.microsoft.com/kb/232136](http://support.microsoft.com/kb/232136) (How to back up a server certificate in Internet Information Services).

After you successfully export the .pfx file (PKCS #12), you must obtain the openssl utility. This utility can be obtained by following an appropriate link as follows:

- [http://www.openssl.org](http://www.openssl.org)
- For Windows compatible versions, use a search engine to search for the terms “Download,” “Win32,” and “OpenSSL”.

With a valid .pfx server certificate backup file and the openssl utility, the following command should be used (choose the appropriate locations for the input and output files):

```
openssl pkcs12 -nodes -in c:\mycertificate.pfx -out c:\server.key
```

You can now use the newly created output key, in Observer, to successfully decrypt and analyze encrypted network traffic.

### Example of a non-encrypted private key file

A normal, non-encrypted private key file should contain text of the following format. Notice the absence of a “Proc-Type: ENCRYPTED” header. A file of this format is usable by Observer.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD7uhNymd6WCOORqH0rd5zs4FEewCX2JrKtm0dmTf44SVaGvFLF1
vakeOYP/sF54aa2aN0FcbFaS2w3IZWum4sCtqtvb8Zii1+13VCdyR+2SRx9GMou
Snol/6FlS6m+C0ghq6g0ILOiTATJNf+MOEC2wbMylkz1jPVUOXE91EG0A0Q1DAQAB
AcgAFQoYogWEvmQRPw2WNN6YxnJKxVGBGcZrPdWfgC0/ITXhYU1t2I47QLd+ni
-----END RSA PRIVATE KEY-----
```

### Example of an encrypted private key file

An encrypted private key file may have the following format, which indicates that the private key file obtained contains an RSA Private Key, where the text for the key itself is encrypted. A file in this format will generate an error dialog stating “Error Loading the Private Key File!” You must decrypt this key file before it will function.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,7BC....
JHQ8U0pDbeFM9h2jZSmiuqdxqo2a2q/MiX43Xa4Es6nKmsu9oI/ZfpIdAh18qwtsD
m25bQRlXD9AXeIry+0tG2ibUaphQEv1995FWUsh8N9dVumsqykmMxSwND7tkbHB
IO/VVSAAL9bV3dbi5nbMwMnPFG+YCI3S90GAK4ZRIqHRQ9fd/ZAvP8kV9ilwCmX6
swFlNBLGuKF1lJ9qkyr+0OqulrAyZAB2UThGCJJetELFtV4mLmIaHdgD1cUgpJp==
-----END RSA PRIVATE KEY-----
```

### Decoding encrypted network traffic

**Prerequisite:** Observer Expert or Observer Suite

Observer can decode network traffic that is encapsulated within Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols, but the traffic must first be decrypted. This feature of Observer allows you to make meaningful interpretation of encrypted traffic that you are authorized to view. A private key is required; you cannot decrypt any traffic without having the private key, ensuring you are the facilitator of the encrypted traffic.

You can also choose whether and how to translate the SSL/TLS port number (443) in the output. For example, if decrypting encrypted HTTP, you may want to change the port number to 80.
You can also optionally strip all TCP flow control packets (the SYN requests and ACKs used to establish and maintain the connection) from the decrypted output.

Decryption can only be performed post-capture, and the actual decryption process is performed locally. There is no central repository for private keys in either Observer or NIMS (if you own it), so each Observer installation wanting to decrypt a stream must have a local copy of the private key.

If you are decrypting network traffic using a private key via a SafeNet HSM card and that card is located on a NIMS server, you must provide the slot number under “Use SSL RSA Private Key From SafeNet HSM Card on NIMS” seen in Figure 24 on page 82.

If you are concerned about security for the decoding of your encrypted traffic, there are three methods available to you:

- **Use SSL Private Key from File.** Even though the private key provides a certain level of security, this is the least secure option because of access to the private key file itself may be compromised. Even this option though provides greater access control than not using any security at all.

- **Use SSL RSA Private Key from HSM.** This is a more secure than the above option because the private key is managed by HSM. Since the HSM maintains the private key, more access control exists.

- **Use SSL RSA Private Key from HSM on NIMS.** This is the most secure option. NIMS controls Observer’s access. Additionally, a key must be issued by the HSM. To use the key, you must know the token name of the HSM and provide it to decrypt the conversation. It is not stored in Observer. Observer passes the token name to NIMS, NIMS compares the name that was passed to its list of names, if one matches, it is passed to HSM where access is granted or denied. No key itself is ever passed during this entire process. Most likely, a security team manages and maintains the HSM and is a separate group from the network administrators. Using the private key from HSM on NIMS, Observer is only able to decrypt the selected client/server connection or port pair. If another client/server connection or port pair must be decrypted, then a new key must be obtained.

To decode encrypted network traffic, complete the following steps.

1. Choose **File > Select Probe Instance to Use for Packet Capture Files from Unknown Locations** and pick the probe instance with the settings you want to use to decode the buffer file. For more details about why this important, see Opening files from unknown locations.

2. Choose **File > Load and Analyze Observer Capture Buffer.**

3. Navigate to the capture file you want to load, and select it.

4. Click Open. The capture file loads into Observer and you arrive at the Decode and Analysis tool.

5. Do one of the following:
   
   - Click the Expert Analysis tab. Then, click the TCP Events or UDP Events group tab and select the target encrypted conversation.
   
   - Click the Decode tab. Then, select the target encrypted conversation.

6. Right-click the encrypted conversation and select Decrypt SSL Conversation. The SSL/TLS Decryption Parameters dialog appears.
7. Provide the location of your private key file.

8. (Optional) Further customize your decryption by changing the extra options, including if you use a SafeNet HSM card for FIPS 140-2 compliance. Contact your SafeNet HSM card administrator or your corporate key librarian for the specifics about the slot number, key name, and user PIN. See Security, privacy, and regulatory compliance for more information.

9. Click OK to begin decrypting the SSL/TLS encrypted conversation. The length of time decryption requires is proportional to how many packets are processed.

You successfully decrypted the conversation and can now decode and analyze its contents.

After completing this task:

If you cannot locate the private key file used for SSL decryption or an error states “Error Loading the Private Key File!,” there are two possible reasons:

- You cannot locate, or do not have access to, the private key file necessary for decryption. You must obtain it.
- The private key file you do have is improperly formatted or encrypted, and will not work. You must decrypt it.

In either of these scenarios, you must find the location of the private key file to begin troubleshooting. The location differs for each web server application, so the following are instructions for Apache Web Server and Windows IIS Web Server. If you don’t use either of these web server applications, please refer to the documentation for your specific web server application.

**Decoding NetFlow or sFlow streams**

If you set up a standard probe instance (non-NetFlow or non-sFlow) to monitor a segment that includes NetFlow or sFlow reporting streams, these packets are treated as any other network traffic. Observer’s statistical displays, such as Top Talkers, do not include the data reported through NetFlow/sFlow.

Therefore, to force Observer to recognize and interpret the NetFlow/sFlow data and update statistical displays accordingly, complete the following steps:
1. Choose **File > Select Probe Instance to Use for Packet Capture Files from Unknown Locations** and pick the probe instance with the settings you want to use to decode the buffer file. For more details about why this important, see *Opening files from unknown locations*.

2. Choose Capture > Packet Capture or load a saved capture.

3. Click the Decode button. The Decode and Analysis window appears.

4. Click the Decode tab, then Choose Tools > Process NetFlow or sFlow data. The Select Data Source window appears.

5. Choose the data source you want to process.

6. (Optional) Change your ToS/QoS settings if necessary.

7. Click OK.

A temporary post-filter buffer is created in memory that interprets the NetFlow or sFlow statistics and updates Observer’s statistical displays accordingly.

**Configuring a NetFlow device**

To configure a NetFlow device to work with Observer, you must first set up a cache on the router or switch to hold statistics for each interface (i.e. device port) being monitored, then define the IP address and UDP port of the collector (i.e., the Observer analyzer or probe). On a Cisco router running IOS, the commands look like this:

1. Define which interfaces to monitor:

   ```
   Router1# config t
   Router1(config)# int ser0/0
   Router1(config-if)# ip route-cache flow
   [Repeat for each interface being monitored]
   ```

2. Define the IP address and UDP port of the collector:

   ```
   Router1# config t
   Router1(config)# ip flow-export version 9
   Router1(config)# ip flow-export destination 192.168.1.12 9996
   ```

**Configuring an sFlow device**

To configure an sFlow device to work with Observer, you must define the collector IP address and UDP port, and optionally configure a polling interval and sampling rate (although in most cases the default interval and sampling rate are appropriate). Here is what the commands might look like on a Foundry Layer 3 switch:

1. Define which interfaces to monitor:

   ```
   Switch1# config t
   Switch1(config)# sflow enable
   Switch1(config)# interface ethernet 1/1 to 1/8
   Switch1(config-mif-1/1-1/8)# sflow forwarding
   ```

2. Define the IP address and UDP port of the collector:

   ```
   Switch1# config t
   Switch1(config)# sflow destination 10.10.10.1 9099
   ```

   Specifying a UDP port is optional; the default is 6343. In most cases, the default polling interval and sampling rate are appropriate, but if you need to adjust them, use the sFlow polling-interval and sFlow sample commands:

   ```
   Switch1# config t
   Switch1(config)# sflow poll-interval 120
   Switch1(config)# sflow sample 30
   ```
This would cause the device to push sFlow data to the target collector every 120 seconds, with a sampling rate of 1 packet in 30.

**Tell me more about IPFIX/NetFlow Data Sources**

This screen allows you to add IPFIX and NetFlow Data Sources so that Observer can create trending data for those devices. Click the Add Entry to add a NetFlow device. Click “Retrieve Interface Names and Speed from Device” to automatically get the device name and speed from the device so that this information is used in reports throughout Observer and Observer Reporting Server.

### Registering custom decode DLLs

Observer allows you to integrate custom-written decode applications into its environment. To do this, choose Tools > Register Custom Decode.

Custom decodes are only available in Observer Suite. Also, Network Instruments does not provide technical support for creating or maintaining custom decodes—only the tool itself.

Observer allows you to write your own protocol decoder, if you have expert knowledge in the following:

- The protocol you are writing the decoder for
- The C++ Programming Language

In addition, it helps if you have Microsoft C++ Developer’s Studio, as Network Instruments has included an example project file for that environment along with the example source code. The Custom Decode Kit is contained in the C:\Program Files\Observer\Drivers\CustomDecodeKit directory (CustomDecodeKit.exe, which is a self-extracting archive). Along with the example project and source files, the Kit also includes an Acrobat PDF file that outlines the steps in building a DLL.

Once you have built a DLL and placed it in the Program Files\Observer directory, select Register Custom DLL from the Tools menu and add the new DLL to the list of registered DLLs. Once a DLL has been registered, the new decode will be available in the Decode and Analysis tree control.

### Replaying a packet capture

**Note:** Replaying a packet buffer is not the same as stream reconstruction. For stream reconstruction, see Reconstructing TCP data streams on page 100.

Replay Packet Buffer mode, like Traffic Generator mode, permits the user to create traffic on the network. Unlike Traffic Generator; however, Replay Packet Buffer mode sends some or all of a previously saved capture buffer onto the network.

To replay a packet capture, you must be using a local probe instance. The probe instance on which you want to replay a packet capture cannot be on a remote system. Choose Tools > Replay Packet Buffer.

- Dial displays—the left dial displays the speed (packets per second) of the buffer as it is being replayed. The right dial displays the speed (bytes per second) of the buffer as it is being replayed.

Statistics pane:

- This pane displays totals transmitted for the replay, bit rates, and animation to show that a replay is in progress.

Settings pane:

- Select buffer and button—allows you to enter the name of the buffer (.BFR) file to be transmitted. Enter the name and address of the file to be transmitted or click the Select buffer button to browse to it.
First packet—allows you to set the number of the first packet in the buffer to be transmitted.

Last packet—allows you to select the number of the last packet in the buffer to be transmitted.

Speed (pkt/sec)—allows you to set the speed, in packets per second, which you would like to attempt to transmit the buffer.

If the speed is set at a higher number than the Observer computer’s NIC is capable of, it will only be able to transmit the buffer at the NIC’s maximum rate.

Generation Mode:

Time period to generate (1-65500 sec)—packets will be generated at the configured speed for the number of seconds specified in the edit box. If the specified contents of the buffer are completely transmitted before the end of that period, the transmission will loop back to the first packet as chosen above.

Number of times to replay this buffer—the buffer file, or the selected portion of it, will be replayed the number of times specified in the edit box.

---

**Working with packets**

1. Choose **Capture > Packet Capture** or load a saved capture.
2. Click the Decode button. The Decode and Analysis window appears.
3. Click the Decode tab, then select a packet.
4. Right-click and a menu appears with many options. Those options are described in **Table 12**.

   This list is configurable and contextual, that is, it varies based on the type of packet that is selected.

**Table 12: Packet options**

<table>
<thead>
<tr>
<th>Menu option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Packet Capture on Hardware/IP Address</td>
<td>Starts a new packet capture filtered on source, destination, or both, using either hardware or IP addresses to identify systems.</td>
</tr>
<tr>
<td>Fast Post-Filter on Hardware/IP Address</td>
<td>Applies a filter to the current buffer. Observer will open a new decode window, loading only the packets you have chosen to include.</td>
</tr>
<tr>
<td>Create Filter on Hardware/IP Address</td>
<td>Same as Start Packet Capture options described above, except these options let you preview and edit the filter without actually starting a capture.</td>
</tr>
<tr>
<td>Set Flag on Hardware/IP Address</td>
<td>Flags all packets that have the same address criteria (source, destination, pair) as the selected packet.</td>
</tr>
<tr>
<td>Remove Offset Flags</td>
<td>Removes any offset flags that have been set.</td>
</tr>
<tr>
<td>Remove Hardware/IP Address Flags</td>
<td>Removes all address flags that have been set.</td>
</tr>
<tr>
<td>Connection Dynamics</td>
<td>Opens a Connection Dynamics chart of the selected TCP conversation. See Using Connection Dynamics on page 98.</td>
</tr>
<tr>
<td>Add Comment</td>
<td>Allows you to add comments to specific packets in the buffer file.</td>
</tr>
<tr>
<td>TCP Dump</td>
<td>Sometimes may options after it such as (HTTP) or (NetBIOS session) when it can identify the type of packets. When selected the packets are processed and appear in the Expert Analysis tab.</td>
</tr>
<tr>
<td>Menu option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reconstruct Stream</td>
<td>Reconstructs the TCP stream and any files or other data objects exchanged. See Reconstructing TCP data streams on page 100.</td>
</tr>
<tr>
<td>Decrypt SSL Conversation</td>
<td>Shows you the decrypted SSL conversation if you have the SSL key.</td>
</tr>
<tr>
<td>Decrypt TACACS+ Conversation</td>
<td>Shows you the decrypted TACACS+ conversation if you have the TACACS+ shared secret.</td>
</tr>
<tr>
<td>Previous/Next Packet in</td>
<td>Lets you follow a TCP conversation backward and forward in time.</td>
</tr>
<tr>
<td>Conversation</td>
<td></td>
</tr>
<tr>
<td>Maximize Pane</td>
<td>Zoom in to the current pane (headers, decode, or hex window).</td>
</tr>
<tr>
<td>Packet List Color Setup</td>
<td>Displays the Color dialog.</td>
</tr>
<tr>
<td>Set Decode Relative Time</td>
<td>Reset timestamps.</td>
</tr>
<tr>
<td>Origin to Selected Packet</td>
<td></td>
</tr>
<tr>
<td>Calculate Cumulative Bytes</td>
<td>Displays the byte count from the beginning of the capture (or the relative time origin) to the current packet.</td>
</tr>
</tbody>
</table>

5. For additional settings, choose **Settings > General tab**. These settings are described in **Table 13**.

**Table 13: Expanded packet options**

<table>
<thead>
<tr>
<th>Menu option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set focus on the last packet</td>
<td>Causes the packet display to set focus on the last (rather than the first) packet in the capture, allowing you to see the most recently captured information. This is particularly useful when viewing a capture live where the user wishes to examine data as it arrives.</td>
</tr>
<tr>
<td>Expand 2nd level trees</td>
<td>Causes the tree decode display to expand all second level trees.</td>
</tr>
<tr>
<td>Expand 3rd level trees</td>
<td>Causes the tree decode display to expand all third level trees.</td>
</tr>
<tr>
<td>Expand 4th level trees</td>
<td>Causes the tree decode display to expand all fourth level trees.</td>
</tr>
<tr>
<td>Use EBCDIC for displaying SNA data</td>
<td>If the packet contains SNA (Service Network Architecture) data, selecting this box causes Observer to use EBCDIC for representing characters as numbers when displaying SNA data. EBCDIC is used almost exclusively on IBM mainframe computers.</td>
</tr>
<tr>
<td>Use EBCDIC for all data</td>
<td>Observer uses EBCDIC for representing characters as numbers when displaying all data. EBCDIC is used almost exclusively on IBM computers.</td>
</tr>
<tr>
<td>Decode TCP payload in packets with bad</td>
<td>Observer decodes the packet payload even if the checksum for that packet fails. The default behavior is to not decode these packet payloads.</td>
</tr>
<tr>
<td>checksum</td>
<td></td>
</tr>
<tr>
<td>Show full duplex 'Port' or 'Link' in 'DCE/DTE' parameters</td>
<td>Observer shows which side of a full-duplex connection the packet was captured from.</td>
</tr>
<tr>
<td>Show preview of summary comment text</td>
<td>Shows a truncated version of any comments you have added to the packet in the packet comment column.</td>
</tr>
<tr>
<td>When loading a local buffer file, exclude</td>
<td>Choose to enable/disable the display of Observer Expert packets (the packets are not actually stripped from the file, they are just filtered from display).</td>
</tr>
</tbody>
</table>
Using the Decode pane

The Decode and Analysis tab is where the captured buffer is decoded and the packet conversations can be examined and analyzed in detail. This pane has several tabs on it that show you specific information about your packet decode. These include:

<table>
<thead>
<tr>
<th>Expert Analysis</th>
<th>Displays all general, non-conversation specific problems that Observer finds when analyzing the packet capture. See Using the Expert Analysis feature on page 94.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decode</td>
<td>Shows the raw packets for you to examine yourself. The tab has three sections. The top section shows the list of packets. Right-click any of the packets to see a list of actions you can take on it. The middle section is detailed information about the selected packet. The bottom section is the contents of the packet in hexadecimal and EBCDIC. Press F4 to maximize this bottom section to see more of the packet contents. There are numerous settings, such as colors and protocol forcing, that you can configure by clicking the Settings button. You can save buffers, search for packets and other actions using options under the Tools menu.</td>
</tr>
<tr>
<td>Summary</td>
<td>Summarizes network details, errors, data rates, packets, and utilization for the traffic Observer saw. The information on the Summary tab is only for the packets seen on the Packet Capture window or in the buffer file you loaded.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Lists the protocols seen and shows how many packets and bytes of that protocol were seen, what percentage of the total packets or bytes that is, and utilization.</td>
</tr>
<tr>
<td>Top Talkers</td>
<td>Shows what devices are the most active on your network. The MAC address, DNS name, IP address are listed. There are several tabs to see the data in different ways. There are numerous settings that you can configure by clicking the Settings button. This feature is very similar to the Top Talkers covered in Discovering current top talkers on the network on page 25.</td>
</tr>
<tr>
<td>Pairs (Matrix)</td>
<td>Graphs the top 10 most active device pairs by packets per second. This feature is very similar to the Pairs Matrix in Discovering conversations between local devices and the Internet on page 19.</td>
</tr>
<tr>
<td>Internet Observer</td>
<td>Has three tabs that show a graph of the packets total by device on the Internet Patrol tab, and lists of IP Pairs and IP Subprotocol. There are numerous settings that you can configure by clicking the Settings button. This feature is very similar to the Internet Patrol in Discovering conversations between local devices and the Internet on page 19.</td>
</tr>
<tr>
<td>Application Transaction Analysis</td>
<td>Contains several tabs for the applications that Observer analyzes, including response time and statistics, URL statistics, FIX, and SQL.</td>
</tr>
</tbody>
</table>
For more details about Application Transaction Analysis, see [What is Application Transaction Analysis?](#) on page 152.

**VLAN**

Lists a summary and stations of VLAN activity. Shows packets, bytes, broadcasts, multi-casts, and utilization. You can configure how the list appears by using the Settings button. This feature is very similar to VLAN Statistics described in [Viewing optional VLAN statistics](#) on page 35.

**Forensic Analysis**

Displays anomalies based on Snort rules on the Forensics Summary or Forensics Analysis Log tabs. You can choose what Snort rules to use to analyze the data by clicking the Settings button. This feature is similar to Forensic Analysis described in ../observer/using_network_forensics_to_track_acceptable_use_or_compliance.html.

**Access Point (AP) Statistics**

Shows wireless access point statistics. This is similar to [Viewing wireless access point statistics](#) on page 22.

**Fibre Events**

Shows details related to your Fibre traffic.

**4G LTE Analysis**

Contains several tabs specific to 4G LTE devices, applications, and connections. For more details about 4G LTE Analysis, see [Analyzing 4G LTE packet captures](#) on page 104.

---

**Figure 25: Decode tab**

- **Decode**
- **Packet Header or Right-Click Menu**
- **Packet Header**

After you are in the view screen, select a packet in the top window to display the packet decoded information in the middle window. There are three window panes:

- the packet header pane.
- the decode pane.
- the raw packet display pane.

The three panes are fully sizeable by dragging the borders up or down. Packets that Observer does not recognize are shown in raw mode in the decode and raw panes. Each pane has a context-sensitive right-click menu. For example, you can right-click a packet header, and (if it is not a broadcast packet) immediately jump to a connection dynamics display of the network conversation.
The packet header pane shows the following:

- **Packets**—the number of packets currently in the buffer.
- **First**—the first packet number in the buffer.
- **Last**—the last packet number in the buffer.
- **Offset**—the offset display is only shown if you have highlighted a section of the decode screen. When a section of the decode screen is highlighted, Observer’s active highlight option is activated. This option shows the highlighted sections of actual data in the raw area of the packet decode screen, including the offset of the value from the beginning of the packet. This information can be used to configure an offset filter for that value.

You can highlight an item of the decode in the Raw Packet Display area and right-click it. Two options will be displayed: Start Packet Capture on Segment/Offset or Create Filter on Segment/Offset. These options are only available in this area.

For details about the packet header menu, see *Working with packets on page 85.*

### Using keyboard shortcuts

When focus is on the packet header pane, use the Up and Down arrow keys to move to the previous or next packet in the capture buffer. PgUp and PgDn scroll through a pane of packet headers at a time. CTRL-PgDn (or CTRL-End) moves to the end of the buffer; CTRL-PgUp (or CTRL-Home) moves to the beginning of the buffer.

To move backwards and forwards through a conversation (which consists of packets exchanged between a pair of IP/ports) use CTRL+Shift+Down Arrow and CTRL+Shift+Up Arrow. The F4 key maximizes the current pane; pressing F4 again returns the pane to its previous size.

When focus is on the packet header pane:

- **> or >** Move to the next or previous packet.
- **F7 or F8** Move to the next or previous packet.
- **Ctrl+Shift+> or Ctrl+Shift+>** Move to the next or previous packet in the conversation. A conversation is a set of packets exchanged between IP/Port pairs.

When focus is on the decode pane:

- **> or >** Move to the next or previous line of the decoded packet.
- **> or >** Collapse/expand protocol tree branch.
- **F7 or F8** Move to the next or previous packet in the buffer (same as arrow keys when focus is on the packet header pane).
- **Ctrl+> or Ctrl+>** Move to the next or previous packet in the buffer (same as arrow keys when focus is on the packet header pane).
- **Ctrl+Shift+> or Ctrl+Shift+>** Move to the next or previous packet in the conversation. A conversation is a set of packets exchanged between IP/Port pairs.

When focus is on the hexadecimal pane:

- **> or >** Move to the next or previous line of the hex (or character) display.
- **> or >** Move forward or backward one character at a time.
- **F7 or F8** Move to the next or previous packet in the buffer (same as arrow keys when focus is on the packet header pane).
Ctrl+ > or Ctrl+ >  Move to the next or previous packet in the buffer (same as arrow keys when focus is on the packet header pane).

Ctrl+Shift+ > or Ctrl +Shift+ >  Move to the next or previous packet in the conversation. A conversation is a set of packets exchanged between IP/Port pairs.

**Saving a packet capture**

1. Choose Capture > Packet Capture or load a saved capture.
2. Click the Decode button. The Decode and Analysis window appears.
3. Click the Decode tab, then choose Tools > Save Capture Buffer. The Save Packet Capture dialog opens.
4. Complete the dialog and click Save As and choose a file name. Observer can save the file as BFR, CAP, ENC, PCAP, or XML.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First packet</strong></td>
<td>Allows you to set the first packet in the capture buffer to be saved to the file. By default, this is packet 1.</td>
</tr>
<tr>
<td><strong>Last packet</strong></td>
<td>Allows you to set the last packet in the capture buffer to be saved to the file. By default, this is the last packet in the capture buffer.</td>
</tr>
<tr>
<td><strong>Save as button</strong></td>
<td>Displays a dialog that lets you choose from various formats to use when saving the capture buffer, including Observer’s native file format, various Sniffer formats, and XML. Unless you have a specific reason to do otherwise, choose Observer’s native .BFR format.</td>
</tr>
<tr>
<td><strong>Append packets to existing file</strong></td>
<td>When selected, allows you to add packets to the existing file.</td>
</tr>
<tr>
<td><strong>Recombine ATM Packets</strong></td>
<td>If this box is left unchecked, Asynchronous Transfer Mode (ATM) packets will be saved as they were captured off the wire (in other words, the 53-byte cell units used by ATM switching networks). Check the box to have Observer recombine the packets into Ethernet frames.</td>
</tr>
<tr>
<td><strong>Store alias names inside file</strong></td>
<td>When selected, the Discover Network Names-derived alias list is included with the packet capture. If you do not save the alias information along with the capture buffer, statistical displays will list hardware addresses rather than meaningful names.</td>
</tr>
<tr>
<td><strong>Save Partial Packets</strong></td>
<td>When selected, you can set how much of each packet to save (in bytes). This allows you to collect packet headers without payloads, which may be useful from a privacy or security standpoint.</td>
</tr>
<tr>
<td><strong>Replace hardware address in all saved packets</strong></td>
<td>When selected, enables hardware address substitution in the saved buffer. You can have Observer substitute either MAC addresses, IP addresses, or both. In either case, the controls are the same: Original address—allows you to specify which addresses will be searched for during the replacement. Wildcard substitution with the asterisk character allows you to select multiple addresses. The last 10 specifications entered are conveniently available in a drop-down menu. New address—allows you to specify which hardware address will be substituted in place of the original. An asterisk (<em>) or x used in the same position as the Original address specification causes that portion of the address to be retained in the saved file. For example, specifying Original address: 123.123.100.</em></td>
</tr>
</tbody>
</table>
New address: 10.20.30.*

will replace all addresses that match the 123.123.100 address segments with 10.20.30 and retain the address segment of the original where there is an asterisk. Hence the original address: 123.123.100.12 becomes the new address: 10.20.30.12, and the original address: 123.123.100.4 becomes the new address: 10.20.30.4.

As the changes are made in the saved buffer file, and not in the buffer loaded into Observer, to change several hardware addresses, it will be necessary to change while saving and then reload the buffer file for each subsequent change.

<table>
<thead>
<tr>
<th>Decrypt 802.11 WEP Encrypted Packets</th>
<th>If checked, you can select from several preconfigured WEP key profiles. The profiles themselves are configured as part of 802.11 setup.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decompress FRF.9 compressed packets</td>
<td>If you have captured frames from a Network Instruments WAN probe, Observer can decompress the frames before saving them. Decompression will not work unless the probe captured all the packets from the beginning of a connection initialization between the router and the CSU/DSU. You can force an initialization during data collection by resetting either the CSU/DSU or the router.</td>
</tr>
</tbody>
</table>

**Searching for a specific packet**

1. Choose Capture > Packet Capture or load a saved capture.
2. Click the Decode button. The Decode and Analysis window appears.
3. Click the Decode tab, then Choose Tools > Find Packet. The Find Packet window appears.
4. Using the information in **Table 14** choose how you want to search the capture buffer.

**Table 14: Searching a packet capture**

<table>
<thead>
<tr>
<th>Raw Packet Data</th>
<th>Searches the entire raw (i.e., not decoded) packet for the given string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decoded Data</td>
<td>Searches only the decoded packet for the given string.</td>
</tr>
<tr>
<td>ASCII</td>
<td>Interprets the buffer as ASCII-encoded text and searches for the given sequence. A maximum of 16 characters are allowed in the string. ASCII searches are case-sensitive.</td>
</tr>
<tr>
<td>EBCDIC</td>
<td>Interprets the buffer as EBCDIC-encoded text and searches for the given sequence. A maximum of 16 characters are allowed in the string. EBCDIC searches are case-sensitive.</td>
</tr>
<tr>
<td>Hexadecimal</td>
<td>Interprets the buffer as hexadecimal code and searches for the given sequence of codes (separated by spaces; e.g., C0 FF CC). The maximum value for a code is FF.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Interprets the buffer as decimal code and searches for the given sequence of codes (separated by spaces; e.g., 102 90 87). The maximum value for a code is 255.</td>
</tr>
<tr>
<td>Find Sequence</td>
<td>Allows you to enter the exact string of characters or codes to search for.</td>
</tr>
<tr>
<td>Find All Conversations Containing Search Sequence</td>
<td>Find up to 1024 different IP/port pairs. A list of found pair is displayed. From the list you may choose up to 75 pairs to post filter.</td>
</tr>
</tbody>
</table>
Filtering your saved packet capture

1. Choose Capture > Packet Capture or load a saved capture.
2. Click the Decode button. The Decode and Analysis window appears.
3. Click the Decode tab, then Choose Tools > Post Filter. The Post-Capture Filtering window appears.
4. Select your filter and click OK. The filtered decode appears.

After completing this task:

For more details about the post-capture filters and for a faster filtering method, see Post-filtering your packet captures on page 72.

Processing NetFlow or sFlow data

1. Choose Capture > Packet Capture or load a saved capture.
2. Click the Decode button. The Decode and Analysis window appears.
3. Click the Decode tab, then Choose Tools > Process NetFlow or sFlow data. The Select Data Source window appears.
4. Choose the data source you want to process.
5. Change your ToS/QoS settings if necessary and click OK.

A new Decode and Analysis tab opens with your process flow information.
Chapter 7: Expert Analysis

Preparing expert decoding techniques

Real-Time Expert is the collection of tools in Observer that help you identify network problems and determine a course of action; these tools provide expert decoding techniques. With Real-Time Expert, you can obtain post-capture expert event identification, explore expert analysis, reconstruct TCP streams, and model network traffic.

There are several ways to approach a network problem with Real-Time Expert. As with any network problem, you should first determine if you can reproduce the problem. If you can reproduce the problem, set up a capture to collect data for the entire event (start to finish) and then use the Expert in post-capture mode to identify possible causes of the event. Otherwise, begin using Real-Time Expert while a packet capture is running—this is real-time mode.
To begin using Real-Time Expert and its advanced decoding techniques, you must first configure the Expert system; this is a two-step process, which is described in these sections:

- Configuring global settings on page 96
- Configuring expert thresholds on page 105

Follow the configuration steps described in each section. When both steps are complete, you can begin using Real-Time Expert with confidence in its results.

Using the Expert Analysis feature

Expert Analysis is like having a network-troubleshooting expert on site to tell you what the packet captures mean. It helps you determine whether saturated bandwidth or overloaded servers are causing user-reported delays. With Expert Analysis, you can look at a conversation to see exactly where the errors or delays are occurring.

**Prerequisite:** Observer Expert or Observer Suite

Expert Analysis can be a confusing concept. What exactly is it, and how does one use it? The simple answer is that expert analysis is something you **perform** in Observer from the Expert Analysis tab, where the feature resides. Expert Analysis, as a feature, is your graphical interface to the Real-Time Expert engine within Observer, while expert analysis (i.e. advanced decoding techniques) is what you perform inside of the feature.

To begin using the Expert Analysis feature of Observer, you must always navigate to the Expert Analysis tab. Do this by completing the following steps:

1. Choose **Capture > Packet Capture**.
2. Click Decode. The Decode and Analysis window appears.
3. Click Expert Analysis.
After completing this task:

From here, you are able to use the Expert Analysis feature of Observer. Review Table 15 on page 95 to see the variety of actions you can perform in Expert Analysis.

**Table 15: Expert Analysis tabs**

<table>
<thead>
<tr>
<th>Tab group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expert Summary</td>
<td>Shows a real-time summary graph of utilization, which can be customized in Settings. Also, shows a summary of any triggered network conditions. See Using Expert Summary on page 97.</td>
</tr>
<tr>
<td>TCP Events</td>
<td>Shows all seen TCP conversations, protocols, and relevant statistics. Right-click any result to see additional actions.</td>
</tr>
<tr>
<td>UDP Events</td>
<td>Shows all seen UDP conversations, protocols, and relevant statistics. Right-click any result to see additional actions.</td>
</tr>
<tr>
<td>SCTP Events</td>
<td>Shows all seen SCTP conversations, protocols, and relevant statistics. Right-click any result to see additional actions.</td>
</tr>
<tr>
<td>ICMP Events</td>
<td>Shows the source, destination, type and code of ICMP events seen over the network, including the number of times any are seen. Right-clicking an ICMP event allows you to learn more about the ICMP event type. Prior to version 15, Observer was limited to showing only 10 ICMP events and when Observersaw connection 11, it would discard the oldest connection (i.e., connection #1). In version 15, Observer is still limited to showing only 10 ICMP events, but now considers the connection's status. If connection #1 has critical status and connection #2 is not critical, Observer discards connection #2 and keeps #1.</td>
</tr>
<tr>
<td>IPX Events</td>
<td>Shows all seen IPX conversations, protocols, and relevant statistics. Because IPX is considered legacy in most networks, it is possible no IPX data traverses your network. Right-click any result to see additional actions. This tab is disabled by default.</td>
</tr>
<tr>
<td>Tab group</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>NetBIOS Events</strong></td>
<td>Shows all seen NetBIOS conversations, protocols, and relevant statistics. Right-click any result to see additional actions. This tab is disabled by default.</td>
</tr>
<tr>
<td><strong>VoIP and Videoconferencing</strong></td>
<td>Shows a summary of VoIP activity and call quality statistics. For more details, see Collecting VoIP or video conferencing trending data on page 166.</td>
</tr>
<tr>
<td><strong>Wireless Events</strong></td>
<td>Shows a summary of all wireless access point activity. You can see general information about the access points, details about the frame types, control frames, management frames, data frames, what speed traffic is flowing at, and signal strength.</td>
</tr>
<tr>
<td><strong>Connection Dynamics</strong></td>
<td>Shows a selected conversation graphically, illustrating inter-packet delay as a spacing between packets. See Using Connection Dynamics on page 98.</td>
</tr>
<tr>
<td><strong>Reconstruct Streams</strong></td>
<td>Allows reconstruction of captured TCP data into its original, viewable form. For example, you can reconstruct captured web traffic to see actual web pages that traversed the network. See Reconstructing TCP data streams on page 100.</td>
</tr>
<tr>
<td><strong>TCP/UDP Dump</strong></td>
<td>Allows all of the captured TCP and UDP data to be dumped and viewed in a raw format.</td>
</tr>
<tr>
<td><strong>Time Interval Analysis</strong></td>
<td>The Time Interval Analysis displays TCP or UDP Event conversations in a table format showing the conversation split up by the user-defined period. See Using Time Interval Analysis on page 101.</td>
</tr>
<tr>
<td><strong>Server Analysis</strong></td>
<td>The Server Analysis displays are designed to help evaluate a server’s or system’s response time under various load scenarios. See Using Server Analysis on page 101.</td>
</tr>
<tr>
<td><strong>What-If Analysis</strong></td>
<td>What-If live modeling and analysis offers both a predictive tool for modeling potential response times, utilizations, or packets per second at different network speeds, and also permits you to change different conversational and network metrics to predict changes in performance with the new values. See Using “What-if” modeling on page 102.</td>
</tr>
</tbody>
</table>

**Configuring global settings**

Real-Time Expert allows you to configure its global settings via the Expert Global Settings window. These global settings influence how Real-Time Expert displays its results and how you, as a user, interpret their meaning.

**Note:** This section assumes you are familiar with creating packet captures and the packet capture window in general. See Capturing network traffic on page 59 for more information.

To configure global settings for Real-Time Expert, complete the following steps:

1. Choose **Capture > Packet Capture**.
2. Click the Decode button. The Decode and Analysis window appears.
3. Ensure the Expert Analysis tab is selected.
4. Click the Settings button. The Expert Settings window appears.
5. Change settings in any or all the tabs to suit your needs.
6. Click OK to confirm and save your changes.

You completed the first of two configuration steps for making Real-Time Expert work best on your network. If you previously have not, follow the instructions in the second step, Configuring expert thresholds on page 105.

After completing this task:

The options on the General tab allow you to enable or disable each analysis type (TCP, UDP, and so on). Changes made here are global to the local Observer analyzer and impact the current window and all newly opened windows after making any changes. When an item is disabled, it is not visible on the Expert Analysis tab and the corresponding packet processing does not occur. These changes affect packet decoding only. Network trending is not affected.

What is goodput?

Goodput is a reported value for some events, especially TCP Events, UDP Events, and Time Interval Analysis. Goodput is the application level throughput, i.e. the number of useful information bits, delivered by the network to a certain destination, per unit of time. The amount of data considered excludes protocol overhead bits as well as retransmitted data packets. This is related to the amount of time from the first bit of the first packet is sent (or delivered) until the last bit of the last packet is delivered.

How is Network Delay calculated?

Prerequisite: Observer Expert or Observer Suite

Network delay is calculated by the SYN - SYN/ACK - ACK packets. The time between a client sending a SYN and it receiving a SYN/ACK from the server provides the Server Network Delay, and the time between the server sending a SYN/ACK to when this server receives an ACK from the client indicates the Client Network Delay.

If you are not seeing any SYN, SYN-ACK and ACK packets, Network Delay cannot be calculated.

How is Response Time calculated?

Response Time is calculated by averaging the differential times between data request to data response.

Using Expert Summary

Expert Summary displays all general, non-conversation specific problems that Observer finds when analyzing the packet capture. Over 700 different expert events can appear here, which you can right-click to further interact with. Expert Summary also provides easy access to viewing utilization rates.

The Expert Summary group tab includes three panels:

- Summary graph (top)
- Network Conditions Summary table (middle)
- Expert Analysis panel (bottom)
The Network Conditions Summary table automatically alerts you of many network events, and one is the presence of duplicate IP addresses. Observer does not have an option that shows cloned MAC addresses. However, seeing duplicate IP addresses can help you see cloned MAC addresses, depending on your network environment.

Furthermore, there are three scenarios which can trigger seeing duplicate IP addresses and potentially retransmissions or duplicate packets because of it:

- Two MAC addresses (IP address is traveling layer 3)
- Two static IP addresses
- Cloned MAC addresses

If you see duplicate packets or retransmissions caused by duplicate addresses, clear the option “IP Duplicate Address and Routing Problems” from the Network tab of the Expert Thresholds (OSI Model) window.

**Note:** Expert Summary panels. The Summary graph shows utilization by percent of bandwidth and packets per second. If an expert threshold has been exceeded, the top line of the graph (labeled with the alarm) will show a red bar; hovering your cursor over the bar will show details of the event. The Network Conditions Summary table shows any expert thresholds exceeded, including the number of occurrences and a description of the event. Right-click any item to view more details. The Expert Analysis display panel offers general instructions on what options are available in the display and may offer a short explanation of the highlighted item.

**Using Connection Dynamics**

Connection Dynamics show a selected conversation graphically illustrating the inter-packet delay as a spacing between packets.

**Prerequisite:** Observer Expert or Observer Suite

Packet-to-packet delay times are shown graphically, allowing instant identification of long latency and response times. Retransmissions and lost packets are flagged in red for quick identification. The packet display can contain either a brief or detailed view of each packet's contents.

To access Connection Dynamics, right-click a conversation in either the TCP Events or the UDP Events and select Connection Dynamics. Once a conversation has been displayed in Connection Dynamics, it can be reviewed by clicking the Connection Dynamics button on the Expert button bar.

Connection Dynamics show a selected conversation graphically illustrating the inter-packet delay as a spacing between packets. Packet-to-packet delay times are shown graphically, allowing instant identification of long latency and response times. Retransmissions and lost packets are flagged in red for quick identification. The packet display can contain either a brief or detailed view of each packet's contents. For example, if you see delays in query response time from a database server, it could mean that your server's processor is overloaded and needs to be upgraded. It could also help pinpoint problems with custom applications running on servers.

After accessing Connection Dynamics—the tool itself—the time line format lets you quickly see long latencies and delayed response times. Retransmissions and lost packets are flagged in red.

Place your mouse cursor over a packet; it will turn from green to blue. At the bottom of the screen (above the lower tabs Expert Analysis, Decode, Summary) more detailed information for that packet is shown. In general, the information has abbreviated titles:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>S¹</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>A¹</td>
<td>Acknowledgment Number</td>
</tr>
</tbody>
</table>
EA\(^1\)  Expected Acknowledgment Number. This value is calculated by Observer and is not part of any byte within the TCP header.

<table>
<thead>
<tr>
<th>W</th>
<th>Window Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Port Number</td>
</tr>
<tr>
<td>DataLen</td>
<td>Data Length</td>
</tr>
<tr>
<td>Seq</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>ExpAck</td>
<td>Expected Acknowledgment Number</td>
</tr>
<tr>
<td>Ack</td>
<td>Acknowledgment Number</td>
</tr>
<tr>
<td>Wnd</td>
<td>Window Size</td>
</tr>
<tr>
<td>Port</td>
<td>Port Number</td>
</tr>
<tr>
<td>AbsoluteTime</td>
<td>Absolute Time</td>
</tr>
<tr>
<td>TSN</td>
<td>Transmission Sequence Number</td>
</tr>
<tr>
<td>DupTSN</td>
<td>Duplicate TSN detected. This value is reported by the SACK packet.</td>
</tr>
<tr>
<td>GapACK</td>
<td>Gap in TSN sequence detected. This value is reported by the SACK packet.</td>
</tr>
</tbody>
</table>

---

1) These are used to validate that data has been received properly. The time difference between packets 9 and 10 is the length of time it took the server side (the system on the right) to respond back to the clients request (the system on the left).

Now, by right-clicking any packet you can:

- jump to the Decode window display of that particular packet,
- toggle the display packet Details on or off, or
- change the zoom level of the Connection Dynamics window.

Press the **Tools** button and select **Find Packet**. This opens the Find dialog box so you may specify search criteria. Use this tool to help you find what you are looking for in a long sequence of packets.

*Tell me more about the Connection Dynamics tool*

The Connection Dynamics display consists of the graphical display and a status bar that changes as you hover your mouse over a particular packet. When no packet is under the mouse, the status bar displays the type of conversation in the display (TCP or UDP), the conversation’s duration (in seconds), and packet count. Connection Dynamics uses the TCP or UDP sequence and acknowledgment numbers to determine the packets color and type.

**Color codes and packet types**

The packet square under the cursor will always be blue. When a packet is not under the cursor, the color of the packet squares and accompanying packet frame gives information about the packet. Packets are colored according to the following rules. You can change the colors associated with various packet types by choosing **Expert Analysis > Connection Dynamics > Settings > Connection Dynamics**.

- Red – Retransmitted packet (shortened to “Retrans”). This is based on Observer seeing two packets with data having the same sequence number.
- Dark magenta – Warning packet. Observer sees a Re-ACK packet. A packet was sent saying that data was received, then another packet is sent again using the same acknowledgment number saying data was received and this new packet contains no data, so it is a duplicate of the previous packet.
Dark yellow – Skipped packet (shortened to “Skip pkt”). Observer sees a sequence number that is higher than the expected acknowledgment. The expected acknowledgment is a calculation that Observer does—it is not something that is in the actual packet. It is the sequence number plus the total data length to determine the expected acknowledgment.

Medium red – Out of order packet. An out of order packet is exactly what it sounds like. It is a packet whose sequence number indicates that packets came into the NIC out of sequence, for example 1, 3, 2, 4 instead of 1, 2, 3, 4).

Dark red – Zero window. The Window Size within the TCP header indicates a size of 0. This means no data can be received by the device sending the Zero Window TCP packet. This halts communication until another packet indicates it has a window size above zero.

Dark green – Rerouted packet. Observer sees a duplicate packet, but the MAC addresses (source and or destination – typically both – are different between the duplicate packets). This usually affects the TTL within the IP header when packets are routed, but Observer ignores this and pays attention only to the sequence numbers.

Dark green – Keep alive packet. A keep alive packet is sent between stations to keep the TCP session open even though no actual data is being sent. This is very typical of an application which requires user input to continue, such as a Telnet session. Eventually the session may time out, but this is due to the application settings and not an issue within the network itself. Observer identifies a keep alive packet by seeing the sequence number from one packet to the next going backwards by 1. If the sequence number of one packet #1 was 938475892 and the second packet was 938475891, and the second packet contained no data, this would be a keep alive packet. If the second packet contained data, it would most likely be a resent packet, though you rarely would ever see a data packet with only one byte of data.

What are skipped packets, and why are they appearing?

When a series of TCP packets comes into Observer, each packet will contain a sequence number. Packets should arrive in numerical order. If, however, a packet is missing, Observer identifies that missing packet as a “Skip pkt” if the client side acknowledges the missing packet.

For example, if you see packets 1, 2, 3, 4, 6, 7, and 8, Observer would identify packet 5 as “Skip pkt”, because there is a gap in the sequence between packets 4 and 6. There are two reasons why this could happen:

- The amount of data coming into the capture adapter is so high that Observer dropped packets. This is indicated by a red line in the Packet Capture tool.
- To resolve this issue, you should limit the amount of data being spanned into the system, as this is a CPU issue on the switch rather than an issue within the Observer application or the hardware it is using to do the capture.

Reconstructing TCP data streams

Prerequisite: Observer Expert or Observer Suite

When analyzing a previously-saved buffer that includes TCP communications, you can right click any such communication from the decode, connection dynamics, or TCP Events displays and choose Reconstruct Stream or TCP Dump from the popup menu.

Stream reconstruction can only be performed post-capture.

Both Reconstruct Streams and TCP Dump show you the stream, but they do show in different manners. If you need a quick view of the stream, choose Reconstruct Streams. If what you need is not available there and you need to dig deeper into the stream, choose TCP Dump.

The streams that Observer can reconstruct are:

- DAAP (iTunes sharing)
- FTP
Several media codecs are supplied with Observer so that Observer can reconstruct numerous media types. If you have an application that uses a codec that is not part of Observer, you can still reconstruct that media stream if the codec is installed on the analyzer system.

**Note:** Before reconstructing a media file Observer searches its own list of codecs. If it does not find a suitable codec, it searches the Windows system for one. If it finds one, you can reconstruct the stream. For a list of supported codecs and protocols, see Protocols supported by Observer on page 342.

Tell me more about stream reconstruction

You can change the display format to raw data, packet headers, or packet headers with links to any files that were reconstructed (which is the default setting). You can also have Observer display only the links. To change the format, right click anywhere on the reconstructed stream display and choose Format from the popup menu, then the format option you wish to apply. Where links are displayed, clicking on them opens the file using the default application for the particular file type. For example, HTML files will be opened in your operating system’s default web browser.

Using Time Interval Analysis

The Time Interval Analysis displays TCP or UDP Event conversations in a table format showing the conversation split up by the user-defined period.

To access the Time Interval Analysis display, right-click a conversation in either the TCP Events or the UDP Events. Select Time Interval Analysis and then choose your connection option.

Time periods can be defined by either right-clicking on the display and selecting Properties, or by selecting the Time Interval Analysis tab from the Expert Global Settings.

Columns include Network Utilization and Network Packets/sec to help determine, for each Time Interval Analysis, what the overall network conditions were and how that may have affected the errors observed.

If you are not seeing any values under Network Utilization, make sure that you have the option to collect Expert Load Information Packets checked on in the Packet Capture setup.

The Notes section displays the type of conversation and the stations listed.

Using Server Analysis

Server Analysis shows how well a server is responding under various load conditions. For best results, you should analyze a packet capture obtained over a range of typical load conditions for that server.
To perform Server Analysis, right-click any connection to the server you are interested in—TCP Events or UDP Events—and click Server Analysis. The Server Analysis window appears.

If there is a smooth, linear increase in response times as the number of simultaneous requests increases, then this kind of pattern (or a chart that shows little increase in response time) means that the server is handling observed loads well. If the chart shows a more exponential increase after a certain number of simultaneous requests, it means that you should perhaps obtain faster processors or hard disks for your database server.

The Server Analysis displays are designed to help evaluate a server’s or system’s response time under various load scenarios. The server in Server Analysis can be selected in several ways. From either the TCP Events or UDP events, right-clicking on any conversation will offer access to Server Analysis for either station in the right-click menu, or by clicking the Server Analysis button and selecting the server from the drop-down list at the top of the display.

The graph on the top of the Server Analysis display shows the response times for each level of simultaneous requests. An average line is shown for baselining purposes.

**Using End-to-End Analysis**

Prerequisite(s):

For End-to-End Analysis to determine the exact time conversations occurred between two network points, the three-way handshake must be seen. Additionally, the handshake must be seen on a known protocol.

Observer monitors point-to-point connections using the End-to-End Analysis feature. With it you can determine the exact time conversations between two network points occurred. Observer provides in-depth conversation information on the exact network delay between the two points.

**Note:**

End-to-End Analysis does not support MultiHop Analysis. For that you must use the MultiHop Analysis feature. See Using MultiHop Analysis on page 105.

To configure end-to-end analysis, complete the following steps:

1. Ensure you have two saved capture files to compare.
2. Choose **Trending/Analysis > End to End Server Analysis**. The End to End Server Analysis tab opens to the Server List tab.
3. Click the Select Files to Analyze button. The End to End Server Analysis Settings window appears to the Files tab.
4. Click Add to select the files to analyze. You may add several files to the list; however, you may only compare two files at a time.
5. If any address translation (NAT) occurs, define the address in the IP Mapping section.
6. Click the General Tab.
7. Click OK.
8. Expand the server list and choose one or more servers and click Server Analysis.

The Server Analysis window shows server and network delay, load, and utilization.

9. To view the connection dynamics, hop summary, and summary statistics, click the End to End Drill Down tab.

**Using “What-if” modeling**

**Prerequisite:** Observer Expert or Observer Suite
Observer What-if Analysis tools lets you virtually test different network and server configuration scenarios based on actual usage patterns captured from your network. It helps you answer the following types of questions:

- Will buying more bandwidth improve response times for my users, or would my money be better spent on faster servers, hard disks, or clients?
- How would telecommuting over a modem or DSL line affect a particular user’s response time?
- How would adding more users to a database application affect server response times?

To display the What-if Analysis for any conversation, right-click any conversation that shows a delayed response time and select What-If Analysis from the popup menu. You can change various parameters in the dialog below the what-if graph and see the results immediately.

The top of the display shows transfer rate, response time, or utilization rate given various network bandwidths, extrapolated from the data measured on your network’s bandwidth (which is identified by a reference line. As with any such extrapolation, the more data sampled, the more accurate the predictions.

**Tell me more about the What-if Analysis tool**

What-If live modeling and analysis offers both a predictive tool for modeling potential response times, utilizations, or packets per second at different network speeds, and also permits you to change different conversational and network metrics to predict changes in performance with the new values.

The What-If Analysis starts with a conversation collected from your network and bases all predictions on your actual network data. Different system formulas are used for different types of systems to be modeled.

To begin your What-If live modeling session, right-click a conversation from either the TCP or UDP Events display and select What-If Analysis.

You can only do What-If modeling on conversations that have a recorded server (the second address in any conversation) delay.

The top of the display will show which stations are currently being modeled. The client is on the left, the server is on the right.

The X-axis of the graph will always display different network speeds. If the data collected was from Observer, a vertical reference line will be displayed showing the network speed at which the data was collected.

The Y-axis will display different values depending on the graph type selected.

A key display will show the different items on the graph and their associated colors.

The items below the graph initially represent the actual data from the captured conversation. Items can be changed to model changes in the network.

Observed Connection Parameters (derived directly from the conversation data collected):

**Average Packet Size (Bytes)**—displays the average size of the packets sent from the client and the server. Changing these values in the Client or Server options will model changes in network performance.

**Latency (mSec)**—displays the average latency time as observed in the transaction conversation. Values are shown for packets sent from the client and the server. Changing these values in the Client or Server options will model changes in network performance.

**Transaction Packet Ratio**—displays the transaction packet ratio of the packets sent from the client and the server.

**Utilization from other sources (%)**—sets the network utilization to simulate. This would be beyond the current conversational conditions recorded, and only changes the modeled values if the option to Include utilization from other sources in What-If Analysis is checked in the Expert Global Settings, What-If tab setup.

User-Defined Parameters are initially set in the Expert Global Settings, What-If tab. Changing the values here will only affect the current calculation and will not be preserved for subsequent modeling sessions.
**Graph type**—changes what modeling results will be displayed in the graphic view. Options include Packets/sec, Response time (sec), and Utilization (%). While all three views are related, select the view that displays the option you are interested in.

**Simultaneous users**—sets the number of users to simulate.

**Processing Time (ms)**—the amount of time, in milliseconds, that the server or client will take to process the request.

Server Characteristics:

**Server type**—options include Database, FTP, Level, and web servers. Each different server selection causes the expert to use a different formula suited for the selection. A level server offers a formula for a typical server.

**Start thread time (ms)**—taken into account when the Server type item is defined as web. The value is the amount of time it takes to process a thread on the server.

**Arrival rate (trans/sec)**—taken into account when the Server type item is defined as Database. The number of transactions per second that are being requested of the (Database) server.

**Maximum adapter card throughput (Mbps)**—taken into account when the Server type item is defined as FTP. This item defines the server’s maximum throughput. This may be the rated speed of the adapter, but most likely it is some fraction of the maximum theoretical speed (utilization) of the network. The default of this item is set in the Expert Global Settings, under the What-If tab.

One way to get a value for this option is to run Observer on the server using the packet generation mode. Set the generation rate very high and view the utilization that the server can create using Observer’s utilization modes. The maximum utilization will reflect the NIC card’s ability to generate traffic.

**Restore Original Values**—resets all values to the initial settings for the analyzed pair.

**Set Reference**—sets the current graph lines to the reference line. For example, if you change the number of simultaneous users from 1 to 100, a What-If prediction line will be displayed and the original reference line will be displayed. If the Set Reference is pressed, the new What-If prediction line will become the reference line for further What-If modeling.

### Analyzing 4G LTE packet captures

Because 4G LTE is encapsulated traffic, most meaningful analysis must be performed “below” the encapsulation wrapper. Observer’s Real-Time Expert engine allows you to do this.

**Prerequisite:** Observer Expert or Observer Suite

Further analysis of 4G LTE traffic includes seeing its end-user devices, applications, hand overs, any errors or failures, and the hardware that serves these connections.

---

**Note:** This process also works with an unsaved, real-time packet capture.

To analyze packet captures containing 4G LTE traffic—below the encapsulation wrapper—complete the following steps:

1. Choose **File > Load and Analyze Observer Capture Buffer**.
2. Navigate to the capture file you want to load, and select it.
3. Click Open. The capture file loads into Observer and you arrive at the Decode and Analysis tool.
4. Click the 4G LTE Analysis tab, located near the bottom of the window.
**Configuring expert thresholds**

Expert thresholds define what parameters are used when determining if a particular event is a problem or not. Thresholds are set for all Expert events, and for some events, more than one threshold is set. For example, for TCP Bad Checksums, only the number of frames during the entire capture process is set. Conversely, for FTP Session delays, values are set for slow connect and slow response, including values for grading marginal and critical for each.

This section assumes you are familiar with creating packet captures and the packet capture window in general. See Capturing network traffic on page 59.

To configure expert thresholds, complete the following steps:

1. Choose **Capture > Packet Capture**.
2. Click the Decode button. The Decode and Analysis window appears.
3. Ensure the Expert Analysis tab is selected.

   ![Expert Analysis tab location](image)

4. Click the Expert Thresholds button. The Expert Thresholds (OSI Model) window appears.

   ![Expert Thresholds button location](image)

5. Click OK to confirm and save your changes.

You completed the second of two configuration steps for making Real-Time Expert work best on your network. If you have not already done so, follow the instructions of the first step, Configuring global settings on page 96.

**Tell me more about expert thresholds**

Expert thresholds are set for all Expert events, and for some events more than one threshold is set. For example, for TCP Bad Checksums, only the number of frames during the entire capture process is set. For FTP Session delays, values are set for slow connect and slow response, including values for grading marginal and critical for each. Values for network and WAN/Internet response times values are also set.

Because of the potentially large number of values that are required and because many different network/WAN/Internet configurations dictate predictable value sets, Real-Time Expert Thresholds permit the user to save profiles for sets of values. The thresholds configuration displays are loosely based on the OSI model, separating different expert items from where in the communications stack the item is found.

**Using MultiHop Analysis**

**Prerequisite:** Observer Expert or Observer Suite
MultiHop Analysis is a powerful tool in Observer; it graphically shows you network conversations that traverse multiple network hops, making it easy to determine if delays are due to a particular router hop. For example, if you have a corporate LAN spread across remote offices, MultiHop Analysis can tell you which routers are causing network delay between remote offices and corporate headquarters.

If you ever encounter problems with MultiHop Analysis, see Troubleshooting synchronization errors on page 110 or call the support team if you encounter issues specific to your network environment.

Network Instruments included sample capture files so you can try MultiHop Analysis. These files are located in the `\data` subdirectory of wherever Observer was installed (C:\Program Files\Observer by default).

Before using the MultiHop Analysis tool, we recommend you become familiar with the user interface and creating packet captures from multiple probe instances—see Capturing from multiple probe instances on page 60 for details.

**Figure 31: MultiHop Analysis - the user interface**

MultiHop Analysis only operates in post-capture mode; therefore, to make the tool work, you must absolutely save (or have saved) your capture files to disk and have access to those files.

To use MultiHop Analysis, complete the following steps:

1. Create and save multiple capture files—simultaneously—from multiple probe instances.
   
   When capturing from multiple probe instances, there exists an option to immediately bring those captures into the MultiHop Analysis tool. For the sake of example, however, the proceeding steps ignore using that option.

2. After capturing from multiple instances, choose Trending Analysis > MultiHop Analysis. The MultiHop Analysis tool opens.

3. Click the Select Files to Analyze button. The MultiHop Analysis Settings window appears.

4. Ensure the Files tab is selected, and click the Add button. The Edit Segment File dialog appears.
5. Type a descriptive name for your segment. In MultiHop Analysis, each capture file is called a segment.
6. Browse to or type the file location of the first capture file.
7. (Optional) If you know or anticipate that IP addresses will not match between hops, enable the Apply IP Mapping option and click the Settings button.
   
   IP mapping keeps track of network entities as they undergo network address translation. For more information about this option and its use, see How to use IP mapping in MultiHop Analysis on page 110.
8. Click OK to confirm this segment's inclusion.
9. Repeat 4 through 8 for each capture file (segment) that you want to add to your MultiHop Analysis session. Up to ten segments can be added during this step; ten is the maximum.
10. Ensure you return to the MultiHop Analysis Settings window (which appeared in 3), and click OK.
   
   You successfully prepared the MultiHop Analysis tool and can now view and analyze the results.

**Tell me more about the MultiHop Analysis tool**

All of the connections detected are listed in the upper left corner of the MultiHop Analysis display. Choose each connection you want to analyze by clicking on its corresponding check box. For the MultiHop Analysis display, it is usually more useful to look at one connection at a time.

**Hop Summary**

The Hop Summary view shows delay data from the selected connections in aggregate, giving you the average delay time from multiple conversations over time. Knowing what is “normal” can help you determine when applications or third party service providers are performing adequately.

Most of the metrics (minimum and maximum delay times in total and by segment, for example) should be self-explanatory. Lost Packet Delay Time measures how much delay was introduced by dropped packets having to be re-sent.

**Summary Statistics**

The Summary Statistics view of MultiHop Analysis gives you a textual display of the selected connections (computed in the MultiHop Delay Analysis – Connection Dynamics view). You may select one or many connections. The statistics summary gives you details on the analyzed packets, such as: number of packets analyzed, delay time, matched packets, direction of packets, dropped packets (will be displayed in red type), time of first packet, and time of last packet.

The first part of the summary shows paths to all of the buffer files currently being analyzed and summarizes settings in effect. The second part of the summary shows essentially the same measurements as the MultiHop

---

**Figure 32: The Edit Segment File dialog**

![Edit Segment File dialog](image)
connection dynamics and MultiHop Analysis displays, summarized in a list format. As in the MultiHop Analysis display, Lost Packet Delay Time measures how much delay was introduced by dropped packets having to be re-sent.

**Quickly using MultiHop Analysis**

Your method of using MultiHop Analysis can differ depending on how you obtain, or obtained, the capture files you want to work with. For example, using MultiHop Analysis can be difficult if you have capture buffer files obtained at different times or from probe instances you have no personal access to but someone else does and has sent you captures. Those circumstances are best handled using the process described in Using MultiHop Analysis on page 105—and not this section.

This section describes the most efficient, easiest, and quickest way to use MultiHop Analysis but unlike the other section, it requires the following criteria be met for the process to work correctly:

- You must have access to all target probe instances from your local Observer analyzer (i.e. from the local machine). Ensure that each is in your probe list, is configured, and connected.
- You must have sufficient capture buffer sizes across all target probe instances; you do not want one of the probe instance capture buffers to max out too early—leaving you with too little data.
- Like other captures, you must have sufficient disk space to save the file(s). This becomes increasingly important when using MultiHop Analysis because you are simultaneously creating and saving more than one capture file, and the disk space required is increased accordingly.

To quickly use MultiHop Analysis, complete the following steps:

1. Choose **Capture > Packet Capture on Multiple Instances**. The Packet Capture on Multiple Instances Settings window appears.
2. Select each probe instance that you want to capture from.
3. (Optional) Set a pre-filter on any probe instance by selecting a probe instance and clicking Set Filter for Selected Instance.
4. Click Start to begin the packet capture on multiple instances.

   The Multiple Instance Packet Capture dialog appears, indicating the capture is actively running. Allow this dialog to remain on your screen.
5. In the Multiple Instance Packet Capture dialog, ensure both “Transfer and Save Packet Captures” and “Start MultiHop Analysis” are enabled.
6. In the Multiple Instance Packet Capture dialog, click Stop. The MultiHop Analysis Settings window appears—automatically loading and listing your new capture files.
7. (Optional) Configure any additional settings now.
8. Click OK. The MultiHop Analysis tool opens, and your analysis can now begin.

You successfully used MultiHop Analysis quickly and efficiently. This method is the quickest way to perform MultiHop Analysis, although this method does have necessary requirements.

**Configuring MultiHop Analysis settings**

Click the Settings button on the MultiHop analysis tool bar to specify capture files and other configuration options. Usually, the default settings will provide satisfactory results; only adjust if you run into performance problems.

The first tab, Settings, has options to specify the methods that MultiHop analysis uses to identify connections and synchronize timestamps on the files.
### File Synchronization Method

File synchronization is at the heart of MultiHop Analysis. By aligning the files in time and determining whether timestamp differences are the result of delay versus clock drift and other collection artifacts, Observer can show you not only aggregate delay, but also the proportion of delay with each hop.

### Identifying how much data to synchronize and where to start

There are many possible methods that Observer can use to synchronize the files. The best one to use depends on two factors:

- How long are the captures?
- How closely in time were the captures started and stopped?

This is because of a phenomenon called clock drift: two system clocks inevitably drift apart because no two clock crystals are exactly the same, and even if they were, ambient temperature differences also affect clock rates.

On shorter captures (i.e., four minutes or less), this is not usually an issue, so choose the first option. For longer captures (more than four minutes), the best method to choose depends on how closely the buffer files’ start and stop times conform to each other.

- Synchronize using all data from both files—This method is best for shorter captures (of four minutes or less) where all the captures were started and stopped within a second of each other, and clock drift is not an issue.
- Synchronize using a sliding window having the smallest variance—Using this method, Observer analyzes the two packet captures to find a window of time where the timestamps coincide with the least variance. This method is best for finding transactions across longer captures that were not very precisely synchronized regarding start and stop times.
- Synchronize at the beginning of the files with a clock drift correction—This method (the default) corrects for the inevitable differences between probe system clocks by comparing the beginning and end packets of all captures to determine clock drift. This method is best for longer captures (of four minutes or more) where all the captures were started and stopped within a few seconds of each other.

<table>
<thead>
<tr>
<th><strong>IP Address + IP ID (Port mapped)</strong></th>
<th>This option is best for networks that implement Network Address Translation (NAT) firewalls between segments.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address + IP ID + TCP/UDP Ports (Ports will match)</strong></td>
<td>Choose this option (which is the default) for networks without address translation or port mapping.</td>
</tr>
<tr>
<td><strong>IP Address + TCP Sequence number (TCP only, port mapped)</strong></td>
<td>Choose this option if your network includes Network Address Translation (NAT) firewalls, and the volume of packets in the captures is causing the IP ID numbers to be recycled (i.e., reset to 0).</td>
</tr>
<tr>
<td><strong>IP Address + TCP Sequence number (TCP only, ports will match)</strong></td>
<td>Choose this option if your network does not have any Network Address Translation or port mapping, and the volume of packets in the captures is causing the IP ID numbers to be recycled (i.e., reset to 0).</td>
</tr>
<tr>
<td><strong>Maximum packets to analyze per connection</strong></td>
<td>Allows you to select the maximum number of packets you want to analyze; only active if the Enable is selected.</td>
</tr>
<tr>
<td><strong>Enable</strong></td>
<td>Allows you to limit the number of packets to be analyzed.</td>
</tr>
<tr>
<td><strong>Defaults</strong></td>
<td>Changes the settings back to their default values.</td>
</tr>
</tbody>
</table>
Identifying synchronization artifacts versus actual delay

Different methods work better for determining synchronization artifacts (such as clock drift and other system clock differences) versus actual delay caused by the network.

- Calculate synchronization using average delay times—Choose this option if delay times are fairly uniform and short (such as delay times typical between local network segments).
- Calculate synchronization using minimum delay times—Choose this option (the default) if there are longer delays between segments, or delay times vary from short to long (such as delay times that would be typical of a WAN connection to a remote segment of your network that experiences congestion).
- Time Synchronization Window (msecs)—Use the default value (20000) in most cases. If packet IDs are being recycled (e.g. reset to zero) because they are being used up too quickly due to the volume of traffic, you can set this value lower.

Use Header following the GRE or GTP Header for Encapsulation/Tunneling—GRE (Generic Routing Encapsulation) and GTP (GPRS Tunneling Protocol) are two encapsulation protocols that may have been deployed on your network. To show the encapsulation IP addresses, leave the box unchecked; to show the nested IP addresses, check the box.

Troubleshooting synchronization errors

File synchronization is essential to MultiHop Analysis, and it is automatically attempted by Observer. By aligning the capture files in time and determining whether timestamp differences are the result of delay versus clock drift and other collection artifacts, Observer shows you not only total delay, but also the proportion of delay with each hop.

This, however, is the reason why synchronization errors are troublesome while using MultiHop Analysis—errors must be avoided for the tool to work as intended. If you cannot avoid synchronization errors, there exists a troubleshooting method called user offset, which could fix the issue.

Typically, user offset never needs adjusting because Observer automatically synchronizes your segments. However, adjusting user offset is useful when manual control is your absolute top priority.

The following steps assume you have already loaded two or more segments into MultiHop Analysis. See Using MultiHop Analysis on page 105 and Quickly using MultiHop Analysis on page 108.

To troubleshoot synchronization errors, navigate to the user offset values by completing the following steps:

2. Click the Settings button.
3. Click the Synchronization tab. This tab lists your loaded segments and the time synchronization(s) currently applied to them.
4. Adjust the values in the User Offset (sec) column.

After completing this task:

Some experimentation may be required when adjusting your user offset values; this process is iterative, so you can keep adjusting until you are satisfied with the results.

How to use IP mapping in MultiHop Analysis

Many devices in your network environment can perform Network Address Translation (NAT), such as routers and load balancers. As NATing occurs, the IP address of the network device changes, and, if not accounted for in Observer, would cause issues with the MultiHop Analysis tool because it is designed to follow an address...
through its entire journey. The IP mapping option exists so you can tell Observer, for example, that local IP address 10.0.36.100 is the same station/device as 218.xx.xx.xx on the full Internet.

IP mapping assumes you know exactly how one IP address translates to another after NATing. After you study how the devices in your network are NATing, IP mapping becomes a quick and simple process.

The following steps assume you have already loaded two or more segments into MultiHop Analysis. See Using MultiHop Analysis on page 105 and Quickly using MultiHop Analysis on page 108.

To use IP mapping in MultiHop Analysis, complete the following steps:

1. Choose **Trending Analysis > MultiHop Analysis**. The MultiHop Analysis tool opens.
2. Click the Select Files to Analyze button.
3. Double-click a file segment to edit it. The Edit File Segment dialog appears.
4. Enable the Apply IP Mapping setting.
5. Click the Settings button. The IP Mapping Settings window appears.
6. (Optional) In the Profile area, click Add to create a new profile.
7. Click the Add button, and type the IP addresses that should correspond to each other after NATing.
   For example, specify that the IP address 10.0.36.100 is the same station/device as 218.xx.xx.xx on the full Internet.
8. (Optional) Repeat the process for each desired IP mapping and for each segment file (if necessary).
9. Click OK twice to confirm and save your changes.
Chapter 8: Logs

Changing log file behavior

To set where log file data is saved, what types of events are logged, and how long to retain information, click the Log Settings button located above the log window. By default, Observer logs the following event types to a daily log file:

- Alarm
- SNMP
- Probe
- Information
- VoIP

The daily log file is stored in the LogWindow folder in your Observer installation directory. The log file is written (or appended to) each time you close Observer, or automatically at midnight if Observer is running when the date changes.

To change the behavior of the log file, complete the following steps:

1. In the bottom portion of Observer’s main window, click Log Settings. The Log Settings window appears.
2. Click the Log Files tab.
3. Change the log file behavior to fit your needs.
4. Click OK to confirm and save your changes.

Disabling logging of certain event types

Logs are a simple and effective way for you to track Observer related events. This section describes which events Observer can log and how to control the behavior of Observer log files in general.

By default, Observer logs the following event types to a daily log file:

- Alarm
- SNMP
- Probe
- Information
- VoIP

This section describes how to disable logging of any event type. If you have no reason to disable logging of certain event types, this section has little to offer you. As an alternative, see Changing log file behavior on page 112 instead.

To disable logging any or all event types, complete the following steps:

1. In the bottom portion of Observer’s main window, click Log Settings. The Log Settings window appears.
2. Disable any or all event types from being logged.
3. (Optional) Disable logging for specific devices and/or probe instances from this menu.
4. Click OK to confirm and save your changes.
Figure 34: The Log Settings window

Disabled event types do not appear in the log window of Observer’s main window and are not recorded in the log file.
Chapter 9: Alarms

Configuring and using alarms

Alarms are a powerful and often overlooked feature of Observer. Using alarms, you can trigger pre-defined actions to occur when network conditions are met, making network management simpler and more predictable. Best of all, alarms allow you to proactively manage your network no matter where you are physically located.

There are two locations in Observer where alarms can be enabled, disabled, and configured. You may enable or disable all alarms associated with a specific probe instance or you may choose to disable individual alarms.

Enabling probe instance alarms

Probe instance alarms are tied directly to your probe instances. Each probe instance alarm is the alarm gatekeeper for one probe instance. This means individual alarms only function if its respective probe instance alarm is enabled. The benefit of this design allows you to enable or disable all alarms without affecting the enabled/disabled status of the underlying individual alarms.

Note: If you are using Observer in analyzer mode and switch to its Expert Probe interface, any alarms you had directed to the analyzer are automatically disabled. You should direct the probe instance to a different Observer analyzer before switching to the Expert Probe to receive those alarms.

To enable a probe instance alarm, complete the following:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window (circled in the image).

Figure 35: Click the Alarm Settings button

2. Enable any probe instance alarm by enabling your chosen probe instance.
3. Click OK to save your changes.

You successfully enabled the probe instance alarm for your chosen probe instance; this setting persists until disabled. Individual alarms can now be configured and used, and such information can be found in Enabling individual alarms on page 116.

**Enabling individual alarms**

Individual alarms are individual, trigger-based network alarms. Before these alarms can prove useful, they must be enabled. There are four basic types of alarms in Observer:

- **Predefined Alarms**–These are alarms created by Network Instruments and includes alarms for packet size, checksum, Bit Torrent, duplicate IP addresses, microbursts, VoIP, and more.
- **Trading Multicast Dropped Sequence Alarms**–These alarms must be wholly created and configured by you because it requires specific details about your trading and network environment. There are several pre-defined trading multicast protocols that you can import for the alarm.
- **IPTV Alarms**–These alarms must be wholly created and configured by you because it requires specific details about your multicast stream and device environment.
- **Filter Based Alarms**–These alarms based on packet capture filters that exist in Observer.

**Note:** You cannot set an alarm for excessive retransmissions or high latency, nor can either be custom created. Instead, you can see these events (if they occur) using Expert Analysis. See Using the Expert Analysis feature on page 94.

Enable individual alarms by completing the following steps:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Enable each alarm you want to enable.

Until you customize the alarms, Observer uses the built-in, default triggers and actions for each. If necessary, see these pages:

# Customizing triggers and actions on page 118

# Creating filter-based alarms on page 117

5. (Optional) Select “Enable Probe SNMP trap generation” and configure up to 10 Observer analyzers or other network management systems (for instance, HPOpenView or IBM Tivoli) to receive the SNMP traps. By enabling SNMP trap generation here, an SNMP trap is generated even when no Observer analyzers are connected to the probe.

6. Click OK to save your changes.

You successfully enabled individual alarms. Remember, individual alarms remain disabled if the probe instance alarm they are associated with is disabled—even if the individual alarms are enabled.

Creating filter-based alarms

A filter-based alarm is an individual alarm created from an Observer filter. This means any filters you create in Observer can be used as alarms.

The first step in creating a filter-based alarm is to become familiar with Observer alarms in general; see Configuring and using alarms on page 115 if you have not already.

To create a filter-based alarm, complete the following steps:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. In the Filter Based Alarms area, click New. The Alarm Filter window appears.

Figure 37: Creating a new filter-based alarm

5. Now, select a filter you previously created from the list, or click New Filter to create a new filter.
6. Save all of your filter changes (if any), and select the new alarm to enable it.
7. Click OK to confirm and save your changes.

Your filter-based alarm is now enabled and triggerable. If you need to customize the triggers, follow the procedure in Customizing triggers and actions on page 118.

Remember, you can enable any number of filter-based alarms, but each filter-based alarm can only be created from one filter.

Resetting statistical alarms

Statistical alarms (as opposed to filter-based alarms) maintain cumulative counts of various network statistics, triggering only once upon exceeding the threshold. Therefore, triggered (tripped) statistical alarms must be reset before they can trigger once again.

SNMP devices have a different method for resetting alarms. To reset SNMP device alarm counters, of a currently selected SNMP device, choose Actions > Reset SNMP Device Alarm Counters.

**Tip!** To reset SNMP device alarm counters for all SNMP devices, choose Actions > Reset All SNMP Devices Alarm Counters.

To reset the counters and enable the alarms to once again trigger, click Alarm Settings at the bottom of the log window. Select the probe with the alarms you want to reset by clicking on the probe list, then click Reset Probe Alarms.

**Customizing triggers and actions**

An alarm has two components: a trigger and an action. Explore how a simple car alarm works: a thief breaks a car window (the trigger) and the car responds by sounding a loud siren (the action). Observer alarms behave in the same manner, except you can customize your own triggers and actions—and any amount of them.

Before continuing, we recommend becoming familiar with enabling individual alarms.
Customizing alarm triggers

Alarms triggers are highly flexible; you can customize the sensitivity of each trigger based on your needs. There are almost 200 predefined alarm triggers. Different background colors are used to distinguish one type of alarm from another type.

Some notes about the triggers.

- Analysis interval–The analysis interval can be unique for each trigger. It can be as low as 1 second. For VoIP the minimum analysis interval is 60 seconds (1 minute for the “Repeat alarm for chronic condition” setting). For triggers that do not have a configurable analysis interval, it is 15 seconds.
- Minimum active calls—For VoIP triggers, the minimum active calls is the number of active calls during that analysis interval. It does not mean the number of active calls above or below your defined threshold.

Try customizing some triggers yourself:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Enable any alarms by selecting them. At least one alarm must be enabled before step 5 operates correctly.
5. Click the Triggers tab. Triggers for all enabled alarms now appear.
6. Customize any or all alarm triggers to your liking.
7. Click OK to save your changes.

You successfully customized the triggers of your enabled individual alarms. You can repeat this process at any time in the future and for any reason.

Customizing alarm actions

**Prerequisite:** Observer Suite

Alarm actions are extremely powerful as they allow Observer to automatically react to triggered alarms any way you feel necessary. Customize the actions of any of your enabled alarms by completing the following steps:

By default, Observer uses the same alarm actions for all enabled individual alarms.

Note: If, instead, you want to configure independent alarm actions per individual alarm, disable this setting: Apply the Same Action to All Enabled Alarms (end-result shown in Figure 38 on page 120).

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Select each alarm you want to enable. At least one alarm must be enabled before step 5 operates properly.
5. Click the Actions tab. Actions for all enabled alarms now appear.
6. Customize any or all alarm actions to your liking.
7. Click OK to save your changes.

You successfully customized the actions of your enabled individual alarms. You can repeat this process at any time in the future and for any reason.

Sharing alarms with others

Observer alarms can be shared using the included import and export functions. Sharing is useful for making your alarms uniform across multiple installations, and it can even be used as a backup tool. This section describes the exporting and importing processes.

How to export alarms

To share alarms, the alarms must first be saved to a file. Create your file by following this export process:

1. Click the Alarms Settings button, near the bottommost portion of the Observer window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Select each alarm you want to export.
5. Click the Export Checked Alarms button.
6. Give your file a name, and click Save.

You successfully exported your alarms to an *.ALM file. You can now share this file with other Observer installations or keep it as a backup copy.

How to import alarms

To import alarms, you need access to an exported *.ALM file. You must bring this file back into Observer using the import process described here:

1. Click the Alarms Settings button, near the bottommost portion of the Observer window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Click the Import Alarms button.
5. Navigate to, and select, your file; click Open.
You successfully imported an alarm file. The alarms contained within are now part of your local collection, including the triggers and actions associated with each alarm.

**Related Topics**

Enabling individual alarms on page 116
Chapter 10: Reports

Administering Observer reports

Web and e-mail reports are available to licensed Observer Suite installations, making Observer’s analysis available to any authorized user with a standard web browser or e-mail connection.

Web reports can only be created from Observer Suite, and they require Network Trending be configured and running to get the maximum benefit. We recommend always running Network Trending. Doing so ensures a complete view of your networks’ usage patterns.

Observer reports allow a network administrator, end-user, or consultant to view network trending data from any web browser. As the Observer administrator, you can selectively make trending information available either to anybody with a web browser and TCP/IP connectivity to the Observer system, or only to those who have been provided a password.

Configuring the Observer web server

1. In Observer, choose Options > Web Reporting Configuration.
2. On the Server Options tab, configure the options to your requirements.

<table>
<thead>
<tr>
<th>Web server port</th>
<th>Sets the port that will be used for accessing the web server. Changes to the web server port will take effect the next time that the Observersystem or the web server itself is restarted. If you are concerned about secure access to your reports, you may want to use a non-standard report (something other than port 80) and restrict access to the web server to certain IP ranges using your firewall.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Web Browser Color Theme</td>
<td>Allows you to choose a color theme for you reports.</td>
</tr>
</tbody>
</table>

Viewing reports in a web browser

Prerequisite(s):

- Internet Explorer 8.0 or later
For some reports, Network Trending must be running on the Observer system. Network Trending must be enabled by the Observer administrator. Contact that person if you are not seeing the data in your reports that you expect.

If one of Network Instruments preconfigured reports does not meet your needs, you can add your own customized report to the tree list, not through your Web browser, but through Observer. In Observer, click Options > Web Reporting Configuration and then the Reports tab where you can create a custom report.

To view a report generated by Observer, follow these steps:

1. Open a web browser and connect to your Observer web server by typing this URL in your web browser:
   
   $\text{http://ObserverPC/Observer/}$

2. Log in using your user name and password. The default user account is Administrator. There is no pre-defined password for the account.

3. Select the probe from the Probe list.

4. Choose the time period from which the report will be generated. If you choose Custom from the drop-down menu, additional controls are displayed that let you enter a date or select a range from a calendar.

5. The tree listing on the left side of the display shows available reports. Click the check mark icon to set configuration options for the report; click the title of the report to display the report itself. The first time you run a Web Server or Internet Usage Report, you must configure a range of local IP addresses before Observer can produce the report.

**Note:** When attempting to view a web report and you receive the message "The username or password is incorrect," the issue may not be account-related. If you are positive that the user name and password are correct, then verify that your web browser accepts cookies. Cookies must be enabled (specifically: not set to Block All Cookies) in your web browser to view web reports for Expert Probe.

There are many different report options available across the top of the browser window. Consider these:

- If you want to modify your reports, click Settings. The Settings page allows you to change how reports are displayed. You can change a report for a single user or for all users. Every report has numerous other options for changing what information is displayed and how it is shown. Experiment with the various options.

- If you have any scheduled reports, click Scheduled Reports to open the page with the list of your saved scheduled reports. Click the report name to view it.

- If you want to view an SNMP report, click SNMP Reports.

Some reports provide a legend to describe the meanings of lines. Table 16 on page 123 lists the meanings of lines and colors for some reports.

**Table 16: Meanings of report colors**

<table>
<thead>
<tr>
<th>Color Description</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green, vertical bar</td>
<td>Shows the data range for the time period from minimum to maximum.</td>
</tr>
<tr>
<td>Red, vertical bar</td>
<td>Indicates that data was unavailable for the time period.</td>
</tr>
<tr>
<td>Blue, horizontal line</td>
<td>Shows the average for the time period represented by the green, vertical bar.</td>
</tr>
<tr>
<td>Dashed, red horizontal line</td>
<td>Indicates the average for all time periods (i.e., the average of the blue, horizontal bar).</td>
</tr>
</tbody>
</table>
Securing access to reports

Web reports can be protected by user accounts with passwords. User accounts can either be made for actual individuals or for groups, such as one, view-only account for all consultants to use. Because each user account is linked to only one email address, you may need to be creative when creating an account for a group.

Each time a new report is created, the new report is given default user permissions. You must set user permissions for each new report manually. This behavior also applies to newly created probe instances and their user permissions.

To create user accounts, and secure access to reports in the process, complete the following steps:

1. Choose Options > Web Reporting Configuration. The Web Reporting Configuration window appears.
2. Click the User Accounts / Access Permissions tab.
3. Click New. The Edit User Account dialog appears.
4. Type the user credentials to be used.
5. Select which access permissions are granted to this account.
6. Click OK to confirm and save your changes.

The user account has been created and can be used to secure your web reports. For extra security, we recommend having a good firewall policy in place to restrict unauthorized networks from accessing your Observer web server. See Configuring the Observer web server on page 122.

Publishing reports based on a schedule

Prerequisite: Observer Suite

Publishing reports at predetermined times is a straightforward process. This section describes how to schedule the generation of a network trending report. Before you begin you may want to complete the following tasks; however, these are not required:

- Create user accounts—Securing access to reports on page 124
- Set up email—Setting up email notifications on page 125

To publish reports based on a schedule, follow these steps:

1. Choose Options > Web Reporting Configuration. The Web Reporting Configuration window appears.
2. Click the Scheduled Reports tab.
3. Click New. The Schedule wizard appears.
4. Type a name and description for your scheduled report.
5. Select a probe instance that supplies the data you want to report.
6. Set the report’s time range settings—the timespan of collected data to appear in your report.
7. Select which file format you want the report to be generated as.
8. Click Next. Follow the on-screen steps for the remainder of the wizard.
9. When you return to the Web Reporting Configuration window, click OK to save your changes.

Setting up email notifications

For Observer to send reports and other notifications to email addresses, you must configure Observer’s outgoing email settings.

To set up email notifications, configure your outgoing email server settings by completing the following steps:

1. Choose Options > Observer General Options. The Observer General Options window appears.
2. Click the Notifications tab.
3. In the E-mail Settings area, provide your outgoing SMTP server credentials.
4. (Optional) Click the E-Mail Test button to test your settings.
5. Click OK to save your changes.

Observer can now send reports and other notifications to email addresses. If receiving notifications as text messages on your mobile device sounds enticing, see Setting up text message notifications on page 125.

Setting up text message notifications

Observer can also send notifications to your mobile device/phone in the form of text messages. Receiving notifications via text messages could, sometimes, arrive quicker than receiving an email, or perhaps you share a common mobile device with others in shifts—these are both good reasons to set up text message notifications.

Remember, text messages notifications are not facilitated by Network Instruments’ servers; the entire process described in this section relies solely on an established connection between your outgoing SMTP server, your wireless carrier, and the target mobile device.
Network Instruments cannot guarantee the following email address conventions will work indefinitely, although they were operational at the time of writing. Contact your wireless carrier for more details.

To set up text message notifications, complete the following steps:

1. Become familiar with the section Securing access to reports. Described there is the tool for editing user accounts and the email address each is linked to.

2. Create or edit a user account, and type an email address reflecting the conventions.

<table>
<thead>
<tr>
<th>Wireless carrier</th>
<th>Email-to-text address convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;T</td>
<td><a href="mailto:mobilenumber@txt.att.net">mobilenumber@txt.att.net</a></td>
</tr>
<tr>
<td>Verizon Wireless</td>
<td><a href="mailto:mobilenumber@vtext.com">mobilenumber@vtext.com</a></td>
</tr>
<tr>
<td>T-Mobile</td>
<td><a href="mailto:mobilenumber@tmomail.net">mobilenumber@tmomail.net</a></td>
</tr>
<tr>
<td>Sprint PCS</td>
<td><a href="mailto:mobilenumber@messaging.sprintpcs.com">mobilenumber@messaging.sprintpcs.com</a></td>
</tr>
<tr>
<td>Virgin Mobile</td>
<td><a href="mailto:mobilenumber@vmobl.com">mobilenumber@vmobl.com</a></td>
</tr>
<tr>
<td>US Cellular</td>
<td><a href="mailto:mobilenumber@email.uscc.net">mobilenumber@email.uscc.net</a></td>
</tr>
<tr>
<td>Nextel</td>
<td><a href="mailto:mobilenumber@messaging.nextel.com">mobilenumber@messaging.nextel.com</a></td>
</tr>
<tr>
<td>Boost Mobile</td>
<td><a href="mailto:mobilenumber@myboostmobile.com">mobilenumber@myboostmobile.com</a></td>
</tr>
<tr>
<td>Alltel</td>
<td><a href="mailto:mobilenumber@message.alltel.com">mobilenumber@message.alltel.com</a></td>
</tr>
</tbody>
</table>

Setting up pager notifications

You may have to modify some settings to adapt to the local environment. It will be necessary to choose among the provided services or install a new paging service and substitute the local pager access number, if any, for the supplied one.

When a Network Instruments application (except ORS) starts, it also starts a separate Windows process called Network Instruments Paging Service, which you can find in the system tray. After configuring the pager, verify the settings for the paging service match your needs.

**Note:** Choose **Tools > Program Options > Notifications** to display the pager settings and change them. You may have to modify some settings for your location and paging service. Choose among the provided services or install a new paging service and substitute the local pager access number, if any, for the supplied one.

1. Select the Default pager configuration from the menu.
   
   If your pager is not on the list, click the New button. The Paging Service Properties dialog will be displayed.

2. To view the initial pager configuration dialog, click the Properties button. The Paging Service Properties dialog will be displayed.

3. Enter the Service name. This is the name of the service used to access the pager; the Service name you selected from the list is your default.
4. Enter the Service phone number—use the international number format (e.g., +1 (123) 1234567) to allow TAPI to work with the Windows location settings.

   This option will not be displayed if you are using a SNPP pager service, as SNPP uses TCP/IP to communicate with the paging service, rather than a modem.

   If it is necessary to wait for an outside line, insert one or more commas at the beginning of the string (e.g., ,, +1 (123) 123-4567).

   Additional spaces and the hyphen in the phone number are optional; they make the number more easily readable by you, but will be ignored when dialing: Observer will dial only the numbers and pause for approximately one-half second for each comma character.

5. Select a Service protocol from the list. Observer supports four different pager service protocols: TAP, UCP, SNPP, and Voice. Selecting the appropriate service protocol and clicking the Configure button enables you to enter service-specific configuration data. Each protocol displays a different set of options that need to be set. Those options are described below for each protocol.

6. Enter the maximum message length for the pager.

7. Click the OK button.

8. Check the Apply advanced pager settings and click the Advanced button to display the Phone Pager Schedule dialog.

9. Check the desired scheduling option. You can add or edit start times by using the buttons at the bottom of the dialog.

   After the paging server starts, you can send a page or view logs of what pages have been sent. See Sending a page on page 127 and Viewing the Paging Server logs on page 127.

**Sending a page**

After you have configured the paging server using the instructions in Setting up pager notifications on page 126, you can choose to send a page.

![Image]

The paging server is running in the Windows task bar.

1. Right-click the paging server and choose Send Page.

2. Type your message and click Send now.

**Viewing the Paging Server logs**

After you have configured the paging server using the instructions in Setting up pager notifications on page 126, you can choose to send a page.

The paging server is running in the Windows task bar. Right-click the paging server and choose View Logs.

**How to export report data to XML**

Sometimes it is advantageous to bring report data out of its native format and into third-party tools. If needed, you can accomplish this by exporting your report data to XML.

Your can generate hundreds of reports, all of which can be configured as you need and provide you visibility and analytics about your network. After creating a report, there may be times where you want the data from only part of a report so you can store the data elsewhere or manipulate it using another tool. Using settings only available from the report in your web browser, you can access the data on a report.
You can access report content in its raw format and then process the data with your tools. Just some of the raw data you can access includes SLA measurements for use in a MOM, security alerting inside a SIEM, or compliance monitoring data.

Unlike nearly every task described in this guide, which describes using the user interface to configure reports, this feature is only available after the report is created and you are viewing it in your web browser.

To export your report data to XML:

1. Open a web browser and type the following URL: `http://Observer/Observer` where `Observer` is the host name or IP address of the system running Observer.

2. In the upper left, ensure the desired probe instance is selected from the list.

3. Click **Settings** in the upper right. The Report Settings page opens.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Show Report Element Link when clicking on the report element title bar | Used for embedding report elements in a third-party tool. This allows you to click the title bar of any report element (graph, table, etc.) and obtain a link to that element and then embed the link in your tool. Hover your mouse over an element title and click it. This opens a pop up window from which you can open the element in another browser window or use in your third party tool.  

   The report (or report element — table, graph, etc.) you selected is processed and displayed in your third party dashboard. This report is from the source which it was generated, including any associated data sources and filters applied.  

   In the URL, you may see a start time and end time for the report. This happens when you generate the report using a fixed time criteria. These fields are in **epoch** and can be modified within the URL to provide the report on whatever fixed time period you wish.                                                                                                                                 |
| Show XML Export button                           | Allows the user to manually export the XML of a report (in its entirety, including all elements) to a XML file. An “XML Export” button appears at the top right. Click the button to generate an XML file which is saved to your hard drive. Use the XML file as you wish.                                                                                                     |
| Show XML Report Link button                      | Similar to the Show XML Export button, but instead of needing to click the button to generate the XML, you can generate the URL once and then use the XML data request URL in your third party tool. The resulting XML will be for the entire report, including all elements.  

   Similar to the “Show Report Element Link…”, the start and end times can be modified if using fixed time periods, and all business group sources and filters will apply.                                                                                                                                 |

128 | Observer® (pub. 17.Sept.13)
Creating or modifying Observer and GigaStor reports

Web Reporting has two configuration options. You may:

- Configure which statistics are available to browsers on a probe-by-probe basis or for all probes, and/or
- Configure password access to view the configured statistics.

1. Do one of the following:
   - For Observer reports, choose Options > Web Reporting Configuration.
   - For GigaStor reports, in the GigaStor Control Panel choose Settings > Reports Setup.

2. Click the Reports tab to see the default reports or to create your own report. On this tab you can create a new report, edit a report, or delete a report. You can also save the position of reports.
   
   If you create any reports that are sub-reports of another one, then enable “Edit report positioning” option and reposition the sub-report so that it is beneath the main report. Then click the Save Positioning button.

3. If you are using Observer Suite, you can schedule reports. Click the Schedule tab. For details about creating scheduled reports, see Publishing reports based on a schedule.

Creating a new report

1. Do one of the following:
   - For Observer, choose Options > Web Reporting Configuration.
   - For GigaStor Control Panel, in the GigaStor Control Panel choose Settings > Reports Setup.

2. On the Reports tab, click New (or select a report and click Edit). The Report Setup window appears.

3. Use the information in Table 17 for details about the fields on the General Options tab.

4. Click the Layout tab to add a table, graph, break, comment, or search.

Table 17: General Options tab

<table>
<thead>
<tr>
<th>Report name</th>
<th>Type a name for your report.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report description</td>
<td>Type a description for your report. This can be helpful if you have numerous reports or have people looking at the report lists who are unfamiliar with what each report contains.</td>
</tr>
<tr>
<td>Drill down report</td>
<td>Enable this option if you want the report to be a sub-report of another report that you have already created. After the report is created you must move the report by clicking the “Edit report positioning” option and then dragging your report to its desired location.</td>
</tr>
<tr>
<td>Observer Reports Only</td>
<td></td>
</tr>
<tr>
<td>Show filter information</td>
<td>Enable this option if you want sub-reports, associated with this report, to display the filter criteria that was applied (verbose mode). See Filtering at the report element level on page 134.</td>
</tr>
<tr>
<td>Redirect to external Web site</td>
<td>Select this option if you want your report to behave solely as a URL hyperlink in the web interface. Only available for Observer reports.</td>
</tr>
<tr>
<td>GigaStor Reports only</td>
<td></td>
</tr>
</tbody>
</table>
Adding and configuring a table

Thinking ahead and visualizing what you want your tables to look like or what data they should contain will help you when creating your table.

For DHCP reports with systems using DHCP, you may notice a difference between the probe and trending file's address book. If your report seems different than what you expect, use the other address book. In general, the trending file's address book will be more current and should be your default choice.

1. On the Report Setup – Layout tab, click the Add Item button at the bottom of the tab. This opens a dialog. Choose Table. The Table Column Setup window appears.
2. Type a name for the table. This name appears on the Layout tab and in the heading of the table when the report is displayed in your web browser.
3. In the Data Source Selection area, choose the trending source, sub-source, and report type. (This list matches what is shown in Observer in Trending/Analysis >Network Trending Viewer.) The trending source that you choose determines what sub-sources and reports are available.
4. Use the Available Columns section to choose what information you want in your table.
5. Choose which address this report should use. For details about the Address Book, see Building and saving an address book.
6. Use the Table layout section to change the order of the columns in the table. The top entry is the first (leftmost) column in your table while the last entry is the rightmost.
   - Arrows—Changes the order of the columns.
   - Remove—Deletes the column from the table.
   - Set as Sort Column—Sets the selected column as the key column and sorts the data from highest to lowest (descending) value. Click the button again to sort the data lowest to highest (ascending).
   - Edit Field Display Name—Sets the display name of the selected field to a custom text string.
   - Show Baseline Value Column—Adds a secondary, identical column beside your selected column; the secondary column is populated with observed baseline values to compare against.
   - Edit Filter—Allows you to apply a filter to some of the columns for the report. The type of data that may be filtered varies by the table you have selected.
7. Click OK to close the Table Column Setup. Your table now appears on the Layout tab. After you add a table, there are still several options available to configure the table to show you the data just as you want it.
8. Select the table you want to configure. On the left you can see the tables, graphs, or other items you have added. On the right are the options for the selected table.
9. Use Table 18 for details about the options for tables.
10. Click OK to save your changes to the table.

Table 18: Table options

| Station Address | Uses the MAC address from the trending file for that day. The address book is written in the trending data each day when the first trending file is recorded. |
Adding and configuring a graph

Expectation ahead and visualizing what you want your graphs to look like or what data they should contain will help you when creating your graph.

2. Select Graph, and click OK. The Graph Setup window appears.
3. Type a title for the graph. This name appears on the Layout tab and in the heading of the graph when the report is displayed in your web browser.
4. In the Data Source Selection section, choose the trending source, sub-source, report type, and graph type. The trending source that you choose determines what sub-sources and reports are available.
5. Use the Available Columns section to choose what information you want on your graph.
6. Use the Graph layout section to change the order of columns in the columns. The top entry is the first (leftmost) column in your graph while the last entry is the rightmost.

- Arrows—Changes the order of the columns.
- Remove—Deletes the column from the graph.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address from Address Book</td>
<td>Uses the IP address from the address book maintained by the probe. Should the IP address change on the probe, it is transferred to the Observer analyzer during the next data transfer.</td>
</tr>
<tr>
<td>DNS Name from Address Book</td>
<td>Uses the DNS name from the address book maintained by the probe. For details about the Address Book, see Building and saving an address book on page 36.</td>
</tr>
<tr>
<td>Alias</td>
<td>Uses the alias defined in the trending file. The address book is written in the trending data each day when the first trending file is recorded. Should the address book change during the day a new address book is written in the next trending file, and the newest address book is used for Observer for reports showing that day.</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows you to make changes to your table.</td>
</tr>
<tr>
<td>Max items</td>
<td>Limits the maximum number of items that may appear in the table. The default is 10.</td>
</tr>
<tr>
<td>Large number format</td>
<td>Choose how you want large numbers to be displayed. Choose between Actual, Exponential, and Metric.</td>
</tr>
<tr>
<td>Table shading</td>
<td>Choose how you want the table to be shaded, if at all.</td>
</tr>
<tr>
<td>Two row headers</td>
<td>Select this option if you want columns with long heading names to break across two rows. This makes columns narrower, which may be desirable for many columns.</td>
</tr>
<tr>
<td>ORS drill down report</td>
<td>Choose an ORS sub-report if you want to be able to jump from this report directly to it.</td>
</tr>
<tr>
<td>Observer drill down report</td>
<td>Choose an Observer sub-report if you want to be able to jump from this report directly to it.</td>
</tr>
<tr>
<td>Enable GigaStor drill down</td>
<td>Select this option to be able to connect to your GigaStor for more reports. This requires that you have a GigaStor probe.</td>
</tr>
</tbody>
</table>
# Set as Sort Column—Sets the selected column as the key column and sorts the data from highest to lowest (descending) value. Click the button again to sort the data lowest to highest (ascending).

# Edit Field Display Name—Sets the display name of the selected field to a custom text string.

# Edit Filter—Allows you to apply a filter to some of the columns for the report. The type of data that may be filtered varies by the table you have selected.

7. Click OK to close the Graph Setup. Your graph now appears on the Layout tab.

After you add a graph, there are still several options available to configure the graph to show you the data just as you want it.

8. Select the graph you want to configure. On the left you can see the tables, graphs, or other items you have added. On the right are the options for the selected graph.

9. Use Table 19 for details about the options for graphs.

10. Click OK to save your changes to the graph.

**Table 19: Graph options**

<table>
<thead>
<tr>
<th><strong>Edit</strong></th>
<th>Allows you to make changes to your graph.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max items</strong></td>
<td>Limits the maximum number of items that may appear in the graph. The default is 10.</td>
</tr>
<tr>
<td><strong>Large number format</strong></td>
<td>Choose how you want large numbers to appear. Your choices are: actual, exponential, and metric.</td>
</tr>
<tr>
<td><strong>Minimum graph height</strong></td>
<td>Sets the minimum height of a graph. This is pixels. For most monitors there are 96 pixels in one inch (96 pixels in 2.54 cm).</td>
</tr>
<tr>
<td><strong>Legend rows</strong></td>
<td>Choose how many rows you want in your legend.</td>
</tr>
<tr>
<td><strong>Vertical title</strong></td>
<td>Select this option if you want the title of the graph to appear vertically instead of horizontally.</td>
</tr>
<tr>
<td><strong>Observer drill down report</strong></td>
<td>Choose an Observer sub-report if you want to be able to jump from this report directly to it.</td>
</tr>
<tr>
<td><strong>Enable GigaStor drill down</strong></td>
<td>Select this option to be able to connect to your GigaStor for more reports. This requires that you have a GigaStor probe.</td>
</tr>
</tbody>
</table>

**Adding and configuring a break**

This option is only available for Observer reports.

Break elements are the simplest report elements; they are only used for introducing visual “breaks” in your report. Because each break element converts to a report header in your report, they are useful when you anticipate viewing or printing lengthy reports.


2. Select Break, and click OK. Your break now appears on the Layout tab.

   There are no configurable options for breaks.

3. (Optional) Reposition the break by using the arrow buttons.

4. Click OK to save your changes and close the window.

**Adding and configuring a comment**

This option is only available for Observer reports.
Comment elements are used for delivering extra information to viewers. For example, you could use a comment to provide viewers the contact information of your service providers, or you could use one to remind viewers of upcoming scheduled maintenance.

2. Select Comment, and click OK. Your comment now appears on the Layout tab.

   After you add a comment element, there are still several options available to configure the comment.
3. Select the comment you want to configure. On the right are options for the selected comment.
4. Use Table 20 for details about the options for comments.
5. Click OK to save your changes and close the window.

Table 20: Comment options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text entry formatting</td>
<td>Allows you to apply simple formatting to your comment text. Your choices are: bold, underline, and italic.</td>
</tr>
<tr>
<td>Text entry window</td>
<td>Type text here that you wish to appear in your comment and resulting report.</td>
</tr>
<tr>
<td>Insert image</td>
<td>Allows you to import and insert an image into your comment. Supported formats: JPG, GIF, BMP, and PNG.</td>
</tr>
<tr>
<td>Edit HTML</td>
<td>Allows you to include, or edit existing, HTML tags in your comment.</td>
</tr>
<tr>
<td>Show separator</td>
<td>Sets the status and location of the separator. Your choices are: none, above comment, and below comment.</td>
</tr>
</tbody>
</table>

Adding and configuring a search

This option is only available for Observer reports.

Search elements are used for filtering report data within the web interface. Unlike persistent filters, which are applied by an administrator, searches are temporary filters for any authorized user to use. This filter only affects your own web session; it does not change the information seen by other users. Furthermore, the searches—because they are filters—do not add additional overhead to the network.

2. Select Search, and click OK. Your search now appears on the Layout tab.

   After you add a search element, there are still several options available to configure the search.
3. Select the search you want to configure. On the right are options for the selected search.
4. Use Table 21 for details about the options for searches.
5. Click OK to save your changes and close the window.

Table 21: Search options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trending source</td>
<td>Sets the trending source from which you select a sub-source.</td>
</tr>
<tr>
<td>Sub-source</td>
<td>Sets the sub-source of your search. Your choice affects which search fields are available.</td>
</tr>
<tr>
<td>Fields to search</td>
<td>Allows you to include or exclude specific search fields.</td>
</tr>
<tr>
<td>Show search tip</td>
<td>Shows a search tip under the currently selected search field, reminding you of valid inputs.</td>
</tr>
</tbody>
</table>
Filtering at the report element level

You can filter individual report elements if desired. Meaning, the smallest building-blocks of your reports, like tables and graph elements, can be filtered to focus on specific portions of your network.

Moreover, filtering at the report element level will not displace or modify your underlying data, nor is such the intended purpose. The intended purpose of element filtering is to narrow the scope of report criteria, so the end result (i.e. a graph) is specific and easily understood by viewers.

Related Topics
- Configuring your network trending settings on page 158
- Collecting network trending data on page 156
- Securing access to reports on page 124
- Viewing reports in a web browser on page 122
- Configuring the Observer web server on page 122
- Publishing reports based on a schedule on page 124
- Setting up email notifications on page 125
- Creating or modifying Observer and GigaStor reports on page 129
Chapter 11: Security and Privacy

Security, privacy, and regulatory compliance

Security and privacy concerns are a reality for most businesses—perhaps even greater for worldwide enterprises. Fortunately, Observer accommodates virtually any privacy or security need that arises within or outside of your company, including any governmental regulations.

Observer is a software application that collects network traffic, and as sensitive or personal information flows over the network (as it does), it too is collected. The following are some examples of sensitive information that Observer may collect:

- IP and MAC addresses
- Web form submissions, including passwords
- Email and visited web sites
- Instant messages and chats
- Application usage statistics
- Downloaded and uploaded content
- Sensitive files on network storage
- Employee or client records
- Payment transactions
- Phone calls (VoIP only)

Regardless of how any sensitive information is gathered, being a processor of it subjects your institution to all regulations, laws, statutes, and policies that may apply, and Observer can help you achieve and maintain compliance with many of them.

Observer is compatible with hardware security modules that comply with the Federal Information Processing Standards (FIPS) number 140. See Decoding encrypted network traffic on page 80 for more information.

To become better aware of how you might follow regulations, here are some (non-exhaustive) examples of decisions to consider while configuring Observer and/or GigaStor:

- Data retention length—how long should you keep data?
- User accounts—who gets access to privileged data?
Encryption—does our data need to be impenetrable?
Exclusions—should some data never be collected, ever?
Sharing—how can we share our data safely and securely?
Physical security—do we need to isolate our equipment?
Notification—who else should know we collect data?

Ultimately, your institution alone is responsible for regulation compliance, but Observer can help you meet those requirements.

Securing communication between probes and analyzers

Connections to probes and GigaStor units are secured end-to-end using the Triple DES (3DES) encryption algorithm, making Observer’s transmissions over the network highly resistant to eavesdropping. These secured connections are facilitated by the Observer analyzer and cannot be disabled—only improved.

You may further encrypt all analyzer/probe communication by requiring all analyzers and probes to use an Observer encryption key. Using an Observer encryption key forces users to have a private key stored locally rather than knowing a password to log in.

Choose Options > Observer General Options > Security tab. Then, select Use Observer Encryption Key for Secure Connections.

Using the added protection of an Observer encryption key file adds an additional layer of 3DES encryption to the already encrypted data.

Figure 40: Securing your connections

After the option is enabled, you must then create or obtain the Observer Encryption Key file:

- If you have an existing Observer Encryption Key file (*.OEK), you must copy the encryption key file into the installation directory (usually C:\Program Files\Observer) of each probe or analyzer that you want to authorize.
- If you do not have an Observer Encryption Key file (*.OEK), generate a key file; click the “Launch Encryption Key Generator” button. Its online help explains its use and how to set up the keys it generates.

Along with securing your connections, we recommend authenticating your users. See Requiring a user account to open Observer on page 140 for more information.

Securing communication between the analyzer and probes

User authentication plays a key role in securing Observer. One best practice is to add the extra layer of security that authentication provides. Doing so ensures that authorized persons are genuine, not spoofed, and probe redirection can only be performed by the right people.
To enable user authentication, you must first tell Observer to encrypt all connections by securing communication between probes and analyzers.

To require user authentication, enable the Authenticate Users option.

User authentication is conceptually different than creating user accounts in Observer and setting user permissions.

### Setting security options for the analyzer

There are several options available to you to tighten access to the Observer analyzer. Many of the options are used along with NIMS, but some can be used by the Observer analyzer by itself.

To view and change the security settings for an Observer analyzer, in the Observer analyzer choose **Options > Observer General Options > Security**. Use the information in **Table 22 on page 137** to configure the analyzer’s security and NIMS options.

#### Table 22: Security tab options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Require Observer Login</strong></td>
<td>When enabled, this option forces a user to provide a user name and password to open the Observer analyzer. The user name can be stored locally if you are not using NIMS, or maintained by NIMS if the “Authenticate Observer login with NIMS“ option is enabled. This option is not visible unless you have a special license enabling it. &lt;br&gt;Observer Login Credentials—Type a user name and password. This information is encrypted and stored locally. Only one user account is allowed per system. If you want numerous people to have access to the Observer analyzer with different user accounts, you must use NIMS. &lt;br&gt;Administrative Credentials—An local administrative user account that allows you to create a non-administrator account and to set security options for NIMS. Do not lose this password! There is no way to recover a lost administrative password.</td>
</tr>
<tr>
<td><strong>Use Observer Encryption Key file for secure connections</strong></td>
<td>Strong encryption is available for Observer Expert and Suite users. Observer Encryption Key (.OEK) files let you use private encryption keys to ensure that unauthorized persons do not have access to the data flowing between Observer analyzers and probes. &lt;br&gt;To use Observer Encryption Key files, you must copy the encryption key file into the installation directory (usually C:\Program Files\Observer) of each probe or analyzer that you want to authorize. To generate a key file, click the “Launch Encryption Key Generator“ button. Its online help explains its use and how to set up the keys it generates. &lt;br&gt;Each analyzer and each probe must have the .oek file. Observer encryption keys are required if you want to use NIMS.</td>
</tr>
<tr>
<td><strong>Authenticate users (for redirected Probe instances)</strong></td>
<td>Forces users to authenticate with NIMS before using remote probes. User accounts belong to user groups in NIMS and through the user groups access to probe instances can be granted or restricted. Only probe instances to which the user has access will be visible in the analyzer. This option does not control whether users can openObserver. That is done through the “Authenticate Observer login with NIMS“ option.</td>
</tr>
<tr>
<td><strong>Manage Observer /Probe license with NIMS</strong></td>
<td>An Observer or probe license can be stored and managed locally at each analyzer or probe, or it can be managed centrally by NIMS. If unchecked, it is managed locally and you must provide a license for each analyzer/probe. If selected, then</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>you can provide a pool of licenses in NIMS and the analyzer or probe will take an available license when the analyzer or probe starts.</td>
<td></td>
</tr>
<tr>
<td>Get list of Probe Instances available for redirection from NIMS</td>
<td>When selected all probe instances to which you the user has access to through group permissions set in NIMS are available when connecting to a probe. When unchecked only the local probe instances are available and no probe instances are listed when connecting to a remote probe.</td>
</tr>
<tr>
<td>Share filters with NIMS</td>
<td>When selected you may create filters and share them with others. You can also get any filters created by others. Whenever a filter is updated, you can be informed and update your local version. The list is maintained by NIMS.</td>
</tr>
<tr>
<td>Synchronize user protocol definitions through NIMS</td>
<td>When selected you can have NIMS manage your protocol definitions and share them with other Observer analyzers in your network. Protocol definitions created or modified on one Observer analyzer are shared and synchronized with all other Observer analyzers. The list is maintained by NIMS.</td>
</tr>
<tr>
<td>Primary/Secondary server</td>
<td>Provide the IP address of the primary NIMS server. If you are also using a failover NIMS server, type its IP address in the Secondary server box.</td>
</tr>
<tr>
<td>Allowed to modify shared filters</td>
<td>When selected, you can get a shared filter from someone else, modify it locally, then upload your modified version to NIMS thereby making your new version available to everyone else. When disabled, you can only get filters from NIMS and upload your own. You cannot modify any filters you get from NIMS. This option requires that you have the ability to share filters with NIMS.</td>
</tr>
<tr>
<td>Authenticate Observer login with NIMS</td>
<td>This option works in conjunction with the “Require Observer Login” option. This forces Observer to use NIMS to authenticate users rather than Observer’s local user list. A user list is maintained in NIMS.</td>
</tr>
<tr>
<td>Require a password to change partial packet capture size</td>
<td>Select this option if you want to require someone to provide a password before they may change the partial packet capture size. This is a central password and all users must use the same password.</td>
</tr>
<tr>
<td>Launch Encryption Key Generator</td>
<td>Click this button to open the Network Instruments encryption key generator. If you want the GigaStor payload to be encrypted using 256 bit AES encryption before it is stored, select the “Encrypt GigaStor network traffic…” option. An encryption key is needed on the GigaStor (or a location accessible by the GigaStor) to encrypt and decrypt the data. The AES key is not needed on workstations, probes, or other collection points. A special license is required for this feature. Contact Network Instruments for this license.</td>
</tr>
</tbody>
</table>

**Setting security options for probes**

There are several options available to you to tighten access to a Multi Probe or Expert Probe. Single probes cannot be secured. Many of the options are used along with NIMS, but some can be used with the Observer analyzer without NIMS.

To view and change the security settings for a probe, in the probe choose Options > Probe Options. Use the information in Table 23 on page 138 to configure the probe’s security and NIMS options.

**Table 23: Probe security options**
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Observer Encryption Key file for secure connections</td>
<td>Strong encryption is available for Observer Expert and Suite users. Observer Encryption Key (.OEK) files let you use private encryption keys to ensure that unauthorized persons do not have access to the data flowing between Observer analyzers and probes.</td>
</tr>
<tr>
<td></td>
<td>To use Observer Encryption Key files, you must copy the encryption key file into the installation directory (usually C:\Program Files\Observer) of each probe or analyzer that you want to authorize. To generate a key file, click the &quot;Launch Encryption Key Generator&quot; button. Its online help explains its use and how to set up the keys it generates.</td>
</tr>
<tr>
<td></td>
<td>Each analyzer and each probe must have the .oek file. Observer encryption keys are required if you want to use NIMS.</td>
</tr>
<tr>
<td>Use NIMS for user authentication</td>
<td>This option works along with the &quot;Require Observer Login&quot; option. This forces Observer to use NIMS to authenticate users rather than Observer’s local user list. A user list is maintained in NIMS.</td>
</tr>
<tr>
<td>Manage Observer /Probe license with NIMS</td>
<td>An Observer or probe license can be stored and managed locally at each analyzer or probe, or it can be managed centrally by NIMS. If unchecked, it is managed locally and you must provide a license for each analyzer/probe. If selected, then you can provide a pool of licenses in NIMS and the analyzer or probe will take an available license when the analyzer or probe starts.</td>
</tr>
<tr>
<td>Primary/Secondary server</td>
<td>Provide the IP address of the primary NIMS server. If you are also using a failover NIMS server, type its IP address in the Secondary server box.</td>
</tr>
<tr>
<td>GigaStor data analysis time slice</td>
<td>Available only when using Expert Probe software on a GigaStor. If your GigaStor is writing data to disk at near capacity of the disk speed and you then mine data from the disk, it is possible that the GigaStor will drop some packets from being written to disk. You can prevent this by reducing the data analysis percentage from 100% to something lower. Writing to disk will always be 100%, the reading or mining of data will be at the percentage you choose.</td>
</tr>
<tr>
<td>GigaStor Capture Payload Encryption</td>
<td>Available only when using Expert Probe software on a GigaStor. If you want the GigaStor payload to be encrypted using 256 bit AES encryption before it is stored, select the “Encrypt GigaStor network traffic…” option. An encryption key is needed on the GigaStor (or a location accessible by the GigaStor) to encrypt and decrypt the data. The AES key is not needed on workstations, probes, or other collection points; however you must generate the key from an Observer analyzer. A special license is required for this feature. Contact Network Instruments for this license.</td>
</tr>
</tbody>
</table>

## Configuring user accounts for secure access

If you want to restrict access to packet captures and reporting provided by a probe instance, you can create user accounts, permissions, and define security attributes of the local probe.

If you are using Network Instruments Management Server (NIMS) to control user accounts (if Authenticate Users is enabled; Figure 40 on page 136), you must control accounts from the NIMS interface.

Again, configuring user accounts for secure probe access is conceptually different than requiring a user account to open the analyzer.
Requiring a user account to open Observer

With a special Observer license, you can require users to log in to the Observer analyzer. To enable this option, choose Options >Observer General Options > Security tab, then select Require Observer Login. For more details, see Setting security options for the analyzer on page 137.

Requiring a user account to open Observer does not restrict access to probes or probe instances. That is done by user accounts on the probes or by NIMS. See Configuring user accounts for secure access on page 139.

Creating or editing a user account for the local probe

A user account used to open Observer does not restrict access to probes or probe instances. That is done by user accounts on the probes or by NIMS. See Configuring user accounts for secure access on page 139.

To create or edit an Observer user account, choose Options > Selected Probe or Local Observer Instance, Memory and Security Administration, and click the Security tab.

Alternatively, right-click any probe instance and select Administer Selected Probe; then click the Security tab.

From the security tab, click User Accounts to view all configured probe instances. Then, use the drop-down to select any existing user account.

Figure 41: Selecting an existing user account

To create a new user account, click New User. The New User Account dialog appears, allowing you to create a new user name and password, plus tell Observer if the user should have administrator rights and access to some or all probe instances.

The setup options for editing a user account are identical to creating a new one; just select a user and click Edit User.

Setting user permissions for the local probe

Observer is a powerful application that can store a wealth of data—some of which may be personally identifiable. Therefore, you may want to deactivate some features of the software on a per user basis; this ensures that not everyone has access to sensitive data and features.

For example, deactivate the ability of some users to replay VoIP calls if you are concerned about the potential for abuse. Again, this is accomplished by setting user permissions. A special Observer license also exists to disable VoIP audio playback entirely.

To set user permissions, select a user account.
Important information about NIMS

The Network Instruments Management Server (NIMS) simplifies probe administration, management, security, and maintenance for IT professionals responsible for maintaining multiple Network Instruments probes across enterprise networks.

For network managers, NIMS offers added security, centralized licensing, a centralized update service, and failover redundancy. For network administrators, NIMS provides shared access to analysis tools, including Observer and probe filter libraries.

**Note:** The Network Instruments Management Server (NIMS) is only used for centralized user and probe management; it does not eliminate the need for running the Observer application on a local machine.

Documentation for the Network Instruments Management Server (NIMS) is not included in this user guide; see the NIMS User Guide.

Sharing packet captures with third-parties

Unless necessary, it is generally unwise to share “full” packet captures with outside sources because you could end up sharing too much information—information that should not be shared.

To prevent this from happening, Observer allows you to create a filtered packet capture from a larger capture. Filtered captures behave exactly like full captures—as they are indeed a complete capture file—except they only contain packets of your choice.

Creating a filtered capture can be done either before or after the initial capture is made. We recommend you become familiar with both processes before continuing.

**Note:** You can also configure Observer to create partial packet captures regardless of protocol. See Configuring Observer to capture partial packets on page 59.

To create a filtered packet capture fit for sharing, ensure the full packet capture is loaded in Observer then:

1. Choose **Actions > Filter Setup for Selected Probe**. The Active Filters window appears.
2. From the Active Filters window, click **New Filter**. Give your filter a name, and click OK.
3. Right-click the new filter, and select **Edit Rule As > Packet Partial Capture**.
4. Within the Partial Packet Payload for TCP/UDP Filter window, set up rules for how the filter is applied. Specifically, the uppermost portion of the window is for filtering by IP address, range or subnet, and MAC or IPv6 address. The lowermost portion is for filtering application or protocol.

5. Click OK to confirm your changes.

6. Click OK to save your filter.

7. Enable your new filter to activate it, and click OK to save your changes.

Password protecting the ability to change partial packet capture size

To password protect the ability to change partial packet capture size, choose Options > Security tab, and enable Require a Password to Change Partial Packet Capture Size.

Password protecting this option helps ensure your partial captures remain partial, saving you disk space and enhancing data subject privacy because payload is not recorded in full.

Trimming data from your captures

Typically, packet headers contain the most useful information because they contain routing information and protocol information; The packet payload counterpart, however, is sometimes wasteful to collect because most troubleshooting is done just with the header.

Under these circumstances, you may want to truncate most payload data from the packet header(s). In Observer, the result is a partial packet capture.

Some benefits of partial packet captures include:

- Smaller capture sizes
  - More overall storage space for packet captures
  - Greatly increases the effective storage size of a GigaStor (or other capture buffer)
- Performance metrics remain intact
- Increased overall privacy
- Least resource intensive capturing

Some disadvantages of partial packet captures include:

- Not all network traffic is stored to disk
Forensics may be hindered without full payload data
Data stream reconstruction may not work
Most resource intensive capturing
Increases CPU utilization

To configure Observer to trim all packet data beyond the first 64-bytes, choose Capture > Packet Capture > Settings > Capture Options tab, and enable Capture Partial Packets (Bytes).

Figure 43: Configuring partial packet captures

It is possible to decrease or increase the default 64-byte partial packet capture size. Click the Change Size button to set a custom value. From then on, each packets’ bytes following the target value are discarded from capture.

How to encrypt captured data

Captured data can be encrypted using the 256-bit Advanced Encryption Standard (AES) algorithm. This significantly increases the security of your at-rest data.

You must have a special Observer license to enable and use this feature. There is no extra charge for the license.

Data at rest encryption is prevent visibility into any packets or even the metadata about the packets stored on the GigaStor. Any packets that are captured by the GigaStor are considered "data" and while they are stored on the GigaStor they are considered "at rest." Should any of the drives in the GigaStor be removed or misplaced, the data on the drives is protected. There is no remote access to this data apart from Observer’s own analyzer, and the data tagging methods for organizing and retrieving data can only be used in conjunction with the Observer analyzer.

The GigaStor can capture 10 Gb line rate while simultaneously encrypting the traffic with AES-256 encryption without any significant performance impact on write or read speeds of the GigaStor.

These instructions describe how to apply data at rest encryption to a GigaStor already in your possession. If your GigaStor shipped from the warehouse with the data at rest security already enabled, you do not need to complete this process unless two or more drives in your RAID have failed.

Caution! This procedure deletes all of the data on your GigaStor! Ensure you have a backup of any data you wish to keep.

1. Download the latest firmware for the Areca 1882 Series RAID card or contact Network Instruments Support for the file.
2. Choose Start > All Programs > Areca Technology Corp > ArcHttpSrvGui > Areca HTTP Proxy Server GUI. The program starts. You should see something similar to this image.
3. Select Controller#01 and click Launch Browser. If the controller is not running, click the Start button then launch the browser. The Areca RAID application attempts to connect to its web server.

4. Type the user name and password. The default user name is **admin**. There is no default password. Click OK to open the browser.

   In the browser you can see the RAID set, IDE channels, Volume, and capacity.

5. In the web browser, choose **System Controls > Upgrade Firmware**. In the **Browse** field, choose each of the four files from the firmware package you downloaded or received from Technical Support in step 1 and click **Submit**. Choose the files in the order they are listed below. After adding the arch1882firm.bin file you are prompted to restart the system. Ignore that restart request and add the fourth file.

   - ARC1882BIOS.BIN
   - ARC1882BOOT.BIN
   - arc1882firm.bin
   - ARC1882MBR0.BIN

6. Restart the GigaStor.

7. Choose **Volume Set Functions > Delete Volume Set**. Select the volume, then select **Confirm The Operation** and click **Submit**. This deletes all of the existing data on the RAID.

8. Choose **Volume Set Functions > Create Volume Set**. Set the following options to these values, select **Confirm The Operation**, and click **Submit**.

<table>
<thead>
<tr>
<th>Volume RAID Level</th>
<th>Raid 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater Two TB Volume Support</td>
<td>64bit LBA</td>
</tr>
</tbody>
</table>

   **Volume Initialization Mode**

   Background Initialization. It may take several hours (six hours for 48 TB) to initialization the volume. While the volume is being initialized, the GigaStor cannot be used. If you choose Foreground Initialization, you may use your GigaStor, but it
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Stripe Size</td>
<td>128</td>
</tr>
<tr>
<td>Volume Cache Mode</td>
<td>Write Back</td>
</tr>
<tr>
<td>Volume Write Protection</td>
<td>Disabled</td>
</tr>
<tr>
<td>Full Volume Encryption</td>
<td>256Bit Key, AES Key</td>
</tr>
<tr>
<td>Tagged Command Queueing</td>
<td>Enabled</td>
</tr>
<tr>
<td>SCSI Channel</td>
<td>0:0:0</td>
</tr>
<tr>
<td>Volumes To Be Created</td>
<td>1</td>
</tr>
</tbody>
</table>

will take significantly longer to complete and performance will be negatively affected.

9. Open Observer and apply your new license. Restart Observer. Because this is the first time that Observer is opened with the new license, it does not yet have a key for the encrypted volume. A window appears indicating that the volume is locked. Click **Generate Key** and save the key file. This is the key necessary to write to and read from the RAID volume. You can choose to remember the key file location so that Observer opens automatically, or, if left cleared, each time Observer is opened you must provide the path to the key file.

   Every time Observer opens it looks for the encryption key that allows access to encrypted volume. Without the key present neither packet capture nor packet analyzation can occur.

10. Close Observer until the rest of this procedure is complete.

11. In **Control Panel > Administrative Tools > Computer Management > Storage > Disk Management** select the RAID volume, right-click and choose **Initialize**. In the Initialize Disk window, select Disk 1 and GPT (GUID Partition Table). Convert the volume to a Simple Layout, assign a drive letter (typically, D:), and provide a name (typically, DATA).

12. Repeat this process for each RAID volume for your GigaStor.

13. Open Observer.

**Related Topics**

- Configuring user accounts for secure access on page 139
- Securing communication between probes and analyzers on page 136
- Important information about NIMS on page 141
- Requiring a user account to open Observer on page 140
- Pre-filtering your packet captures on page 66
- Post-filtering your packet captures on page 72
Chapter 12: Network Trending

Network Trending

Network trending provides a broader view of your network and gives you trending information about network applications. This information may be useful for solving a specific problem or can be used for long-term planning. For example, you can collect statistics about the applications on your network for weeks, months, or years and be able to create reports showing the changes over time.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing current network activity</td>
<td>++</td>
<td>+</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Viewing long-term network activity³</td>
<td>–</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>Viewing network errors (CRC, alignment, etc.)</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Capturing packets for analysis</td>
<td>–</td>
<td>++</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Analyzing servers and applications</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>+</td>
</tr>
<tr>
<td>Analyzing routers and devices</td>
<td>++</td>
<td>+</td>
<td>+</td>
<td>++</td>
</tr>
</tbody>
</table>

Legend: – not recommended, + suitable, ++ recommended

¹) Observer’s Network Trending tool without the aid of a GigaStor hardware appliance.
²) NetFlow and sFlow probe instances behave differently than most other types.
³) Long-term is considered any duration lasting one hour or longer.

Network trending is fundamentally different from packet captures and real-time statistics.

Observer’s Network Trending tool, along with the Network Trending Viewer, allows you to collect, store, view, and analyze network traffic statistics over long periods of time. At the software level, these two components
function independently, meaning the Network Trending tool collects the information, and the Network Trending Viewer allows you to view the information as reports in your web browser.

Within Network Trending there are two similar tools that serve very different purposes: Application Performance Analysis (APA) and Application Transaction Analysis (ATA). APA tracks all traffic passing through your server or application while ATA is only looking at a specific application (such as HTTP or SMTP). APA is used for statistics about Layer 4 of the OSI Model and ATA is for Layers 5-7.

When analyzing your network and viewing reports with APA and ATA, you may come across the terms 'network delay' and 'server delay.' Network delay is the extra time added because of the network. Server delay is the additional time added because of the application. Server delay is not a combination of network delay plus server delay plus application delay.

### How to configure Application Performance Analysis

**Prerequisite(s):**

If you are unfamiliar with Application Performance Analysis, see [What is Application Performance Analysis? on page 149](#) before beginning.

To customize your Application Performance Analysis settings, complete the following steps:

1. Choose **Trending/Analysis > Network Trending** from the Observer main menu.
2. Click the Settings button. The Network Trending Settings window appears.
3. Click the Application Performance Analysis group tab.
4. Settings can be changed in each tab. Noteworthy settings for each are listed in the following tables:

![Network Trending Settings](image)

**Figure 45: Configure your network trending settings here**

**Table 24: General tab**

---

*How to configure Application Performance Analysis | 147*
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default selection or value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track only servers using IP addresses with associated ports defined in “Protocol Definitions and Server Application Discovery”</td>
<td>Enable this setting to track only defined servers. See Discovering server applications on the network on page 39.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Track only new connections in every collection interval</td>
<td>Keep this option disabled if you want to continue tracking connections that have already been established. Depending on network traffic conditions, disabling this option may require more disk space and more CPU utilization. See Figure 47 on page 151 for further details of this setting.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Count rerouted as resent</td>
<td>Choose this if you want rerouted TCP transmissions to be considered resent, instead.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Retransmission too fast</td>
<td>Set this value if necessary, but the default is appropriate in most cases. This value defines when a retransmission is too fast.</td>
<td>180 (ms)</td>
</tr>
<tr>
<td>Resent minimum time</td>
<td>Set this value if necessary, but the default is appropriate in most cases. This value defines the minimum amount of time needed for a resent to be considered such.</td>
<td>100 (ns)</td>
</tr>
</tbody>
</table>

### Table 25: Applications tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default selection or value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track servers using the following applications (tracking all applications when unchecked)</td>
<td>Allows APA to track servers using the protocols in the protocol list. Enabling this option allows changes to be made in this tab.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Protocol (list)</td>
<td>When “Track servers using the following protocols” is enabled, the protocols in this list are tracked in APA.</td>
<td>N/A</td>
</tr>
<tr>
<td>Add button</td>
<td>Click the Add button to add an application protocol to the list of tracked servers.</td>
<td>N/A</td>
</tr>
<tr>
<td>Remove button</td>
<td>Remove an application protocol from the list by selecting one or more and clicking Remove. You can use SHIFT-click to select</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Table 26: Subnet Ranges tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default selection or value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit tracked server connections</td>
<td>Allows IP subnet ranges to be defined in this tab. This setting must be enabled for any settings in this tab to be active.</td>
<td>Disabled</td>
</tr>
<tr>
<td>to defined IP subnet ranges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Choose the IP type of the target address range. Your options are IP (IPv4) or IPv6.</td>
<td>IP (IPv4)</td>
</tr>
<tr>
<td>Servers are located in this subnet</td>
<td>Enable this setting if servers are located in the leftmost subnet range (the subnet range on the left side of the arrow icon). If left disabled, all tracked server connections from this subnet are seen as clients.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Filter traffic between two subnets</td>
<td>Enable this setting if you want to track server connections between two unique subnet ranges. If left disabled, server connections are tracked between one subnet and any others.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

What is Application Performance Analysis?

**Prerequisite:** Observer Expert or Observer Suite

Application Performance Analysis (APA) is a feature of the Network Trending tool. Analyzing Layer 4 of the OSI Model, APA allows you to monitor response time trends for any server or application with a known TCP port. Application Performance Analysis cannot account for whether fulfillment of the application took place as expected by the user. In many ways, this means APA is broad but limited. Also, response times in Application Performance Analysis are calculated as shown Figure 46 on page 150. Response times are always calculated by actual data packets, not SYN or SYN-ACKs.
Figure 46: Response time calculation in Application Performance Analysis

Application Performance Analysis collects response times based on Layer 4, which is the Transport Layer (TCP in this case). All statistics which include server response time, client response time, server network delay, client network delay and round trip delay in the TCP events window of Expert Analysis corresponds to analysis performed on the transport layer data packets and not SYN, SYN-ACK, and ACK packets.

For “network delay” statistics, Observer tracks the average total time taken to establish a TCP connection looking at the timestamps on the SYN, SYN-ACK and ACK packets. The total time taken to establish this connection before data is transferred forms the “network delay” statistic in APA.

The **Track only new connections in each collection interval** affects what connections are part of a collection interval. The start of a connection is when Observer sees the SYN, SYN-ACK, and ACK handshake. This applies whether this option is selected or cleared. When the handshake is seen, the server/client connection is put into memory. See below for details about how to change the number of connections.

This list describes what occurs when **Track only new connections in each collection interval** is selected or cleared:

- When selected, any connection that starts and ends in the current collection interval is tracked in its entirety.
- When selected, any connection that starts in the current collection interval but spans into the next interval is tracked up to the end of the current interval. No statistics are kept about it beyond the interval in which it was first seen.
- When selected, any connection that started in a previous collection interval is ignored during any subsequent collection intervals.
- When cleared, any connection that starts in the current interval is tracked for its entirety even if it spans one or more collection boundries.

In the image below, you can see NetFlow has a roughly 42 minute connection (last example) and then a second, shorter duration connection starts at about the 43 minute mark. The entire 42 minute conversation is tracked in the last example because **Track only new connections in each collection interval** is unchecked. In the other two examples, the NetFlow connection is not tracked beyond 30 minutes (first example) or 10 minutes (second example) because **Track only new connections in each collection interval** is selected and the connection spanned collection interval boundaries. (The statistics collection interval is set on **Trending/Analysis > Network Trending > Settings > General**. For more details, see Choosing your network trending types on page 158.)

The **Track only new connections in each collection interval** option is selected by default. You may wish to track conversations in their entirety; doing so may cause a slight performance degradation because of the nominal amount extra processing required. The default number of connections tracked is 800. To change the maximum number of connections, select the probe instance, right-click and choose **Administer Selected Probe**. On **Memory Management**, select the probe instance and choose Configure Memory. Click New, give
your memory profile a name, and locate **Trending: Application Performance Analysis** to change how much memory is allocated for APA.

Figure 47: Collection intervals explained

Analyzing servers and applications using ATA

Critical application servers should be added to Expert Analysis for Application Transaction Analysis.

**Prerequisite:** Observer Expert or Observer Suite

Application Transaction Analysis (ATA) is a tool that shows you the following information about your applications and servers in Layers 5-7.

- Application response time
- Application errors (if any)
- Total application requests
- Network delay
- FIX Statistics

If you are not sure why you would want to add any servers or applications to ATA, see Network Trending on page 146.

**Tip!** Until you configure the tool, nothing useful appears. Follow the steps provided in this section to complete the prerequisite configuration process and begin using Application Transaction Analysis. If you need a better idea of what ATA provides, see Figure 48 on page 152 for an example.

All response times shown in Observer are relative to the location where the capture takes place (that is, wherever the probe is located). If your probe is in London and you are in New York with your Observer analyzer, the capture times are relative to the time in London, not New York. Be mindful of this during any analysis.
To begin configuring Application Transaction Analysis, complete the following steps:

1. Choose how to add the server.
   - Right-click an expert conversation and choose Add Server to Application Transaction Analysis.
   - Complete the following steps.

2. Choose **Trending > Application Transaction Analysis**.

3. Click the Settings button. The Application Transaction Analysis Settings window appears.

4. Ensure the Response Time Analysis grouping is selected, located at the leftmost portion of the window.

5. Click **Discover** or Add. The Add Server to Application Analysis dialog appears.

6. Ensure **Live Statistics** and **Network Trending Statistics** are selected.

**What is Application Transaction Analysis?**

Application Transaction Analysis (ATA) is a feature of the Network Trending tool. Using Layers 5-7 of the OSI Model, ATA allows you to monitor response time, error, request and response trends for any server application protocol listed in Table 27 on page 153. Most importantly, ATA can track and trend successes and failures of these client-server transactions, including response times at the application layer as calculated as shown in Figure 49 on page 153.
Application Transaction Analysis is unique because it can be configured and used outside of the Network Trending tool. Meaning, the Network Trending tool is not required for Application Transaction Analysis to function because they operate independently. You can have the Network Trending tool run Application Transaction Analysis.

**Table 27: Protocol name**

<table>
<thead>
<tr>
<th>Application’s protocol name</th>
<th>Acronym or abbreviation</th>
<th>Transport layer protocol(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Internet File System</td>
<td>CIFS</td>
<td>TCP</td>
</tr>
<tr>
<td>Server Message Block</td>
<td>SMB</td>
<td>TCP</td>
</tr>
<tr>
<td>Cisco Skinny Call Control Protocol</td>
<td>SCCP</td>
<td>TCP</td>
</tr>
<tr>
<td>Citrix Independent Computing Architecture</td>
<td>ICA</td>
<td>TCP</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol</td>
<td>DHCP</td>
<td>UDP</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol for IPv6</td>
<td>DHCPv6</td>
<td>UDP</td>
</tr>
<tr>
<td>Domain Name System</td>
<td>DNS</td>
<td>UDP</td>
</tr>
<tr>
<td>Diameter</td>
<td>Diameter</td>
<td>TCP, SCTP</td>
</tr>
<tr>
<td>Financial Information eXchange</td>
<td>FIX</td>
<td>TCP</td>
</tr>
<tr>
<td>File Transfer Protocol</td>
<td>FTP</td>
<td>TCP</td>
</tr>
<tr>
<td>H.245 (control channel)</td>
<td>H.245</td>
<td>TCP</td>
</tr>
<tr>
<td>H.255.0 (gatekeeper comm. or RAS)</td>
<td>H.255.0</td>
<td>UDP</td>
</tr>
<tr>
<td>H.255.0 (end-to-end communication)</td>
<td>H.255.0</td>
<td>TCP</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol</td>
<td>HTTP</td>
<td>TCP</td>
</tr>
<tr>
<td>Internet Message Access Protocol</td>
<td>IMAP</td>
<td>TCP</td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol</td>
<td>LDAP</td>
<td>TCP</td>
</tr>
<tr>
<td>Media Gateway Control Protocol H.248</td>
<td>MEGACO/H.248</td>
<td>UDP</td>
</tr>
<tr>
<td>Microsoft Remote Procedure Call</td>
<td>MSRPC</td>
<td>TCP</td>
</tr>
<tr>
<td>Network File System</td>
<td>NFS</td>
<td>TCP</td>
</tr>
<tr>
<td>Network File System</td>
<td>NFS</td>
<td>UDP</td>
</tr>
<tr>
<td>Post Office Protocol</td>
<td>POP3</td>
<td>TCP</td>
</tr>
<tr>
<td>Application's protocol name</td>
<td>Acronym or abbreviation</td>
<td>Transport layer protocol(s)</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Remote Authentication Dial In User Service</td>
<td>RADIUS</td>
<td>UDP</td>
</tr>
<tr>
<td>Session Initiation Protocol</td>
<td>SIP</td>
<td>UDP</td>
</tr>
<tr>
<td>Simple Mail Transfer Protocol</td>
<td>SMTP</td>
<td>TCP</td>
</tr>
<tr>
<td>Simple Network Management Protocol</td>
<td>SNMP</td>
<td>UDP</td>
</tr>
<tr>
<td>Tabular Data Stream</td>
<td>TDS</td>
<td>TCP</td>
</tr>
<tr>
<td>Telnet</td>
<td>Telnet</td>
<td>TCP</td>
</tr>
<tr>
<td>Oracle Transparent Network Substrate</td>
<td>TNS</td>
<td>TCP</td>
</tr>
<tr>
<td>WebSphere MQ</td>
<td>WebSphere MQ</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Understanding response time distribution values**

The Response Time Distribution tab shows how applications are performing on a relative or absolute basis. The response times shown in the header are configurable. They are set when you add a server to Application Transaction Analysis.

To view the Response Time Distribution tab:

1. Choose **Trending/Analysis > Network Trending**.
2. Click the Analysis button at the top of the Network Trending window. The View Network Trending Data dialog appears.
3. Choose Transfer and view current day statistics and click OK. The data is transferred and the Network Trending Viewer opens.
4. At the bottom of the Network Trending Viewer window, click the Response Time Distribution tab.
Importing or exporting a server profile

You can import or export servers that you monitor from one Observer analyzer to another. This can save time and reduce typing errors if you have several Observer analyzers which you want to have the same servers be analyzed for application transaction analysis.

**Tip!** You can also logically group server applications and switch between profiles quickly by choosing a profile from the Profiles list.

1. Choose **Trending/Analysis > Application Transaction Analysis**.
2. Click the Settings button to define any application servers you want to monitor.
3. Click the Import or Export button.

   First you must define the server applications and then export the server to create the *.ata file that you can later import.

**Does network trending have any limitations?**

The volume of data passing through a large network is usually very high, and monitoring network statistics over a long period of time can impose limitations on the amount that can be monitored and stored in the statistics buffer. Therefore, monitoring every packet may not be practical.

Observer, like other protocol analyzers, deals with this problem using a mechanism called **sampling**. Sampling monitors only a portion of the total data flowing on a network, at any one moment, and statistically adjusts the results to represent a statistically accurate total based on the sample size of the data monitored.
This means that a protocol analyzer, through sampling, processes only one packet in every X number of packets. Here, the number X is called a sampling divider. If your processor(s), memory, buffer sizes, and installation of Observer can handle monitoring every single packet, both in high and low traffic conditions, you may be able to set your sampling divider to one (1). Typically, however, protocol analyzers that try to monitor each incoming data packet tend to drop packets during high traffic bursts and less in slower traffic periods.

More about the sampling divider

The sampling divider plays a key role in Network Trending. Network trending is statistical sampling of your network traffic. There are millions and millions of packets traversing your network. Over a long enough time frame the statistics are going to be equally valid if you sample every 10 or 100 or 1000 packets rather than every single packet. Also if you are using Observer Reporting Server, it gets its data based on the collection settings you choose for Network Trending.

Network trending is not packet analysis. Statistics from network trending serve a different role than actual packets. Statistics are intended to give you an indication of what is happening with your network. If the statistics indicate you may have an issue, then you can use the actual packets saved in your probe to further analyze the traffic.

The sampling divider represents a trade-off between accuracy and processor (CPU) cycles. The higher the sampling divider, the smaller the potential sample size of monitored data; thus, you risk the potential for less accurate trending during shorter periods of time. However, a higher sampling divider does reduce the utilization of your processor, allowing it to perform other functions (e.g. operating system services) without issue. The lower the sampling divider, the higher the likelihood of data being dropped during a collection interval, which can affect overall results.

Choose a sampling divider appropriate for your network. An approximate rule for the sampling divider in Observer is the maximum expected bandwidth utilization divided by four (4). This means that if the bandwidth utilization on the network often reaches 80% (quite high), consider using a sampling divider of 20—or higher for slower systems.

You can change the sampling divider from the Network Trending Settings window.

Collecting network trending data

To collect network trending data, complete the following steps:

The initial collection can take up to an hour depending on the amount of time you set for the Statistics Collection Interval.

1. Choose Trending/Analysis > Network Trending from the Observer main menu. The Network Trending window appears.
2. (Optional) Click the Settings button to configure your collection parameters.
3. Click the Start button. If you see progress bars, Observer is actively collecting data.

After completing this task:
To schedule the collection of network trending data—instead of on demand as described in this section—see Configuring your network trending settings on page 158.

Viewing network trending data

Network Trending Viewer allows you to view collected network trending data in a series of reports in your web browser. To view collected network trending data, choose Trending/Analysis > Start Network Trending Viewer. Along the left is a column with various categories. Expand these sections to see the reports. Click a report to have it open in the main section of your web browser.

Deleting your network trending data files

Network trending has the possibility to produce large amounts of data that it stores on your hard drive. If your trending files are large, you may want to implement a management strategy so that you have the information that you need for as long as you need it, but that you delete information you no longer need.

By default the trending files are kept for each trending instance in C:\Program Files\Observer\NetworkTrending. You can delete them using Windows Explorer. You can also change where the files are stored by choosing Options > Observer General Options > Folders. Additionally, Observer automatically can delete old trending data for you when you set the option in Trending/Analysis > Network Trending > Settings > General.

If you are using Observer Reporting Server (ORS), you can safely delete the trending files after the data has been transferred to ORS, which typically happens on a scheduled basis every 10 minutes. If you are not using ORS, then delete the trending files only if you are certain you no longer need the data.
Configuring your network trending settings

Network trending can be configured to monitor only the kinds of statistics you want to store, thereby limiting resource consumption to the information that interests you.

If you want the ability to view web reports, Network Trending must be configured using the steps in this section. Then, Network Trending must be running/collecting data. For more details about reports, see Administering Observer reports on page 122.

There are two high-level tasks you must complete for network trending to function. First, you need to configure your network trending settings as described in this section. Network trending settings include trending types, specific servers to monitor (if any), and a schedule (if any). Second, you need to actually collect the network trending data.

To configure your network trending settings, follow these steps. These point to other locations in this section, which provide the steps you need to complete:

1. Choose the trending types you want to follow—see Choosing your network trending types.
2. Schedule the collection of data from those trending types—see Scheduling your network trending data collection.
3. Add specific servers to trend—Adding specific servers to network trending.

Choosing your network trending types

Trending types are categories of network traffic, and they loosely follow the OSI Layer model. To choose which network trending types you want to monitor, follow these steps:

This section represents one of several steps required for configuring your network trending settings. To return to the overall list of steps, see Configuring your network trending settings on page 158.

1. Choose Trending/Analysis > Network Trending from the Observer main menu.
2. Click the Settings button. The Network Trending Settings window appears. Change the Collection Settings.
Figure 52: Configure your network trending settings here

3. If you are using a NetFlow or sFlow instance, click the **SNMP Settings** button to add your SNMP devices.
4. Click OK to save your changes.

<table>
<thead>
<tr>
<th>Trending type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4G LTE</td>
<td>The 4G LTE trending type allows you to monitor 4G LTE traffic information, including seeing end-user devices, applications, handovers, any errors or failures, and the hardware that serves these connections.</td>
</tr>
<tr>
<td>Application Transaction Analysis</td>
<td>Application Transaction Analysis (ATA) is a feature of the Network Trending tool. Using Layers 5-7 of the OSI Model, ATA allows you to monitor response time, error, request and response trends for certain applications.</td>
</tr>
<tr>
<td>Application Performance Analysis</td>
<td>Application Performance Analysis (APA) is a feature of the Network Trending tool. Analyzing Layer 4 of the OSI Model, APA allows you to monitor response time trends for any server or application with a known TCP port.</td>
</tr>
<tr>
<td>IP Trending</td>
<td>The IP Trending trending type does not monitor data unless one or more sub-types are enabled. These include Internet Patrol, IP Pairs, and Protocols by IP Address. Overall, this trending type is very important for long-term monitoring of IP-to-IP connections.</td>
</tr>
<tr>
<td>IPTV</td>
<td>The IPTV trending type allows you monitor multicast issues on your network specifically related to video.</td>
</tr>
<tr>
<td>Trending type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Microburst</td>
<td>The Microburst trending type allows you to monitor for microbursts on your network just like you can from the GigaStor Control Panel, except that trending provides a couple of differences from the packet capture analysis for microbursts done in the GigaStor Control Panel. First, packet capture does not need to be running for Microburst trending to see any microbursts. Second, Microburst trending can also be pushed to Observer Reporting Server and aggregated with Microburst trending information from other probes in your network so that you have a fuller picture of where and when microbursts are occurring.</td>
</tr>
<tr>
<td>Trading Multicast</td>
<td>The Trading Multicast trending type allows you to monitor multicast issues on your network specifically related to stock exchanges. The streams can track UDP sequence numbers, multiple protocol data units (PDUs) within a UDP packet, and stream type or ID. There are several trading streams available by default, but you must import their definitions. Default stream definitions include: Bats—BATS Global Markets CME—Chicago Mercantile Exchange Edge—Enhanced Data Rates for GSM Solutions FTEN—FTEN Generic FIX-FAST—Financial Information eXchange and FIX Adapted for Streaming JSE—Johannesburg Stock Exchange LSE—London Stock Exchange MoldUDP 64—Mold UDP 64 SIAC—Securities Industry Automation Corporation, used by New York Stock Exchange and American Stock Exchange.</td>
</tr>
<tr>
<td>MAC Layer</td>
<td>The MAC Layer trending type does not monitor data unless one or more sub-types are enabled.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN trending type must be enabled if you want long-term monitoring of VLAN data.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Replace network interface names with newly discovered names—Network names for devices can change. Select this option if you want Observer to replace any network interface names with any new name it finds if the name has changed.</td>
</tr>
<tr>
<td>Trending type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>IP Address</strong>—The IP address of the NetFlow or sFlow agent.</td>
</tr>
<tr>
<td></td>
<td><strong>Timeout</strong>—Sets how long Observershould try to contact the agent.</td>
</tr>
<tr>
<td></td>
<td><strong>Retries</strong>—Sets how many times Observershould try to contact the agent.</td>
</tr>
<tr>
<td></td>
<td><strong>SNMP version</strong>—Tells Observer what version of SNMP runs on the agent. Observersupports SNMPv1, SNMPv2, and SNMPv3. SNMPv2 includes a superset of the SNMPv1 features. SNMPv3 adds security and encryption to SNMPv2, while remaining backward compatible with SNMPv1 and SNMPv3. Some SNMP devices do not support SNMPv2 and SNMPv3. If in doubt, leave this setting at the default, SNMPv1.</td>
</tr>
<tr>
<td></td>
<td><strong>Security user name</strong>—User name by which Observer will access the agent.</td>
</tr>
<tr>
<td></td>
<td><strong>Context engine ID</strong>—The context engine ID uniquely identifies the SNMP entity; check the HEX box if you wish to enter the string as a hexadecimal entry (for example, 80 FF 00).</td>
</tr>
<tr>
<td></td>
<td><strong>Community string</strong>—This is typically public. By convention, SNMP uses the community name and management station IP address the same way login name and password are used in a telnet (terminal) session.</td>
</tr>
<tr>
<td></td>
<td><strong>SNMPv3 Security</strong>—Pick or provide the security settings to access your SNMPv3 agent. If necessary, see the administrator of the device for the security details.</td>
</tr>
<tr>
<td>VoIP and Videoconferencing</td>
<td>The VoIP and Videoconferencing trending type does not monitor data unless one or more sub-types are enabled. Overall, this trending type is essential for long-term monitoring of VoIP connections.</td>
</tr>
<tr>
<td>IPFIX/NetFlow Data Sources</td>
<td>This screen allows you to add IPFIX and NetFlow Data Sources so that Observer can create trending data for those devices. Click the Add button to add a NetFlow device. Provide the flow agent information:</td>
</tr>
<tr>
<td></td>
<td><strong>Name</strong>—A descriptive name for the IPFIX/NetFlow data source. We recommend including the word &quot;ingress&quot; or &quot;egress&quot; in the name to easily track which direction is being monitored.</td>
</tr>
<tr>
<td></td>
<td><strong>Source IP address</strong>—The source IP address of the IPFIX/NetFlow agent.</td>
</tr>
<tr>
<td></td>
<td><strong>Source ID</strong>—If a source ID is needed, provide it here. If a source ID is required but you do not know the ID, you can leave it to &quot;0&quot; to accept any source ID.</td>
</tr>
<tr>
<td>Trending type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Destination IP address</strong></td>
<td>The destination IP address of the IPFIX/NetFlow agent.</td>
</tr>
<tr>
<td><strong>Destination port</strong></td>
<td>Port 9996 is the default destination port. Change the port if necessary.</td>
</tr>
<tr>
<td><strong>SNMP Settings</strong></td>
<td>Provide your SNMP settings by clicking this button.</td>
</tr>
<tr>
<td><strong>Collect Data by</strong></td>
<td>Choose between Interface Index or Autonomous System. If you are unsure which is correct for your configuration, try Interface Index first.</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td><em>Ingress or Egress.</em> If Ingress is selected, traffic originating from outside the network that is destined for inside the network is monitored. If Egress is selected, traffic that begins inside the network and is destined outside of the network is monitored.</td>
</tr>
<tr>
<td><strong>Sampling divider</strong></td>
<td>The <em>sampling divider</em> means every Nth packet is used for statistical analysis where N is the value in the field. Due to the large number of packets on most networks, the default value of 10 is appropriate in many, but not all, cases. Setting the value higher or lower may also be appropriate. Setting the value to 1 means that every packet contributes to statistical sampling, but may negatively affect performance. For more information about the sampling divider, see More about the sampling divider on page 156.</td>
</tr>
<tr>
<td><strong>Statistics Collection Interval</strong></td>
<td>The <em>collection interval</em> defines the length of time during which statistics are collected before they are summarized and written to disk. It also defines the granularity of web reports. For example, a collection interval of 60 minutes means web reports are never show statistics in less than 60 minute intervals. At the end of each interval, the statistics are reset to zero before the next interval starts. On Network Trending, you can view statistics for counts, packets, bytes, and more for each trending type. A status bar shows what percent of the collection interval is complete. When choosing a short collection interval, beware that very large trending files may result because of the extensive amount of statistics that are collected.</td>
</tr>
<tr>
<td><strong>Delete oldest trending data...</strong></td>
<td>When selected, this option automatically deletes any trending data older than the specified time on a first in, first out basis. That is, the oldest data will always be deleted while keeping the newest data. For more information, see Deleting your network trending data files on page 157.</td>
</tr>
</tbody>
</table>
### Trending type

<table>
<thead>
<tr>
<th>Trending type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use current filter</td>
<td>When selected, any filters that you applied to your probe instance are also applied to your network trending statistics.</td>
</tr>
</tbody>
</table>

You configured the Network Trending tool to monitor data from the trending types you enabled. This data does not appear until you actually start monitoring it. Continue to the next step of configuring your network trending settings: Scheduling your network trending data collection on page 163.

#### Scheduling your network trending data collection

You can configure Observer to run network trending data collection continuously or at certain days and times. To do this, complete the following steps:

This section represents one of several steps required for configuring your network trending settings. To return to the overall list of steps, see Configuring your network trending settings on page 158.

1. Choose Trending/Analysis > Network Trending from the Observer main menu.
2. Click the Settings button. The Network Trending Settings window appears.
3. Ensure the General group tab is selected, and click the Schedule tab.
4. Select a scheduling type for network trending data collection.
5. Click OK to save your changes.

The trending types you enable continue to be collected according to schedule. You have configured your network trending settings and should continue on to Adding specific servers to network trending on page 163.

#### Adding specific servers to network trending

When you add specific servers to the Network Trending tool, you are adding server applications that Application Transaction Analysis recognizes. See Table 27 on page 153 for a complete list of applications you can add; you cannot add servers—using the method described in this section—that do not use an application appearing in Table 27 on page 153.

This section represents one of several steps required for configuring your network trending settings. To return to the overall list of steps, see Configuring your network trending settings on page 158.

More information about Observer's address book can be found at Building and saving an address book on page 36.

If you have already created the server definition on a different Observer analyzer, you can import it here. See Importing or exporting a server profile on page 155.

1. Choose Trending/Analysis > Network Trending from the Observer main menu.
2. Click the Settings button. The Network Trending Settings window appears. Repeat step 5 through step 14 to add another server.
3. Click OK to save your changes.

You successfully added a server to the Network Trending tool. Each added server is monitored for response time and other metrics, so, over time, you can see long-term trends in these areas.

#### Enabling NetLive trending collection

NetLive trending is specific to Observer Reporting Server (ORS)—a separate application—and focuses on reports. NetLive reports are similar to Network Trending reports except that each is a scrolling, previous-hour
scope report of trending data that is updated every 20 seconds. Therefore, unlike a trending report, NetLive only sees the past one hour and the report is always scrolling. If you need to see something older than one hour, you must use a trending report.

To enable NetLive trending data collection, follow these steps:

NetLive trending data and the reports the data produces are only usable in Observer Reporting Server (ORS). Observer does not make ad hoc use of this data.

1. Choose Trending/Analysis > Network Trending from the Observer main menu.
2. Click the Settings button. The Network Trending Settings window appears.

Figure 53: Configure your network trending settings here

3. Ensure the General tab is selected.
4. In the lowermost portion of the window, enable NetLive collection for any or all trending types.
5. Click OK to save your changes.

You enabled NetLive collection via the Network Trending Settings window. Observer collects this information to be passed to Observer Reporting Server for NetLive reports.

Related Topics
- What is Application Transaction Analysis? on page 152
- Choosing your network trending types on page 158
- Viewing network trending data on page 157
- How to configure Application Performance Analysis on page 147
- What is Application Performance Analysis? on page 149
- Choosing your network trending types on page 158
- Viewing network trending data on page 157
- Configuring your network trending settings on page 158
Network Trending on page 146
Collecting network trending data on page 156
Choosing your network trending types on page 158
Scheduling your network trending data collection on page 163
Adding specific servers to network trending on page 163
What is Application Transaction Analysis? on page 152
What is Application Performance Analysis? on page 149
Searching for microbursts on page 313
Collecting VoIP or video conferencing trending data on page 166
How to configure Application Performance Analysis on page 147
Collecting VoIP or video conferencing trending data

Prerequisite: Observer Expert or Observer Suite

By default, VoIP data is not collected by Observer’s network trending tool. Instead, you must manually add it to the list of data streams that network trending collects. This section describes how to enable the collection of VoIP data.

Because VoIP features and functionalities are spread throughout the Observer software, it became necessary to consolidate its help material, and the result is this section. The VoIP section describes the use of VoIP-related features in one central location.

You can learn more about Observer’s network trending tool by seeing Network Trending on page 146—a wealth of information is provided there should you need it.

Note: Despite enabling the collection of VoIP data in Observer, VoIP data streams can only be parsed by Observer if it (the analyzer) has visibility of RTP or RTCP packets. Usually, this visibility is regulated by the VoIP system itself; please refer to your VoIP system documentation for more details.

To enable VoIP data collection in network trending—so Observer collects VoIP data—complete the following steps:

2. Click the Settings button. The Network Trending Settings window appears.
3. Enable the VoIP Trending data collection type.
4. Click OK to confirm and save your changes.

You successfully configured network trending to collect VoIP data. You can further configure your VoIP collection settings by seeing Configuring network trending settings for VoIP or video conferencing on page 170.

After completing this task:
Alternatively, you can start the actual collection process by following the instructions at Collecting network trending data on page 156.

**Importing and exporting VoIP or video conferencing settings**

Settings for VoIP can be imported or exported into the Network Trending tool. Doing either is very useful depending on what you are trying to accomplish. For example, if you want to backup your settings or share your VoIP settings with other Observer installations, you should export your VoIP settings.

To import and/or export your VoIP settings, complete the following steps:
1. Choose **Trending/Analysis > Network Trending**. The Network Trending tool opens.
2. Click the Tools button.
3. Click Import or Export Settings. A file dialog appears, which allows you to complete the process.

**Analyzing VoIP or video conferencing traffic**

Analyzing VoIP traffic follows the same rules and behaviors as when analyzing any packet capture; you can analyze the packets in either real-time or post-capture modes. Real-time mode is simply analyzing packets as
they arrive (i.e. the packet capture is currently running), while post-capture is analyzing packets from inside a saved packet capture file at a later time. This section describes both real-time and post-capture VoIP analysis.

You cannot create a pre-filter that filters for a specific phone number. However, you can select “Find in VoIP ID stream” from a right-click search through the VoIP Events / Calls tab based on a phone number. After you find the conversation in question, right-click it and select the Fast Post Filter option to filter out the particular VoIP call.

You can learn more about decoding/analyzing network traffic by seeing Decoding network traffic on page 77—a wealth of information is provided there should you need it.

To analyze VoIP traffic, begin by starting a packet capture or loading a saved capture file. If necessary, see the instructions for doing so at Capturing network traffic on page 59.

After you have started a packet capture or loaded a capture file, complete the following steps:

1. Choose **Capture > Packet Capture**.
2. Click the Decode button.
3. Ensure the Expert Analysis tab is selected.
4. Click the VoIP Events group tab.
5. (Optional) Click the VoIP Settings button to view or change VoIP-specific settings.

   These settings are shared with the settings described in Configuring network trending settings for VoIP or video conferencing on page 170.

6. (Optional) Click the Expert Threshold button to view or change settings that determine VoIP-specific decode settings.

From the VoIP Events group tab, you can perform meaningful decoding of VoIP packets, including the ability to see call statistics as they arrive.

The Table 28 on page 168 lists the abbreviations used in the VoIP Events tab for various packet types.

**Table 28: VoIP Events tab abbreviations**

<table>
<thead>
<tr>
<th>A</th>
<th>Audio</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Control</td>
</tr>
<tr>
<td>D</td>
<td>Data codec (non-audio or video data)</td>
</tr>
<tr>
<td>Q</td>
<td>Quality for RTP Packets (always RTCP)</td>
</tr>
<tr>
<td>V</td>
<td>Video</td>
</tr>
</tbody>
</table>

**How to extract VoIP and video calls from your GigaStor**

VoIP and videoconferencing calls can be extracted from a GigaStor if you know the approximate time the events occurred.

Prerequisite(s):
You must understand how to select a time frame from your GigaStor. See ../observer/voip_and_video_sip_extraction.html.

**Note:** This process is only compatible with SIP data.

Locating and extracting SIP-based voice and video data from your GigaStor is a straightforward task. All of the SIP setup and teardown packets are extracted along with any payload, such as audio and video, to ensure you retrieve complete sessions. This includes all person-to-person audio calls and videoconferencing as well as conference calls and conference video where multiple endpoints are present. And *endpoint* could be a person holding a handset, wearing a headset, or a line that is open for hold music or for recording.

To extract VoIP and videoconferencing calls from your GigaStor:

1. Select a time frame you want to analyze.
2. Click the Update Reports button to get the latest data from the time frame selected.
   
   This step is unnecessary if **Auto-update GigaStor chart on statistics tab or selection change** is enabled in the GigaStor settings. See ../observer/non_gigastor_specific_settings.html.

3. Click the Analyze button.
4. In the **Analysis Options** section, choose VoIP and Videoconferencing calls by SIP tag. Click the **Settings** option and choose your call search criteria.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A --&gt; (ANY)</td>
<td>Extract call(s) where pattern A is in the SIP “From” field.</td>
</tr>
<tr>
<td>A &lt;-- (ANY)</td>
<td>Extract call(s) where pattern A is in the SIP “To” field.</td>
</tr>
<tr>
<td>A &lt;-&gt; (ANY)</td>
<td>Extract call(s) where pattern A is in the SIP “From” or “To” field.</td>
</tr>
<tr>
<td>A &lt;-&gt; B</td>
<td>Extract call(s) where pattern A and pattern B is in either the SIP “From” or “To” field.</td>
</tr>
<tr>
<td>A --&gt; B</td>
<td>Extract call(s) with pattern A in the SIP “From” field and pattern B is in a SIP “To” field.</td>
</tr>
<tr>
<td>Call-ID</td>
<td>Extract call(s) with the specified pattern in the SIP “Call-ID” field.</td>
</tr>
</tbody>
</table>

5. (Optional) Enable one or more search pattern modifiers:

   - Use regular expression(s)—Perl 5 regular expressions. For details and examples, see http://www.regular-expressions.info/tutorial.html
   - Match case—case sensitive search

6. Type a string for the GigaStor to search for in the Call-ID Pattern.
7. Choose one of the result options:

   - Stop searching when one matching call is found. This provides you the results more quickly, but the tradeoff is that if the endpoints identified by search criteria had multiple separate calls within the timeframe selected, only the first call is extracted and any subsequent calls are excluded.
   - Search for all matching calls within the GigaStor analysis time range (up to the filtering limit).

8. Click OK to save your settings.
9. Choose your analysis type. The options are described in ../observer/analyzing_data_by_combining_gigastor_control_panel_and_observer_filters.html.

   # Expert analysis and decode
   # Decode without expert analysis
   # Third party decoder

If your search pattern found results, the results are displayed in a new tab and can be further analyzed.

**Configuring network trending settings for VoIP or video conferencing**

**Prerequisite:** Observer Expert or Observer Suite

Just as network trending has a menu for general settings, it also has a menu specifically for VoIP settings. This section describes how to access the VoIP settings menu and guides you through its most noteworthy settings. We recommend visiting these settings only after you are comfortable using the network trending tool.

To configure network trending settings for VoIP, complete the following steps:

1. Choose **Trending/Analysis > Network Trending**. The Network Trending tool opens.
2. Click the Settings button. The Network Trending Settings window appears.
3. Click the VoIP and Videoconferencing group tab.

**Figure 56: The VoIP settings menu**

You successfully accessed the VoIP settings menu. Like most other menus in Observer, this menu consists of multiple tabs. Each tab brings you to a specific subset of settings, and they are described in the proceeding sections.

After completing this task:

Learn more about each tab’s settings from the following related topics:
General tab

The General tab allows you to specify how Observer interacts with VoIP packets, such as which packets identify a new call and how jitter is displayed. See Table 29 on page 171 for a list of noteworthy settings.

Table 29: VoIP General tab

<table>
<thead>
<tr>
<th>Setting(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying new calls</td>
<td>These settings tell Observer which VoIP packets are recognized as a new phone call. If you ever have trouble seeing VoIP calls in network trending, try experimenting with these settings.</td>
</tr>
<tr>
<td>Allow multiple concurrent calls on an IP pair</td>
<td>Some VoIP phones allow multiple, concurrent calls between the same IP addresses. By default (setting disabled), Observer stops looking for calls once it finds setup information exchanged between a pair of IP addresses until that call is closed. Enabling this setting causes Observer to further process the packets to look for multiple call streams, which can take more time but allows for more accurate call tracking.</td>
</tr>
<tr>
<td>Track SIP by IP pair and Call-ID</td>
<td>When selected, Observer identifies a VoIP call based on an IP address/port pair combination along with a Call ID. The call ID is generated by the telephone initiating the conversation. If unchecked, only the IP address/port pair is used. Disabling this option is not recommended.</td>
</tr>
</tbody>
</table>

MOS tab

The MOS tab allows you to specify which sources of delay are used in MOS score calculations, and it allows you to configure your E-Model parameters if its defaults do not suffice. This tab becomes especially important for tracking the performance and clarity of VoIP calls. See Table 30 on page 171 for a list of noteworthy settings.

If you are using a VoIP codec that Observer does not recognize by default, change the value of the E-Model parameter impairment for unrecognized codecs to the appropriate value shown in Table 31 on page 172.

The E-model based on conditions, equipment, and expectations at your site. Some of the values (Send and Receive Loudness Ratings, for example) are functions of your phone specifications. Others (Room Noise levels, for example), are functions of ambient conditions at your site. Typically, the default values should work fine. To fine-tune the E-model to exactly match the conditions at any particular site is an involved process that requires test equipment and a thorough understanding of the E-model. See the ITU G.107 specification for a more detailed discussion of the E-model.

The default settings in the MOS tab do not need to be changed unless there is reason for doing so—the defaults work well for many VoIP networks!

Table 30: MOS settings

<table>
<thead>
<tr>
<th>Setting(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOS score network delay</td>
<td>These settings tell Observer which source of delay should be used in MOS calculations; the first found source of delay is used, and the items at the top of the list take precedence over lower items.</td>
</tr>
<tr>
<td>E-Model parameters</td>
<td>These settings allow you to customize your E-Model parameters. The E-Model parameters have a direct effect on how your MOS score is determined. We</td>
</tr>
<tr>
<td>Setting(s)</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>recommend leaving these at their default values until you have reason to change them. If you are using a VoIP codec that Observer does not recognize by default, change the value of the E-Model parameter <em>impairment for unrecognized codecs</em> to the appropriate value shown in Table 31 on page 172.</td>
</tr>
</tbody>
</table>

**Defaults button**

Clicking the Defaults button will restore the E Model parameters to their original values. This button does not affect the MOS score network delay settings.

### Table 31: Codecs

<table>
<thead>
<tr>
<th>If you use this codec</th>
<th>Use this value…</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711</td>
<td>7</td>
</tr>
<tr>
<td>1016 8K</td>
<td>17</td>
</tr>
<tr>
<td>G.721</td>
<td>7</td>
</tr>
<tr>
<td>G.723</td>
<td>17</td>
</tr>
<tr>
<td>DVI4 8K</td>
<td>17</td>
</tr>
<tr>
<td>DVI4 16K</td>
<td>17</td>
</tr>
<tr>
<td>G.722</td>
<td>17</td>
</tr>
<tr>
<td>16 Bit Linear (2 Channel)</td>
<td>17</td>
</tr>
<tr>
<td>16 Bit Linear (1 Channel)</td>
<td>17</td>
</tr>
<tr>
<td>QCELP 8K</td>
<td>21</td>
</tr>
<tr>
<td>MPA 90K</td>
<td>17</td>
</tr>
<tr>
<td>G.728 8K</td>
<td>13</td>
</tr>
<tr>
<td>DVI4 11K</td>
<td>17</td>
</tr>
<tr>
<td>DVI4 22K</td>
<td>17</td>
</tr>
<tr>
<td>G.729</td>
<td>15</td>
</tr>
<tr>
<td>G.711 (a-Law) 64K</td>
<td>7</td>
</tr>
<tr>
<td>G.711 (a-Law) 56K</td>
<td>17</td>
</tr>
<tr>
<td>G.711 (u-Law) 64K</td>
<td>7</td>
</tr>
<tr>
<td>G.711 (u-Law) 56K</td>
<td>17</td>
</tr>
<tr>
<td>G.722 56K</td>
<td>17</td>
</tr>
<tr>
<td>G.722 48K</td>
<td>17</td>
</tr>
<tr>
<td>G.722-1</td>
<td>17</td>
</tr>
<tr>
<td>G.722-2</td>
<td>17</td>
</tr>
<tr>
<td>G.723-1</td>
<td>17</td>
</tr>
</tbody>
</table>
## Device IP Addresses tab

The Device IP Addresses tab allows you to add VoIP devices to network trending via their IP addresses. After you add the IP addresses of any VoIP devices on your network, each will be recognized and “trended” by the network trending tool now and in the future. See Table 32 on page 173 for a list of noteworthy settings.

### Table 32: Device IP Address options

<table>
<thead>
<tr>
<th>If you use this codec</th>
<th>Use this value...</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.723-1 Annex C</td>
<td>17</td>
</tr>
<tr>
<td>G.726-16</td>
<td>40</td>
</tr>
<tr>
<td>G.726-24</td>
<td>25</td>
</tr>
<tr>
<td>G.726-32</td>
<td>7</td>
</tr>
<tr>
<td>G.726-40</td>
<td>2</td>
</tr>
<tr>
<td>G.728</td>
<td>7</td>
</tr>
<tr>
<td>G.729</td>
<td>15</td>
</tr>
<tr>
<td>G.729 Annex A</td>
<td>20</td>
</tr>
<tr>
<td>G.729 Annex B</td>
<td>20</td>
</tr>
<tr>
<td>G.729 Annex A &amp; B</td>
<td>20</td>
</tr>
<tr>
<td>G.729 Extensions</td>
<td>20</td>
</tr>
<tr>
<td>IS11172</td>
<td>11</td>
</tr>
<tr>
<td>IS13818</td>
<td>11</td>
</tr>
<tr>
<td>GSM Full Rate</td>
<td>20</td>
</tr>
<tr>
<td>GSM Half Rate</td>
<td>23</td>
</tr>
<tr>
<td>BV 16K</td>
<td>17</td>
</tr>
<tr>
<td>BV 32K</td>
<td>17</td>
</tr>
<tr>
<td>VBD</td>
<td>17</td>
</tr>
<tr>
<td>ILBC</td>
<td>17</td>
</tr>
<tr>
<td>Speex</td>
<td>17</td>
</tr>
<tr>
<td>IMA ADPCM</td>
<td>17</td>
</tr>
<tr>
<td>LPC10</td>
<td>17</td>
</tr>
<tr>
<td>Telephony Event</td>
<td>17</td>
</tr>
<tr>
<td>Audio Tone</td>
<td>17</td>
</tr>
<tr>
<td>G.711 (A-law) with PLP</td>
<td>17</td>
</tr>
<tr>
<td>G.711 (U-law) with PLP</td>
<td>17</td>
</tr>
</tbody>
</table>
Setting(s) | Description
---|---
VoIP device list | A list of all your configured VoIP devices. After you populate the list, you can simply use the Device IP Addresses tab as an organizational tool for VoIP devices.
Add button | Clicking the Add button allows you to add VoIP devices to the list. See the list of device types in Table 33 on page 174.

If you choose to add a VoIP device, you are asked to tell Observer which type of VoIP device is being added. The types are described in Table 33 on page 174.

**Table 33: VoIP device types**

<table>
<thead>
<tr>
<th>VoIP device type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration/Registration Server IP</td>
<td>A server which performs administration/registration operations but does not act as a call server. An example would be a SIP registration server which handles only the SIP REGISTER message and not the INVITE messages. When configured as this type, an IP may be listed as a server for admin calls but not for normal calls.</td>
</tr>
<tr>
<td>Control Processor IP</td>
<td>Avaya’s proprietary server for managing call setup and tear down.</td>
</tr>
<tr>
<td>Media Processor IP</td>
<td>Avaya’s proprietary server for managing actual voice data.</td>
</tr>
<tr>
<td>Non-server IP</td>
<td>An IP which should not be interpreted as a server on any call. This type provides a mechanism to override our normal inference of servers based upon traffic between IPs. In other words, it should generally only be used if we are incorrectly presenting a non-server IP as a server.</td>
</tr>
<tr>
<td>Outside IP</td>
<td>Link to PSTN or other outside network.</td>
</tr>
<tr>
<td>Server IP</td>
<td>Generic VoIP Server such as Cisco.</td>
</tr>
</tbody>
</table>

**Caller ID Determination tab**

The Caller ID Determination tab allows you to tell Observer which source of information creates the caller ID text displayed on calls. Connection and devices IDs, too, are determined from settings in this tab. See Table 34 on page 174 for a list of noteworthy settings.

**Table 34: Caller ID Determination tab**

<table>
<thead>
<tr>
<th>Setting(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify call IDs</td>
<td>These settings tell Observer which source of information creates the caller ID text. The first found source of information is used, and the items at the top of the list take precedence over lower items.</td>
</tr>
<tr>
<td>Specify device IDs and connection IDs</td>
<td>These settings tell Observer which source of information creates the device ID shown in VoIP network trending. The first found source of information is used, and the items at the top of the list take precedence over lower items.</td>
</tr>
</tbody>
</table>

**IP Range Filters tab**

The IP Range Filters tab allows you to specify which IP addresses, ranges, or subnets are either included or excluded from VoIP network trending. See Table 35 on page 175 for a list of noteworthy settings.
Table 35: IP Range Filters tab

<table>
<thead>
<tr>
<th>Setting(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examine/exclude</td>
<td>Allows you to change Observer’s behavior toward the IP ranges you add to the list. Only one behavior can be used.</td>
</tr>
<tr>
<td>Add button</td>
<td>Clicking the Add button allows you to add an IP address, range, or subnet to the list. Each entry in the list is subject to the examine/exclude behavior selected in this tab.</td>
</tr>
</tbody>
</table>

**Enabling VoIP alarms**

Alarms are a powerful and often overlooked feature of Observer. Using alarms, you can trigger pre-defined actions to occur when network conditions are met, making network management simpler and more predictable. Best of all, alarms allow you to proactively manage your network no matter where you are physically located.

You can learn more about Observer alarms by seeing Configuring and using alarms on page 115—a wealth of information is provided there should you need it.

To enable alarms for VoIP, complete the following steps:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.

![Figure 57: Enable VoIP alarms here](image)

4. In the alarm list, click VoIP Alarms to expand the list of VoIP-specific alarms.
5. Enable one or more VoIP alarms by checking the appropriate boxes. Likewise, you can disable any VoIP alarm by clearing them.

   Until you customize the alarms, Observer uses the built-in, default triggers and actions for each. If necessary, see Customizing triggers and actions on page 118 and Creating filter-based alarms on page 117.

6. Click OK to save your changes.
You successfully enabled one or more VoIP alarms, and you can repeat this process at any time.

**VoIP Top 10 best practices**

Use this valuable list of the best practices when implementing or troubleshooting VoIP. Keeping these steps in mind will help you get the most from your VoIP network.

1. **Understand and measure call quality components**
   
   There are a variety of metrics you can use to assess VoIP call quality, including jitter, MOS, R-Factor, gap density, burst density, Quality of Service prioritization, and compression techniques. Ensure you are accurately analyzing VoIP communication by learning how to measure these attributes.

2. **Implement Quality of Service prioritization**
   
   Incorrectly set QoS precedence for VoIP traffic leads to delays in packet delivery and reduced call quality.

3. **Conduct site surveys**
   
   The more you know about your network, the better prepared you are to properly integrate VoIP. Conduct a site survey to review current WAN bandwidth levels, traffic flows, and existing switches for bottlenecks and choke points. Then, identify or determine specific needs through testing and modeling.

4. **Deploy analysis tools strategically for maximum visibility**
   
   Placing network analysis consoles and probes on your network requires a clear understanding of VoIP traffic patterns. Are you concerned with monitoring VoIP traffic locally, over WAN links, both? Depending on your objectives, place your analysis tools to ensure optimal visibility of VoIP communications.

5. **Implement VLANs to isolate and monitor VoIP issues**
   
   Organize your VoIP traffic by VLAN user groups. This practice will greatly simplify problem resolution.

6. **Monitor rollouts to ensure a positive user experience**
   
   Determine whether users are receiving a positive experience by reviewing cumulative VoIP metrics, codecs, and other network performance variables during VoIP deployment. By evaluating VLAN setups and overall link utilization, you can judge overall network performance and quickly make adjustments during implementation.
7. **Compare jitter to overall network bandwidth utilization to understand response time**

When jitter becomes a problem, look at the big picture. A correlation between jitter and bandwidth usage means the problem is overall network usage. If there is no direct correlation, excessive jitter might be caused by isolated network factors that require further investigation.

8. **Set up Observer to proactively monitor VoIP activity**

Utilize monitoring and notification tools to speed problem resolution. Determine “normal” or “acceptable” levels of activity for your network and its users. Then set up thresholds within your analyzer to alert you when thresholds are broken or in danger.

9. **Automate problem resolution**

Expert Analysis functionality eliminates unnecessary trial and error when troubleshooting VoIP issues by automating problem resolution. Utilize Expert Analysis on VoIP communication to quickly pinpoint the source of common VoIP problems.

10. **Baseline network traffic**

For comprehensive understanding of VoIP traffic, capture and store long-term network data. Only with critical trending data can you accurately perform baselining activities. Baselining validates VoIP performance, helps future capacity planning efforts, and provides long-term understanding of VoIP health.

**Network Jitter and Delay**

Real-time voice communications are sensitive to delay and variation in packet arrival times. Codecs require a steady, dependable stream of packets to provide reasonable playback quality. Packets arriving too early, too late, or out of sequence result in jerky, jumbled playback. This phenomenon is called jitter.

Because no network can guarantee a perfectly steady stream of packets under real-world conditions, VoIP phones use jitter buffers to smooth out the kinks. A jitter buffer is simply a First-In, First Out (FIFO) memory cache that collects the packets as they arrive, forwarding them to the codec evenly spaced and in proper sequence for accurate playback.

Increasing jitter buffer size can help, but only to a point. While a jitter buffer can successfully mask mild delay and jitter problems, severe jitter can overwhelm the jitter buffer, which results in packet loss (see below). Increasing the size of the jitter buffer can help, but only to a point: A jitter buffer that increases overall round-trip delay to 300 ms will make normal conversation difficult.
VoIP packets can arrive at a receiving phone out of sequence, late, or not at all. IP phones use a jitter buffer to reconstruct the packet stream at the receiving end, duplicating missing packets or filling in with white comfort noise when necessary.

While a jitter buffer can successfully mask mild delay and jitter problems, severe jitter can overwhelm the jitter buffer, which results in packet loss (see below). Increasing the size of the jitter buffer can help, but only to a point: A jitter buffer that increases overall round-trip delay to 300 ms will make normal conversation difficult.

**Packet Loss**

Packet loss can be the result of the jitter buffer being overwhelmed.

Other reasons include landline media failure and poor wireless signal quality. The latter can be a big problem with VoFi (Voice over WiFi) service. Regardless of the source, VoIP phones and gateways attempt to conceal this type of signal degradation by duplicating packets to fill in the missing data. As with jitter, these techniques can maintain voice quality only to a point.

Packet loss on data networks has long been characterized as a “bursty” phenomenon, which is another way of saying “it never rains, it pours.” Networks tend to either sporadically drop single packets (these periods are called “gaps” in packet loss), or large numbers of contiguous packets in a “burst.” Packet loss concealment techniques typically have no problem handling packet loss during gap periods; it is the sustained bursts you must watch out for.

**Managing VoIP Quality**

You can manage only what you can measure. Managing a VoIP deployment therefore requires some hard numbers beyond subjective user assessments of quality (although these are obviously important as well).

Beyond monitoring the network parameters discussed in this paper, having an overall quality score such as a Mean Opinion Score (MOS) or R-factor score can also be a useful VoIP network health index.

VoIP monitoring tools calculate the MOS and R-factor scores using a formula known as the E-model. Using the statistics it has collected from the network, the analyzer calculates how much the various impairment factors (such as codec compression, jitter, delay, and packet loss) would affect the typical user’s perception of call quality.

MOS and R-factor are used to gauge user satisfaction with call quality. MOS levels under 3.5 and R-factor below 80 mean trouble.
VolP terminology

This section describes common VolP terminology. If you are new to VolP networking or just need more information about a certain term, this section may help.

Table 36: VoIP terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-factor and MOS</td>
<td>These are overall quality ratings, based on the E-model, which take into account network conditions, equipment ratings, and other variables to come up with an objective Quality score. The R-factor is a scale from 0-100; MOS ranges from 1 to 5. In both cases, higher readings indicate better quality.</td>
<td>The R-factor is more useful for live, real-time assessment of what users are experiencing. Unavoidable degradation means that 93.2 is the highest reading you will see on an actual VoIP call; scores below 80 typically result in dissatisfied users. The MOS (Mean Opinion Score) measures how a user would assess quality, from 1 (poor) to 5 (excellent). Although it is also useful as a real-time measure of VoIP health, it is especially useful for pre-deployment tests where you compare the MOS scores of call data from both ends of various connections to identify and resolve bottlenecks. Scores of 3.5 or less typically result in dissatisfied users.</td>
</tr>
<tr>
<td>Jitter</td>
<td>Using computer networks to transmit and reproduce sound requires a steady, predictable stream of packets to arrive at the receiving devices. Jitter is the variability in arrival time, too much of which can degrade call quality.</td>
<td>Understanding jitter can help you improve overall call quality by adjusting jitter buffers or providing more bandwidth through QoS prioritization or other mechanisms.</td>
</tr>
<tr>
<td>Bursts and Gaps of packet loss</td>
<td>Packets can get dropped for many reasons on a network, some more serious than others. For example, a temporary spike in bandwidth utilization causing a few packets to get dropped is usually not a problem, as VoIP equipment is designed to fill in the missing data. Following long-standing conventions of telephony</td>
<td>Understanding the density and duration of bursts and gaps can help you quickly respond to (and sometimes prevent) voice degradation on the VoIP network. For example, an extremely high burst density (20% or more) coupled with extended burst duration times (more than a second or two) can suggest problems with hardware either failing or being completely overwhelmed by traffic.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Significance</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Definition</strong></td>
<td><strong>Significance</strong></td>
</tr>
<tr>
<td>periods where packet loss is minimal are called gaps. In contrast, burst periods (i.e., periods when a high percentage of packets are being lost) usually does degrade call quality, and may point to more serious problems. Density refers to the rate of packet loss during bursts and gaps.</td>
<td>Gap densities climbing over time, coupled with low-density, short-duration “burstiness” can mean the VoIP network is attempting to service too many calls given the available bandwidth.</td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>Also called a Type of Service (ToS) or Precedence, the QoS bit is part of the TCP header that certain routers and switches recognize so they can prioritize traffic according to what particular kinds of applications require. VoIP typically requires the highest level of priority.</td>
<td>Incorrectly set QoS can lead to contention of VoIP and other data on a network. Contention can cause VoIP jitter and packet loss, leading to poor voice quality and dissatisfied users.</td>
</tr>
<tr>
<td>Codec</td>
<td>Codec is an abbreviation for Coder/Decoder, referring to the algorithm used to convert the analog voice signal into packets on the network, and back again. Different codecs use different sampling rates to implement different levels of compression. Lower sampling rates can compromise call quality, although sometimes a lower sampling rate can reduce contention and prevent worse degradation. Here are some of the more common codecs and their sampling rates: G.711: 64kbps (no compression) G.729: 8kbps G.723: 6.3kbps, 5.3kbps</td>
<td></td>
</tr>
<tr>
<td>E-Model</td>
<td>The E-Model is based on conditions, equipment, and expectations at your site. Some of the values (Send and Receive Loudness Ratings, for example) are functions of your phone specifications. Others (Room Noise levels, for example), are functions of ambient conditions at your site. To fine-tune the E-model to exactly match the conditions at any particular site is an involved process that requires test equipment and a thorough understanding of the E-model. See the ITU G.107 specification for a more detailed discussion of the E-model. R-Factor and Mean Opinion Scores (MOS) are derived from the E-Model. The E-Model is based on ITU-T Recommendation G.107, and takes into account the many types of network impairments that can affect voice quality. VoIP, unlike some other network applications, is quite sensitive to packet delay and jitter. To prevent network conditions from affecting voice quality, many VoIP deployments use Quality of Service (QoS) prioritization so that VoIP traffic is favored over other less delay-sensitive traffic. Even with QoS, a saturated network can mean poor voice quality, which will be reflected in lower R-factor and Mean Opinion Score (MOS) readings. In most deployments, users will start to complain about quality when MOS scores fall below 3.5 and R-Factor scores fall below 80 or so.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

Decoding network traffic on page 77
Decoding encrypted network traffic on page 80
Introduction to SNMP

Prerequisite: Observer Suite

SNMP Management Console is available in Network Instruments’ Observer Suite, bringing the cross-platform Simple Network Management Protocol (SNMP) standard to the Observer analyzer.

Simple Network Management Protocol (SNMP) is not as simple as its name implies; it is a difficult concept to understand. This section provides a brief overview and description of SNMP, yet it is by no means a comprehensive tutorial. Ultimately, using Observer’s SNMP Management Console becomes easier with a basic understanding of how SNMP works.

Any network administrator, systems consultant, or network programmer will find SNMP Management Console useful. SNMP Management Console and its related utilities are designed to meet the needs of network professionals, ranging from beginner to expert.

SNMP Management Console is most useful for network administrators who want to monitor their LANs and manage SNMP-aware devices from a single location.

Simple Network Management Protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. The SNMP system consists of three parts: SNMP Manager, SNMP Agent, and MIB.

- SNMP manager—uses information in the MIB to perform operations on each object.
- SNMP agent—gathers data from the MIB, which is the repository for information about device parameters and network data. The agent also can send traps, or notifications of certain events, to the manager.
- Management Information Base (MIB)—stores the information about each managed object.

From the perspective of a network manager, network management takes place between two major types of systems: those in control, called managing systems, and those observed and controlled, called managed systems. The most common managing system is called a Network Management System (NMS). Managed systems can include hosts, servers, or network components such as routers or intelligent repeaters.

The exchange of information between managed network devices and a robust NMS is essential for reliable performance of a managed network. Because some devices have a limited ability to run management software, most of the computer processing burden is assumed by the NMS. The NMS runs the network management applications that present management information to network managers and other users.
Instead of defining a large set of commands, SNMP places all operations in a GetRequest, GetNextRequest, GetBulkRequest, and SetRequest format. For example, an SNMP manager can get a value from an SNMP agent or store a value in that SNMP agent. The SNMP manager can be part of a NMS, and the SNMP agent can reside on a networking device such as a router. If SNMP is configured on a router, the SNMP agent can respond to MIB-related queries being sent by the NMS.

Figure 60: SNMP simple diagram

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetRequest</td>
<td>supplies a list of objects and values they are to be set to (SetRequest). The agent returns GetResponse.</td>
</tr>
<tr>
<td>GetNextRequest</td>
<td>retrieves the next instance of information for a particular variable or device.</td>
</tr>
<tr>
<td>GetResponse</td>
<td>informs the management station of the results of the GetRequest or SetRequest by returning an error indication and a list of variable/value bindings.</td>
</tr>
<tr>
<td>GetBulkRequest</td>
<td>similar to GetNextRequest, but fills the GetResponse with up to a maximum repetition number of GetNext interactions.</td>
</tr>
<tr>
<td>SetRequest</td>
<td>alters the value of objects which can be written to the MIB.</td>
</tr>
<tr>
<td>Trap</td>
<td>an unsolicited message sent by an SNMP agent to an SNMP manager indicating that some event has occurred.</td>
</tr>
</tbody>
</table>

With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within the MIB.

In a managed device, specialized low-impact software modules, called agents, access information about the device and make it available to the NMS. Managed devices maintain values for several variables and report those, as required, to the NMS. For example, an agent might report such data as the number of bytes and packets in and out of the device, or the number of broadcast messages sent and received. In the Internet Network Management Framework, each of these variables is referred to as a managed object. A managed object is anything that can be managed, anything that an agent can access and report back to the NMS. All managed objects are contained in the Management Information Base (MIB), a database of the managed objects.

An NMS can control a managed device by sending a message to an agent of that managed device requiring the device to change the value of one or more of its variables. The managed devices can respond to commands such as set or get commands. The set commands are used by the NMS to control the device. The get commands are used by the NMS to monitor the device.

**Enabling SNMP CPU and Memory usage stats on Windows servers**

The performance MIB for Windows XP enables access to CPU and memory statistics via SNMP. This Microsoft-supplied software works in conjunction with Observer’s SNMP request file, and the “NT Server MIBs” MIB file that is included with the Observer Suite.

To install PerfMon SNMP support on your Windows server, you must perform these steps on the Windows system you wish to monitor:

1. Install the Windows SNMP Agent. Please read the Windows help file for the setup information.
2. Extract all the files from the self-extracting zip archive WinNT_2000_XP_PerfMib_Setup.zip into any temporary folder and run Win2000-XP_Setup.bat for Windows.

3. Restart the system.

All performance counters will now be accessible through Observer Suite's SNMP Console.

Configuring Observer Suite for SNMP devices

Included with Observer Suite is a full-function SNMP management console that allows you to poll and configure any device that has an SNMP agent, regardless of make or manufacturer.

To query and manage SNMP devices on your network, you must first define these devices within Observer Suite's SNMP Console. For each SNMP device you wish to monitor with Observer Suite, you must know:

- The IP address of the device
- The SNMP community string for the device (either read or write, but must be write if you want to manage and also monitor the device)
- The version of SNMP supported by the device (if unsure, choose SNMPv1, which every SNMP device supports)
- The make, model, and manufacturer of the device can be helpful as well

1. To set up an SNMP device in Observer Suite, choose Actions > Add SNMP device from the Observer main menu.

2. For the device type, click the button to display a list of request files for various SNMP devices that Network Instruments has included for your convenience. Request files provide a mechanism for filtering complex MIB definitions down to relevant information, delivered in the format you want. If you cannot find a request file that exactly matches your device, you can easily build one yourself using Observer Suite's MIB Editor. Rather than create the whole request file from scratch, you can make a copy of the "standard" request file (conforming to RFC1213), and modify as necessary. Beyond the general settings on the first tab, two other tabs let you set notification and logging options. They are optional.

3. Repeat the Add Device process for every SNMP device on your network you want to monitor and manage. As you add devices, they are displayed in the SNMP Devices Tree on the left side of the Observer main window.

What can Observer’s SNMP console tell me about a problem switch?

After you have narrowed down a problem to a particular switch, Observer Suite lets you easily look up any SNMP-supported statistic or registered value to further diagnose the problem.

1. Click a device in the SNMP device list to expand the tree of available SNMP objects included in the request file for that device.

   You can select a different request file in the Probe or Device Properties dialog, which is available by right-clicking on the SNMP device.

   To add or change charts, tables, and forms within a request file, use Observer Suite's MIB Editor, which is described in Adding triggers based on SNMP chart values on page 192.

2. Click any chart or other request file item in the tree to display data in the agent information window. For example, the supplied request file for a Cisco 2900-3500 XL switch returns the Utilization by Port Per Sec chart.

3. If you have opened multiple charts, use the tabs at the bottom of the agent information window to browse the open request file results.
Long-term trending using the SNMP console

If you want to track any charted SNMP statistic for the long-term, you can easily configure Observer Suite to log the relevant data for later viewing in the Network Trending viewer or as a web report.

1. In the SNMP Devices tree on the left, choose a device and expand it.
2. Expand Charts and then select a chart. That chart appears on the right.
3. From the chart’s Tools menu, select Collect SNMP Trending Data.
4. A dialog asks “Do you want to turn on recording of the SNMP trending data for the chart?” Click Yes. Trending data for that chart will be recorded until you turn recording off by toggling the floppy disk button or closing the chart.

As with other trending reports, SNMP trending reports are web accessible.

6. Click SNMP Trending. Choose a device, and the SNMP Trending Report form is displayed, which lets you select the range of dates, chart type to use, and statistics to include when generating the report.
7. Fill out the form and click the Show Report button. Click the button if you need a more detailed explanation of the form controls.

Resetting SNMP device alarm counters

1. To reset SNMP device alarm counters, do one of the following:

   - To reset SNMP device alarm counters of a currently selected SNMP device, choose Actions > Reset SNMP Device Alarm Counters.
   - To reset SNMP device alarm counters for all SNMP devices, choose Actions > Reset All SNMP Devices Alarm Counters.

About MIBs

A Management Information Base (MIB) is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP).

The unit of data collected is called the SNMP object. For each device, a set of SNMP objects and rules for addressing the objects are defined in a MIB file. MIBs are key to the logical, orderly functioning of SNMP. MIB objects (OIDs) are represented by a tree hierarchy; each object has a unique address based on its position in the tree. The address count begins from the root of the object tree; one number is added to the address with each new branch. The root of the tree is unnamed and splits into three main branches: Consultative Committee for International Telegraph and Telephone (CCITT), International Organization for Standardization (ISO), and joint ISO/CCITT.
These branches and those that fall below each category have short text strings and integers to identify them. Text strings describe object names, while integers allow computer software to create compact, encoded representations of the names.

The object identifier in the Internet MIB hierarchy is the sequence of numeric labels on the nodes along a path from the root to the object. The Internet standard MIB is represented by the object identifier 1.3.6.1.2.1. It also can be expressed as iso.org.dod.internet.mgmt.mib. The format of the MIB is defined as part of the SNMP. (All other MIBs are extensions of this basic management information base.) MIB-I refers to the initial MIB definition; MIB-II refers to the current definition. SNMPv2 includes MIB-II and adds some new objects.

Each MIB has a name, a syntax, and an encoding.

- **Name**—identifies the object
  
  1.3.6.1.2.1.1.1 = the object identifier  
  SYSDESCR = the object descriptor

- **Syntax**—defines the object’s structure (e.g., octet string, integer).

- **Encoding**—an object’s representation using the object’s syntax (e.g., the local IP address for this TCP connection, Read Only, or Mandatory).

Object: TCPConnLocalAddress  
Syntax: Integer  
Definition: The local IP address for this TCP connection  
Access: Read only  
Status: Mandatory

When requested, the SNMP agent transfers an SNMP message across the network in a standard format, as specified by the set of SNMP Request for Comments (RFCs). Related MIB objects often are combined into MIB groups. MIB groups make it easier to manage a large number of MIB objects. Some MIBs, such as the standard MIB-2, contain many MIB groups. Proprietary MIBs usually have only one, or a few, groups.
Introduction to SNMP Management Console

During the last decade, reliance on local and wide area networks has increased steadily. As networks grow larger in size and more complex, so does the importance of effective network management.

While many methods exist for monitoring network activity, one of the most important emerging standards is SNMP. Unlike protocols designed to monitor network traffic, SNMP is a standard for monitoring specific network devices, providing an efficient and highly flexible way to collect and organize the information needed to optimize network performance.

Network Instruments designed SNMP Management Console as a highly functional, easy-to-use feature of Observer Suite to help you take advantage of SNMP's capabilities. SNMP Management Console includes an SNMP management plug-in for Observer, a MIB compiler, and a graphical forms editor/viewer—a complete RFC-compliant implementation of SNMP for the Microsoft Windows 2000/XP platforms.

Whether you're a network administrator, network user, programmer, network application developer, or network product tester, SNMP Management Console delivers features that will help you get the most from SNMP and your network.

SNMP Management Console offers:

- Greater network control—in addition to helping you collect network management information, SNMP Management Console can set or configure writable objects. You may, for example, switch modes on a network printer or reconfigure a 100BaseT Ethernet hub or switch.

- Extended Management Information Base (MIB) support—since SNMP Management Console supports any MIB-2 (RFC1213) agents installed on most Windows 2000/XP, Windows NT, UNIX, Linux, and NetWare systems and devices, SNMP Management Console lets you install MIB definitions for SNMP agents from different vendors. If your network includes SNMP devices from different vendors, separate MIB definitions can be installed and used simultaneously by SNMP Management Console.

- Ease of use—SNMP Management Console's modular design makes it both powerful and easy to use. Different SNMP functions are divided among the main windows, and multiple agent data can be viewed simultaneously.

Who should use SNMP Management Console?

Any network administrator, systems consultant, or network programmer will find SNMP Management Console useful. SNMP Management Console and its related utilities are designed to meet the needs of network professionals, ranging from beginner to expert.

SNMP Management Console is most useful for network administrators who want to monitor their LANs and manage SNMP-aware devices from a single location. SNMP Management Console helps administrators make decisions based on hard facts instead of guesswork.

In many cases, SNMP provides more information or different information that is not accessible using other network analysis tools, helping the administrator pinpoint problems and determine solutions that might be overlooked otherwise.

SNMP Management Console main components

The SNMP Management Console software package includes the following components:

- The MIB Compiler compiles SNMP MIBs into the binary format used by SNMP Management Console and offers a drag-and-drop interface for creating custom requests from MIB objects.

- Global Event Log displays general SNMP events and traps.

- Agent windows display all lists, charts, forms, tables and the local event log.
SNMP agents and SNMP agent request lists show all agents, and when an agent is selected, the set of requests that have been configured for the agent.

SNMP Management Console is integrated into the Observer interface. All SNMP functionality is available concurrent with Observer’s functionality.

Preparing to use SNMP Management Console

SNMP Management Console and its utilities are powerful, yet can be learned with only a few hours’ study. The programs are designed primarily for network administrators, but this manual includes information that may be of interest to anyone who wants to learn more about their network from an SNMP perspective.

Install additional MIBs

SNMP Management Console includes a number of preinstalled MIBs. These MIBs are for various common devices (e.g., servers) and include the standard MIB RFC1213.

The standard MIB (RFC1213) should work on any SNMP-enabled device. You may find that the standard MIB or the provided MIBs provide enough information so that no additional proprietary MIB installation is required.

Should you want to install a vendor-specific MIB, select File > Compile MIB File and specify your MIB file.

This option is only available from the File menu when the MIB Editor is visible. To make the MIB Editor visible, select View > MIB Editor.

SNMP Management Console will import and compile your MIB. The MIB will now be available for selecting requests in the MIB viewer.

Enable SNMP network agents

Although many devices are advertised as SNMP-compatible, you may need to install or enable manufacturer-provided SNMP agents on your specific device. For example, you may need to configure and run SNMP services on your UNIX or Windows system. You will also need to check whether there is (or has been) a community name specified on the agent and what the community name is on the specific system.

Typically, the default community name is public.

Check the device or server manuals for more information on installing or enabling SNMP agents.

Configuring SNMP Management Console

After installation, SNMP Management Console will generally require little, if any, configuration before it can be used.

General SNMP Management Console options are defined in Options > Observer General Options > SNMP Tab.

Configuring SNMP agents

For the SNMP Management Console to work with SNMP agents on the network, both must be configured, and this section describes how to accomplish that.

In this section, the term SNMP agent is used to mean the actual agent on the network device, rather than the representation of that device in Observer’s SNMP Extension.

First, the SNMP agents on the network must recognize SNMP Management Console as a management station that is permitted to access their MIB information. To poll the agents for information, the SNMP Management Console must know the IP addresses and community names of each agent.

A device’s community name is, in effect, its password. In many environments, the default read community name is public and the default write community name is private.

To add a new agent entry, complete the following steps:
1. Choose **Actions > Add SNMP Device**. The Network Device Properties window appears.
2. Type the SNMP agent’s information; provide as much detail as possible.
   A device’s community name is, in effect, its password. In many environments, the default read community name is public and the default write community name is private.
3. Click OK to add the agent entry to Observer and save your changes.

After completing this task:
Repeat this process for every SNMP device on the network. Remember, the overall implementation of SNMP may vary for each SNMP agent on your network, so we recommend you refer to each device’s documentation for more information on configuring and enabling SNMP.

**OIDs**

An Object Identifier (OID) is a unique identifier assigned to a specific object. The identifier consists of a sequence of numbers that identify the source of the object, as well as the object itself. This sequence of numbers is variable in length, so in addition to the sequence of numbers, there is a length field. OIDs are organized in a tree structure; the sequence of numbers identifies the various branches of the subtree that a given object comes from.

The root of the tree is the ISO (International Standards Organization) trunk. Its value is one (1). Each branch below the root further identifies the source of the given object. All SNMP objects are members of the subtree identified by iso.org.dod.internet or 1.3.6.1.

Each additional component further defines the exact location of an object. The numbers for each subtree are assigned by the IETF to ensure that all branches are unique. While it is good to know that OID identification structure exists, in general, OID management is done by SNMP Management Console and no specific OID knowledge is required to use SNMP Management Console.

**SNMP Management Station**

The SNMP Management Station is a program designed to poll SNMP agents, collect information, and display the collected information in an easy-to-view format. Because each SNMP agent on a network can support a unique MIB, the SNMP management station must load MIB information for all the agents it intends to access. Without this information, the management station cannot make sense of proprietary MIBs and cannot obtain information from their agents.

The management station polling process typically includes the following steps:

- The management station composes an SNMP request that includes one or more MIB objects.
- The management station sends the request packet to an agent, located on a network device.
- The agent receives the request, checks the values of the objects requested, composes a reply packet, and sends it back to the management station.
- In the case of SNMP Management Console, the data is displayed in chart, form, list, or table format.

Through the management station, SNMP agents can provide information to a network administrator without the administrator physically attending to the device.

Almost any network device can be equipped with an SNMP agent. However, because the addition of an SNMP agent typically will increase the cost of the device, many devices are available without the SNMP agent installed. Typical examples of SNMP-aware devices are: routers, network cards, Ethernet and Token Ring switches, network printers, UNIX hosts, NetWare servers, and Windows 2000/XP servers and stations.
Using SNMP Management Console

The SNMP Management Console is integrated into the Observer interface. Make certain that you have the SNMP Management Console Agent List visible by selecting View > Advanced, RMON and SNMP Probe Lists from Observer’s main menu.

Figure 62: SNMP Panes

When Observer is licensed to include SNMP Management Console, the Console is running at all times. To view the Console windows, just click on one of the SNMP agents in the List of SNMP Agents.

When an agent is selected, Observer’s interface turns into the SNMP Management Console interface. You will notice that the menus, button bars, and main display areas change. You can return to the Observer interface by selecting a probe from the List of Probes.

The SNMP Management Console interface is divided into three main sections:

- **List of SNMP Agents pane**—displays each agent as an icon. Agents are queried by request files that define five types of requests: charts, forms, lists, tables, and traps. When an agent is selected, the requests are displayed in the SNMP Agent Requests pane.

- **SNMP Agent Request pane**—SNMP Agent Requests are shown in this pane. Selecting a chart, form, list, table, or trap will display the associated request output in the Agent Display pane.

- **Agent Display pane**—all data is displayed in one window per agent. Each item (charts, forms, lists, tables, and traps) is selected by the associated tab at the bottom of the Agent window.

Additionally, SNMP agents can be displayed in map format alongside of Observer probes. The map format lets you display graphically (either geographically or topologically) your network layout, including the positions of SNMP agents and the connections between them and Observer probes. You can scan in or draw a map or diagram and place your servers, hosts, and other SNMP agents in their appropriate locations. SNMP
Management Console includes a set of bitmaps for different devices, or you may add your own bitmaps for map objects (in Windows BMP format).

SNMP Management Console lets you add, edit, or delete agent entries. When you add a new agent entry, you must associate a request file with it. Assigning a MIB also makes available a set of preconfigured menu requests used to poll the agent for data. A request file defines a set of objects for monitoring from one or more MIB groups. You can remove request items or create and add new request items using the MIB Editor.

SNMP Management Console polls SNMP agents and displays the collected information in a chart, form, list, or table. To accomplish this, the SNMP Management Console creates request packets in SNMP format and sends these packets to agents using the UDP protocol as the carrier. The SNMP packet, often called a PDU (Protocol Data Unit), consists of one or more SNMP objects.

When SNMP Management Console sends an SNMP packet to an SNMP agent, it either asks for information about an object (a Get request), or asks to set the value of an object (a Set request). When the agent receives the SNMP packet, it checks whether the object exists in the agent’s MIB, finds object values, creates a reply packet, and returns the reply packet to the SNMP Management Console.

Because SNMP uses UDP (User Datagram Protocol) to transfer requests and replies, and because the UDP protocol does not require the receiving station to acknowledge receipt of a packet, there is a chance that either the request or reply packet will be lost.

To address this potential problem, SNMP Management Console uses a timeout-retry mechanism. You can specify the amount of time SNMP Management Console will wait before deciding that the request was lost and the number of times SNMP Management Console will resend the packet. When the maximum number of retries is reached and no reply has been received, SNMP Management Console considers the SNMP agent not present, out of order, or turned off, and displays a timed out message in the agent log.

Using the MIB editor

The SNMP agent on the device must send the trap. Refer to the manufacturer’s documentation to determine what traps the device’s agent can send. If the manufacturer supplies a MIB file that includes the supported traps, you can use that MIB after it has been compiled to drag and drop the traps into your request file. If the manufacturer of the device does not supply a MIB, the standard MIB-2 (supplied with Observer) includes most standard traps and may be useful to you.

Observer Suite’s Trace Window (the bottom pane of the Observer main window) shows you any traps it has received, whether or not the trap is included in your request file.

The request file lets you set actions (such as emails, pages, or program launches) that are triggered when a trap is received.

To add a trap to a request file, follow these steps:

**Note:** The OID can be searched by its name, but not by its location.

1. Choose Tools > SNMP MIB Editor. The MIB editor appears. The MIB Editor has two panes: compiled MIBs are displayed in the left pane; request files are in the right pane:

2. Select a MIB from the Model Compiled MIBs folder that includes the traps you are interested in.

3. Because the Network Instruments-supplied request files are locked, you must make an unlocked copy of the request file before you can modify it. Right-click the request file and select Copy Model Device Type As from the pop-up menu. A writable copy of the request file will be placed in the request file pane’s browser.

4. To easily find all the traps embedded in a particular compiled MIB, right-click on the MIB and choose Find.
5. Check the Find traps only box. Type a search string in the Find what field if you are looking for a particular trap. Otherwise, leave the space blank to find all traps in the MIB. Click Find to list the OIDs of any traps that are found.

6. After you have located the trap or traps you want to include in the request file, click each trap in the compiled MIB pane, and drag it to the appropriate request file’s trap section.

7. After you have added all the traps, you can configure them by right-clicking on the trap in the request file pane and choosing Properties. Click the Set Triggers tab to configure the trap.

8. Check each box to set the desired action. Click the action (rather than the check box) to display the configuration options for that action (for example, you can enter a pager or email message). The pager numbers and email address for notifications are set in the Observer General Options dialog. Click OK to save the changes when finished.

**Adding triggers based on SNMP chart values**

Observer Suite’s SNMP request file format also allows you to set triggers on any SNMP value. For example, if the request file includes a bandwidth utilization chart, you can configure an email alarm to trigger when a utilization threshold has been exceeded.

Observer Suite’s SNMP functionality does not just provide read access to SNMP objects. You can use an SNMP form request to manage your network from the Observer analyzer.

1. To configure a request file chart item to set alarms triggered by SNMP values, open a writable request file and select the chart for which you want to set an alarm. Right-click and choose Properties from the pop-up menu.

2. Double-click on any item in the chart to edit its properties. The Chart Item Properties wizard appears.

3. Click Next three times.

4. Check the upper and/or lower threshold you want to set an alarm for, and click the Edit Alarm Response button to set up log, pager, email, or application launch behavior when the given threshold is met. Click Finish to return to the MIB Editor. To save your work, right-click on the unsaved request file icon and choose Save file from the popup menu. The request file icon changes to show that all edits have been saved to disk.

**Adding, modifying, and deleting SNMP agents**

To collect information from your SNMP-enabled network devices, you must add an agent entry for each SNMP agent on your network.

To add a new agent entry, select Actions > Add SNMP Device or right-click in the SNMP Agents pane and select the Add SNMP Device item. Either action will open the Network Device Properties dialog.

<table>
<thead>
<tr>
<th>Name</th>
<th>Name that is displayed to the right of the agent icon in the SNMP Agents list. Enter any descriptive name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the SNMP agent you want to add.</td>
</tr>
<tr>
<td>Device type</td>
<td>A request file based on the RFC1213 standard MIB request file is included with SNMP Extension. Click the browse (…) button to browse the desired request file.</td>
</tr>
<tr>
<td>Comment</td>
<td>Allows you to fill in any comment you want here.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>SNMP Management Console supports both SNMPv1, SNMPv2, and SNMPv3. SNMPv2 includes a superset of the SNMPv1 features. SNMPv3 adds security and encryption to SNMPv2, while remaining backward compatible with SNMPv1 and SNMPv2. Some SNMP devices do not support SNMPv2 and SNMPv3. If in doubt, leave this setting at the default, SNMPv1.</td>
</tr>
</tbody>
</table>
### Security user name
Provide the user name by which Observer will access the agent.

### Context engine ID
The context engine ID uniquely identifies the SNMP entity; check the HEX box if you wish to enter the string as a hexadecimal entry (for example, 80 FF 00).

### Community/context name
The community name. This is typically public. By convention, SNMP uses the community name and management station IP address the same way login name and password are used in a Telnet (terminal) session.

Some SNMP agents will respond to a menu request only if the management station IP address exists in the agent's list and if the request contains the proper password.

In SNMPv1 and SNMPv2, the community string provides rudimentary password protection. To remain accessible to any SNMP station, most SNMP agents use the default community name public.

If you do not specify the correct community name (or, in the case of those agents who maintain an IP address table, if your SNMP Management Console IP address is unknown to the SNMP agent), the agent will not respond to your requests. SNMP Management Console will re-send the request until it times out.

If you are polling the SNMP agent for the first time, a failure to respond may be caused by any one, or more, of the following:

- The SNMP agent is up and running, but SNMP Management Console is not entered as a management station in the agent's database.
- The community name is wrong.
- SNMP services are not enabled on the device.
- The SNMP agent's device is down.

If you have previously successfully polled the SNMP agent, only the last one is possible, unless the configuration of the SNMP agent's device has changed.

### Table 37: SNMP security options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply USM key localization to passwords</td>
<td>USM key localization allows a principle to share unique authentication and encryption key with each remote engine, while maintaining only a single set of keys locally.</td>
</tr>
<tr>
<td>Authentication protocol menu</td>
<td>Specifies the mechanism used for authentication: noAuth (none), HMAC - MD5, HMAC - SHA1</td>
</tr>
<tr>
<td>Authentication password (key)</td>
<td>The password used for authenticating users.</td>
</tr>
<tr>
<td>Privacy protocol</td>
<td>Specify the encryption method to use when transferring data between the agent and the management console.</td>
</tr>
<tr>
<td>Privacy password (key)</td>
<td>Specify the password to use when transferring data between the agent and the management console.</td>
</tr>
<tr>
<td>Authentication time window (seconds)</td>
<td>When messages are delivered outside the time window, SNMPv3 security will not process them. This provides a way of ensuring that previously captured messages are not being replayed.</td>
</tr>
</tbody>
</table>

### Notify on Trap/Alarm:

- **e-mail address**—allows you to enter the e-mail address to send notifications to (from traps or alarms for this agent).
This is a different issue from the IP address (of the computer running Observer with SNMP Extension) to which the SNMP agent itself is to send traps. In this case, you are specifying the e-mail address of the person who is to be notified when a trap message is received by SNMP Extension.

Time to log data (24 Hour Clock):—You can choose to have device data logged all the time, or schedule times to collect and log data on particular days of the week within particular hours.

Keep polling even if not logging Chart Request data—Check this box to have the SNMP agent poll the device even if it is not logging chart request data.

Using agent information windows

The information collected from agents by SNMP Extension is displayed, upon request, in an Agent Information Window. When you select an agent entry from the SNMP Agents list, or from the map display, an Agent Display pane opens.

Figure 63: Agent Information Window

An agent display is an MDI child window. It cannot be moved outside the display area. You can open multiple agent windows simultaneously and tile them in horizontal, vertical, or cascading formats. One window per agent is opened. Select a tiling choice from the Windows menu or click the appropriate tiling choice on the button bar.

The total number of agent windows you can open simultaneously is limited only by your available Windows resources.

Each agent window can display any combination of lists, charts, tables, or forms. Each new list, chart, table, or form creates a new tab at the bottom of the agent window.

When multiple agent windows are open, you can select an active window by selecting it from the Windows menu. The Windows menu also includes commands for arranging icons and closing all open windows.
Agent windows can be minimized (its icon will appear at the bottom of the Agent Display Area) or maximized to completely fill the Agent Display Area. When the agent window is maximized, it will change in size as the Agent Display Area is resized.

Each agent information window contains an Event Log tab that displays the local event log. This window cannot be closed. Errors appear only if the agent is down or malfunctioning. When an agent is down, the Event Log displays a message indicating that SNMP Management Console exceeded the number of retries while attempting to poll the agent. Another type of error is reply packet parsing errors. If these errors appear, either the SNMP agent is malfunctioning or it's sending reply objects not supported by SNMP Extension.

**Collecting SNMP agent information**

After opening an Agent Information window, you may collect information from SNMP agents for display in charts, lists, forms, or tables. Charts are used for time-dependent information. Lists and tables are used for both time-dependent and time-independent information. Forms display SNMP data in a graphical format.

**Collecting chart information**

Chart displays are limited to numerical time-dependent information; therefore, MIB objects such as IP addresses, octet strings, hardware addresses, bitfields, enumerated integers, and different constant integers are not candidates for chart requests. In general, three types of variables do not fit well in charts:

- Non-numerical variables that cannot be displayed in any reasonable way in the chart format (e.g., names).
- Constants: change of a value in time (the differential of the value) will always be equal to zero.
- Table objects are not displayed in charts.

Chart requests are created and modified using the MIB Editor. See The MIB Editor on page 198 for details.

To receive chart information from an agent, select the Charts tree item in the SNMP Agent Requests area. Then double-click on the chart you would like to view. This will display the chart in the current agent information window if one is open, or will open a new agent information window if one is not currently running.

When you select a chart request, SNMP Extension begins polling the agent. You can define the length of the request period and define chart display parameters by right-clicking on the chart and selecting Chart Properties. See Building and modifying charts on page 202.

Chart information can be saved from the agent window. You can save the chart data in a file then import it into a spreadsheet program (e.g., Microsoft Excel or Lotus 1-2-3).

*Customizing charts*

When changes are made to a chart from the Chart Properties display window, the changes are effective for the present session only. Persistent changes must be made to the chart from the MIB Editor.

1. When agent information is displayed in chart format, several options are available for customizing the display. To define the following settings, right-click on the chart and select Chart Properties.

**Collecting list information**

When you request agent information using the list format, SNMP Extension polls the agent once to receive a snapshot of agent objects defined in the list request.

Lists have only one limitation regarding type of object: they cannot display tabular objects. Lists can display text, IP addresses, descriptions, and numeric variables, but not tables.

Lists are best for objects that have a one-to-one relationship. For example: a statistic that does not change, such as SystemName; or a statistic that does not have a variable number of data points, such as RouteMetrics. Tables
are best to display items that may have a variable number of responses, such as a list of current connections by IP address.

To receive list information from an agent, select the Lists item in the SNMP Agents request area, then select the List tree item you wish to view.

List requests are created and modified using the MIB Editor.

When you select a list menu request, SNMP Management Console sends the request to the agent and (if the agent is running and configured properly) receives a reply, which can be viewed in the list display in the agent information window. If necessary, SNMP Extension will re-send the request.

**Read Values Display**

Some objects in the list are writable, which means you can use SNMP Management Console to set the value of the object remotely. Writable objects display [RW] in the Access column of the display. Read-only objects show [RO] in the Access column.

*Writable Object Setting*

To define a setting for a writable object:

1. Select the writable object entry in the agent window.
2. Enter or select a new value for the object in the box that is displayed at the bottom of the window.
3. Click the Set button. SNMP Management Console sets the value of the writable object and repeats the original request to make sure that the value was changed.
4. The updated list information will be displayed.

After completing this task:

Depending on the type of table and the constraints imposed by the agent MIB design, you may be able to change the values of writable table objects, add additional lines to the table, or both.

**Collecting forms information**

Forms are SNMP Management Console’s way of displaying SNMP data in a flexible graphical format. Forms can be groups of items that show objects in a clean, colorful formatted view; bitmaps of devices with ports that change color, depending on the value of the SNMP response; or multiple choice writable SNMP lists for configuring a server.

Any type of SNMP object can be placed on a form. Each object’s display format can be adjusted to meet the needs of your display requirements. Example forms include an IP route form that allows you to view or set the status of multiple IP routes from the devices route table, or a System Information form that lets you set certain system information writable objects.

To modify the sampling behavior of a form, right-click on the form and select Form Properties. The Form Properties dialog will be displayed.

Forms are created and modified using the Forms Designer in the MIB Editor. List requests are created and modified using the MIB Editor.

**Collecting table information**

SNMP tables are collections of different types of objects. Picture the SNMP table as a spreadsheet. Each row contains fields of data related to an object. Access to the SNMP MIB table is similar to reading the spreadsheet row by row.

SNMP works in the following way: SNMP Extension requests the values of all or some objects from the first line in the SNMP MIB table. After receiving a reply, it displays the values in the table and requests information for the
next line. SNMP Extension continues to collect information row by row until it reaches the end of the table. This process is called traversing the table in SNMP terminology.

To receive table information from an agent, select the table tree item in the SNMP Agent Request area, and double click on the table you wish to view.

**Figure 64: IP Address table**

![IP Address Table]

Tables are created and modified using the Forms Designer in the MIB Editor. List requests are created and modified using the MIB Editor.

**Read Values Display**

SNMP Extension will read the table and display the values of the table objects line by line. Tables can contain more than one writable object. Writable objects display [RW] in the Access column of the display. Read-only objects show [RO] in the Access column.

**Traps**

An SNMP device may be configured by its manufacturer to send trap messages which notify the SNMP management station (in this case, SNMP Extension) of certain conditions. Unlike get and set requests, a trap message doesn’t require a request from SNMP Extension. It’s sent by the device automatically when there is an error, a certain level of activity, or other condition. SNMP Extension collects incoming trap messages constantly.

Trap and trap message are used interchangeably.

To receive trap messages with SNMP Management Console, SNMP Management Console's IP address must be included in the trap configuration table of the SNMP agent. Trap configuration is usually separate from general SNMP configuration.

If you configure one but not the other, you may be able to poll the SNMP agent, but receive no trap messages.

The SNMP agent doesn’t expect confirmation for trap messages. If the message doesn’t reach its destination, SNMP Management Console has no way of knowing the message was sent, and the agent has no way of knowing whether a message was received.

Under normal circumstances most of the trap messages do reach their destinations. The limitation of traps comes from the lack of verification capabilities built into the relevant RFC specifications.
The MIB Editor

The MIB Editor is where MIBs are compiled and MIB objects are placed in requests to create SNMP Management Console lists, charts, tables, forms, and traps.

- **MIB**—a MIB is a text file in Abstract Syntax Notation One (ASN.1) format, which describes in a structured way the objects an SNMP device supports.
- **Compiled MIBs**—a compiled MIB is a binary file created from a MIB file in preparation for creating requests to be submitted to an SNMP agent.
- **Device Types (Requests)**—a request file is the actual file sent to an SNMP agent, polling and/or setting the states of various MIB objects or OIDs.

The MIB Editor displays compiled MIBs on the left pane of the window and request files on the right pane. Both compiled MIBs and requests are displayed in a familiar Windows tree format. The MIB Editor is used to compile MIBs and create/edit requests.

MIB

MIBs are text files that the creator of an SNMP agent provides to describe the variables the particular agent keeps track of. These variables are called SNMP objects.

Often, in the context of SNMP, they are simply referred to as objects.

MIBs have a very specific structure for the organization of objects; any SNMP management console (SNMP Management Console in this case) can use the MIB to form queries of the SNMP agent on a specific device. MIBs are supplied by the manufacturer of the device.

There are two logical sets of statistics that every agent (in theory) should keep track of:

- The standard MIB-2 (RFC1213) set or MIB-1 (RFC1066), and
- Any proprietary MIB(s) objects.

SNMP is structured this way so that each device can offer standard (MIB-1/2) data that would be common between all network devices (e.g., packets in, packets out), and data that is device-specific (like number of sheets printed on a network printer). MIB-2 is a superset of MIB-1. Sometimes these two sets of MIB objects are combined into one MIB file. Other times you may find that the manufacturer only provides you with a proprietary MIB and expects you to use the RFCMIB-2 (or MIB-1) to view the standard data objects. Unfortunately, there are manufacturers that only offer a subset of objects in the standard MIB(s). In these cases, you can ask the agent for the objects that are missing, but the agent will not respond.

All SNMP agents keep track of some or all of the objects in the standard MIBs (MIB-1 or MIB-2). If you do not have access to a proprietary MIB for your device, you may be able to get all the information you require from the standard MIBs.

A Request File

A request file is built within SNMP Management Console to organize, group, and define specific SNMP requests that may be made of an agent. Each request can be for one or more SNMP objects, and the response to the request may be displayed in list, chart, table, or form format. A number of request files come with SNMP Management Console, but in general, request files are built by you to suit your specific needs with regards to the matrix that your site needs to collect.

When SNMP Management Console polls an SNMP agent for information, a request allows it to receive information about many different objects simultaneously. You can create your own requests (or edit the requests provided) using the MIB Editor.
Compiled MIBs

SNMP Management Console compiles the MIB prior to using it to create requests. This is done to save on memory when parsing request responses and to make drag-and-drop request building faster.

Your path to begin building requests (lists, charts, tables, or forms) will begin by determining whether SNMP Management Console includes a suitable MIB for your device.

If you have a specific MIB that was included with your device, you should begin by compiling the MIB. See Compiling MIBs below.

If you do not have a specific MIB for your device and the device is not listed on the list of MIBs, you can still use the standard MIBs to create requests for that device. In that case, you will use the standard RFC1213 or RFC1066 MIB to build your requests.

Compiling MIBs

Prior to building a request, you may need to compile a MIB. You will need to do this if you have a MIB that was distributed with your device or have received a new MIB for a device. If you don't have a specific MIB for your device and want additional information on what the standard MIBs provide, you must obtain a MIB from the manufacturer.

Once you have the MIB, you compile it using the MIB Editor. Compiling the MIB is not much more complicated than opening a file. However, some companies do not strictly follow the MIB file format, so you may need to modify the MIB text file. Also, after compiling the MIB file, you must create your own requests.

The MIB Compiler parses MIB text files and converts them into a format that can be used by SNMP Management Console and its utilities. The MIB Compiler is used when you don't have a pre-compiled MIB for a particular SNMP device. You may also need to use the MIB Compiler to recompile a MIB after editing the device MIB file (for example, to correct an error in a manufacturer-supplied MIB file) or to update a manufacturer-supplied MIB file for a new device.

The MIB Compiler expects ASN1-formatted MIB text files which have the MIB Management Console (e.g., RFC1213.MIB).

ASN.1 (Abstract Syntax Notation One) is the standard way, defined by two ISO (International Organization for Standardization) standards, to describe a message that can be sent or received in a network.

ASN.1 is defined in two different places:

The rules of syntax for describing the contents of a message in terms of data types and content sequence or structure is defined by the ISO 8824/ITU X.208 standard.

How you actually encode each data item in a message is defined by the ISO 8825/ITU X.209 standard.

The compile process

1. To compile a new MIB, open the MIB Editor by selecting Tools > SNMP MIB Editor.
2. Select Compile MIB Source File. This opens the Import MIB Source dialog, which lets you select a file to compile.
3. Select the MIB file (*.MIB) you wish to compile. The Save Compiled MIB As dialog will be displayed.
4. Insert the desired file name and click the Next button.
5. The MIB will be compiled and the resulting file (with a .MIC extension) will be placed in the Program Files \Observer\SNMP directory.
6. Once the MIB is successfully compiled, it will be automatically listed in the MIB Editor with the other compiled MIBs.
7. Should the compiler have problems compiling your MIB, the compiler will exit to the MIB Editor and the log will display the errors, listing which MIB line caused the error. Click the Edit Source button to edit the MIB file and correct the error.

8. After correcting the error, simply compile the MIB again. If there are any further errors, the compiler will stop again. Repeat until the MIB successfully compiles.

Building requests

As described earlier in this section, requests are built from MIB objects and can be displayed in list, chart, table, or form format. Requests are grouped together in a request file. Request files contain folders for each format of request: chart, list, table, form, and trap.

SNMP Management Console includes a number of pre-built request files that can be used as is or modified to suit your specific needs. Most users will find that the included request files, possibly modified, will serve quite well.

Requests can contain objects from one MIB or many separate MIBs. Once built and saved, requests are displayed in a tree structure for each agent that the request file is associated with.

When adding a new SNMP Agent, you must specify a request file. All configured requests for the agent become available each time the newly-registered SNMP agent entry is selected. You can remove requests from an agent or add newly-created requests to an agent using the MIB Editor.

To receive information about an object, SNMP Management Console polls an SNMP agent by sending a request packet. The request packet can combine one or more object IDs. When the agent receives the request, it searches its databases, retrieves object values, composes a reply, and sends the reply as a reply packet back to SNMP Management Console.

The structure of the SNMP polling process suggests that an SNMP request can be considered a single object. By combining several SNMP objects in a single request, the same requests can be used for all SNMP agents using the same MIB.

The MIB Editor provides this functionality for SNMP Management Console by allowing you to design requests for each agent. When you configure a new SNMP agent, you designate its request file in the SNMP Agent Properties dialog.

Why build custom requests?

The request files that are included as part of the SNMP Management Console package will serve most user’s needs most of the time; however, there may be situations where it can be advantageous to build custom requests. RFC1213 includes methods for manufacturers to define SNMP objects not specifically defined (in effect, proprietary MIB objects). In some cases, a manufacturer may not have precisely adhered to the RFC1213 specification and mislabeled an object.

Custom requests allow the SNMP Management Console to work with SNMP agents that interact with objects not directly defined in RFC1213, and in dealing with badly-formed SNMP agents.

Another advantage of custom requests is the ability to share them. For example, a network administrator in a large corporation may need to create a periodic report about network traffic. Four other network administrators from the same corporation, located in different states, must create similar reports about their network segments. By creating a single, uniform custom request, it is possible to easily compare the performance of the network segments on the important criteria.

Yet another advantage of custom requests is to avoid data overload. While SNMP and its proprietary features can provide a mountain of information, only some of it will be relevant in a given situation. By either modifying standard requests to eliminate extraneous data, or by creating custom requests from scratch, you will be able to create displays of information that are useful to your specific situation. For example, RFC1213 defines twenty different ICMP objects, but much of the time, most network administrators will find themselves interested in
only one or two. By creating a custom chart, the network administrator can focus more on what’s relevant by eliminating the display of the extraneous.

Custom requests also provide a way for a network administrator to:

- Design a standard for obtaining exactly the information needed;
- Prepare information in a way more easily understood by less technically-oriented people, and;
- Share the standard with other administrators.

Through discussion and testing, a comprehensive set of custom requests can be developed to obtain consistent sets of data customized for an organization’s particular needs.

Adding support for a new SNMP device by creating a custom request file

1. To create a custom request file, from the MIB Editor click on the Create New Request icon.
2. The Add New Device Type dialog will be displayed.

Figure 65: Custom request file

3. Name the request file.
4. Leave the Add default RFC1213 requests to the new file selected, if desired.
5. Click the Create button.
6. The new request tree on the right hand side of the MIB Editor will be displayed. Note the new request items that are now available: Charts, Expressions, Forms, Lists, Tables, and Traps.
Building and modifying charts

Much of what is done in the MIB Editor when building and modifying charts is similar to what can be done from the Agent Display window. There are two significant differences when modifying a chart from the MIB Editor:

- Changes, once saved, are permanent. When changes are made from the Agent Display, they are for that session only.
- More features of the chart can be modified by the MIB Editor.

1. To create a new, blank chart, right-click on Charts and select New Chart. A new chart, entitled New Chart will be created.

2. Drag-and-drop any non-table MIB object from the left-hand pane of the MIB Editor onto the chart (remember: charts cannot display tabular data).

A MIB object can be copied from any available compiled MIB. Only those MIB objects that have been copied to the chart can be monitored by the chart.
After completing this task:
While it’s certainly possible to copy a myriad of MIB objects to the chart and only use a few, it’s generally a better idea to copy only those objects you plan on charting with that particular chart.

Building Expressions
Expressions permit you to take SNMP agent data and derive useful mathematical results.

Raw data that SNMP Management Console receives from SNMP agents can be very useful but, often it’s only the starting point. An SNMP agent on a switch may keep track of the number of data packets the switch has received, the number of packets it has discarded, and the number of packets it has passed along. However, the network administrator may be more interested in the percentage of packets discarded since this may signal a problem with the system.

1. To create a new expression, from the MIB Editor, click on Expressions, then select Mode Commands > New Expression or right-click and select New Expression.

2. From the left pane of the MIB Editor, select any MIB objects that you intend to use in the expression and drag-and-drop them on the new expression.

   There may be a slight performance penalty caused by including unnecessary MIB objects in an expression. In terms of system efficiency, it’s best to add only those you need. If you find you need additional MIB objects to create your expression, you can easily add them at a later time by the same drag-and-drop method.

3. Right-click on the new expression to rename it, if desired.

4. Right-click on the renamed expression and select Edit Expression to display the Modify Expression dialog.
The Modify Expression dialog box is, in effect, a numeric calculator, permitting the creation and modification of mathematical expressions using selected MIB objects, constants, and mathematical operations.

5. Numbers can be entered from the keyboard; mathematical functions can be entered either via the keyboard, or from the buttons of the dialog. The Insert MIB Object button can be used to insert MIB objects that have been dragged to the expression.

6. Click OK to save the edited expression.

Now that the new expression has been built, it can be used in a chart. Building and modifying charts on page 202

Building list and table requests

The same actions can be taken to build tables.

1. To create a new list, from the MIB Editor, click on Lists, then right-click and select New List.
2. SNMP Management Console will create a new list. Rename the list whatever you find appropriate.
3. Open the MIB tree for the MIB you would like to use.
4. Display the objects you want to include on your list, highlight the objects, and drag the objects from the MIB tree listing to the request file tree.
   
   You may use MIB objects from two or more different compiled MIBs.

5. Once complete, click the Save Request File icon. The new list will be available for all Agents that use this request file.

Building trap requests

A trap is an event that an SNMP Agent (the actual hardware or software agent, not SNMP Management Console’s Agent request) can be configured to automatically report to the management program, in this case SNMP Extension. RFC1157 defines seven traps, any, all, or none of which may be supported by a given SNMP Agent.

To find out which, if any, SNMP traps your device supports, please consult the documentation for that device.

When the Agent has been configured to report a trap and a trap event occurs, the Agent will report the trap to the management program without having to be polled.

For example, one defined trap is the coldStart trap. A device with an SNMP agent that supports this trap will issue this trap when the device is performing a cold boot (or reboot), one where the device’s configuration or implementation may be altered. Another is the warmStart trap, which is issued when a warm boot is occurring.
The advantage of a trap is that the management program does not have to repeatedly query the agent for the trap condition. Like an alarm clock going off at a pre-set time, when a configured trap event occurs, it notifies SNMP agent without having to be asked.

There are some inherent limitations to traps. A trap can only be sent from a properly-functioning SNMP Agent, so it’s impossible for a router to send a trap announcing that it’s down. Since a trap is configured in the SNMP Agent itself, it’s relatively inflexible. Further, since traps are sent via UDP (a protocol that does not include method for verifying that a packet has been received), the SNMP Agent has no way of knowing if the trap has been received and acted on.

1. To add a trap to an SNMP request, simply drag a trap from a compiled MIB and drop it on the trap tree of the MIB request.
2. Right-click on the trap to bring up the Trap Properties dialog. The boxes on the Trap Properties tab will always be grayed out, as there is no configuration of the traps themselves; traps are simply either monitored or not monitored by SNMP Management Console.
3. Click on the Set Triggers tab to configure the trap’s alarms and to display the Set Triggers tab.
   Alarm actions can be set independently. It is possible to configure some, none, or all of the possible alarm actions to happen when the trap is received.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send e-mail message</td>
<td>if selected, a triggering event will cause an e-mail message to be sent to a designated recipient as configured in Options &gt; Observer General Options &gt; e-mail Notifications. Enter the message in the e-mail message.</td>
</tr>
<tr>
<td>Page phone number</td>
<td>if selected, a triggering event will cause a pager message to be sent to the recipient designated in Options &gt; Observer General Options &gt; Notifications.</td>
</tr>
<tr>
<td>Play sound file</td>
<td>if selected, a triggering event will cause a sound file to be played.</td>
</tr>
<tr>
<td>Execute command line</td>
<td>if selected, a triggering event will cause a DOS or Windows program to be run. Only one command will be executed. If you need or wish to have more than one program run, you may set up a batch file (e.g., WARNINGS.BAT) as the command line to be executed. You can then use a text editor to create WARNINGS.BAT and enter multiple commands in that batch file.</td>
</tr>
</tbody>
</table>

**Designing and building forms**

SNMP Extension’s Forms Editor is a full-function forms designer enabling you to display information in a variety of formats and to actively interact with SNMP devices. While SNMP Management Console comes with several sample forms, it is possible for you to design custom forms.

1. To build a new form, from the MIB Editor, click on Forms, then right-click and select New Form.
2. SNMP Management Console will create a new form. Rename the form whatever you find appropriate.
3. Open the MIB tree for the MIB you would like to use.
4. Display the objects you want to include on your list, highlight the objects, and drag the objects from the MIB tree listing to the Request file tree.
5. Right-click on the form and select Edit Forms Control to display the Form Editor dialog.
You can toggle the form between Edit Mode and Preview Mode. In Preview Mode, while the form will not display any actual data, it is possible to test buttons and list forms.

**Setting an expression**

1. Click the Set Expression button. The Choose Expression dialog box will be displayed.
2. The upper pane will contain those expressions available in the present SNMP request. Select any expression and click the Next button.
3. The Set Expression Indexes dialog will be displayed.
4. Select the index you wish to modify and enter your chosen value in the Assign index value. Click the Finish button.
5. The Edit Field Properties dialog will be redisplayed.

*Edit Ranges/Values*

**Figure 71: Edit Range and Values**

1. Click on the __ line.
2. Click on the icon to choose the default bitmap to be displayed.
3. For each value or range of values you wish to be represented by a different bitmap, click on the Add new button.
4. Enter the value or range in the appropriate edit boxes, then click on the icon to set the bitmap for that range.
Adding new MIB objects and traps to request files

Rather than re-compiling a MIB to add a new object or trap, sometimes it is convenient to add new items to a MIB that is already compiled. The SNMP MIB editor lets you accomplish this by right-clicking on objects in the request file pane (right side of the MIB editor) and choosing the appropriate option from the pop-up menu. Once you have created the new object or trap in the request file, you can simply drag the item from the request pane to the compiled MIB pane (left side of the MIB editor).

Adding a new MIB object

This section describes how to add a new MIB object and the MIB Object Properties.

1. To add a new MIB object to a request file, right-click on the request to which you want the object added, and select New MIB Object from the pop-up menu.

Figure 72: Add New MIB Object

The following dialog is displayed:

2. ID—The Object ID (O.I.D.) of the object you wish to add.
3. Name—A descriptive name for the MIB object.
4. Object Type: The data type of the object (i.e. Integer, counter, etc.). Choose an option from the drop-down menu.
5. Access—Define whether the object can be changed. Choose an option from the drop-down menu.
6. Enumerated values—For MIB objects of type Integer, define the possible values for the integer by clicking the Add (or Edit) buttons to the right of the Enumerated Values table. A dialog is then displayed that allows you to define and label the enumerated value.
7. Description—A free-form text description of the object.
8. Absolute value—When selected the current absolute value is used, otherwise the delta between the current poll and the previous poll is used.
9. After you have filled out all of the fields appropriately, Click OK to add the new MIB object to the compiled MIB.
Adding a Trap

1. To add a trap to a compiled MIB, right-click on the Trap branch of the MIB to which you want to add a trap and choose New Trap from the pop-up menu.

Figure 73: Adding a trap

2. The New Trap dialog is displayed

3. Fill out the fields as described below:

<table>
<thead>
<tr>
<th>Name</th>
<th>A descriptive name for the trap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>An integer specifying the generic trap type. How an integer is interpreted is defined by the MIB.</td>
</tr>
<tr>
<td>Enterprise OID</td>
<td>The trap’s base Enterprise Object Identifier.</td>
</tr>
<tr>
<td>Enterprise Name</td>
<td>The name of the last node in the OID chain of the compiled MIB.</td>
</tr>
<tr>
<td>Variables</td>
<td>List the variable data fields bound to the trap, separating variable names with a comma. These are for user reference only.</td>
</tr>
<tr>
<td>Reference</td>
<td>Optional textual cross-reference to a trap, event, or alarm, defined in some other document or MIB module.</td>
</tr>
<tr>
<td>Description</td>
<td>A free-form text description of the trap.</td>
</tr>
</tbody>
</table>

Using the MIB Walker

SNMP MIB Walker lets you walk a MIB to determine what objects it contains. To do this, choose Tools > SNMP MIB Walker.

The MIB Walker automatically browses through the hierarchy of an SNMP Management Information Base (MIB) and displays what objects it contains.

To open SNMP MIB Walker, select Tools > SNMP MIB Walker. If this is the first time you have run the mode, the setup screen is displayed, which allows you to select and configure MIB Walker profiles:

Select a device or click New Device to configure a new device. The MIB walker profile creation dialog includes the following controls:

After you have a profile (or multiple profiles) defined:

1. Select a MIB Walker profile.
2. By default, the initial OID for the walk will be 1.3.6.1.4.1. If you prefer to have your MIB walk begin from another OID, enter it in the Initial OID or use the drop-down arrow if you have recently used another starting point.

3. 1.3.6.1.4.1 is the root of the proprietary part of the MIB tree. A walk from 1.3.6.1.4.1 will give you information on the proprietary OIDs. To get information from the standard OIDs, start the walk at 1.3.6.1.2.1.

4. Click the Start button to start.

5. SNMP Extension’s MIB Walker will step through all higher branches of the MIB tree (starting at the initial OID) and display the results in the Walk Network Device MIB Table Viewer.

<table>
<thead>
<tr>
<th>Profile name</th>
<th>Choose a name that is descriptive enough to be meaningful to you later.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Allows you to enter the IP address to be used for the profile.</td>
</tr>
<tr>
<td>Community</td>
<td>Allows you to enter the community for the profile (public or private).</td>
</tr>
<tr>
<td>SNMP version</td>
<td>Allows you to select the SNMP version.</td>
</tr>
<tr>
<td>Initial OID</td>
<td>Allows you to enter the initial OID.</td>
</tr>
<tr>
<td>Comment</td>
<td>Allows you to enter comments regarding this walk.</td>
</tr>
<tr>
<td>Choose existing SNMP devices</td>
<td>Allows you to pick an SNMP device to create a MIB profile from a list of SNMP devices that have already been defined in or discovered by Observer.</td>
</tr>
</tbody>
</table>

**Viewing the MIB tree**

Selecting the View Tree button from the Walk Agent MIB dialog displays the Walk Agent MIB Tree Viewer. The Walk Agent MIB Tree Viewer displays the structure, although not the values, of the discovered MIB tree.

**Setting values**

One of the main uses of the MIB Walker and the Walk Agent List Viewer is to permit you to explore the SNMP agent by setting values to see what effect different values have on the actual device and to be sure that objects are writable.

1. To set a value, double click any object on the Walk Agent List Viewer. The Set Value dialog will be displayed. Before attempting to make any changes, note the present value, so that you can restore the device to its original state.

2. Type an appropriate real or test value into the Value box.

3. Click the Set Value button. SNMP Extension will attempt to set the given OID to the entered value.

4. If the attempt to set the value succeeds, the dialog box will be redisplayed with the Status line reading Done. Be careful to use the proper type of value when setting the value. If you attempt to set an integer SNMP value to a character string (e.g., Bob) it will be set to zero.

5. If the attempt to set the value fails, an error dialog will be displayed, and the Status line on the Set Value dialog box will read Failed instead of Done.

After completing this task:

Failure can happen for one or both of two reasons:

- The MIB object you are attempting to set is Read-Only and cannot be reset, or
- You do not have the proper read-write community name for this device.
SNMP MIB Walker

The MIB Walker is accessed by selecting an SNMP device from the SNMP Agents pane and clicking Tools > SNMP MIB Walker.

1. To walk an agent MIB, right-click on the desired SNMP Agent in the SNMP Agent pane and select Walk Network Device MIB.

Figure 74: MIB Walker

2. By default, the initial OID for the walk will be 1.3.6.1.4.1. If you prefer to have your MIB walk begin from another OID, enter it in the Initial OID or use the arrow if you’ve recently used another starting point. Note that 1.3.6.1.4.1 is the root of the proprietary part of the MIB tree. A walk from 1.3.6.1.4.1 will give you information on the proprietary OIDs. To get information from the standard OIDs, start the walk at 1.3.6.1.2.1.

3. Click the Start button to start.

4. SNMP Management Console’s MIB Walker will step through all higher branches of the MIB tree (starting at the initial OID) and display the results in the Walk Network Device MIB Table Viewer.

SNMP technical overview

Simple Network Management Protocol (SNMP) was proposed in 1988 as a set of Requests for Comments (RFCs) defining the basic principles and implementation for a protocol that would establish a standard for Internet monitoring and management, as a replacement for the myriad of vendor-specific network management solutions available at the time.

Since then, SNMP has gained considerable popularity. Although it hasn’t replaced all proprietary solutions, it has become a widely accepted standard for network management. Subsequent RFCs for SNMP have corrected problems and supplemented the original standard Management Information Base (MIB).

The standard MIB, defined by RFC1213, defines numerous objects in ten groups—system, interfaces, address translation, IP, ICMP, TCP, UDP, EGP, transmission, and SNMP.

However, manufacturers are constantly adding capabilities to their products, and some of them are not covered by the standard objects and groups. To bring the benefits of SNMP monitoring and control to additional features, software and hardware vendors have developed proprietary MIBs.
Most major computer hardware manufacturers now offer lines of networking products that support SNMP, including network cards, hubs, bridges, routers, switches, and printers. Because adding an SNMP agent to network hardware often increases the price of the product, manufacturers usually offer versions with and without SNMP support.

Most operating systems, including UNIX and Microsoft Windows systems, implement SNMP agents in their architecture.

In early 1990, the original SNMP specifications were revised and updated. New MIB groups were added and some old MIB objects became obsolete. In general, the new MIB specification, called MIB II (or MIB-2) is compatible with the original MIB, now called MIB I.

By the end of 1991, the standard SNMP MIB specification was extended by the Remote Network Monitoring MIB (RMON). RMON provides a set of SNMP objects related to network analysis and monitoring. Information provided by RMON is somewhat different in scope from the typical SNMP information provided by network devices. Usually, a device collects information about the device itself, in connection to either operation of the device or its relationship to the network. The RMON agent, on the other hand, attempts to collect information about network traffic to and from other devices on the network (aside from the agent device), including network statistics, history, information about hosts on the network, connections, and events. An RMON agent can set filters and capture traffic to and from specific devices on the network.

Security concerns related to SNMP prompted development of a secure SNMP called S-SNMP, and the first S-SNMP RFCs appeared in mid-1992. S-SNMP adds security enhancements to the original SNMP protocol but does not offer any additional functionality. S-SNMP is not compatible with the original SNMP.

About the same time, a considerable design effort focused on enhancing the SNMP protocol, incorporating the security features provided by S-SNMP and adding new MIB functionality. The result of this effort is SNMP Version 2, or SNMPv2.

SNMPv2 was not received enthusiastically by many software and hardware vendors. Many had devoted considerable effort to the development of SNMP MIB I and MIB II agents, and in many cases security was not important for users. Most agents currently provided by vendors are SNMP MIB II, not SNMPv2.

SNMP MIB II with proprietary functionality is currently the defacto standard among SNMP users. This overview addresses the general principles of SNMP without addressing the details of SNMPv2.

**General principles**

SNMP is designed around the concept of a relationship between a management station and managed agents. A management station is the location where a network administrator can view, analyze, and even manage local network devices. A management station can be a dedicated computer or workstation, or software running on a general-purpose workstation—like a personal computer running SNMP Extension on Windows 2000/XP.

An SNMP agent is a program that runs on the managed device. It collects information about device operation. For example, if the object is a TCP/IP router, the agent can collect information about network traffic passing through the router and information about the behavior of the router itself under different load conditions.

The SNMP agent maintains a database called the Management Information Base (MIB). The agent uses the MIB to track and systematically update data. Information in a MIB is organized in a tree structure. Each piece of data can be considered a leaf on various branches of the tree. Individual pieces of data are called data objects.

When the management station needs information from an SNMP agent, it sends an SNMP request. SNMP specifications allow the station to ask for more than one MIB object in a single request.

When the SNMP agent receives the request, it searches its local MIB, finds the current values of the requested data, forms a response packet (PDU), and sends the PDU back to the management station.
The management station receives the PDU, decodes it from the SNMP PDU format, and displays the information as a list or in a graphical format that allows the network manager to view, analyze, and modify the information. The following sections review the concepts above in more detail.

**SNMP MIB objects, groups, and addresses**

A MIB is a set of SNMP objects organized in a tree address structure. Each object in a MIB has a unique address called an object identifier, and each branch on the tree is identified by a number. The ISO 8824 specification defines the lower branches of the SNMP MIB tree as:

iso(1).org(3).dod(6).internet(1) or, as expressed in Structure of Management Information (SMI) language, 1.3.6.1 (see illustration).

The SNMP tree resides under the Internet subtree. Four branches after the Internet subtree can be used by SNMP: The directory(1) subtree is reserved for future use by OSI.

- The mgmt(2) subtree includes standard SNMP MIBs I or II (RFC1156 and RFC1213).
- The experimental(3) subtree is reserved for Internet experiments.
- The private(4) subtree provides space for vendor-specific MIBs. All private MIBs are located under enterprises(1) branch. Any private object ID (OID) should begin from the base address 1.3.6.1.4.1.

The address 1.3.6.1.2.1 or iso.org.dod.internet.mgmt.mib represents the address of the standard SNMP MIB I or II on the ISO tree. Inside the MIB branch, SNMP objects are organized beneath higher level branches called MIB groups. Because of the large number of objects—the standard MIB II includes almost two hundred—MIB groups have been created to simplify addressing. Groups consist of related objects: for example, ICMP, TCP, EGP, and other statistics object groups.

The object address is the path from the MIB’s root to an object. For example, the object sysDescr in the MIB(1) System Group has the address 1.3.6.1.2.1.1.1 (see illustration).

**Types of SNMP MIB objects**

SNMP objects accommodate many different types of data in the tree structure, including numbers, text, addresses, bitfield assigned descriptions, and object IDs. Two specifications are used to describe the MIB objects: Abstract Syntax Notation One (ASN.1) and Basic Encoding Rules (BER).

**Abstract Syntax Notation One (ASN.1)**

ASN.1 describes objects in textual MIB descriptions. It describes rules for writing consistent MIBs that compile without errors, both standard and proprietary. ASN.1 includes basic types such as INTEGER, OCTET STRING, OBJECT, NULL, and SEQUENCE.

For example, the following is a sample of the ASN.1 object sysDescr from the MIB II System Group:

SNMP over IPX
Chapter 15: Integrating Observer with HP OpenView or Tivoli

Integrating with IBM Tivoli NetView

Some third-party applications integrate with Observer especially well, and this section describes how to configure them to work in tandem with Observer.

1. On the system running Observer, find and copy the NETINST-MIB.MIB in C:\Program Files\Observer\SNMP to the system running NetView.
2. On the NetView system, in NetView choose **Tools > MIB > Loader**, then click Load and choose the NETINST-MIB.MIB file. Click Load again and the file appears on the Loaded MIBs list in that window.

3. Choose **Options > Trap Settings**, then select NETINST from the Enterprise list.

4. Click the New button, and provide input for the New Trap dialog.
   - **Trap Type**—Default
   - **Trap Name**—choose a name like NIEvent or NICriticalEvent
   - **Event Description**: $A $12 $4

After completing this task:

See the NetView help for an explanation of these and other available parameters for Event Description.

**Integrating with HP OpenView**

All Observer-family analyzers include the tools you need to integrate Observer into Hewlett-Packard’s OpenView administrative interface. This will allow you to see and control Observer-equipped PCs from the HP OpenView administrative interface.

Observer’s HP OpenView integration is compatible with any currently supported version of HP OpenView Network Node Manager (NNM). You must install Network Node Manager from HP OpenView before you can install the Observer integration support files.

To install the Observer support files for HP OpenView integration, simply copy the contents of the NNM directory (located in the HPOV_Integration directory within the Observer installation directory) into the HP OpenView's NNM directory:
1. Browse to the C:\Observer Files\HPOV_Integration directory (or wherever you installed Observer) and right-click on the NNM directory. Choose Copy from the popup menu.

2. Browse to the HP OpenView directory (by default, this will be in the Windows Program Files\HP OpenView directory). Right click and choose Paste from the popup menu. This merges the contents of Observer’s NNM directory with HP OpenView’s NNM directory.

   The next time you start HP OpenView’s Network Node Manager, you can to perform the following Observer functions from within HP OpenView:

3. Launch Observer from HP OpenView’s Tools > Observer menu.

4. Associate an Observer probe instance with the current NNM map. Because Observer may have multiple probe instances, it is necessary to define which Observer probe instance to use when setting filters and capturing packets on a particular map. You will be prompted to define the association the first time you try to set a filter or capture packets. In subsequent sessions the association is remembered.

5. Associate the currently selected network interface object with an Observer probe instance. As a rule, multiple interface objects within an NNM map should be associated with separate Observer probe instances.

6. Set up a filter based on the currently selected node (or pair of nodes, or on the network interface object) from within HP OpenView. This is useful if you want to add additional filter rules (such as filtering for errors) on the NNM-managed nodes. After setting up the filter, you can start capturing the desired packets.

7. Start an Observer packet capture immediately on a network node (or pair of nodes, or on a network interface object) by selecting the object(s) from the NNM map and choosing the corresponding Observer integration menu item. This sets up the correct filter rules and automatically starts the packet capture.

After completing this task:

The packet capture and filter options are also accessible by right-clicking on a NNM network device or interface object. You can also associate a probe instance with a network interface or the NNM map through the right-click menu. If you right-click on an NNM object when multiple objects are selected, the menu actions will only apply to the object that you right-clicked on. To capture packets or set up filters on pairs of devices, select the devices and use the Tools > Observer menu.
Chapter 16: Observer Suite Custom Decode Kit

Using the Custom Decode Kit

The DLL code can be built using the Microsoft Development Studio C++ compiler. The DLL entry points are of extern C type for maximum compatibility.

You can use any other C or C++ compiler as long as the entry point API function definitions are preserved intact and the functions are explicitly exported in a .def file.

A new decode DLL can be renamed to something other than CustomDecode.DLL by changing the output module name and a LIBRARY name in the CustomDecode.DEF file. It is necessary to use multiple, distinct names if Observer Suite is going to use multiple decode DLLs.

Currently, Observer supports up to eight (8) simultaneously loaded custom decode DLLs.

The code can be written in generic C++ or the programmer can create a DLL project with MFC support and include in it CustomDecode.cpp, CustomDecode.h, CustomDecode.def, UserDefinedFunctions.cpp and UserDefinedFunctions.h. In this case, it will be necessary to name the project something other than CustomDecode and to delete the DllMain() function code from CustomDecode.cpp file.

Introduction

Prerequisite: Observer Suite

Observer Suite’s Custom Decode Kit gives an experienced C++ programmer the ability to add custom, proprietary, or additional protocols to Observer decodes.

The Custom Decode Kit is provided as a Microsoft Development Studio v6.0 C++ project. This project should be used as an example and template.

The Custom Decode Kit is an add-on for Observer Suite and is not available with the basic Observer or Real-Time Expert products. To upgrade your Observer to the Observer Suite, please contact your Network Instruments’ sales representative, dealer, or distributor.
Warranty

The Custom Decode Kit is provided as is and without any warranty. Network Instruments does not give technical support for the Custom Decode kit, instruction in C++ programming, or training on how to use the Custom Decode Kit.

Installation

To install the Custom Decode Kit, run CustomDecodeKit.exe. This will, by default, be found in the C:\Program Files\Observer\Drivers\CustomDecodeKit folder. Specify the location where you want to install the Custom Decode Kit. By default, it will install to C:\CustomDecodeKit

Run Microsoft Development Studio and open the Custom Decode project.

How the Custom Decode API Works

The Custom Decode API provides an interface that displays custom decodes in Observer’s decode module. A custom decode is inserted in the protocol decode window (the middle pane in Observer’s Decode and Analysis window).

The purpose of the Custom Decode DLL is to add lines to the Tree Control in Decode and Analysis.

The Custom Decode DLL entry point functions: CustomDecodeFrame(), CustomDecodeIP(), CustomDecodeUDP(), and CustomDecodeTCP() are called from Observer to permit a programmer to add a custom decode.

For example, if you decide to write a decode for UDP port 8765, when your CustomDecodeUDP() function is called, you have to check in the UDP header whether or not the port is 8765.

If it is, you do your decode, adding lines to the Tree Control in a way similar to the CustomDecode sample project. When you are finished, you return TRUE from CustomDecodeUDP().

If the port is not 8765, just return FALSE from CustomDecodeUDP() and Observer will perform the default processing. See the Custom Decode sample project code for more details.

Files Included

The CustomDecode project includes the following files:

CustomDecode.cpp, CustomDecode.h, and CustomDecode.def

These files include four entry point functions, defined as follows:

```
//decode starting at a frame protocol header
extern C BOOL FAR PASCAL CustomDecodeFrame
void * pFrameStart,
void * pProtocolFieldStart,
long nProtocolLength,
long nOffsetFromBeginningOfPacket,
long nBitmapLevel,
DWORD dOpenTreeList,
HWND hwndTree,
void * pPrintStruct);
//decode starting after IP protocol header
extern C BOOL FAR PASCAL CustomDecodeIP
(void * pIpHeaderStart,
void * pIpHeaderStart,
void * pIpDataStart,
long nIpDataLength,
long nOffsetFromBeginningOfPacket,
long nBitmapLevel,
DWORD dOpenTreeList,
HWND hwndTree,
void * pPrintStruct);
//decode starting after UDP protocol header
extern C BOOL FAR PASCAL CustomDecodeUDP (;
void * pUdpHeaderStart,
void * pUdpDataStart,
long nUdpDataLength,
long nOffsetFromBeginningOfPacket,
long nBitmapLevel,
DWORD dOpenTreeList,
HWND hwndTree,
void * pPrintStruct);
//decode starting after TCP protocol header
extern C BOOL FAR PASCAL CustomDecodeTCP (;
void * pTcpHeaderStart,
void * pTcpDataStart,
long nTcpDataLength,
long nOffsetFromBeginningOfPacket,
long nBitmapLevel,
DWORD dOpenTreeList,
HWND hwndTree,
void * pPrintStruct);

In addition, the files include helper functions used in the user-defined sections of the code.

**UserDefinedFunctions.cpp and UserDefinedFunctions.h**

These files include the user code. They contain implementation functions that map all four functions onto user modifiable functions. They also contain a very simple example decode in the SimpleDecodeSample() function.

**StdAfx.cpp and StdAfx.h**

These are the standard Microsoft Development Studio AFX files.

Only an experienced C++ programmer should modify any of the source files in the Observer Suite Custom Decode Kit.
Chapter 17: Probes and Probe Instances

Introducing Probes

As a network administrator, when something goes wrong on your network, seeing what is happening on the wire can quickly lead you to a solution. Use this guide to assist you with choosing, deploying, configuring, and using your probes. The probes, along with the Observer analyzer software, let you see all traffic on the network to which it is connected. To monitor multiple networks from a single analyzer, probes must be installed at every point where network visibility is required.

Probes collect and report network traffic and statistics (usually from a switch) to an Observer analyzer. This enables you to detect and anticipate problems on both local and remote portions of the network. Probes gain insight and visibility into every part of the network, access remote networks as easily as local networks, eliminate the time and expense of traveling to remote sites, and speed troubleshooting.

A probe is a hardware device on your network running Network Instruments probe instance software. Each hardware probe has at least one probe instance that captures packets from your network to analyze. The probe hardware device could be an appliance purchased from Network Instruments or you could install the probe software on your own hardware.

The probe can be located on the same system as the analyzer (every Observer analyzer includes a “local probe”), or the probe can communicate with remote analyzers over TCP/IP.

Probes monitor the following topologies:

- 10/100 Mb, 1/10/40 Gb Ethernet (half- and full-duplex)
- Wireless (802.11 a/b/g/n)

Figure 76 on page 220 shows how probes provide visibility into your network. It may be obvious, but it also shows that you cannot see traffic on portions of your network where you do not have a probe. Finally, you can put the Observer analyzer anywhere on your network so long as it has TCP connectivity to the probe.
What is a probe instance?

The Observer analyzer uses probes to capture network data. In some cases you may want or need more than one probe in a specific location. You can achieve that through probe instances. A probe instance provides you the ability to look at multiple network interfaces, have multiple views of the same interface, or to publish to multiple Observer analyzers.

Observer has only one kind of probe instance: the probe instance. If you have a GigaStor then you have two special probe instance types available to you: the active probe instance and the passive probe instance.

Table 38 on page 220 compares the features of active and passive probe instances with an Observer probe instance found on all non-GigaStor probes.

Table 38: Active vs. passive GigaStor instances and Observer probe

<table>
<thead>
<tr>
<th></th>
<th>GigaStor Active probe instance</th>
<th>GigaStor Passive probe instance</th>
<th>Observer Probe (^1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better suited for troubleshooting</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Better suited for data capture</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start packet capture</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Stop packet capture</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Start GigaStor packet capture</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schedule packet capture</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Change directories where data is stored</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Able to set permissions</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Able to redirect to different analyzer, etc.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

\(^1\) An Observer probe is the Single Probe, Multi Probe, or Expert Probe software running on a non-GigaStor probe.
A passive probe instance may capture packets to RAM and allows you to do reactive analysis or look at real-time statistics for troubleshooting.

The passive probe instance binds to whichever network adapter you want. You can change whichever adapter a passive probe instance is bound to without affecting any active probe instance.

With a GigaStor you have the option of which NIC to bind the passive probe instance. Do not bind any passive probe instances to the Gen2 adapter if at all possible. A copy of all packets is sent from the adapter to every passive probe instance attached to it. If you have several passive probe instances attached to the Gen2 adapter, the Gen2's performance is significantly affected. Instead attach the passive probe instances to either a 10/100/1000 adapter or to a non-existent one.

If you have a passive probe instance connected to a GigaStor, you can mine data that has already been written to the RAID disk by using an active probe instance. There should be one passive probe instance for each simultaneous Observer user on a GigaStor. By using a passive probe instance, instead of an active probe instance, only one copy of data is being captured and written to disk, which reduces the processor load and the required storage space. For troubleshooting and most uses in Observer passive probe instances are appropriate.

By default a passive probe instance uses 12 MB of RAM. You can reserve more memory for passive probe instances if you wish.

An active probe instance on a GigaStor captures network traffic and writes it to the RAID array. An active probe instance should have as large of a RAM buffer as possible to cushion between the network throughput rate and the array write rate.

Like a passive probe instance, it can also be used to mine data from the hard disk, however a passive instance is better suited for the task. An active probe instance cannot start a packet capture while the GigaStor Control Panel is open.

By default there is one active probe instance for GigaStor. It binds to the network adapter and its ports. If you have a specific need to separate the adapter's ports and monitor them separately, you can do so through passive probe instances or you can create separate virtual adapters.

Only one active probe instance per GigaStor.

Set scheduling to Always for the active probe instance so that it is constantly capturing and writing data. Use a passive probe instance to mine the data.

Do not pre-filter, unless you know exactly what you want to capture. Of course, if something occurs outside the bounds of the filter, you will not have the data in the GigaStor.

Do not allow remote users access to the active probe instance.
Figure 77 on page 222 shows how one active probe instance captures and writes to the GigaStor RAID. Passive probe instances 1 and 2 mine data from the RAID array. As a best practice, the passive probe instances are bound to the slowest network adapter in the GigaStor.

Additionally, passive probe instance 3 and 4 are each capturing packets separate from each other and separate from the active probe instance. However, since they are also bound to the same adapter as the active probe instance, they are capturing the same data as the active probe instance.

**Which software probe is right for you?**

For companies that cannot invest in dedicated hardware probes, Network Instruments’ software probes provide a low-cost monitoring option and are easy to install and configure. Software probes support Ethernet, Gigabit and wireless and are appropriate for analyzing speeds of up to 1000 Mbps or for low-utilization gigabit networks via a SPAN/mirror port on a switch. The Observer software can handle fast network speeds (including 40 Gigabit), but it is the network adapter that is the bottleneck on home-grown systems. Network Instruments uses a custom-designed network adapter removing the bottleneck in our probes. These levels of software probes are available:

- **Single probe**—Single probes have only one probe instance and it is not user-configurable. Single probes are appropriate for sites with small administrative staffs where only one user needs to look at a probe at a time. (Not sure what a probe instance is, watch [this video](#).)

- **Multi Probe**—Multi probes may have one or more probe instances. Multi probes allow multiple users to each connect to the probe and use their own probe instance. Each probe instance can be looking at the same packet capture or different capture.
Expert probe—Expert probes are the same as a Multi probe except that they have local expert analysis and decode capabilities in the probe that allows for remote decoding and expert analysis in real time. The Expert probe software comes pre-installed on most hardware probes from Network Instruments.

<table>
<thead>
<tr>
<th>Hardware &gt;</th>
<th>GigaStor, Portable probes, Probe Appliances, 3rd party hardware</th>
<th>Dual port Ethernet Probe, 3rd party hardware</th>
<th>Ethernet Single probe, 3rd party hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed software &gt;</td>
<td>Expert Probe</td>
<td>Multi Probe</td>
<td>Single Probe</td>
</tr>
<tr>
<td>Sends entire buffer$^1$</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Alarms</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trending</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Triggers</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wireless</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encrypts buffer transfer on page 253</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>NIMS support on page 250</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Simultaneous multi-topology support</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Simultaneous users$^2$</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Supports multiple NICs on page 242</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Use reserved memory outside of Windows on page 242</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>User security on page 249</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Able to switch between probe and analyzer mode on page 256</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full-duplex$^3$</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS on page 236</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow on page 265</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port bonding on page 265$^4$</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote decode of GigaStor captures</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sends expert summary &amp; decode packets$^4$</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware &gt;</td>
<td>GigaStor, Portable probes, Probe Appliances, 3rd party hardware</td>
<td>Dual port Ethernet Probe, 3rd party hardware</td>
<td>Ethernet Single probe, 3rd party hardware</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Installed software &gt;</td>
<td>Expert Probe</td>
<td>Multi Probe</td>
<td>Single Probe</td>
</tr>
<tr>
<td>sFlow on page 267</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP expert, APA, ATA on page 255</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1) Buffers are sent to the Observer analyzer where the decoding and analysis is performed. This is less efficient than sending the expert summary and decode packets, which is available with Expert Probe.

2) Simultaneous users are supported when each user has his own probe instance.

3) Only available on hardware probes from Network Instruments.

4) Decoding and expert analysis are performed by the probe and a summary is sent to the Observer analyzer reducing network bandwidth use.

5) Application Performance Analysis and Application Transaction Analysis. Applications are generally OSI Layer7 applications like HTTP, FTP, RTSP, SMB, and so on.

### How probes work with switches

The purpose of a switch is to isolate traffic to the local network, thereby reducing the amount of traffic each device on that network must see and process. Although a protocol analyzer puts a network interface card in “promiscuous” mode, the analyzer only sees packets addressed to or transmitted from the port that it is connected to on the switch.

To operate a probe in a switched environment, you must choose a method that provides network visibility to the port where the probe is connected. Most switches provide a function that “mirrors” all packets received or transmitted from either a single port of interest (for instance, a server or router), or multiple ports of interest. The mirrored traffic can then be captured or analyzed by connecting your analyzer (or in this case, the probe) to the “mirror port” (which is sometimes called a SPAN port).

Switches typically provide two options for configuring the SPAN/mirror port settings. You can either use a command line interface (CLI) or web-based interface included with your switch to set the port (or ports) to be mirrored.

To SPAN/mirror ports, Observer can use SNMP to directly query your switch and report port-based statistics or use RMON to report any internal RMON statistics the switch may have. Selecting the method right for you depends on your switch, and the level of detail you need to troubleshoot the problem at hand. For packet capture, decode and Expert Event identification, only static port mirroring provides all the information required for a complete picture of what is happening on your network.

### Related Topics
- Packet capture buffer and statistics buffer on page 268
- Running Observer with reserved memory on page 270
Expert Probe Software

System requirements and installing or upgrading the software

Prerequisite(s):

- The user running the probe software or Observer—as well as the user installing the software—must have local Administrator rights on the Windows system.
- Standard network cards do not support “raw” wireless packets, nor do they enable “promiscuous” mode by default. Promiscuous mode captures all packets for the analyzer, not just those addressed to the network card. Both “raw” wireless packets and promiscuous mode are required by Observer. ErrorTrak drivers were needed in earlier versions of Observer. They are no longer necessary.
- If you do not meet the minimum requirements, the system may seem to operate in the short term, but be aware that even if a sub-minimum installation works momentarily, a later, heavier load on the system can cause it to fail. Network Instruments sells hardware probes that are guaranteed to keep up with heavy loads. See the Network Instruments website for details.
- You may install the probe software on a virtual machine so long as it meets the system requirements. The installation process is the same. You may also want to consider using a virtual TAP. See Using the probe as a virtual TAP on page 257.

This section describes the installation process and minimum requirements if you are installing the Observer analyzer or probe on your system. This applies to physical and virtualized servers. If you virtualize the server, each server must meet these specifications.

<table>
<thead>
<tr>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Dual core Pentium</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows XP</td>
</tr>
<tr>
<td>Network Card</td>
<td>Server-class</td>
</tr>
<tr>
<td>Capture Card</td>
<td>Server-class</td>
</tr>
</tbody>
</table>

1) If your system has 4 GB of RAM, you cannot reserve any memory for Observer. This is a limitation of Windows known as the BIOS memory hole. Either add more RAM or take some out.

2) Supported operating systems are: Windows XP (32-bit SP3, 64-bit SP2); Windows Vista (32-bit SP1 or higher, 64-bit SP1 or higher); Windows 7 (32-bit SP1 or higher, 64-bit SP1 or higher); Windows Server 2003 Enterprise, Standard, Web (32-bit SP3 or higher, 64-bit SP3 or higher); Windows Server 2008 Enterprise, Standard, Web (32-bit SP2 or higher, 64-bit SP2 or higher); Windows Server 2008 R2 Enterprise, Standard, Web (SP1 or higher)

3) A second network card that acts solely as a capture card is required (and must be in “promiscuous mode”). Alternatively, a dual-port NIC can be used. For further details, see Capture card driver requirements on page 7.

The installer program has two versions of Observer and the GigaStor /probe software: 64-bit and 32-bit. It chooses the one appropriate for your operating system. If the version of Observer or GigaStor that you are upgrading was installed on a 32-bit operating system and you have upgraded the operating system to 64-bit, the installer upgrades existing installation to 64-bit version keeping the same path.

To install or upgrade the Observer analyzer, follow these steps:
1. Insert the installation CD in your CD drive or use the latest installation image from our FTP site. If you copied
the installation files from our web site, start the installation program.


2. When the setup program runs, follow the onscreen instructions.

3. Choose to install:
   - Observer.
   - Advanced Probe. Choose this for Single Probe or Multi Probe. Your license determines whether it is a
     Single Probe or Multi Probe.
   - Expert Probe

4. After the files have been installed on your system you must restart Windows. You will not be able to run the
software until you restart your computer.

After completing this task:
- License your software. See FAQ: Licensing and updating on page 6.
- If you are using a wireless network adapter to capture traffic, see Installing the wireless NIC driver on
  Windows 7/Vista on page 229.
- If you are using a USB wireless network adapter to capture traffic, see Installing a third-party USB wireless
  adapter on page 230.

Comparing software probe features

Single Probes are appropriate for sites with smaller administrative staffs. This type of probe communicates with
only one Observer analyzer at a time.

If you have a need for multiple network administrators to view packet decodes and analysis from the same
probe simultaneously, choose a Multi Probe. The Multi Probe allows you to run multiple probe instances of the
probe on a single system, which means that:
- You can install multiple network interface cards in a single Multi Probe system, allowing multiple “points of
  visibility” from that probe.
- You can connect multiple sessions of Observer to the same Multi Probe system. Any Observer analyzer
  session can see all of the networks available on the Multi Probe. The probe instances are securely encrypted
  and password-protected.

Although Multi Probes behave similarly to Single Probes, the Multi Probe has a different user interface for
configuring the probe.

For the highest level of distributed performance, choose an Expert Probe. AnExpert Probe provides Expert
Analysis and capture/decode capabilities. This saves bandwidth when performing remote expert analysis, and
also allows remote decode views and expert analysis in real time.

The Expert Probe can be configured to run as an Observer analyzer when you need to perform troubleshooting
from where the probe is located.

<table>
<thead>
<tr>
<th>Hardware &gt;</th>
<th>GigaStor, Portable probes, Probe Appliances, 3rd party hardware</th>
<th>Dual port Ethernet Probe, 3rd party hardware</th>
<th>Ethernet Single probe, 3rd party hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed software &gt;</td>
<td>Expert Probe</td>
<td>Multi Probe</td>
<td>Single Probe</td>
</tr>
<tr>
<td>Sends entire buffer</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Installed software &gt;</td>
<td>Expert Probe</td>
<td>Multi Probe</td>
<td>Single Probe</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Alarms</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trending</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Triggers</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wireless</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encrypts buffer transfer on page 253</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NIMS support on page 250</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Simultaneous multi-topology support</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Simultaneous users(^2)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Supports multiple NICs on page 242</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Use reserved memory outside of Windows on page 242</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>User security on page 249</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Able to switch between probe and analyzer mode on page 256</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full-duplex(^3)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS on page 236</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow on page 265</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port bonding on page 265(^4)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote decode of GigaStor captures</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sends expert summary &amp; decode packets(^4)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sFlow on page 267</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP expert, APA, ATA on page 255(^5)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Buffers are sent to the Observer analyzer where the decoding and analysis is performed. This is less efficient than sending the expert summary and decode packets, which is available with Expert Probe.

Simultaneous users are supported when each user has his own probe instance.

Only available on hardware probes from Network Instruments.

Decoding and expert analysis are performed by the probe and a summary is sent to the Observer analyzer reducing network bandwidth use.

Application Performance Analysis and Application Transaction Analysis. Applications are generally OSI Layer7 applications like HTTP, FTP, RTSP, SMB, and so on.

Capture card driver requirements

If you are going to use a third-party capture card in your probe, the capture card must meet certain requirements so that Observer can report statistics and errors. The network card used to monitor or capture network traffic must have all of the mandatory and optional NDIS functions. The Network Instruments Gen2 capture card has all of the necessary features.

Most NIC vendors provide solid, functional NDIS drivers for all cards available within the Ethernet, Token Ring, and FDDI marketplace.

Accessing a standard network with a “normal” network device is somewhat different from what a protocol analyzer requires. While both share a number of driver functions, a protocol analyzer requires a set of features and functions that the average network device will never need. Examples of these optional functions are promiscuous mode, error tracking, and network speed reporting. (Examples of mandatory functions would include functions to determine the maximum packet size, functions to verify the number of sent packets, and functions to specify or determine a packets' protocol.)

Microsoft made a number of the less used (by “normal” network users) functions “optional”, as opposed to “mandatory” regarding driver requirements. The result has been that most vendors support all (or most) mandatory functions with the first release of the driver. As time passes, and the initial chaos of the first release of the card and driver passes, most manufacturers add some or all of the optional functions, as well as fix or complete all of the mandatory functions.

As part of the optional section of defined NDIS functions, Microsoft specified a number of counters that can be kept for Ethernet frame errors. These counters include CRC errors, Alignment errors, Packets Too Big (Jabbers), and Packets Too Small (Runts). Collisions are counted, but there are limitations of NDIS collision statistics. Four important points should be considered:

- These optional counts only provide a numerical value to the total number of errors on the segment (i.e. the number of CRC errors found), they do not specify where (which station) the error originated from.
- After the error packet is identified and the proper error counter is incremented, the packet is discarded, and not sent to Windows (this is the reason it is impossible to determine the source of an Ethernet error packet with standard NDIS drivers).
- A number of vendor’s NDIS drivers return a positive acknowledgment when the NDIS error function is queried for existence, but the error statistic is not actually kept.
- A few vendors (3COM, for example) do not keep any error statistics whatsoever.

If a NIC driver both reports that the optional Ethernet error statistics are being kept, and actually keeps data on these errors, Observer reports these statistics in the Network Vital Sign Display.

How collisions are counted

How collisions are counted by NDIS is a bit different than other errors, and thus a brief explanation is in order. NDIS drivers only count the number of collisions that the actual station where the NDIS driver is running has encountered. For example, if you are running an NDIS driver on station A and there is a collision between
stations B and C, A will not increment its collision counter. If a packet from station A collides with station C (or if C collides with A), then station A’s collision counter is incremented.

In an effort to provide a more realistic view of how many collisions are occurring on a LAN segment, Observer has an option (“on” by default when using the Vital Sign mode) to run the “Collision Test”. When turned on, this test sends packets onto the LAN at specific intervals, and records the number of collisions that the Observer station experiences. This test provides a good idea of what any station may see - with regards to collisions - during normal network usage. The collision statistic reported by Observer is an approximation of what any one station may be experiencing, as opposed to an aggregate statistic for the entire LAN segment (as is the case with CRC, Alignment, Jabbers and Runts).

Additionally, Observer includes the “Collision Expert” that both generates packets to approximate each station’s collision potential, and reports which stations are most likely to re-send directly after a collision and which stations were sending just prior to a collision. This information is then reported in an expert dialog and is key in helping to determine the station(s) that are causing the collisions on the segment.

**Observer’s NDIS drivers for Errors-by-Station**

While the aggregate errors that are kept by NDIS provide a general view on the health of a LAN segment, when a high level of segment errors are encountered, the immediate question becomes “Where are these errors coming from?”. This station specific error information has historically been only available from hardware based protocol analyzers. The reason was that hardware-based analyzers have not been limited by the aggregate statistics provided in NDIS. That is not a limitation of Observer.

Network Instruments has worked with a number of NIC vendors and chip manufacturers to extend the standard NDIS drivers to both collect statistics on the aggregate errors on a LAN segment, but also to move the actual error packet information up the NDIS stack for further examination by Observer’s error displays. This allows Observer to report both general error statistics and error source addresses to help pinpoint troubleshooting down to the specific station with a problem.

Using the extended NDIS drivers included with Observer, administrators and technicians can see complete network errors broken down by type and (source) station. This can be done from within the standard Windows environment, without the need to re-boot, without proprietary drivers, and without sacrificing any standard network functionality. This dual functionality is achieved because the Network Instruments NDIS driver is a highly optimized NDIS driver with the addition of a module to collect and process error packets – these drivers have all the functionality of a standard NDIS driver, plus the ability to pass error packets to Observer.

*Installing the wireless NIC driver on Windows 7/Vista*

See the information in Monitoring a wireless access point on page 256, which contains details about raw packets and promiscuous mode for the network card.

Follow these instructions to install the wireless driver for your network card:

1. Click Start and then right-click on the ‘Computer’ icon and choose Properties.
2. Click Device Manager.
3. Right-click on the wireless adapter you want to use as your capture card and choose Update Driver Software.
4. Choose “Browse my computer for driver software.”
5. Choose “Let me pick from a list of drivers on my computer.”
6. Click Have Disk and use the drivers in this location:
   
   C:\Program Files\Observer\DRIVERS\Wireless\Atheros_Vista

7. Click Next and Windows installs the driver for your wireless card.

To confirm that you correctly installed the driver for the wireless network card, open Observer. If the probe instance shows (Wireless) behind it, then it is correctly configured.
Figure 78: Probe instance using wireless adapter

If the probe instance shows (Ethernet), then either the network card driver was not correctly installed or the probe instance is not configured to use that network card. You can confirm the correct network card is selected, by choosing Actions > Select Network Adapter Card.

After completing this task:

- License your probe by following the instructions in Licensing and updating on page 6.
- If your wireless network uses an encryption key, you must add the encryption key information. See Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling on page 243.

Installing a third-party USB wireless adapter

The Belkin F9L1101v1 N600DB USB wireless adapter was tested for use with your systems. The USB wireless adapter is only supported on systems running Windows Vista or 7 (32- or 64-bit).

**Note:** Only Belkin N600DB USB wireless adapters with the revision number “F9L1101v1” are compatible. These adapters have a Broadcom chipset. The second revision, “F9L1101v2” does not have a Broadcom chipset and is incompatible.

**Caution!** For some wireless adapters you must install the software for the USB wireless adapter before you attach the adapter to your computer. This is not an Observer requirement, but one of the wireless adapter. If you attach the USB adapter before installing the software, unplug the USB adapter, uninstall the software, restart your system, and then proceed with 1 on page 230.

1. Install the software that came with your USB wireless adapter.
2. Attach the USB wireless adapter to your system.
3. Choose Control Panel > Network and Sharing Center > Change adapter settings and then select your USB wireless adapter. Right-click and choose Properties.
4. On the Networking tab, click Install > Service > Add. Click Have Disk and locate this file: NiNdismon.inf
   - 64-bit: C:\Program Files\Observer\DRIVERS\Wireless
   - 32-bit: C:\Program Files (x86)\Observer\DRIVERS\Wireless
5. Click OK to install the software as Windows service.
6. Restart your system. This allows the software and the adapter to be fully recognized by your system and the Windows service to start. Observer will not be able to use the wireless adapter until you restart.
7. Start Observer, select the probe instance you want to associate with the USB wireless adapter, and choose Actions > Select Network Adapter Card.
8. Choose the USB Wireless Adapter you just installed.

The probe instance is now configured to use the USB wireless adapter. You can confirm this because the word "[Wireless]" appears after the probe instance name, and the Wireless 802.11 tab of the probe instance is visible.
Installing Windows updates and updating virus protection

From time to time Microsoft releases updates for the operating system used for your probe or your virus protection software vendor updates their virus definitions. You should apply those updates as soon as feasible, however, you should always apply the updates manually. We do not recommend that you allow Windows to automatically install the updates and restart the system. By manually applying the updates you ensure that the system restarts properly and that the probe starts correctly whether running as a Windows service or as an application.

For your antivirus software, follow these guidelines:

- Ensure TCP ports 25901 and 25903 are open. All Network Instruments products communicate on these ports.
- Ensure UDP ports 25901 and 25903 are open if you use NIMS.
- For all probes, disable any scanning of the Observer installation directory (typically C:\Program Files\Observer) and of D:\ (RAID) drive as scanning greatly diminishes the performance of writing data to disk.
- The performance of the operating system may be greatly diminished when using antivirus software.

Upgrading the probe software

The Observer analyzer and probe software must be within the same major release. This may require you to upgrade your probe software.

The installer program has two versions of Observer and the GigaStor/probe software: 64-bit and 32-bit. It chooses the one appropriate for your operating system. If the version of Observer or GigaStor that you are upgrading was installed on a 32-bit operating system and you have upgraded the operating system to 64-bit, the installer upgrades existing installation to 64-bit version keeping the same path.

When upgrading to version 16, if your operating system is 64-bit, the 64-bit version of Observer or GigaStor is installed. If you previously installed a 32-bit version, the same installation directory is used.

Use information from this section when upgrading to a new major version of the probe software. Before upgrading have the following available:

- Your probe license information.

If you are using encryption keys with Observer, you can continue to use your existing keys or transfer them to your probe (and analyzer) as necessary.

Upgrading the probe software directly

On the probe:

1. Run the ObserverSetup.exe installation program. Follow the on screen instructions and choose your probe type.
2. After the installer completes, restart the system. New major builds may have new drivers or other files that require a restart.
3. Connect the probe to an Observer analyzer.

Remotely upgrading the probe software from within the Observer analyzer

The Observer analyzer can push an upgrade of the probe software to the probe. When upgrading the probe software, you must restart the probe, and because of this, you should schedule the upgrade at a convenient time for the probe’s users.
If the probe software is running as a Windows service, you can choose to have the probe restart automatically. This is a configuration option in the probe’s settings and especially useful for remote probes where there is not a local administrator. See Configuring a probe’s name and other probe options on page 239.

1. In the Observer analyzer, select the probe instance you want to upgrade. Right-click and choose Probe or Device Properties. The Probe Properties window opens.

2. Click the Observer Autoupgrade tab. The Autoupgrade tab has three options:
   - Upgrading within minor versions (for instance, 15.0 to 15.1)
   - Upgrading within major versions (for instance, 15.0 to 16.0)
   - Forcing the autoupgrade of the probe

3. Select the second option: Autoupgrade Probe for major version release.

4. Click the Enter Licensing Information button.

5. Provide your probe’s license information. Click OK to close the licensing window.

6. Give the probe a few minutes to receive the new software version. The log window in the Observer analyzer shows that the analyzer is connecting to the probe and pushing the upgrade to the probe.

7. If the probe has not reconnected to the analyzer in about ten minutes, you may need to use Windows Remote Desktop to ensure that the probe is not displaying a Windows system message about restarting the system.

FAQ: Licensing and updating

Some customer concerns deal with licensing and updating issues. Explore this good resource for licensing and updating help, or call the Technical Support department for further assistance.

Network Instruments probes must be licensed before use. If your probe is not licensed, the licensing dialog appears the first time the program is run.

Probes require two unique numbers for licensing: an identification number and a license number.

Note: Your license number (for your product version) is based on your identification number, and your identification number is based on your real name and company name.

The license number determines whether the probe is a Single Probe (one probe instance) or a Multi Probe (capable of running multiple probe instances and allowing multiple Observer analyzers to connect simultaneously).

When you first open a probe, it prompts you for license information. These executable files, found in the Observer installation directory, are the probes and must be licensed.

- Single and Multi Probe: NiProbe.exe
- Expert Probe: observer.exe

If the software is already running, choose Help > License.

After the software is licensed, you can begin using it.

What type of license do I have?

The type of license you have is described in your license document. Each license document contains a license number, and the document describes which version of Observer the license number applies to. If it does not, or you notice any other error, please call our support team for assistance.
Why is my license number not working?

Each license number is case-sensitive, so be sure to type it in exactly the way it was given to you. Also, if you copy-pasted the license number into the activation prompt, be sure you did not introduce a leading or trailing space character—those are not part of your license number.

Also, ensure you are licensing the correct version of Observer. License numbers are version specific. Each license number works only within equal major version numbers of the product. For example, an Observer 16.0 license can be used to activate 16.0 and 16.1, but not 15.0, 15.1, etc.

If you are still unsuccessful, please call our support team so we may assist you, whether that entails sending a correct license number or to discuss the upgrade policy for that product.

Could I have my license re-sent to me?

Yes. If you lost the original information containing your license number, please contact us so we can resend your license document(s).

Should I uninstall Observer before updating it?

First, verify that you are licensed to use the Observer version you wish to update to.

If you wish to update your existing Observer software to a newly released version within the same major release number, you do not need to uninstall your existing version for the update process to succeed. Simply install the new version over the old.

As with all software, it is a best practice to back up your existing installation and settings before updating to a new version.

**Backing up your Observer**

You can back up most Observer settings and configuration data. Backups are useful when migrating to new hardware or recovering from data loss.

Your Observer may not have each directory and file referenced in this topic, but you can back up any it does. Use whatever backup method or software is best for you, which, at a minimum, would be manually copying these to a different drive.

To back up many Observer settings and files, do the following:

1. Copy the files and directories in Table 39 to a backup location.

    These are the default installation directories that contain Observer settings and configuration data:

    # For 32-bit Windows: C:\Program Files (x86)\Observer
    # For 64-bit Windows: C:\Program Files\Observer

**Table 39: Directory or files to back up**

<table>
<thead>
<tr>
<th>Directory or file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Trending</td>
<td>C:\Program Files\Observer\NetworkTrending</td>
</tr>
<tr>
<td></td>
<td>This contains your Network Trending data. If you have changed the default location for Network Trending data, you must to back up the new location.</td>
</tr>
<tr>
<td>Directory or file</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Protocol Definitions</strong></td>
<td>C:\Program Files\Observer\ProtocolDefs &lt;br&gt;This contains any modifications or additions you have made to the protocol definitions list for each probe instance. Back up in all cases.</td>
</tr>
<tr>
<td><strong>Multicast Definitions</strong></td>
<td>C:\Program Files\Observer\MulticastDefinitions &lt;br&gt;This contains the templates for defining trading multicast streams for Network Trending. Back up if you use trading multicasts in Network Trending.</td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>C:\Program Files\Observer\Settings &lt;br&gt;This contains alarms and triggers. Back up if you heavily use alarms or have alarm/trigger customizations that need to be retained.</td>
</tr>
<tr>
<td><strong>SNORT Rules</strong></td>
<td>C:\Program Files\Observer\Forensics &lt;br&gt;This contains your SNORT information, such as rules, for detecting malicious activity in your packet captures. Back up if you use SNORT.</td>
</tr>
<tr>
<td><strong>Expert Thresholds</strong></td>
<td>C:\Program Files\Observer\ExpertSettings &lt;br&gt;This contains your thresholds stored in Expert settings. These include TCP/UDP events and some triggers for problem identification. Back up if you have modified any Expert thresholds and want to retain those customizations.</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td>C:\Program Files\Observer\SNMP &lt;br&gt;This contains any custom MIBs, compiled MIBs, request files and SNMP trending data. Back up if you have made SNMP changes or have SNMP trending data. Use Options &gt; Observer General Options &gt; Folders tab to verify which folder is used for SNMP.</td>
</tr>
<tr>
<td><strong>Address Tables</strong></td>
<td>C:\Program Files\Observer\LocalAddressTable &lt;br&gt;This contains your Discover Network Names list. Back up if you have run Discover Network Names and have saved the alias list.</td>
</tr>
<tr>
<td><strong>C:\Program Files\Observer\ProbeAddressTable</strong>&lt;br&gt;This contains the Discover Network Names list from any remote probe that has connected to this Observer analyzer. Back up if you have run remote Discover Network Names and saved the alias list.</td>
<td></td>
</tr>
<tr>
<td><strong>Scripts</strong></td>
<td>C:\Program Files\Observer\Scripts &lt;br&gt;This contains the scripts for Observer. Back up if you have created or modified a script.</td>
</tr>
<tr>
<td><strong>Windows Registry</strong></td>
<td>Using Regedit export the following registry key: &lt;br&gt;32-bit Windows OS running any version, or 64-bit Windows OS running version 16 or higher: &lt;br&gt;HKEY_LOCAL_MACHINE\SOFTWARE\Network Instruments &lt;br&gt;64-bit Windows OS and running version 15 or older: &lt;br&gt;HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Instruments</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>Make note of the license information in Help &gt; License Observer. You need the contact/department, company, identification number, and license number.</td>
</tr>
</tbody>
</table>
Creating a probe instance

**Prerequisite:** Multi or Expert Probe.

When you open Expert Probe for the first time, you assign memory to a probe instance. You can choose to use this one probe instance, or you can create other probe instances. Multiple probe instances are useful if you need multiple users using the same probe simultaneously or if you have specific needs for each probe instance (for instance, packet capture, trending, and so on). See Configuring connections to multiple NICs or Observer analyzers on page 242 for why you would want to use multiple probe instances.

**Note:** There are several different probe instance types. These include a packet capture-based probe instance used to capture packet traffic, two NetFlow collectors, an sFlow collector, and an MPLS probe. This section describes creating a packet-based probe instance, but the process is similar for the other probe instances, some of which are only available on the Expert Probe. For NetFlow, see Creating a NetFlow collector or NetFlow Trending collector on page 265. For MPLS, see Creating and configuring an MPLS probe instance on page 236. For sFlow, see Creating an sFlow collector on page 267.

To set up a probe instance, follow these steps:

1. Do one of the following:
   - On the probe: Click the Adapters and Redirection tab.
   - In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Adapters and Redirection tab.

2. In the upper left, click New Instance. The Edit Probe Instance wizard opens.

   If the New Instance button is grayed out, it probably means you do not have enough Observer-allocated memory to add another instance.

   If you get a message that says that there is not enough reserved memory to create a probe instance, you must reduce the amount of memory used by another probe instance. By default all of the reserved memory on a GigaStor is assigned to the “Instance 1” active instance. By releasing some of the reserved memory you re-allocate memory from one probe to the pool of reserved memory from which you can create other probe instances, including passive probe instances on the GigaStor. Click the Configure Memory button and reduce the amount of memory for the packet capture buffer.

   You must have a minimum of 256 MB RAM to run the probe with a single instance, plus 12 MB for each additional probe instance. See Setting the total system memory reserved for probes on page 242 for details on allocating memory for Observer probes.

3. Ensure “Probe” is selected in the Instance type. Type a name and description and click Next.

4. Choose an appropriate capture buffer size given the local system's available memory and how much traffic you plan on capturing from the given network.

   Statistical reporting uses different memory—and much less of it—than packet capture.

   Although it is possible to customize the amounts of memory used by various Observer statistical displays (by choosing a statistics memory configuration), for most situations the defaults work perfectly well. For additional information, see Customizing statistics and capture buffers for probe instances on page 241.

   a. If you need to create your own memory configuration, click New. The New Statistics Memory Configuration window opens.

   b. Type a name and choose a default memory configuration to use. Click Finish. After choosing the memory configuration, you can change how the memory is allocated.
c. Select your newly created memory configuration and click Edit. The Edit Statistics Memory Configuration window opens.
d. Choose your network type. For each Observer statistic, choose how much memory is allocated for it. Click OK.
e. Click Next to continue, and the Select Network Adapter and Redirection configuration dialog is displayed.

5. Ensure the correct network adapter is selected and type the IP address of your Observer analyzer. Click Finish.

Creating GigaStor active and passive probe instances

**Prerequisite**: Expert Probe

This feature is only available when you are using the Expert Probe *locally* on a GigaStor probe. It is not available if you connect to the Expert Probe from a remote Observer analyzer.

If your GigaStor RAID has more than 256 TB, see [Using additional storage volumes for your GigaStor active instance on page 237](#) before continuing.

By default, the GigaStor has an active probe instance called “Instance 1” but does not have any passive probe instances. We recommend that you

- Rename the active probe instance by selecting Instance 1 and clicking Rename. Choose a name that is meaningful to you for the probe instance name and click OK. A typical name might be the physical location of this GigaStor.
- Have only one active GigaStor instance, unless you have specific reasons to have more.
- Create passive probe instances to use.
- See details about active and passive probe instances discussed in [What is a probe instance?](#).
- After creating your active instance, if you want to change how much disk space is reserved for that active instance, click Configure Instance Storage.

To create a passive probe instance, follow the steps in [Creating a probe instance on page 235](#). When you create a probe instance for an Expert Probe on GigaStor, it is automatically created as a passive probe instance.

If you want to change a passive probe instance to an active probe instance, follow these steps.

1. Do one of the following:
   - On the GigaStor probe: Click the GigaStor Instances tab.
   - In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the GigaStor Instances tab.

2. Select the passive probe instance you want to promote to an active instance and right-click.
3. Choose Make Instance Active. Your passive probe instance is now an active probe instance.

After completing this task:

You should then create passive probe instances for it.

Creating and configuring an MPLS probe instance

**Prerequisite**: Expert Probe

See [Creating a probe instance on page 235](#) for details about creating an MPLS probe instance. In 3 on page 235 choose MPLS Probe and follow the on-screen instructions.

After the probe instance is created, you may want to configure the probe to tell it what type of traffic is seen.

1. In Observer analyzer, select a probe instance, right-click and choose Probe or Device Properties. The Probe Properties window opens.
2. On the General tab, use the options in the MPLS Analysis Settings to choose whether Observershould auto
determine IPv4 and IPv6, what all other traffic is (ATM or Mac Header), and whether to use a four byte
pseudowire word.
3. Click OK.

**Using additional storage volumes for your GigaStor active instance**

**Prerequisite:** Expert Probe

The maximum NTFS disk volume is 256 TB, but with a GigaStor you can have more storage than that by using
the expanded disk arrays or striping through Windows. If you have expanded your disk array beyond 256 TB, for
performance reasons you will want to add the additional volumes to your GigaStor active instance.

**Note:** This feature requires a special license key. Contact your Network Instruments sales person
for that key. After you have the license key, enter it on the GigaStor probe by choosing Help > License
probe. This enables the necessary feature.

1. On the GigaStor probe, click the GigaStor Instances tab.
2. Select the “Use additional storage volumes” option and click Configure. A message box appears, click Yes.
3. Select the additional storage volumes you want to assign to your active probe instance and click OK.
4. A message box appears, click Yes and the additional storage is allocated. This may take a few moments.

**Changing the monitored network adapter**

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe
on Network Instruments or third party hardware.

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe
on Network Instruments hardware.

If your probe has multiple network cards in it, you can choose which card you want to monitor.

If you have a network card in your system, but it is not being seen or recognized by Observer, follow the
instructions in No network adapter available.

If you are seeing only broadcast traffic, you do not have the correct network card selected or you do not have
your switch port configured correctly as a SPAN/mirror port. Change the network adapter you are monitoring or
configure the SPAN/mirror port.

1. When choosing the monitored adapter from within the Observer analyzer for all probe versions:
   a. In the Probes list, select the probe instance.
   b. Choose Actions > Select Network Adapter Card. The Select Network Adapter window opens.
   c. Select the network adapter you want to monitor and click Select.
2. When choosing the monitored adapter on the probe for Multi Probe and Expert Probe:
   a. Click the “Adapters and Redirection” tab.
   b. Select your probe instance and click the Configure Adapter/Redirection button. The Edit Probe Instance
      window opens.
   c. In the Selected Network Adapter section, change the network card you are monitoring.

The probe instance is now using the newly selected adapter.

**Connecting to a probe for the first time from the Observer analyzer**

1. In the Observer analyzer, select Actions > Redirect Probe.
2. Click New to add the probe to the Probe Administration and Redirection list.
3. Type the IP address that you assigned to the probe and click OK. You may leave the other fields blank. If you type a name, the name will change after the Observer analyzer connects to the probe. The probe appears in the list of available probes.

4. Select the probe and then click Redirect Selected Probe.

5. Select the probe instance and click Redirect Selected Instance.

6. Choose the “Redirect to this Observer” option, then click the Redirect button. Within 30 seconds the probe will connect with the analyzer.

   Probe redirection can be password protected or disabled. Please see Connecting the Multi Probe or Expert Probe to an Observer analyzer on page 238 for details. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling on page 243.

7. Close the Probe Instance Redirection window.

Connecting the Multi Probe or Expert Probe to an Observer analyzer

Prerequisite: Multi or Expert Probe.

There are two ways to connect the probe to an Observer analyzer. The method described here is from the perspective of the probe. All actions are done on the probe itself.

Each probe instance can be connected to only one Observer analyzer at a time. Connecting the probe instance with the analyzer is called “redirecting” it. This is because the probe instance may not be connected to any Observer analyzer or it may be connected to a different Observer than the one you want to connect it to. The connection can be done from within the analyzer or from the probe. This section describes how to redirect a probe instance from the probe and assumes that the probe software is running and that you already have a probe instance.

1. Click the Adapters and Redirection tab.

2. Select the probe instance you want to redirect and click the Configure Adapter/Redirection button at the top. The Edit Probe Instance window opens.

3. Select the “Redirect to a specified IP address or DNS name” option and provide the IP address or DNS name. When the probe instance is connected the “Redirected to” column lists the IP address of the Observer analyzer system. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa.

4. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.

Connecting to a probe instance from an Observer analyzer

Prerequisite: Multi or Expert Probe.

Probe instances can be redirected from one Observer analyzer to another or disconnected from any analyzer. This is done from the Observer analyzer.

1. In Observer, select Actions > Redirect Probe.

2. Select the probe instance you want to redirect and click the Redirect Selected Probe Instance button at the bottom. The Edit Probe Instance window opens.

3. If this is the first time you are connecting to the probe from the Observer analyzer, you must add the probe to your list. See Connecting to a probe for the first time from the Observer analyzer.

4. If the probe is not connecting, Probe redirection might be password protected or disabled. Please see Connecting the Multi Probe or Expert Probe to an Observer analyzer for details. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa.

5. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.
Connecting the probe to an Observer analyzer

There are two ways to connect the probe to an Observer analyzer. The method described here shows you from the perspective of the probe. The second way is described in Connecting the Multi Probe or Expert Probe to an Observer analyzer on page 238. All actions are done on the probe itself.

1. Choose **Options > Probe Redirection Settings**. The Probe Redirection Settings dialog opens.
2. Use Table 8 to complete the settings. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa.

<table>
<thead>
<tr>
<th>Observer IP address</th>
<th>Type the address of the Observer analyzer you want this probe to connect to.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Probe redirection for remote users</td>
<td>Allows remote users to redirect the probe to their Observer analyzer. If you want the probe to be able to connect to only one Observer analyzer, leave this option unchecked.</td>
</tr>
<tr>
<td>User name</td>
<td>By default any user can connect to the probe and no password is required.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the user account.</td>
</tr>
</tbody>
</table>

3. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.

Configuring a probe’s name and other probe options

The probe has many options that you can configure.

1. Choose **Options > Probe Options**. The Probe Options dialog opens, which lets you configure the probe.
2. Use this table to complete the settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe name</td>
<td>Allows you to specify a name for the probe which appears in the Observer analyzer probe list. The default name is a random mix of numbers and letters. We suggest renaming the probe to something meaningful to you. The name may be its physical location or any other standard you choose. The probe name is not the same as the probe instance name, although with a Single Probe you only have one probe instance. You define the probe instance name elsewhere. See Creating a probe instance on page 235.</td>
</tr>
<tr>
<td>Network trending folder</td>
<td>Allows you to specify where the network trending data is saved. The default is C:\Program Files\Observer\NetworkTrending. Unless you have a specific reason to use another directory, we suggest using the default.</td>
</tr>
<tr>
<td>Folder for GigaStor</td>
<td>Allows you to specify where the GigaStor and network packet data will be saved. The default is C:\Program Files\Observer\Data. Unless you have a specific reason to use another directory, we suggest using the default.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Maximum IP DNS resolution entries</td>
<td>Defines the maximum number of DNS entries the probe should maintain. The probe will keep up to the number of entries defined or what the probe can maintain in 10 MB, whichever is less. The probe keeps the first 1000 entries (or whatever amount you define) it sees; it does not keep a rolling list of the last 1000. After the limit is reached, no more entries are kept. They are discarded.</td>
</tr>
<tr>
<td>Use Observer Encryption Key file for secure connections</td>
<td>If selected, the probe will not connect with an analyzer unless a matching Observer Encryption Key (.oek) file is present. The .oek file must be in both the analyzer and probe installation directories. See “Encrypting the data sent between the probe and analyzer on page 253” for details.</td>
</tr>
<tr>
<td>Use Network Instruments Management Server at IP Address</td>
<td>Choose this option if you have licensed and installed NIMS. NIMS centralizes user/password administration superceding the probe security tab settings. Matching Observer Encryption Key files are required in the installation directory of both analyzer and probe for the connection to complete. Not available for the Single Probe.</td>
</tr>
<tr>
<td>Manage licenses with NIMS</td>
<td>Select this option if you are using NIMS to manage your licenses. Provide the primary and secondary server addresses. You may choose to export them for use on another system. Not available for the Single Probe.</td>
</tr>
<tr>
<td>Run Probe as Windows Service</td>
<td>Select this option if you want to run the probe as a Windows service. This allows the probe to start without requiring a user to log in and start the probe. The probe starts whenever the system starts, which can be especially important for a remote probe. The change takes effect on the next system restart. When running the probe as a Windows service, some options are available to you that you do not have when running the probe as an application. Specifically, you can set Networking Trending and see CPU load of each probe instance. In both modes, you can configure memory management, configure security for each probe instance, reserve Windows memory for the probe, adjust for time drifts through clock synchronization, and enable the probe to be a virtual TAP.</td>
</tr>
<tr>
<td>When running as a service, allow autoupgrade</td>
<td>Allows you to elect to have the system restart automatically after the probe is upgraded. Will restart the probe only if probe runs as a Windows service.</td>
</tr>
<tr>
<td>Enable Probe HTTP responder</td>
<td>Allows you to enable the Web Probe Snapshot. The probe offers a “snapshot” of general data by connecting to the probe using a standard web</td>
</tr>
</tbody>
</table>
### Customizing statistics and capture buffers for probe instances

**Prerequisite:** Multi or Expert Probe.

Before changing any of the buffer sizes, you should understand how any changes you make affects the probe. See [How a probe uses RAM on page 267](#).

- To change memory allocation for probe instances, see [Running Observer with reserved memory on page 270](#).
- To fine-tune the Statistics Memory Configuration, see [Tweaking the statistics memory configuration](#).

#### Setting | Description
--- | ---
Browser. Information includes the state of the probe and the general network statistics that the probe displays within its own interface.
Open your web browser to http://probe_host_name. The probe sends more extensive and specific statistics to Observer than is available through the web interface.

**Auto-refresh Web page every 10 seconds** | Allows you to configure the probe to refresh the browser display every 10 seconds.

**Probe HTTP port (default=80)** | Allows you to specify which port to use for reporting of web information. For example, if your probe’s web server is configured to use port 3605, the URL is http://probe_host_name:3605.

**GigaStor data analysis time slice** | Available only when using Expert Probe software on a GigaStor.
If your GigaStor is writing data to disk at near capacity of the disk speed and you then mine data from the disk, it is possible that the GigaStor will drop some packets from being written to disk. You can prevent this by reducing the data analysis percentage from 100% to something lower. Writing to disk will always be 100%, the reading or mining of data will be at the percentage you choose. The tradeoff is that all packets are captured, but data mining is slower. You must find that balance that is right for you and your users.

**GigaStor Capture Payload Encryption** | Available only when using Expert Probe software on a GigaStor.
If you want the GigaStor payload to be encrypted using 256 bit AES encryption before it is stored, select the “Encrypt GigaStor network traffic…” option. An encryption key is needed on the GigaStor (or a location accessible by the GigaStor) to encrypt and decrypt the data. The AES key is not needed on workstations, probes, or other collection points; however you must generate the key from an Observer analyzer. A special license is required for this feature. Contact Network Instruments for this license.
Configuring probes to collect data even when not connected to an analyzer

Probes (and probe instances) can be configured to collect data only when you tell it to—including manually starting/stopping the collection, having collection always running, or based on a schedule. The schedule and settings are saved with the probe instance. This means if you choose to have packet capture always running or running on a schedule that the probe instance does not need to be connected to an Observer analyzer.

To configure when packet capture should run, complete these steps:

1. In Observer, select a probe instance in the Probes list.
2. Choose Capture > Packet Capture. The Packet Capture window opens. Along the top of the window are several buttons, including Start, Stop, Settings, and Decode.
3. Click the Settings button. The Packet Capture Settings window opens.
4. Click the Schedule tab.
5. Choose the schedule you want (Always, daily, or specific days).
6. If you want to control the capture buffer’s size, click the Capture Options tab. The data is saved on the probe in C:\Program Files\Observer\Data.

Setting the probe’s time clock synchronization settings

At times your capture card drivers time clock may drift. They can be synchronized with the system clock, if you wish. Unless you notice a reason to enable this feature, we recommend that you do not synchronize your capture card’s time clock. Some Other things to consider:

- The capture card synchronizes itself with the system clock at when the system starts.
- Generally, you are interested in relative time between packets, not the actual time a packet was seen. If you need to have very accurate times, then consider using an external time server on your network, or by using the optional GPS timing device for Network Instruments’ Gen2 cards. See ../gsprobes/ connecting_your_gigastor_to_a_gps_system.html.

1. Do one of the following:
   # On the probe: Click the Synchronization tab.
   # In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Synchronization tab.
2. Click the Edit Schedule button.
3. Choose when and how you want the capture card’s time clock to synchronize with the system clock and click OK.

Configuring connections to multiple NICs or Observer analyzers

Prerequisite: Multi or Expert Probe.

With a Multi Probe, you can configure the probe to view multiple networks if multiple NICs are installed on the local system and to provide multiple Observer analyzers with views of the local network interfaces.

The probe accomplishes these capabilities by allowing multiple instances of itself. A probe instance is a virtual probe with attributes that define:

- Which network interface on the local system to capture data from.
- Which Observer analyzer (local or remote) to direct the data to.

Setting the total system memory reserved for probes

Prerequisite: Multi or Expert Probe.

Memory use is an important and vital part of using an Observer probe successfully. Before changing any of the reserved memory, you should understand how any changes you make affects the probe.
Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on Network Instruments or third party hardware.

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on Network Instruments hardware.

After connecting the probe instance to the Observer analyzer, there still may be some additional configuration that you must do. This is completely dependent on your network environment and your needs.

In the Observer analyzer:

1. Select a probe instance in the Probes list.
2. Right-click and choose Probe or Device Properties.
3. Use the following tabs to further configure the probe for your environment. Not all of these tabs are present at all times. What tabs are visible depends on the type of probe you are configuring. For instance, the Gigabit tab is only visible when you are configuring a Gigabit Probe. For details about the fields on each tab, see the online help.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Set the statistics sampling divider and MPLS settings. For field descriptions, see Table 40 on page 244.</td>
</tr>
<tr>
<td>Adapter speed</td>
<td>Verify that the adapter speed is registering correctly. Change the adapter speed if necessary. Changing the adapter speed here may be useful and necessary, because statistics, graphs, and reports generated by Observer are set using the adapter speed as the maximum. If, for some reason, Observer is not able to correctly identify your adapter speed your reports may be inaccurate. For field descriptions, see Table 42 on page 245.</td>
</tr>
<tr>
<td>Autoupgrade</td>
<td>Choose whether you want your probe to be automatically upgraded when a newer version is available; that is, the Observer analyzer is a newer version than the probe to which it is connecting. See Remotely upgrading the probe software from within the Observer analyzer on page 231. For field descriptions, see Table 43 on page 245.</td>
</tr>
<tr>
<td>ToS/QoS</td>
<td>Ensure these settings match your needs paying particular attention to the IP precedence bit for the ToS/QoS of your network. What you set here affects how the Observer analyzer displays information about VoIP, NetFlow, sFlow, and capture decodes. For field descriptions, see Table 44 on page 246.</td>
</tr>
<tr>
<td>Gigabit</td>
<td>Define the maximum frame size for your network. The default is 1514 bytes (excluding the frame checksum), which is appropriate for standard Ethernet. If the network link you are analyzing is configured to support jumbo frames (frames larger than 1514 bytes), you may want to change this setting to match the frame size of the Gigabit network, up to a maximum size of 9014 bytes. Observer will then discard frames that exceed this maximum frame size, generating a “Frame too large” error.</td>
</tr>
<tr>
<td>Wireless 802.11</td>
<td>Define what channels you want to monitor, what antenna you use for the wireless card, and your wireless encryption key if you use one for your network. See Monitoring a wireless access point on page 256. For field descriptions, see Table 45 on page 246.</td>
</tr>
<tr>
<td>D3/E3/HSSI</td>
<td>Choose your WAN type, then choose the frame check sequence standard. You must set encapsulation to match the frame relay settings on the CSU/CDU. If ATM</td>
</tr>
</tbody>
</table>
or LAPB is selected, you must also choose a subprotocol. Set the bandwidth to match the channel settings of the fractionalized HSSI link. For field descriptions, see Table 46 on page 247.

**T1/E1**
Choose your WAN type, then set encapsulation to match the frame relay settings on the frame relay router. If ATM or LAPB is selected, you must also choose a subprotocol. Pick a line frame that matches your network. If your link is fractionalized, select that option. For field descriptions, see Table 47 on page 247.

**Virtual adapters**
See Configuring virtual adapters on the Gen2 card.

Your probe instance is now configured. You can begin collecting network traffic and statistics using it. Typically, this is done in the Observer analyzer by choosing Capture > Packet Capture and clicking the Start button. See Configuring probes to collect data even when not connected to an analyzer on page 242 for details. You do not, however, need to start a packet capture to see statistics. See the list of statistics available under the Statistics menu in Observer.

**Probe Properties field-level descriptions**

This section include details about many of the fields and options for a probe.

**Table 40: General tab**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication timeout</td>
<td>Allows you to define how long Observer will wait for the Probe to communicate before it assumes the connection is lost. Values are from 2 to 60 seconds.</td>
</tr>
<tr>
<td>Probe report period or local Observer information refresh time</td>
<td>Allows you to set how often the Probe sends a refresh packet or how often the local Observer’s dialogs are refreshed. This value has a minimum of 2 seconds with no maximum.</td>
</tr>
<tr>
<td>Statistics report (refresh) period</td>
<td>Allows you to set the statistics display refresh period. This value has a minimum of three seconds with no maximum.</td>
</tr>
<tr>
<td>Vital signs report (refresh) period</td>
<td>Allows you to set the Network Vital Signs refresh period. Values are from 10 to 600 seconds.</td>
</tr>
<tr>
<td>Sampling Divider</td>
<td>On probes with less processing power, high traffic rates (such as those typical of gigabit connections) can overwhelm the probe’s ability to keep up. A sampling divider tells Observer to only consider one of every n packets when calculating statistical displays, where n is the sampling divider. This setting only affects statistical displays such as Top Talkers, Internet Observer, etc. (packet captures are unaffected). A sampling divider of 2 registers every other packet; a sampling divider of 10 registers every tenth packet. Some statistical displays consider every packet regardless of this setting. Bandwidth Utilization looks at traffic as whole, so does Wireless Site Survey.</td>
</tr>
<tr>
<td>Encapsulated Traffic Analysis</td>
<td>GRE (Generic Routing Encapsulation) and GTP (GPRS Tunneling Protocol) are two encapsulation protocols that may have been deployed on your network. To show the encapsulation IP addresses, leave the box unchecked; to show the nested IP addresses, check the box. This setting also applies to L2TP and IPv4.</td>
</tr>
<tr>
<td>Nortel OEL2 Metro Ethernet Analysis Settings</td>
<td>Choose if frame headers should be analyzed as OEL2 headers.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MPLS Analysis Settings</td>
<td>Choose whether Observer should auto determine IPv4 and IPv6, what all other traffic is (ATM or Mac Header), and whether to use a four byte pseudowire word. Also choose whether to use the MAC addresses from encapsulated MPLS header.</td>
</tr>
</tbody>
</table>

**Table 41: Parameters tab**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network type</td>
<td>Displays the probe’s network topology, such as Ethernet, Token Ring, wireless, and WAN.</td>
</tr>
<tr>
<td>Network speed</td>
<td>Displays the network speed. The distinction here is between the actual, measured speed of the network and the speed that the NIC card, possibly incorrectly, reads from its connection. For example, a 10/100Mb NIC card on a 10/100Mb connection to a switch on a network where all the other stations are running at 10Mb will report the network speed as 100Mb. This item is the actual number that the NIC card driver sends Observer, so 10Mb Ethernet will be reported as 10,000,000. 100Mb Ethernet will be reported as 100,000,000.</td>
</tr>
<tr>
<td>NIC card name</td>
<td>Displays the name of the card as reported by the NDIS driver to the registry.</td>
</tr>
<tr>
<td>Probe version</td>
<td>Displays the probe version used by the local Observer or probe.</td>
</tr>
<tr>
<td>Number of adapters</td>
<td>Displays the number of cards the local Observer or probe has configured.</td>
</tr>
<tr>
<td>Instance memory (MB) and Capture Buffer (MB)</td>
<td>Displays the amount of RAM the instance or probe has available for statistics and capture buffer. Observer has no limitations on the amount of RAM that can be used for a buffer. The maximum allowable buffer size is displayed in the Options &gt; Selected Probe or SNMP Device Properties &gt; Probe Parameters tab.</td>
</tr>
<tr>
<td>View Probe Instance Memory Allocation</td>
<td>Lets you view and edit how the memory used for statistics is allocated for this probe instance.</td>
</tr>
<tr>
<td>Network errors Supported by the NIC NDIS driver</td>
<td>Displays the aggregate errors that your NDIS driver provides statistics for.</td>
</tr>
</tbody>
</table>

**Table 42: Adapter Speed tab**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Network Speed</td>
<td>Your current speed reported by the network card.</td>
</tr>
<tr>
<td>Network Adapter Speed</td>
<td>Choose to let Observer and the NIC automatically determine the network speed, or to select from various values (in megabits per second) for the network speed to be used for calculations. The primary use of this is to correct a mistaken NIC’s impression of overall network speed. A network card connected to a 10 megabit hub on a gigabit network will think that the entire network is only 1% as fast as it actually is.</td>
</tr>
</tbody>
</table>

**Table 43: Autoupgrade tab**
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoupgrade probe within minor version release</td>
<td>Activates the autoupdate feature for minor version (i.e., point) releases (which do not require a new license).</td>
</tr>
<tr>
<td>Autoupgrade probe for major version release</td>
<td>Activates the autoupdate feature for major version releases. You must supply an ID and license key to update probes with a major version release. If the probe includes a Gen2 capture card and the upgrade includes a Field Programmable Gate Array (FPGA) firmware update, the system must be manually shut down and restarted before the firmware update can take effect. A system restart will not complete the firmware upgrade (a shut down is required); however, the autoupgrade process will restart the probe system, thus completing the probe software upgrade. In most cases, the probe will still be operable with a software-only upgrade, but any of the benefits of the firmware update are not activated until you manually shut down and restart the probe.</td>
</tr>
<tr>
<td>Force Probe Autoupgrade to the current Observer version</td>
<td>This provides a manual mechanism for updating a probe.</td>
</tr>
</tbody>
</table>

Table 44: ToS/QoS tab
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect Protocol Distribution by QoS</td>
<td>When enabled, QoS data is collected.</td>
</tr>
<tr>
<td>Use 802.11e Wireless TID/QoS</td>
<td>When enabled, QoS for wireless networks is collected.</td>
</tr>
<tr>
<td>IP ToS/QoS Standard</td>
<td>This tab is used for NetFlow and VoIP analysis. IPv4 supports the Type of Service (ToS) byte, also known as the Precedence byte. Different RFCs define different ways to interpret the byte: Default (RFCs 1349, 1195, 1123, and 791) OSPF V2 (RFCs 1248 and 1247) DSCP (RFC 2474) User Defined The information on the right shows the bit assignments. User-defined interpretations are also allowed. for the currently selected option. The User defined option displays entry fields that allow you to define the meaning of each bit position in the ToS byte.</td>
</tr>
</tbody>
</table>

Table 45: Wireless 802.11 tab
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Profile</td>
<td>Site profiles allows you to save and retrieve wireless parameters, rather than re-keying the parameters every time you change sites.</td>
</tr>
<tr>
<td>Monitor Wireless Traffic by</td>
<td>Choose one of the following:</td>
</tr>
</tbody>
</table>
### Probe Properties field-level descriptions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Channels</td>
<td>Click the Channel Map button and choose which channels you want to scan, then choose how often you want to scan them.</td>
</tr>
<tr>
<td>Scan Interval</td>
<td>Define the scan interval.</td>
</tr>
<tr>
<td>Fixed Channel</td>
<td>Pick a channel to monitor.</td>
</tr>
<tr>
<td>BSSID</td>
<td>Specify the Basic Service Set ID of the Access Point you want to monitor.</td>
</tr>
<tr>
<td>ESSID</td>
<td>Specify the Extended Service Set ID of the network you want to monitor.</td>
</tr>
<tr>
<td>Use encryption keys</td>
<td>If your wireless network is secured, you must provide an encryption key for Observer to be able to capture and decrypt the wireless traffic. Select the Edit Encryption Keys button and provide your wireless encryption key.</td>
</tr>
<tr>
<td>Antenna to use</td>
<td>The type of antenna connected to your system. Specify one of the following:</td>
</tr>
<tr>
<td></td>
<td>Antenna Diversity—Use the stronger signal from the two antenna ports. This is the recommended setting for the standard snap-on antenna.</td>
</tr>
<tr>
<td></td>
<td>Primary Antenna Only—If you are not using the standard snap on antenna, choose this option if the antenna you are using is connected to the primary antenna port (see your NIC manual for details).</td>
</tr>
<tr>
<td></td>
<td>Secondary Antenna Only—If you are not using the standard snap on antenna, choose this option if the antenna you are using is connected to the secondary antenna port (see your NIC manual for details).</td>
</tr>
</tbody>
</table>

### Table 46: DS3/E3/HSSI tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Type</td>
<td>Choose DS3 (T3), E3 or HSSI to match the type of link you are analyzing, then choose the frame check sequence (FCS) standard: CRC-16 (the default) or CRC-32.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>You must set this to match the settings on the frame relay CSU/DSU.</td>
</tr>
<tr>
<td>Subprotocol</td>
<td>If ATM or LAPB is the selected encapsulation method, you must choose the sub-protocols on the link.</td>
</tr>
<tr>
<td>Fractionalized</td>
<td>Check if your link is configured for fractionalized operation. Fractionalized DS3 and E3 are not supported.</td>
</tr>
<tr>
<td>Bandwidth (HSSI)</td>
<td>Set to match the bandwidth and channel settings of the fractionalized HSSI link under analysis.</td>
</tr>
</tbody>
</table>

### Table 47: T1/E1 tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN/Frame Relay Type</td>
<td>Choose T1 or E1 to match the type of link you are analyzing.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>You must set this to match the settings on the frame relay CSU/DSU.</td>
</tr>
<tr>
<td>Subprotocol</td>
<td>If ATM or LAPB is the selected encapsulation method, you must choose the sub-projects on the link.</td>
</tr>
</tbody>
</table>

### Link 1 and Link 2 Channel Settings

(Note that for the link and settings to be activated, you must check the On check box for that link.)
<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fractionalized</td>
<td>Check if this link is configured for fractionalized operation.</td>
</tr>
<tr>
<td>Channel selector check boxes</td>
<td>Choose the channels you want to be included in the analysis.</td>
</tr>
<tr>
<td>Include in Util. Thermometer</td>
<td>Check if you want to include statistics from this link in the Bandwidth Utilization Thermometer.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Using the probe as a virtual TAP on page 257
- Installing the wireless NIC driver on Windows 7/Vista on page 229
- Upgrading the probe software directly on page 231
- Upgrading the probe software directly on page 231
- Remotely upgrading the probe software from within the Observer analyzer on page 231
- What is a probe instance? on page 220
- How a probe uses RAM on page 267
- How to allocate the reserved RAM on page 273
- Running Observer with reserved memory on page 270
Security and Encryption

Restricting access to probes with user accounts

Prerequisite: Multi or Expert Probe.

If you wish to restrict access to packet captures and reporting provided by a probe instance, you can define security attributes of the probe by clicking the Security tab.

To display security information by user account, click the User Account button to the right of the Probe Instances button. This lets you see what permissions the currently selected user has access to on each instance of the probe.

When displaying a user account’s permissions, you can use the check boxes to fine-tune the permissions that each user has on each account by clicking on the Permissions check boxes.

By default there is an “Anyone” account with administrator rights. That means that anyone, regardless of user name, can connect to the probe instance and use it. We suggest you delete or limit this account after you have created other user accounts. The Anyone account does not require a password.

Note: You cannot delete the Anyone account for a Single Probe. If you are having connection issues, see the issue about the Anyone account in A probe is not connecting to the analyzer or vice versa.

1. Do one of the following:
   # On the probe: Click the Security tab.
   # In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Security tab.

2. Click the New User Account button. To edit an existing account, select the account and click Edit User Account. The setup options are the same whether you are creating a new account or editing an existing account.

3. Type a user name and password. The user cannot change this password. If it is feasible you may wish to have the user type their own password.

4. If you want the user to have administrator rights, enable the option.

5. Select which probe instances the user will be allowed to use and click OK. By default, any new probe instances are accessible by all user accounts.

6. Select which access permissions the user will have for the probe instance. See Configuring access permissions for probe instances.

Configuring access permissions for probe instances

Prerequisite: Multi or Expert Probe.

Note: If you have purchased and configured the NIMS option, user authentication is configured through NIMS rather than the probe’s Security tab, which is unavailable if the Use Network Instruments Management Server option is selected in Options > Probe Options.

Tip! To display security information by probe instance instead of by user account, click the Probe Instances button in the upper left. This lets you see what permissions each user on the probe has for the probe instance.

If you have already created user accounts described in Restricting access to probes with user accounts on page 249, then you are ready to continue with configuring access permission for the probe instances.
1. Do one of the following:
   ♦ On the probe: Click the Security tab.
   ♦ In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Security tab.

2. Use the check boxes to fine-tune the permissions that each user has on each account by clicking on the check boxes to select or deselect the particular option. The different types of access permissions are described in Table 48.

If there is a green check mark, the feature is enabled. If the option is unchecked, the feature is unavailable. If the option is grayed out, the user does not have access to that probe instance.

**Table 48: Probe instance security options**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt data</td>
<td>Data sent to the analyzer is Triple DES encrypted during transmission. By making Triple DES encryption passes, it increases the effective key length to 168 bits. Only use this option if you need strong encryption, because it imposes a significant performance cost. Even with this option turned off, the probe does not send raw, easily-readable data; the data is concealed by a proprietary compression algorithm.</td>
</tr>
<tr>
<td>Configure</td>
<td>User is allowed to change the probe’s configuration options (such as memory usage, etc.).</td>
</tr>
<tr>
<td>Redirect</td>
<td>User is allowed to change the destination analyzer for probe analysis data.</td>
</tr>
<tr>
<td>Select Adapter</td>
<td>User is allowed to change the capture adapter for the probe.</td>
</tr>
<tr>
<td>Capture Packets</td>
<td>User is allowed to view captured packets from the probe’s network.</td>
</tr>
<tr>
<td>Network Trending</td>
<td>User is allowed to view Network Trending data from the probe’s network.</td>
</tr>
<tr>
<td>Internet Patrol</td>
<td>User is allowed to run Internet Patrol on the probe’s network.</td>
</tr>
<tr>
<td>WAN Configuration</td>
<td>User is allowed to change WAN probe settings such as encapsulation type and Committed Information Rate (CIR). Only applicable to Network Instruments WAN hardware probes.</td>
</tr>
<tr>
<td>Modify Partial Packet Captures</td>
<td>User is allowed to change the partial packet capture setting in the Packet Capture Settings dialog for this probe.</td>
</tr>
<tr>
<td>Modify Protocol Definitions</td>
<td>User is allowed to modify user-defined protocol definitions. These definitions can be shared with other Observer analyzers through NIMS.</td>
</tr>
<tr>
<td></td>
<td>Shared Filters: User is allowed to modify shared filters. This feature works in conjunction with NIMS and modifying filters must also be enabled in NIMS.</td>
</tr>
<tr>
<td>Reconstruct Data</td>
<td>User is allowed to reconstruct data and view the data in Reconstruct Stream or TCP Dump.</td>
</tr>
<tr>
<td>Replay VoIP</td>
<td>User is allowed to replay audio or video VoIP data.</td>
</tr>
<tr>
<td>Transfer Capture Files</td>
<td>User is allowed to move capture files.</td>
</tr>
</tbody>
</table>

*Forcing users to authenticate before connecting to a probe*

**Prerequisite:** Expert Probe
Using NIMS for user authentication plays a key role in securing Observer, so it is a best practice to add the extra layer of security that authentication provides. Doing so ensures that authorized persons are genuine, not spoofed, and probe redirection can only be performed by the right people.

Note that to enable user authentication, you must first tell Observer to encrypt all connections. Also note that user authentication is conceptually different than creating user accounts in Observer and setting user permissions.

**How to encrypt captured data**

Captured data can be encrypted using the 256-bit Advanced Encryption Standard (AES) algorithm. This significantly increases the security of your at-rest data.

You must have a special Observer license to enable and use this feature. There is no extra charge for the license.

Data at rest encryption is prevents visibility into any packets or even the metadata about the packets stored on the GigaStor. Any packets that are captured by the GigaStor are considered "data" and while they are stored on the GigaStor they are considered "at rest." Should any of the drives in the GigaStor be removed or misplaced, the data on the drives is protected. There is no remote access to this data apart from Observer’s own analyzer, and the data tagging methods for organizing and retrieving data can only be used in conjunction with the Observer analyzer.

The GigaStor can capture 10 Gb line rate while simultaneously encrypting the traffic with AES-256 encryption without any significant performance impact on write or read speeds of the GigaStor.

These instructions describe how to apply data at rest encryption to a GigaStor already in your possession. If your GigaStor shipped from the warehouse with the data at rest security already enabled, you do not need to complete this process unless two or more drives in your RAID have failed.

**Caution!** This procedure deletes all of the data on your GigaStor! Ensure you have a backup of any data you wish to keep.

1. Download the latest firmware for the Areca 1882 Series RAID card or contact Network Instruments Support for the file.
2. Choose Start > All Programs > Areca Technology Corp > ArcHttpSrvGui > Areca HTTP Proxy Server GUI. The program starts. You should see something similar to this image.
3. Select Controller#01 and click Launch Browser. If the controller is not running, click the Start button then launch the browser. The Areca RAID application attempts to connect to its web server.

4. Type the user name and password. The default user name is admin. There is no default password. Click OK to open the browser.

   In the browser you can see the RAID set, IDE channels, Volume, and capacity.

5. In the web browser, choose System Controls > Upgrade Firmware. In the Browse field, choose each of the four files from the firmware package you downloaded or received from Technical Support in step 1 and click Submit. Choose the files in the order they are listed below. After adding the arch1882firm.bin file you are prompted to restart the system. Ignore that restart request and add the fourth file.

   ARC1882BIOS.BIN
   ARC1882BOOT.BIN
   arc1882firm.bin
   ARC1882MBR0.BIN

6. Restart the GigaStor.

7. Choose Volume Set Functions > Delete Volume Set. Select the volume, then select Confirm The Operation and click Submit. This deletes all of the existing data on the RAID.

8. Choose Volume Set Functions > Create Volume Set. Set the following options to these values, select Confirm The Operation, and click Submit.

<table>
<thead>
<tr>
<th>Volume RAID Level</th>
<th>Raid 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater Two TB Volume Support</td>
<td>64bit LBA</td>
</tr>
<tr>
<td>Volume Initialization Mode</td>
<td>Background Initialization. It may take several hours (six hours for 48 TB) to initialization the volume. While the volume is being initialized, the GigaStor cannot be used. If you choose Foreground Initialization, you may use your GigaStor, but it</td>
</tr>
</tbody>
</table>
9. Open Observer and apply your new license. Restart Observer. Because this is the first time that Observer is opened with the new license, it does not yet have a key for the encrypted volume. A window appears indicating that the volume is locked. Click Generate Key and save the key file. This is the key necessary to write to and read from the RAID volume. You can choose to remember the key file location so that Observer opens automatically, or, if left cleared, each time Observer is opened you must provide the path to the key file.

Every time Observer opens it looks for the encryption key that allows access to encrypted volume. Without the key present neither packet capture nor packet analyzation can occur.

10. Close Observer until the rest of this procedure is complete.

11. In Control Panel > Administrative Tools > Computer Management > Storage > Disk Management select the RAID volume, right-click and choose Initialize. In the Initialize Disk window, select Disk 1 and GPT (GUID Partition Table). Convert the volume to a Simple Layout, assign a drive letter (typically, D:), and provide a name (typically, DATA).

12. Repeat this process for each RAID volume for your GigaStor.

13. Open Observer.

Encrypting the data sent between the probe and analyzer

Prerequisite: Expert Probe

Connections to probes and probe units are secured end-to-end using the Triple DES (3DES) encryption algorithm, making Observer’s transmissions over the network highly resistant to eavesdropping and any meaningful interpretation of data. These secured connections are facilitated by the Observer analyzer and cannot be disabled—only improved.

You can further enhance the security by enabling probe to analyzer communication by turning on the “Encrypt Data” feature. See Configuring access permissions for probe instances on page 249.

Along with securing your connections, if you have NIMS we recommend authenticating your users. See Forcing users to authenticate before connecting to a probe on page 250 for more information.

After completing this task:

After the option is enabled, you must then create or obtain an Observer Encryption Key file:

- **If you have an existing Observer Encryption Key file (*.OEK)**
  
  You must copy the encryption key file into the installation directory (usually `C:\Program Files\Observer`) of each probe or analyzer that you want to authorize.

- **If you do not have an Observer Encryption Key file (*.OEK)**
  
  Generate a key file; click the “Launch Encryption Key Generator” button. Its online help explains its use and how to set up the keys it generates.

**Related Topics**

- Setting security options for the analyzer on page 137
- Setting security options for probes on page 138
- Encrypting the data sent between the probe and analyzer on page 253
- Restricting access to probes with user accounts on page 249
Using the Probe

**Using the Expert Probe software**

**Prerequisite:** Expert Probe

The Expert Probe is a step above the Multi Probe software and is the only probe software that runs on the GigaStor. The Expert Probe includes all the functionality of the Multi Probe, plus it displays remote expert analysis in real time for faster troubleshooting. If you are using the Expert Probe on a GigaStor (rather than a non-GigaStor probe) there are even more features available. Just like the Multi Probe, the Expert Probe has a number of tabs that allow you to control probe network connections and memory usage, administer probe security, and monitor probe activity.

**Figure 81: Expert Probe on a GigaStor**

An Expert Probe transfers decode data to an Observer analyzer only when you select the packet from the one-line summary pane, which is updated with packet header information in real time. This conserves network bandwidth by analyzing all data locally and sending only the results. This eliminates the need to transfer data packets over the wire. This differs from the Single Probe and Multi Probe because those probes send the entire buffer to the analyzer and the decoding and analysis happens on the analyzer.

Another feature exclusive to the Expert Probe is its ability to switch between being a probe or an analyzer. This can be very useful depending on your needs. This gives you flexibility in using the probe both remotely and on site.

**VoIP Expert, Application Performance Analysis, and Application Transaction Analysis**

**Prerequisite:** Expert Probe

The Expert Probe provides unique insight into your OSI Model Layer 7 applications that the Multi Probe and Single Probe cannot provide. This is especially true for VoIP.

There is nothing that you need to configure on the probe to enable these features, but this information is only available when viewing the probe instance of an Expert Probe.

To use and configure VoIP, ATA, or APA:

1. In the Observer analyzer, choose **Trending/Analysis** > **Network Trending**. The Network Trending window opens.
2. Use the General, Application Transaction Analysis, Application Performance Analysis, and VoIP tab to configure your options.
3. Click the Start button to begin monitoring.
4. After you have collected some data, click the Analysis button. The View Network Trending data dialog opens.
5. Choose “Transfer and view current day statistics” and click OK. This opens the Network Trending Viewer in a new tab where you can see your data.
Switching between the probe and analyzer user interfaces

Prerequisite: Multi or Expert Probe.

Depending on how you want or need to use your Expert Probe, it can be either an Observer analyzer to help you view your network data or it can be a probe to capture data and to which other Observer analyzers can connect. The Expert Probe software cannot simultaneously be an analyzer and a probe.

To change the Expert Probe interface to load as a fully-featured Observer analyzer, choose Options > Switch Between Observer and Expert Probe Interface. You must restart the application to see the change.

For a GigaStor, the Expert Probe software is running as a Windows service. You must stop the Expert Probe service before you can change its interface.

1. Right-click the Probe Service Configuration Applet in the system tray and choose Open Probe Configuration.

   ![Probe Service Configuration Applet](image)

   Figure 82: Probe Service Configuration Applet

2. The Probe Administration window opens. Click the Probe Options tab.

3. In the Service Settings section, clear the “Run Probe as a Windows Service” option and click OK. This removes the Network Instruments Expert Probe service from Windows.


5. Choose Options > Switch between Observer and Expert Probe Interface. The Choose Program Interface window opens.

6. Choose Observer and click OK. You must close Observer and restart it to switch into the analyzer interface. Click OK on the message dialog.

7. Click Start > All Programs > Network Instruments Observer > Observer to open the analyzer interface.

After completing this task:

When switching back to an Expert Probe on the GigaStor, you must reverse these steps and then you must manually start Expert Probe from the Windows Service Control Manager. It may take a moment before the service starts. You may need to restart the GigaStor for the setting changes to fully set.

Enabling Network Trending and setting which statistics are collected

A probe can provide many different statistics about your network, but you must enable the collection of those statistics. Network Trending does not capture packets, but collects statistics about the traffic on your network. Many reports in Observer use the trending information, and we recommend you enable Network Trending.

1. To turn on the collection of a specific statistic, in the Observer analyzer choose Statistics > and then select the statistic you want to have the probe collect and report.

2. To turn on Network Trending, in the Observer analyzer choose Trending/Analysis > Network Trending. The Network Trending window opens.

Monitoring a wireless access point

You can capture all wireless traffic with a wireless network card on a laptop or any system with a wireless network card if you use the Network Instruments wireless driver. The default driver for your wireless card is not sufficient for Observer.

Standard network cards do not support “raw” wireless packets, nor do they enable “promiscuous” mode by default. Promiscuous mode captures all packets for the analyzer, not just those addressed to the network card.
Both “raw” wireless packets and promiscuous mode are required by Observer. The Network Instruments wireless driver enables these options.

When a network card is running in promiscuous mode, it cannot connect to a wireless access point. It can only capture traffic. If you are using a laptop and want to capture traffic and at the same time connect to a wireless access point, your laptop must have two wireless cards.

If you are using the probe software on your laptop, you need two network adapters. Typically, one adapter is an Ethernet card for communication and one wireless adapter for analysis. You could also use two wireless cards. You may also need special drivers.

If your wireless network uses an encryption key or specific wireless channels, you can specify that information for the wireless adapter.

Use private keys to authenticate with a RADIUS server, then dynamic keys are used to encrypt communication on a user by user basis, with no two users ending up with the same keys. Observer cannot decrypt the data from a site that implemented EAP/LEAP, but this does not mean Observer is not useful. Because all management and control packets are not encrypted, wireless troubleshooting is not affected even if you use EAP/LEAP.

**Note:** If you want to troubleshoot the actual data in the conversation, collect the data on the wired side where there is no encryption and all protocols can be decoded. Observer supports both wired topologies (i.e. Ethernet, Token Ring and FDDI) as well as wireless topologies to troubleshoot both sides of a conversation (wireless management+control AND full wired data) you only need one product.

---

**Using the probe as a virtual TAP**

**Prerequisite:** Multi or Expert Probe.

The Virtual TAP (sometimes called a vTAP) allows you to configure a virtual tap to monitor traffic within a virtual host environment.

Most virtual environments provide virtual adapters for each virtual machine, and these virtual adapters are logically connected to a virtual switch managed by the virtual host system. The virtual switch manages traffic flow to and from the virtual adapters by mapping each virtual adapter to a physical adapter in the host. When promiscuous mode is enabled on a virtual adapter (or virtual switch), all traffic flowing through the virtual switch—including local traffic between virtual machines and remote traffic from outside the virtual host—is sent to the promiscuous virtual adapter and can be monitored by Observer.

To use the virtual tap you must monitor all virtual machines in a host from a virtual machine within the host. This assumes you can use a SPAN/mirror port or the virtual NIC has a “promiscuous mode” setting. This functionality is available in VMware’s ESX and ESXi. It may also be available in other virtual server products.

Using the virtual TAP, you can then collect and re-direct all traffic internal to the virtual switch to a dedicated virtual NIC within the monitoring virtual machine that is then connected to Observer.

If there is any internal communication between virtual machines, the only way to monitor this data is by using a separate monitoring virtual machine with an analysis service (for instance, probe) gathering data from the internal virtual switch. Should you need to analyze or store data on a GigaStor, installing a Virtual TAP within the monitoring virtual machine provides complete visibility into all data flowing on the internal virtual switch.

You can create a port group on a switch and use a virtual machine (VM1) to monitor traffic of a second virtual machine (VM2) that resides on the same switch but in different port.

If you already have a 64-bit Windows virtual machine, we suggest you use it, because installing the probe there will be less resource intensive on the host than installing a new virtual machine on the host.

1. Do one of the following:
   
   # On the probe: Click the Virtual TAP tab.
In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Virtual TAP tab.

2. Click Modify to set the source and destination adapters for the virtual tap.

3. Choose your source and destination adapters and select the Enable Virtual Tap option.

   You have now configured what you need to within Observer to enable the virtual tap feature, but you must modify a setting for your virtual switch.

4. Set the virtual NIC on the virtual switch within the host in SPAN/mirror mode, sometimes also called promiscuous mode. See your virtual machine’s documentation for further details.

When to use a virtual TAP

Monitoring network and application traffic in a virtualized environment containing one-to-many relationships between physical hardware devices (virtual hosts) and virtual application servers (virtual machines) presents a number of concerns.

Virtual environments are designed to include a virtual adapter (vNIC) for each virtual machine within the system. The vNIC is logically connected to a virtual switch, which is managed by the virtual host system (see the diagram below). This addresses communication which would remain in the VM host. In order to enable communication into and out of the VM host, a logical connection between the vNIC and the pNIC must be established.

Depending on the virtual server technology you have decided to implement, you have a number of options for network and application traffic visibility, and for the use of external devices for analysis. If all virtual machine communications take place between the virtual machines and the “outside” (i.e., outside the physical host), then monitoring the data flow from outside the host server may be the least complicated method by which to gain flow visibility. If there is any internal communication between virtual machines, the only way to monitor this data is by using a monitoring virtual machine (separate or existing) with an analysis service (i.e., probe) gathering data from the internal virtual switch. Should you need to analyze or store data on an external purpose-built device, installing a virtual TAP within the monitoring virtual machine provides complete visibility into all data flowing on the internal virtual switch.

Within the VMware ESX and ESXi environments, a virtual adapter can be set in “promiscuous mode.” When promiscuous mode is enabled on a virtual adapter, all traffic flowing through the virtual switch—including local traffic between virtual machines and remote traffic originating from outside the virtual host—is sent to the promiscuous virtual adapter.
A number of challenges are presented when attempting to monitor applications with a virtualized environment.

1. **Lack of visibility.** Traffic between virtual machines within a virtual host will not be visible outside of the host. This causes a number of problems:
   a. Network engineers cannot monitor multi-tier applications partially or wholly located on multiple virtual machines within a single host.
   b. Should a virtual machine be compromised by malicious code or security breach, other virtual machines within the same host may also be compromised.

2. **Lack of analysis functionality.** A separate solution is required to push data streams flowing within virtual machines out to an external tool or a purpose-built device. This functionality is necessary for network and application monitoring and analysis, compliance, and security audits. Virtual TAPs (software applications placed inside a virtual machine to export all data through a designated pNIC to an external device) can alleviate this problem.

**Options**

The goal is to not only see all traffic flowing within a VM host but also export that data for powerful analytics and reporting. There are three primary ways to monitor both traffic flow from within applications on virtual machines and from the virtual host:

1. Monitor the host using an external analysis device as you would any other system, via SPAN technology or a physical TAP. This option works well for environments not needing to track internal virtual machine-to-machine traffic within a host. However, it may not catch a security breach compromising multiple virtual machines within a host.
2. Monitor all virtual machines in a host by establishing a new virtual machine within the host. This option assumes the ability to SPAN or set in promiscuous mode the virtual switch within the host. This option provides visibility at the statistics and packet levels of all traffic within a virtual host. It does not, however, allow packet-level traffic to be analyzed by an external physical device (IDS, retrospective analysis device, etc.).
3. Use a virtual TAP to collect and redirect all internal virtual machine traffic to a dedicated virtual NIC within the monitoring virtual machine that is connected to an external purpose-built device for analysis or compliance enforcement. Depending on the functionality of the external device the traffic is being copied to, this option may provide all the functionality of option two while taking advantage of the physical capabilities of the purpose-built external device.
Option two combined with option three offers the most extensive and comprehensive monitoring solution. In a VMware environment, you can use promiscuous mode on the internal virtual switch and direct a copy of all traffic from all virtual machines to a virtual machine monitoring instance. This allows you to collect metrics and perform real-time analysis; and using a virtual TAP, you can re-direct packet streams out a separate NIC to a GigaStor probe.

**Benefits of a virtual TAP**

Mirroring all traffic within a virtual host to an external device provides a number of advantages, including total visibility into VM application traffic and the ability to run greater analytics for comprehensive reporting and faster problem resolution. For example:

- **Application Performance Monitoring.** Feed VM traffic to an enterprise reporting engine for comprehensive monitoring of virtualized environments. Set and track performance baselines and respond quickly when performance deviates from the norm. Tracking VM traffic over time helps determine if your VM server load has increased to the point of requiring action.

- **Application Performance Troubleshooting.** The virtual TAP can also output data to a GigaStor probe, which stores it for later access. The GigaStor can help isolate problems within your virtual environment and troubleshoot these issues using Application Analytics.

The Virtual TAP option bridges the visibility gap, allowing complete real-time analysis, Retrospective Network Analysis, and full-scale reporting on all virtualized traffic.

**Configuring VMware ESX Server**

**Prerequisite:** Multi or Expert Probe.

A free physical NIC is required on the VMware ESX server to perform this configuration.

In the virtual switch to be monitored, add a virtual port group and set it to run in Promiscuous Mode.
Do not choose the same source and destination for the Virtual TAP Settings. This could cause broadcast/multicast loops and would noticeably impact your network.

The default policy for Promiscuous Mode for the vSwitch itself should remain in the Reject setting. Only the new port group within the vSwitch should be set to Accept Promiscuous mode.

You can use the virtual machine properties dialog to identify the Network Connection, listed in the Windows Network Connections dialog, by unchecking the “connected” option.

1. Open VI Client and highlight the VMware ESX Server Entry.
2. Click to the Configuration tab.
3. Click Hardware – Choose Networking.
4. Find the vSwitch for which you would like to monitor traffic and choose Properties.
5. In the vSwitch Properties dialog (Ports tab), click Add.
6. In the Add Network wizard, choose Virtual Machine [port group], give the group a name (“Promiscuous Port Group”), and finish the wizard.
7. In the vSwitch Properties dialog, highlight the new port group and click Edit.
8. Click the Security tab.
9. Select the Promiscuous Mode Policy Exception option and change the list to Accept.

Figure 83: VMware ESX Server

Figure 84: vSwitch Properties
10. Setup a second virtual switch and bind a second physical NIC to that virtual switch. See Figure 84 Virtual Infrastructure Client > Configuration tab. Then see Figure 86 Add Networking > Add Network Wizard > Virtual Machine.

11. Create a virtual switch.

12. Select the appropriate NIC entry (i.e. Physical NIC 2 on ESX Server).

13. Name the vSwitch (i.e. “vTAP OUT to GigaStor”) and finish.

The result should be similar to Figure 85 on page 264. See your VMware ESX Server documentation if you need more detailed information on adding a virtual switch.

Figure 85: VMware Add Network Wizard

14. Edit the Virtual Machine that contains the Observer to use the Port Monitor Group and second vSwitch.

15. Select the first network adapter.

16. Change the Network label to the new Port Monitor Group, and add a 2nd virtual NIC if needed.

17. Select the second virtual NIC and change the Network label to the second vSwitch (i.e., vTAP OUT to GigaStor) and click OK.

18. Verify that the Virtual Machine containing Observer is located in both virtual switches.

Figure 86: Virtual Machine Properties

19. Within the virtual machine, setup Observer to VTAP Local Area Connection 1 to Local Area Connection 2.

20. Connect the cable from “NIC 2” on the VMware ESX Server to the GigaStor Gen2 capture card.
Bonding probe instances to specific ports on the Gen2 card through virtual adapters

Prerequisite: Multi or Expert Probe.

Some probes available from Network Instruments come with a special capture card called the Gen2 capture card. Any probe equipped with a multi-port Gen2 card may be configured to use virtual adapters to bind specific port to specific probe instances.

Capturing full-duplex traffic

Prerequisite: Multi or Expert Probe.

Using a Gen2 capture card, you can capture full-duplex traffic. You can also bond probe instances to specific ports on the Gen2 card.

Using the NetFlow features in Observer

Like many things in Observer a feature is not in just one place, but spread throughout the product. NetFlow is no different. Use this section as a starting place to find what you need regarding NetFlow in Observer.

► Choose the right probe for you.
► Ensure your ToS/QoS is set for your network so that your statistics are correct.
► There are two different types of NetFlow collectors. Learn the differences and see how to create one.
► If you are using a GigaStor probe, you can generate NetFlow statistics using it.
► Capturing NetFlow statistics does have some limitations that are different from packet capture.
► Decoding a NetFlow flow. This section also details how you may need to configure your NetFlow device so that Observer can see the flows.
► Open a saved NetFlow capture.
► Most NetFlow information comes from Network Trending.

Creating a NetFlow collector or NetFlow Trending collector

Prerequisite: Expert Probe

Note: If you want to have scheduled collection of your NetFlow devices, use the settings on the Schedule tab.

NetFlow and sFlow collectors support the following versions of these technologies:

► NetFlow: 1, 5, 7, 9, and 10
► sFlow: 2, 4, and 5

There are two types of NetFlow collectors in Observer. Choose the correct one for your needs, or create two different probe instances—one for the NetFlow collector and another for the NetFlow Trending collector. In most cases, it will likely be the NetFlow Trending collector. The NetFlow Trending collector supports up to 512 NetFlow devices, whereas the NetFlow collector only supports one NetFlow device. That means you must add and configure a NetFlow collector for each NetFlow device in your environment.

<table>
<thead>
<tr>
<th></th>
<th>NetFlow Trending collector</th>
<th>NetFlow collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>One flow per collector</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>NetFlow Trending collector</td>
<td>NetFlow collector</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Up to 512 flows per trending collector</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Collects live statistics(^1)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Collects historical trending(^2)</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

\(^1\) Live statistics are details about the flow that appear in Observer in as few as five seconds.

\(^2\) Historical trending data collection interval can be as few as 60 seconds.

See Creating a probe instance on page 235 for details about creating a NetFlow collector or a NetFlow Trending collector. In 3 on page 235 choose NetFlow collector or NetFlow Trending collector and follow the on screen instructions. After the probe instance is created, there is no other configuration you must do and it is ready to use.

After the probe instance is created, you may want to configure the probe to tell it what type of traffic is seen.

1. In Observer analyzer, select a probe instance, right-click and choose **Probe or Device Properties**. The Probe Properties window opens.
2. On the General tab, configure the Timing and Statistics Packet Sampling sections for your needs and Click OK.
3. Choose **Trending/Analysis > Network Trending**. The Network Trending window opens. If you have already configured the settings for the NetFlow collector, skip to 7.
4. Click the Settings button.
5. In the Collection Settings section, choose a sampling divider and how often you want flow data collected.
   - **Sampling divider**—specifies how many packets should be sampled. The default is one in 10 packets is analyzed. Choosing 1 ensures every packet is analyzed, but increases the amount of CPU required. Choosing a larger number means not every packet is analyzed, but CPU use is reduced. A larger sampling rate still produces statistically accurate information. If you experience high CPU use, make the divider a larger number.
   - **Collection interval**—specifies how often data is collected. The default is 60 minutes. The minimum is one minute.
   - **Use current filter**—If you have a filter defined and you want to use it, select this option. Otherwise, leave it blank.
6. Click OK to close the Network Trending Settings window.
7. Click the Start button to begin monitoring the NetFlow devices.
8. After you have collected some data, click the Analysis button. The View Network Trending data dialog opens.
9. Choose “Transfer and view current day statistics” and click OK. This opens the Network Trending Viewer in a new tab. In the Network Trending Viewer you can see for your NetFlow devices:

   **Station Activity Time**
   **Top Talkers**
   **Packet Size Distribution**
   **Bandwidth Utilization**
   **Protocols**
Creating an sFlow collector

Prerequisite: Expert Probe

See Creating a probe instance on page 235 for details about creating an sFlow collector or a NetFlow Trending collector. In 3 on page 235 choose sFlow collector and follow the on screen instructions. After the probe instance is created, there is no other configuration you must do and it is ready to use.

How a probe uses RAM

A Windows computer uses Random Access Memory (RAM) as a form of temporary data storage. Windows separates all available memory into three sections: protected memory, user memory, and reserved memory. An Observer probe, depending on how it is configured, uses these types of memory differently.

The protected memory is used to load critical operating system files, such as device drivers. If any of this RAM is dedicated to a driver or some other critical file, it cannot be used by another program. However, after Windows finishes loading its drivers, the memory is freed and any program may access the remaining protected memory.

User memory is all available memory beyond the protected memory. It is available to any application at any time. The probe uses this memory to temporarily store statistical information, such as Top Talkers data.

Reserved memory is user memory that you have specifically set aside for use by the Observer probe. Only the probe may use that portion of RAM. When the RAM is reserved for the probe not even the operating system may access it—even when Observer is closed.

By having RAM reserved specifically for the Observer probe, you ensure that the probe has the memory necessary to capture packets and store these packets for statistical processing. If Observer runs without any reserved memory, it requests and uses the operating system’s protected memory for capturing packets. There is no adverse effect of running an Observer probe without reserved memory, but it is not the most efficient way to run the probe. By default, the probe uses no reserved memory. Our recommendation is that you reserve memory for Observer so that the probe runs efficiently and leaves the protected memory for the operating system and other programs to use.

Packet captures are always written sequentially from the first open byte of RAM in reserved memory or in Windows protected memory. They are written until all available space is used. If you are using a circular buffer, then the first packet is overwritten with the newest packet. This is first-in, first out (FIFO). With Windows protected memory, your capture space is limited to about 50 to 80 MB, but with reserved memory you have the potential to store many gigabytes in memory. Figure 87 on page 267 describes the two different ways that Observer runs.

Figure 87: Windows protected memory, user memory, and reserved memory

Whether using protected memory or reserved memory, Observer uses the RAM to store data for things such as (and creates a section within the RAM dedicated to):
Packet capture buffer and statistics buffer

There are two kinds of buffers that a probe uses to store data in real-time: capture buffers and statistical buffers. The capture buffer stores the raw data captured from the network while the statistical buffer stores data entries that are snapshots of a given statistical data point.

Selecting an appropriate capture buffer size given system resources is all most users need to worry about; the default settings for the statistical buffers work perfectly fine in the vast majority of circumstances.

However, if you are pushing the limits of your probe system by creating many probe instances, you may be able to avoid some performance problems by fine-tuning the memory allocation for each probe instance.

For example, suppose you want to give a number of remote administrators access to Top Talkers data from a given probe. You will be able to add more probe instances within a given system's memory constraints if you set up the statistics buffers to only allocate memory for tracking Top Talkers and to not allocate memory for statistics that no one will be looking at.

Observer has no limitations on the amount of RAM that can be used for a buffer.

You can allocate up to 4 gigabytes, limited only by the physical memory installed on your Windows system. Note that when run on a 64-bit Windows, there is no 4 GB limitation for the capture buffer; you are limited only by the amount of physical memory installed on the probe.
In all cases, the actual buffer size (Max Buffer Size) is also reduced by 7% for memory management purposes. Should you try and exceed the Max Buffer Size an error dialog will be displayed indicating the minimum and maximum buffer size for your Observer (or probe) buffer.

For passive probe instances, which are most often used for troubleshooting, the default settings should be sufficient. If you are creating an active probe instance (one that writes to disk and not just reads from it), then you may want to use the following formula as a rough guideline to determine how much RAM to reserve for the probe instance when doing a packet capture. (This formula does not apply when doing a GigaStor capture to disk. It is only for probe instances doing packet captures.)

Use this formula to determine your RAM buffer size:

\[
\text{Network Speed} \times \text{Average Throughput (MB/second)} \times \text{Seconds of data storable in RAM}
\]

**Tip!** You want a buffer that will handle your largest, worst case unfiltered burst.

Use this formula to determine how much hard drive space a capture requires (in GB) and Observer’s write-to-disk capability. There is no limitation to the amount data Observer can write to disk other than the disk size itself.

\[
\frac{\text{(Traffic Level / 8 bit)} \times 3600 \text{ Seconds}}{1024 \text{ bytes}} = \text{Gigabytes per hour}
\]

For instance a fully utilized 1 Gb port (1 Gbps is 125 MBps):

\[
\frac{(125 \text{ MBps / 8 bit}) \times 3600 \text{ Seconds}}{1024 \text{ bytes}} \approx 54.93 \text{ GB per hour}
\]

**Running Observer without reserved memory**

This section discusses how Observer uses the protected memory for packet capture. It applies to all versions of Observer and NetFlow probes. This is the default, but not recommended configuration. It is the default because each network is unique and you must determine how you want Observer to be configured for your system.

This section does not apply to the GigaStor or other hardware products from Network Instruments. They are properly configured at the factory.

If you need more RAM for the statistics queue buffer, you may need to lower the amount of RAM dedicated to packet capture so that it is freed and available to add to the statistics queue.

After you install Observer and first open the program it does not have any reserved memory. Observer allocated a portion of the available protected memory for its use. This creates a “Windows memory pool” for Observer of about 50 to 80 MB (depending on the amount available from Windows, and cannot be increased).

1. Click the Memory Management tab to display the list of probe instances and their buffer sizes.
2. Click the Configure Memory button at the top of the window to view and modify how Observer uses the protected memory for this probe instance. The Edit Probe Instance window opens.

On the Edit Probe Instance window, you can see how memory is allocated for:
You can also see how much protected memory is still available in the Windows memory pool.

### Figure 89: Edit Probe Instance

![Edit Probe Instance](image)

3. Use the arrows to the right of the Packet capture and Statistics queue buffer to increase or decrease the amount of RAM you want dedicated to each. See How to allocate the reserved RAM to help determine how to divide the memory.

4. Click View to see the different types of networks and how the memory is allocated to the numerous statistics collected by Observer. See Tweaking the statistics memory configuration for details about the window and why you may want to change some allocations.

### Running Observer with reserved memory

This section discusses how Observer uses the reserved memory for packet capture and the statistics queue buffer. It applies to Observer Expert, Observer Suite, and Expert and Multi-instance probes. This is not the default configuration, but it is the one we recommend you use.

**Caution!** Never change the reserved memory settings of Network Instruments hardware unless Network Instruments instructs you do so. Reserved memory settings should only be modified on non-Network Instruments hardware, such as a desktop computer running an Observer analyzer.

Although your requirements are unique, there are some general recommendations where the system is dedicated to Observer: For 64-bit, reserve all memory above 4 GB for Observer and for 32-bit, reserve all memory above 400 MB for Observer.

**Tip!** If you need more RAM for the statistics queue buffer, you may need to lower the amount of RAM dedicated to packet capture so that it is freed and available to add to the statistics queue.

Reserving memory allows Observer to allocate RAM for its exclusive use. This ensures that Observer has the necessary memory to store packets for statistical analysis, or for capturing large amounts of data for decoding.
The more memory you reserve for Observer, the larger the packet capture and statistical queue buffers can be. This allows you to store more packets and analyze a longer time period.

If the memory buffer for the statistics queue buffer is too small, you may end up with inaccurate statistical data because some data may get pushed out before it can be processed. Observer processes packets on a first-in, first out (FIFO) basis, so it is important that the buffer be large enough to allow for processing.

If you want to do a packet capture over an extended period of time it is vital that you have a buffer large enough to hold the packets in memory. The only way to ensure you have a large enough buffer is to reserve memory for use by Observer.

When reserving RAM for Observer you are taking RAM away from the operating system. Table 49 on page 271 shows how much memory is required by the operating system. Anything beyond this amount may be reserved for Observer.

**Table 49: Reserved memory requirements**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>RAM required for the operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit with less than 4 GB RAM</td>
<td>800 MB</td>
</tr>
<tr>
<td>64-bit with 4 GB RAM</td>
<td>4 GB *</td>
</tr>
<tr>
<td>64-bit with 6+ GB RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>32-bit</td>
<td>256 MB (although 400+ MB is recommended)</td>
</tr>
</tbody>
</table>

1) Because of how 64-bit Windows loads its drivers when 4 GB of RAM is installed all 4 GB is used by Windows. This is sometimes referred to as the BIOS memory hole and means you cannot reserve any memory for Observer. To capture packets on 64-bit Windows install either more than or less than 4 GB of RAM.

2) 32-bit operating systems do not support more than 4 GB of RAM. Observer cannot use any RAM above 4 GB.

1. To see how much protected memory the probe has, click the Memory Management tab.
2. Click the Configure Memory button at the top of the window to view and modify how Observer uses the protected memory for this probe instance. The Edit Probe Instance window opens.
   - On the Edit Probe Instance window, you can see how memory is allocated for:
     - Packet capture
     - Statistics queue buffer
   - You can also see how much protected memory is still available in the Windows memory pool.
3. Use the arrows to the right of the Packet capture and Statistics queue buffer to increase or decrease the amount of RAM you want dedicated to each. See How to allocate the reserved RAM to help determine how to divide the memory.
4. Click View to see the different types of networks and how the memory is allocated to the numerous statistics collected by Observer. See Tweaking the statistics memory configuration for details about the window and why you may want to change some allocations.
5. After reserving memory for Observer you must restart the system for the changes to take affect. After you restart the system you can allocate the memory to the different probe instances.

**How packet capture affects RAM**

When you start a packet capture (Capture > Packet Capture and click Start), all packets that Observer sees are placed into the packet capture buffer (a specific portion of the protected memory). The packets stay in this
protected memory until the buffer is cleared. If you are using a circular packet buffer, new packets overwrite old ones after the buffer is full.

Figure 90 on page 272 shows how Observer receives a packet and distributes it throughout RAM, and how it is written to disk for packet capture and GigaStor capture.

Packets received by the network card are passed to Observer, where Observer puts each packet into RAM, specifically in the packet capture memory buffer and the statistical queue buffer. If a packet must be written to disk for either a GigaStor capture or a Packet Capture, it is copied from the RAM and written to the disk.

Figure 90: How packets move through Observer’s memory

- The capture card receives data off the network.
- The capture card passes data into RAM. In the RAM it goes into the packet capture buffer and the statistics queue buffer.
- The statistics queue buffer passes the information to the statistics memory configuration.
- The statistics memory configuration passes the data to the real-time graphs.
- The Network Trending Files receive data from the statistics queue buffer through the NI trending service, where they are written to disk.

The following steps occur only if you are writing the data to disk through a packet capture to disk or a GigaStor capture.

If you are using packet capture to disk, the packet capture buffer passes the data to the operating system’s disk.

If you are using GigaStor capture, the statistics queue buffer and the packet capture buffer passes the information to the RAID.

A few notes about how some buffers are used:

- Packets received by the statistics queue buffer are processed and put in the collected statistics buffer.
- Data for network trending comes from the statistics queue buffer, then it is written to disk, and finally flushed from the buffer every collection period.
- The collected statistical buffer does not use first-in, first-out to determine statistics. Therefore, after the statistic limit is reached the remaining data is no longer counted; however, data for known stations continue to be updated indefinitely.
Regardless of whether Observer is using reserved memory, the statistics memory, statistics queue buffer, and packet capture buffer function the same. The storage space available for storing packets in memory increases though when you reserve memory.

How to allocate the reserved RAM

If you have a lot of network traffic, then you may need to allocate at least one gigabyte of RAM to the packet capture buffer, the statistics queue buffer, or both.

After you have the RAM reserved for Observer, you must allocate it for the probe instances. Here are our basic recommendations for allocating the memory. These are just recommendations and may be changed or modified for your circumstances. If you are using a GigaStor, read this section, but also be sure to consider the information in Recommendations for the Gen2 capture cards on page 273.

How many probe instances will you have on this system? How are you using the probe instance(s)? Are you using it to capture packets or to analyze statistics? After you know how you want to use the probe instance, you can decide how to properly divide the memory amongst the probe instances, and further how you will allocate the memory between the packet capture and statistics queue buffers.

You want to create and use as few probe instances as absolutely necessary. Each probe instance you create divides the memory pool into smaller chunks. The more probe instances you have, the more processing the system must do.

For each probe instance determine:

- If you want to mostly capture packets, then allocate 90% of the RAM to packet capture and 10% to the statistics queue buffer. At a minimum, you should allocate 12 MB to collect statistics. If you are using a GigaStor, you should allocate the vast majority of the RAM for the active probe instance to packet capture.
- If you want to collect statistics or trending data, or use analysis, then allocate 90% (or even 100%) of the RAM to the statistics queue buffer.
- If you want to do both, determine which you want to do more of and allocate the memory accordingly.

Recommendations for the Gen2 capture cards

Unless specifically stated, all information in this section applies to both the 1 Gb Gen2 card, 10 Gb Gen2 card, and 40 Gb Gen2 card. The Gen2 card is only available in hardware products from Network Instruments.

There are additional requirements and considerations if you are using a GigaStor. A GigaStor may have one of several different capture cards installed. Here are some special configuration issues to consider when dealing with a Gen2 capture card:

- When using multiple probe instances on a GigaStor, ensure that only one probe instance is associated with the Gen2 card. (If you are using virtual adapters to monitor disparate networks, then you may have more than one active instance bound to the Gen2 card.) For performance reasons, all other probe instances should be associated with a different network card.

If you feel a Gen2 card is not performing as expected, ensure that there is only one probe instance bound to it. If there is more than one, verify that the other probe instances are not collecting any statistics. It is possible that the probe instance you are looking at is not collecting any statistics, but one of the other probe instances may be. (This is only an issue if there are multiple probe instances connected to the Gen2 card. This does not apply if the other probe instances are connected to a regular network card.)
**Tweaking the statistics memory configuration**

There are two kinds of buffers that a probe instance uses to store data in real-time: a capture buffer and a statistical buffer. The capture buffer stores raw data captured from the network; the statistical buffer stores statistical entries and nothing more. This section is only concerned with statistical buffers.

The default statistics configuration is sufficient for most users and does not need to be changed. The memory settings are preconfigured based on network size and network type. Choose the type of network you are monitoring with this probe instance.

Each statistic is collected in its own section of RAM, where the processed data is stored. Alias List Entries is the first entry. It is used in the Discover Network Names portion of Observer. It has 800 allocated entries (stations), which consumes 114.4 kilobytes of RAM. When Discover Network Names is running, the captured packet is passed to the statistics queue buffer. After the data is processed, it is passed to the statistical memory buffer and to each relevant Observer statistic for that particular network type.

Observer collects statistics for numerous types of applications and trending, some of which may not apply to your network. You may increase or decrease the allocated entries as necessary.

For instance, if you are using Discover Network Names it will run until it fills the 800 stations. After it reaches 800 entries it cannot add any more because there is no memory space available. Any stations beyond 800 are not included in the list. You must increase the number of stations that may be allocated. This increases the memory requirements though. If you have 8,500 stations on your network, you will need at least 8,500 entries, which requires 1.2 MB of RAM.

Conversely, if you are not using statistics, such as VoIP, the RAM is still allocated to it. The default VoIP Trending is for 1,500 entries, which requires 12.6 MB of RAM. By reducing the allocated entries to 10 (the minimum) you need only 86.3 KB of RAM — saving nearly 12 MB to be used elsewhere.

By tweaking the statistics allocation, you can fine tune how Observer processes its data.

You cannot modify the default statistics memory configuration. You must create a new profile based on one of the existing profiles (Small, Medium, Large, 4G LTE) and modify it.

1. Click the Memory Management tab to display the list of probe instances and their buffer sizes.
2. Select a probe instance and click Configure Memory to change the packet capture or statistics queue buffer sizes. The Edit Probe Instance window opens.
3. Click the New button to open the New Statistics Memory Configuration window.
4. Type a name and choose which memory configuration on which you want to model yours. Click Finish. You have now created a new statistics configuration, but it is identical to the one you modeled yours on. You must now edit it.
5. Click Edit. Click Yes to the message that appears about needing to restart the probe software after making memory changes. The Edit Statistics Memory Configuration appears.
6. At the top, choose your network type from the list.
7. The statistic’s memory that you can modify are highlighted in yellow. To change the amount of memory for it, click in the Allocated Entries column and provide a new value. Repeat until you have tweaked the statistics memory for your needs.

**Troubleshooting common issues**

Use the information in this section to assist you if you have a problem with your probe not connecting to your analyzer, your probe does not have a network adapter available, or if you are using an nTAP and want to capture
NetFlow traffic or several other common issues. If you feel your probe is slow, see Troubleshooting a slow probe system on page 275.

Although most installations of Observer proceed without any trouble, due to the vast number of network configurations and hardware/software options that Observer supports, sometimes difficulty arises.

If you experience trouble in setting up Observer, keep a number of things in mind.

First and foremost, try to simplify your configuration in any way possible. This means if you have a screen saver loaded, disable it. If you are running some network add-on peer-to-peer jet engine turbo stimulator, remove it. This does not mean that you will not be able to use Observer with your other products but, if you can determine where the problem is, you can focus on that piece of the puzzle and you may be well on your way to solving the problem.

Second, do not trust anyone or anything. The only way to really know what your hardware settings are is to have the card or device in one hand and the documentation in the other. Programs which discover interrupts and other settings only function properly when everything is working correctly — exactly when you do not need them. Do not blindly trust other network drivers — they may or may not be reporting the correct information.

Third, do not, under any circumstances, share interrupts, I/O ports, or memory addresses between adapters. No matter what has worked before or what might work in the future, sharing interrupts or memory settings is not a valid configuration.

Troubleshooting checklist:

Does your network work without any Observer programs or drivers loaded? If not, check your network installation instructions. After your network appears to be running correctly, install Observer again. Try installing Observer on a different system and see if you experience the same problem. This does not mean that you will not be able to use Observer on the desired system. It may give you some insight into the problem that you are having.

Troubleshooting a slow probe system

If a probe is overloaded, consider whether any of the following affect the system. You can clear these one at a time to see if that resolves the system’s issue.

Although all of the settings discussed in this section are configured in the Observer analyzer, they are saved to the probe.

- A scheduled capture can be causing a system slow down. Determine if any scheduled capture is occurring. Capture > Packet Capture > Settings > Schedule tab.

- Some extra processing happens when you have triggers and alarms configured. Determine what alarms are enabled by clicking the Alarm Settings button in the lower left.

- Are you running real-time Expert Analysis? Observer requires some processing resources to get through the data, which could be a lot of data. Real-time expert processes data as it is received. This requires continuous processing of incoming data while the real-time expert is running.

- Are you collecting combined station statistics or protocol distribution summary for your network? If so, these could be causing the system to slow down. To determine if you are, click Options > Observer General Options > General tab. Scroll to the “Startup and runtime settings” and uncheck these, if necessary:
  
  # Collect combined station statistics at all times
  
  # Collect protocol distribution for the whole network

- Are you collecting network trending statistics? If so, is the sampling divider less than 10? If so, increase the sampling divider to 10 or greater. To determine your sampling divider, click Trending/Analysis > Network Trending > Settings > General tab. In the Collection Settings section, change the sampling divider.
A probe is not connecting to the analyzer or vice versa

If the probe is not connecting, it could be one of several reasons. The log window in the Observer analyzer has useful information to give you an idea of why the connection is failing. If the log window is hidden, choose View > Log Window to show it.

Verify the following:

- The probe is licensed. See Licensing and updating on page 6.
- Ports firewall and the traffic is actually passing through it. Observer uses these ports to communicate with the probe. See Ports used by Network Instruments products on page 12. Check any local system firewall as well as any network firewall. See also the information in Suspected NAT or VPN issues on page 279.
- Security and encryption settings match between the Observer analyzer and the probe. If the settings do not match, you will get a message that says “Probe redirection Error <IPAddress> Authentication Negotiation Error” or “Probe authentication failed <IPAddress>.” Either the security feature has been turned off for one side of the connection (but not the other), or their encryption keys do not match. In Observer, click Options > Observer General Options from the menu, then click the Security tab. On the probe, click the Security tab. Verify that the security properties match. If necessary, generate a new key and use that on both the probe and analyzer.
- The user name you are using from the analyzer exists on the probe. Although very uncommon, the default “Anyone” account can disappear. If it does and you use that account to connect, your connections are prohibited. If the Anyone account has been deleted, you can recreate it on the probe by clicking the Security tab, then the New User button. Click the “Create Anyone Account” button.
- If a Single Probe does not have a user name defined in the Options > Probe Redirection Settings, you must create a new account called “Anyone” (without quotes) and use that account to access the Single Probe.
- The probe and Observer analyzer are within the same minor build range. You can have the Observer analyzer automatically force an upgrade of an older probe version. See Upgrading the probe software on page 231.
- You can access the VLAN if the probe or Observer analyzer are on different VLANs. There is nothing you need to configure in Observer or the probe to enable a connection when they are on different VLANs. However, if you do not have network permissions to access a probe on a different VLAN, it is a network configuration issue (usually for security reasons) and you should contact the network administrator.

No network adapter available

After starting Observer, if you do not see any available adapters listed in the “Select Network Adapter” list, it means your NIC does not have the necessary driver or VMONI Protocol settings installed. Use this information to enable your adapter and to install the proper drivers.

1. If Observer is running, close it.
2. Ensure you are logged in to the system with an account with administrator rights.
3. From the Windows Start menu, choose Control Panel > Network and Sharing Center.
4. Click Change Adapter Settings.
5. Right-click any of the Local Area Connections and choose Properties.
6. Look at the list of installed components to verify that the VMONI Protocol Analyzer is listed. Then do one of the following:

# If it is not installed, skip to 7 on page 277.
# If the VMONI driver is listed, remove it. Select VMONI Protocol Analyzer and click the Uninstall button. After the VMONI driver is removed, restart the system and continue with 7 on page 277.

1. If Observer is running, close it.
2. Ensure you are logged in to the system with an account with administrator rights.
3. From the Windows Start menu, choose Control Panel > Network and Sharing Center.
4. Click Change Adapter Settings.
5. Right-click any of the Local Area Connections and choose Properties.
6. Look at the list of installed components to verify that the VMONI Protocol Analyzer is listed. Then do one of the following:

# If it is not installed, skip to 7 on page 277.
# If the VMONI driver is listed, remove it. Select VMONI Protocol Analyzer and click the Uninstall button. After the VMONI driver is removed, restart the system and continue with 7 on page 277.
7. From the Local Area Connection Properties (5), choose Install > Protocol > Add > Network Instruments – VMONI Protocol Analyzer and click OK. If the VMONI driver is not listed, click Have Disk, then browse to the VMONI.SYS file located in the Observer directory on your hard drive, select it, and click OK.

   The VMONI Protocol Analyzer will now be available to install.

8. Restart the computer after you have completed installing the driver.

You should now be able to select an adapter when starting Observer.

Integrated adapters report all sent packets with bad TCP checksum

**Symptoms:** All TCP packets sent from the Observer analyzer or probe station across an integrated network adapter contain bad TCP checksums.

**Causes:** Default driver settings for the card are incorrect. You must update the driver and then disable the “Offload Transmit TCP Checksum” option.

**Solutions:** Upgrade the driver for the integrated network adapter to the Network Instruments/Intel Pro 1000 adapter driver. This driver is located in the `<Observer installation directory>\Drivers\IntelPro1000` directory.

1. After upgrading the driver, right-click the adapter and go to Control Panel > Network Connections > Properties.
2. On the General tab, click the Configure button.
3. Click the Advanced tab and find the Offload Transmit TCP Checksum option and disable it.
4. Restart your system.

“No VLAN” shown while using a Gigabit NIC

**Symptoms:** “No VLAN” is displayed in VLAN Statistics and/or no 802.1Q tag information is shown in your decode. The network adapter you use to capture traffic is a Gigabit NIC.

**Causes:** Observer is not seeing the 802.1Q tag on packets being captured. This is sometimes caused by your switch not sending tagged packets to Observer. See VLAN Statistics tool is not working on page 277 for explanation/resolution before proceeding.

**Solutions:** If you are using a Gigabit NIC to capture the traffic and you have checked the switch configuration, then try using this solution. For BCM5751M NetXtreme Gigabit chips found in IBM T43, HP laptops, and Dell Latitude laptops; there is a registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet can cause the driver and chip not to strip the 802.1Q headers. To set that key, you must find the correct instance of the driver in Windows registry and change it.

1. Open the Windows registry editor. Start > Run > Command and type `regedit`.
2. Search for “TxCoalescingTicks” and ensure this is the only instance that you have.
3. Right-click the instance number (e.g., 0008) and add a new string value.
4. Type `PreserveVlanInfoInRxPacket` and give it the value `1`.
5. Restart the computer.

The Gigabit NIC no longer strips VLAN tags, so the symptom in Observer is resolved.

VLAN Statistics tool is not working

**Symptoms:** “No VLAN” is the only VLAN ID that shows up in the VLANs column in VLAN Statistics. You are not seeing all VLANs you have on the network.
**Causes:** To display VLAN Statistics, Observer checks each packet for a VLAN tag; if no tag is present, the packet is logged as “No VLAN.” Both 802.1Q or ISL VLAN tags are stripped unless the SPAN destination port to which the analyzer is attached has been configured to include VLAN tags.

**Solutions:** Configure the switch to retain the VLAN tags through the monitor port. This may be an option in the Mirror or SPAN command on the switch, or you may have to configure the port as a trunk prior to defining it as a SPAN port. Even if the switch is monitoring a trunk or uplink port it may strip VLAN tags unless you configure that port to retain the tags. Refer to the documentation from your switch for details on configuring VLANs, trunks, and analyzer ports.


If you use a Cisco Catalyst 4500/4000, 5500/5000, or 6500/6000 Series Switch running CatOS you must configure the destination port as a trunk port prior to configuring the SPAN port using the set trunk and set span commands:

```
set trunk
module/port
   [on | off | desirable | auto | nonegotiate]
   [vlan_range] [isl | dot1q | negotiate]

set span
source_port
destination_port [rx | tx | both]
```

For example, to configure module 6, port 2 for monitoring an 802.1Q VLAN setup, you would enter the following commands:

```
switch (enable) set trunk 6/2 nonegotiate dot1Q
switch (enable) set span 6/1 6/2
```

For Cisco Catalyst 2900/3500, 4500/4000 and 5500/5000 Series Switches Running IOS 12.1 or later, encapsulation forwarding is set as a part of the SPAN command, which has the following syntax:

```
monitor session session_number (source | destination)
   interface type/num [encapsulation (dot1q | isl)]
```

To monitor 802.1Q VLAN traffic passing through Fast Ethernet 02 via a SPAN port set up on Fast Ethernet 0/6, you would enter the following commands:

```
C4000 (config) # monitor session 1 source interface fastethernet 0/2
C4000 (config) # monitor session 1 destination interface
   fastethernet 0/6 encapsulation dot1Q
```

For a 6500/6000 Series Switch running Native IOS 12.1 or later you must configure the destination port as a trunk port prior to configuring the SPAN, which have the following syntax:

```
C6500(config)#Interface Type slot/port
C6500(config-if)#Switchport
C6500(config-if)#Switchport trunk encapsulation { ISL | dot1q }
C6500(config-if)#Switchport mode trunk
C6500(config-if)#Switchport nonnegotiate
```

To monitor 802.1Q VLAN traffic passing through Fast Ethernet 02 via a SPAN port set up on Fast Ethernet 0/6, you would enter the following commands:

```
C6500 (config) # interface fastethernet 0/6
C6500 (config-if) #switchport
C6500 (config-if) #switchport trunk encapsulation dot1q
C6500 (config-if) #switchport mode trunk
```
Using Discover Network Names on a Layer 3 switch that uses VLANS

**Symptoms:** While running Discover Network Names against a Layer 3 Switch that uses VLANs, you see only a limited number of MAC addresses, which typically have multiple IP Addresses associated with them.

**Causes:** Layer 3 Switches that have been configured to perform routing replace the originating station’s MAC Address with the MAC Address of the switch port. For example, suppose CADStation1 has a MAC Address of 00:00:03:AB:CD:00 and an IP Address of 10.0.0.1. It is connected to switch port 1 through a hub. Port 1 of this switch has a MAC Address of 00:11:22:33:44:55.

When a probe is connected to a SPAN or mirror port of that switch, it shows CADStation1 with an IP of 10.0.0.1 and MAC address of 00:11:22:33:44:55 rather than 00:00:03:AB:CD:00 because of this substitution.

Now, suppose there is another station (CADStation2) with MAC address of 00:00:03:AB:EF:01 and has an IP address of 10.0.0.2 that is also connected to port 1 of the switch through a hub. Because Discover Network Names stores station information by MAC address (i.e., the MAC address is the unique station identifier), it changes the IP address of switch port 1’s MAC address.

Because a switch configured as such hides originating station MAC addresses from Observer, MAC-based station statistics (such as Top Talkers-MAC, Pair Statistics matrix, etc.) can only be calculated by port. To make the Observer displays more useful, follow this solution.

**Solutions:** By examining the switch configuration you can obtain a list of MAC addresses that are associated with each port of your switch. Then, use Discover Network Names to edit the alias entry for 00:11:22:33:44:55, labeling it “SwitchPort1.”

The IP based statistical modes (Internet Observer, Top Talkers – IP (by IP Address) still show you statistics calculated from individual stations by their IP address. But MAC-based statistical modes (Pairs Statistics Matrix, Protocol Distribution, Size Distribution Statistics, Top Talkers –MAC (by hardware Address) will now show data by Port.

**Suspected NAT or VPN issues**

If you use network address translation (NAT) in your environment, you must make some configuration changes in Observer. Using the TCP/IP port information in Ports used by Network Instruments products on page 12, you should be able to set up the NAT properly.

If the probe is outside the network where Observer is running, you must forward port 25901 from the probe’s address to the system running Observer.

When redirecting the probe, you must specify the NAT outside IP address instead of the address that Observer puts in automatically. By default, Observer tries to use its local IP address, which the probe will not be able to find. Select “Redirect to a specified IP address” in the Redirecting Probe or Probe Instance dialog and type the VPN client’s IP address.

**Running Observer passively affects NetFlow**

When analyzing a link using a TAP, which is common, Observer runs “passively.” Passive operation guarantees that analysis will not affect the link; however, it does have some implications when running NetFlow. Because there is no link over which the system can transmit packets or frames, the following features are unavailable:

- Traffic Generation
- Collision Test
Replay Packet Capture

Daylight Savings Time

Observer is not coded with a specific date in mind. Daylight Savings Time is controlled by the operating system. When the clock rolls backwards or forwards, Observer rolls with it, with one exception: packet capture/decode.

Packet capture provides nanosecond time resolution, which none of the rest of the product does. Because of this, packet capture does not rely on the system clock to provide time stamps. It relies on the processor time ticks. When Observer opens it requests the system time and the number of processor time ticks and uses those. This allows Observer to know what date and time it is when a packet is seen.

Because the Observer only asks the operating system for the system time when Observer is started, packet capture does not know that the time has jumped forward or backward. To get this to happen you need restart Observer after the time change. It is that simple.

Configuring Cisco 6xxx switches using a SPAN port to a full-duplex Gigabit Probe

When using a full-duplex Gigabit Probe to capture directly from a SPAN/mirror port, use a straight-through cable from the Gigabit port on the switch to either port A or B on the Gigabit card in the probe. Do not use the Y-cable or TAP (the TAP and Y-cable should only be used inline).

To use the Observer analyzer with the Cisco 6xxx switch, you must disable auto negotiation. With auto negotiation enabled, the switch and probe may create a link when first starting the probe, but if the cable is unplugged or if a configuration change to the SPAN/mirror port is applied, you will lose connectivity to the switch. To turn auto negotiation off on the switch, follow the directions based on the OS you are using on your switch.

Tip! Disabling Auto Negotiation is recommended on all models/brands of switches when using a SPAN/mirror port to a full-duplex Gigabit Probe.

Cisco CatOS switches

1. To disable port negotiation:
   
   Console> enable
   Console>(enable) set port negotiation mod_num/port_num disable

2. To verify port negotiation:
   
   Console.(enable) show port negotiation [mod_num/port_num]

3. To enable port negotiation (should you remove the gigabit Observer product from the switch):
   
   Console>(enable) set port negotiation mod_num/port_num enable

Cisco IOS switches

1. To disable port negotiation:
   
   Console> enable
   Console# configure terminal
   Console(config)# interface gigabitethernet mod_mun/port_num
   Console(config-if)# speed nonegotiate

2. To verify port negotiation:
   
   Console# show interfaces gigabitethernet mod_mun/port_num

3. To enable port negotiation (should you remove the gigabit Observer product from the switch):
Console(config)# interface gigabitethernet mod_mun/port_num
Console(config-if)# no speed nonegotiate

Ports used by Network Instruments products

Firewalls are necessary for any network. These specific ports must be open to allow Network Instruments products to communicate with each other.

Network Instruments generally recommends that you open inbound and outbound TCP/UDP 25901 through 25905 on your firewalls for its products. This table lists more specifically what ports are used by your product.

<table>
<thead>
<tr>
<th>Ports</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 25901</td>
<td>Observer expert and trending data</td>
</tr>
<tr>
<td></td>
<td>Observer Reporting Server to Observer/GigaStor/Probe</td>
</tr>
<tr>
<td>TCP 25903</td>
<td>Observer/GigaStor/Probe redirection/connection request</td>
</tr>
<tr>
<td></td>
<td>GigaStor/Probe administration</td>
</tr>
</tbody>
</table>

Related Topics

- Network Trending on page 146
- Changing the monitored network adapter on page 237
- Installing the wireless NIC driver on Windows 7/Vista on page 229
- Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling on page 243
- Running Observer passively affects NetFlow on page 279
- Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling on page 243
- Creating a NetFlow collector or NetFlow Trending collector on page 265
- Generating NetFlow records from the GigaStor’s NetFlow Agent on page 295
- Processing NetFlow or sFlow data on page 92
- Choosing your network trending types on page 158
- Comparing software probe features on page 226
- Running Observer without reserved memory on page 269
- Viewing network errors on page 28
Chapter 18: Using Your GigaStor

Getting started using your GigaStor

A GigaStor probe is a hardware device with many terabytes of storage space to capture, store, and analyze your network traffic. All GigaStor probes use the Expert Probe software. Learn more about the Expert Probe in Using the Expert Probe software on page 255.

To get the most out of your GigaStor, you need:

- A good working knowledge of your network. You can use the Observer analyzer to gather information from your routing protocols and verify your network configurations, which is helpful when updating your network map.
- An understanding of the protocols that run on your network.

Follow these steps to get started with your GigaStor. The installation happens in two main parts. The first part is at the GigaStor probe in the server room. The second part continues at a desk using the Observer analyzer to connect to the GigaStor probe.

Before installing your GigaStor probe:

1. Where you should install your GigaStor probe is discussed in .
2. The GigaStor uses probe instances, and in particular a unique probe instance called an “active instance.” Learn more about probe instances and why you want to use them in What is a probe instance?.
3. After you have determined where to place your GigaStor probe, install the unit into your rack. It is important to install the RAID drives into the correct slots. Ensure that monitoring interfaces are connected to the appropriate data feeds (SPAN or mirror ports, TAPs, aggregation devices). Ensure the configuration of these third-party devices is done properly so data flows to the GigaStor.
4. By default the GigaStor probe’s name is a random mix of letters and numbers. Change the name of the GigaStor probe to something identifiable (such as the physical location or purpose). See Configuring a probe’s name and other probe options.

   In a typical installation, the GigaStor probe runs the Expert Probe software as a Windows service and a remote Observer analyzer connects to the GigaStor probe to complete the configuration.

   From the Observer analyzer system, complete the following steps. These steps requires that you have an Observer analyzer installed and licensed separate from the GigaStor probe.
5. Connect to the GigaStor probe from your Observer analyzer. See Connecting to a probe instance from an Observer analyzer.

6. By default the active instance is called “Instance 1” and there are no passive instances. Rename the active instance to something more meaningful (for instance, “Active Instance”) and create at least two passive instances. (You can create more passive instances later if you wish.) Although you renamed the GigaStor probe in 4, renaming the probe instance is different. For details, see Creating GigaStor active and passive probe instances. Pay attention to the special instructions if your GigaStor array is larger than 256 TB.

7. Set the adapter speed for the active instance. See Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.

8. The purpose of a GigaStor probe is to capture and store large amounts of data. By default the GigaStor is not set to capture any data. It must be enabled. To do that, you must have the GigaStor capture running. See Setting a schedule for when data captures should occur.

9. Using a passive probe instance, begin analyzing the traffic you are capturing. See Using the GigaStor Control Panel.

   After you have collected data, you will want to see what is happening on your network. See:
   # Mining data from your GigaStor on page 300.
   # Reconstructing streams of HTTP, VoIP, and more on page 318.
   # Examining your network traffic with forensic analysis on page 306.
   # Analyzing FIX transactions on page 323.

   Although not a complete list, these are common optional settings you may want to change. Use these options along with the rest of the information in this user guide to fine-tune your GigaStor. Although not a complete list, these are common optional settings you may want to change. Use these options along with the rest of the information in Using the GigaStor Control Panel on page 284 to fine-tune your GigaStor.

10. (Optional) If you want to track physical ports individually, ensure you enable “Track statistics information per physical port.” See Setting GigaStor's basic options.

11. (Optional) If you want to define the different subnets of your network so that GigaStor can track and report on them, see Defining your subnets in GigaStor.

12. (Optional) All GigaStor probes come with a Gen2 capture card. Details about this unique capture card, including physical port indexing or virtual adapters, is covered in.

13. (Optional) Since a GigaStor is designed to have several concurrent users attached to it, you should add user accounts to your probe. See Restricting access to probes with user accounts and Configuring access permissions for probe instances.

14. (Optional) Your reports and displays may be more complete and readable if you add devices to the GigaStor probe’s address book and define any custom applications to the list maintained by the probe.

15. (Optional) The default settings for the Observer analyzer is to not be aware of TCP connections that were opened after the GigaStor or packet capture started. You can change this default setting.

   a. Mine some data from the GigaStor. See Analyzing data without any filters on page 304. This opens the Decode and Analysis tab.

   b. Ensure the Expert Analysis tab is selected, then click the Settings button at the top. The Expert Global Settings window opens.

   c. Click the TCP/IP tab and clear the “Follow only newly opened TCP connections” option. A newly opened TCP connection is any connection established after Expert Analysis was started. If the conversation started before Expert Analysis was started, Observer cannot see it.
What is the GigaStor?

The GigaStor is a specialized probe appliance for capturing, storing, and analyzing high levels of network traffic over long periods of time.

It includes a high-performance Redundant Array of Independent Disks (RAID) coupled with the Gen2 capture card in a rack unit. The Gen2 capture card allows you to capture a number of different full-duplex media by swapping standard SFP or XFP modules in and out. When the Observer analyzer is connected to a GigaStor probe, the GigaStor Control Panel is enabled. The GigaStor Control Panel eases many tasks involved in capturing, storing, and retrieving massive amounts of network traffic.

Tip! Place GigaStors in the data center core. Locate near servers to capture their server-to-server traffic. The distribution layer is another optimal position for GigaStor.

By utilizing the included network TAPs, you can insert and remove the GigaStor around the network without disruption of flow. The GigaStor reports back to Observer Expert and Observer Suite analyzers for in-depth analysis.

If desired, GigaStor can be configured as a local console for on-site analysis.

Using the GigaStor Control Panel

This section covers the GigaStor Control Panel, its settings, and its use when you choose Capture > GigaStor Control Panel. It does not cover packet decoding or analysis like TCP, UDP, or VoIP Events, nor does it cover Connection Dynamics.

After the GigaStor probe is up and running on the network, you can use an Observer analyzer to view captures from the probe. In the Observer you use a special section of the analyzer called the GigaStor Control Panel. The major section of the GigaStor Control Panel are listed in Figure 91 on page 284.

Figure 91: GigaStor Detail and Outline Charts

The GigaStor Control Panel shows traffic on a time line graph, allowing you to select packets for decoding, analysis, and display by defining the time period you want to view, and the types of packets you want to include.

Use the sliders at the top of the time line chart to select the time period you are interested in analyzing, then click Update Chart and Update Reports to update everything to the new time frame. Right-click in the top chart to open additional controls.
If desired, you can further constrain the display of packets by MAC Stations, IP Stations, IP Pairs, etc., by clicking on the appropriate Statistics tab and selecting the items you want to see on the Detail Chart.

Press the **Settings** button. Under **General Options**, uncheck **Enable Analysis types** if you are not using 4G LTE, FIX, etc. This will remove them from the Reports/Statistics ribbon.

Use the left/right arrow on the Reports/Statistics ribbon to move it to the right to see the button if needed. Pressing this button maximizes or minimizes the Reports/Statistics section. Now you can more easily work with and view reports and statistics for your selected time frame. You can filter or select a specific area of interest, such as HTTP. Press the **Analyze** button and choose **Filter Using Selected GigaStor Entries** to open Expert Analysis and decode tools focused on just your area of interest.

### Non-GigaStor-specific settings

The GigaStor Control Panel is a portion of the Observer analyzer. Some settings in the Observer analyzer affect the GigaStor. Some things you may want to configure in Observer include:

- Discovering host names so that GigaStor resolves and uses host names. See the Discovery section in the Observer User Guide.
- Protocol definitions. This is particularly important if you have custom protocols you want to monitor. See the Discovery section in the Observer User Guide.
TCP/UDP/Server applications. By defining specific applications Observer can provide more detailed reports to you. Observer has many applications already defined, but you can add more if you wish. See the Discovery section in the Observer User Guide.

The default settings for the Observer analyzer is to not be aware of TCP connections that were opened after the GigaStor or packet capture started. You can change this default setting.

Mine some data from the GigaStor. See Analyzing data without any filters on page 304. This opens the Decode and Analysis tab.

Ensure the Expert Analysis tab is selected, then click the Settings button at the top. The Expert Global Settings window opens.

Click the TCP/IP tab and clear the “Follow only newly opened TCP connections” option. A newly opened TCP connection is any connection established after Expert Analysis was started. If the conversation started before Expert Analysis was started, Observer cannot see it.

**Setting GigaStor’s basic options**

This tab lets you configure many options for the GigaStor.

2. Click the Settings button.
3. Click the General Options tab. See **Table 50** for a description of each field of the GigaStor General Options tab.

   # Packet capture and GigaStor buffer size—This only applies to the active probe instance.
   # Partial packet capture size—This only applies to the active probe instance.
   # GigaStor indexing options—You may need to adjust the indexing information based on your network.
   # Capture and analysis options—What protocols are on your network? Are they all standard protocols, or do you have some custom or home grown protocols?
   # Other general GigaStor Control Panel options.

The Packet Capture Setup dialog is where buffer and packet specific options are set. You can access the Packet Capture Setup dialog by selecting Capture > Packet Capture and then clicking on the Settings button. The Capture Setup dialog is displayed.

**Table 50: GigaStor configuration options**

<table>
<thead>
<tr>
<th>Capture Buffer size</th>
<th>Only available if you are configuring an active GigaStor instance. Allows you to set the amount of Windows memory that Observer will set aside to store captured packets. Observer will show the buffer percentage full and give you an idea of what the best buffer size is for a particular situation. You will want to capture an event in as little time with as little buffer space as possible. Observer has no limitations on the amount of RAM that can be used for a buffer. You can allocate up to 4 gigabytes on 32-bit version of Observer, limited only by the physical memory installed on your system. On 64-bit systems, you are limited only by the amount of physical memory installed on the Observer PC. It is not recommended that you use Observer to view packets going to or coming from the Observer PC. If you need to look at the traffic to/from the Observer PC, install Observer on another PC. There are many reasons why this is not a good idea but, in general, you will see varying amounts of your own data with a protocol analyzer on your own PC. This is due to the architecture of the PC and</th>
</tr>
</thead>
</table>
the inability of Windows to multi-task the receiving and analysis of the data going and coming from the Observer PC.

<table>
<thead>
<tr>
<th>Setting GigaStor’s basic options</th>
<th>287</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capture Partial Packets</strong></td>
<td>by default, Observer will capture the entire packet. This option allows you to define a specific amount of each packet to capture to the buffer. For example, a setting of 64 bytes will result in Observer only capturing the first 64 bytes of every packet. Most of the pertinent information about the packet (as opposed to the information contained in the packet) is at the beginning of the packet, so this option allows you to collect more packets for a specific buffer size by only collecting the first part of the packet. In some forensic situations, a warrant may only allow an officer/agent to collect, for example, e-mail headers. Also, if the system is having trouble keeping up with bandwidth spikes, collecting partial packets can resolve the issue. To change the number of bytes captured in each packet, click the Change Size. This setting affects all analyzers that connect to this probe. You cannot change this setting unless you have administrative privileges to do so.</td>
</tr>
<tr>
<td><strong>Collect and Show GigaStor Information by</strong></td>
<td>Choose whether to show or hide the following tabs in the GigaStor Control Panel: MAC Stations, IP Pairs, IP Addresses, TCP Applications, UDP Applications, VLANs, MPLS, and Physical Ports. These options are for controlling statistical display only. All packets that the GigaStor sees are written to disk and is available for analyzing using the “Analyze” button. The value configured in these boxes determine the maximum number of stations that are indexed by the GigaStor and shown in the GigaStor Control Panel. If you are limiting MAC stations to 1000 (the default), it is the first 1000 MAC stations the GigaStor sees—not the most recent 1000. The maximum allowable IP Pairs is 100,000 (the default is 10,000).</td>
</tr>
<tr>
<td><strong>Capture and Analysis Options</strong></td>
<td><strong>Enable intelligent TCP protocol determination</strong>: Displays only known applications while hiding dynamic ports by using the TCP threeway handshake (SYN SYN+ACK ACK). Clearing this option shows all ports. <strong>Limit to ports defined in “Protocol Definitions”</strong>: Select this option to limit the ports shown to only those listed in the Protocol Definitions. See the Discovery section in the Observer User Guide. <strong>Track statistics information per physical port</strong>: When selected, causes the GigaStor to index the data it collects by Gen2 capture card physical ports. You can then display GigaStor Control Panel statistics by physical port. If this option is selected, then you also may want to enable the “Use physical port selections…” option also on this tab. <strong>Collect counts for all IP protocols in addition to TCP and UDP</strong>: Select this option to collect counts for all IP protocols (such as ICMP, OSPF, Multicast, etc.) not just TCP and UDP. If this option is not selected, TCP and UDP counts are still collected.</td>
</tr>
<tr>
<td><strong>Enable Analysis Types</strong>:</td>
<td>Choose whether to enable the GigaStor Control Panel to process and display these types of data. By unchecking these options the corresponding tab is hidden in the GigaStor Control Panel and you cannot analyze packets for these data types: <strong>Forensic Analysis (uses Snort rules)</strong> <strong>FIX Analysis</strong>: used to process FIX financial transactions. <strong>Microburst Analysis</strong>: used to process data to identify microbursts on your network, typically a concern for network administrators in trading firms, but also other companies.</td>
</tr>
<tr>
<td><strong>GigaStor Packet Sampling</strong></td>
<td>Packet sampling applies to the GigaStor Control Panel statistical displays, not saved packets. On probes connected to highly-saturated networks (especially multi-port probes), sometimes it is desirable to adjust the rate of statistical indexing to conserve probe processing and storage resources. The default (and recommended) setting is for Observer to automatically scale back the packets it uses to update the analyzer display based on system load. Alternatively, you can specify a Fixed Sampling Ratio to consider when updating the GigaStor Control Panel Charts and statistical displays. A sampling ratio of 1 means every packet is analyzed and a ration of 10 means every 10 packets are analyzed. From a statistics perspective analyzing every 10 or even 100 packets will provide the trends you need without burdening the system by analyzing every packet. For even more details, see Differences between statistics and packets on page 291.</td>
</tr>
<tr>
<td><strong>Stop capture when disk is full</strong></td>
<td>When selected, the GigaStor stops capturing packets when the disk array is full. The default behavior is to use circular (i.e.FIFO) disk writes, causing the oldest buffer files to be overwritten as newer traffic is captured.</td>
</tr>
<tr>
<td><strong>Use physical port selections…</strong></td>
<td>If “Stop capture when disk is full” is selected, you can choose this option to display statistics sorted by Gen2 capture card physical port. This is useful when you want to troubleshoot the individual links without having to load the capture buffer by clicking Analyze. If selected, you must also select the “Track statistics information per physical port” option in the Capture and Analysis Options section on this tab.</td>
</tr>
<tr>
<td><strong>Auto-update GigaStor chart…</strong></td>
<td>When selected, causes the listed actions to have the same effect as clicking the Update Chart/Statistics buttons.</td>
</tr>
<tr>
<td><strong>Keep focus on GigaStor…</strong></td>
<td>Keeps the focus in the GigaStor Control Panel instead of switching to the decode pane.</td>
</tr>
<tr>
<td><strong>Update display…in 30 second intervals</strong></td>
<td>When selected all tables will update in 30 second intervals. This does not affect web-based reports, only the real-time displays in the analyzer.</td>
</tr>
<tr>
<td><strong>Display only defined subnets</strong></td>
<td>When selected only defined subnets are displayed. The subnets must be defined on the Subnet tab. See Defining your subnets in GigaStor on page 294 for details about defining a subnet.</td>
</tr>
<tr>
<td><strong>Enable IP DNS resolution</strong></td>
<td>Select this option to enable IP DNS resolution within the GigaStor. If you have several thousand hosts, you may wish to disable this option as it may take a long time to resolve names for reports.</td>
</tr>
<tr>
<td><strong>Enable packet time charting…</strong></td>
<td>When selected packet time charts are created in small intervals if microburst analysis is disabled.</td>
</tr>
</tbody>
</table>

**GigaStor reports**

Tip! The reports in the GigaStor Control Panel share the many of the same options and configurations as reports available in Observer Suite.

There are several default reports available for you.

2. Click the Settings button.
3. Click the Reports Setup tab.
4. Select a report name and click Edit to change the report’s characteristics.
5. Use the arrow buttons to position graphs and tables on your report.
6. Double-click a section of the report to modify its caption, detail, and number format.

Understanding GigaStor protocol and port settings

Allow the GigaStor to get smarter by collecting more information. Over time as the GigaStor sees more of your network’s traffic, it gets smarter about the traffic on your network.

Unless you have a specific reason to do so, we recommend that you leave these options selected:

**Enable intelligent TCP protocol determination**—when checked, all new data collected is indexed by protocol, only if SYN-SYNACK-ACK packets are observed at the start of the conversation. If this combination is found, reports show this conversation by protocol name (or custom name), IANA name, or port number (based on statistics lists setting). Otherwise the conversation is not listed. If you try to analyze data prior to the time that this option was enabled, you will not see this data. Data must be collected with this option enabled for GigaStor reports to present the data correctly using the update reports button. By clearing this option, you ensure you get all protocol information regardless of SYN-SYNACK-ACK packets.

**Limit to ports defined in “Protocol Definitions”**—limits the displayed data to the ports specifically defined in the Options > Protocol Definitions dialog. Again, this is written to internal GigaStor index. This option only shows custom protocols defined on new data collected after a protocol port has been defined. You must also choose “Apply Protocol to all Instances” to ensure this data is shown on all instances used for analysis. By having this option unchecked, all ports are used.

If you want to track statistical information for each port on your capture card, then you should ensure **Track statistics information per physical port** option is selected.

For even more information about what these settings affect, see Differences between statistics and packets on page 291 and Understanding GigaStor indexing on page 292.

Capturing packets with the GigaStor

A GigaStor can accumulate terabytes of stored network traffic. To manage the sheer volume of data, the GigaStor probe indexes the data. You use the GigaStor Control Panel within the Observer analyzer to manage the capture, indexing, and storage of large numbers of packets over long periods of time. While the GigaStor Control Panel is active, standard packet captures are unavailable for that probe instance. You cannot run the two types of captures simultaneously.

While actively capturing packets, the GigaStor Control Panel tracks network statistics and indexes them by time as it saves the packets to disk. This allows you to quickly scan the traffic for interesting activity and create filters to focus on specific traffic using the slider controls and constraint options.

The GigaStor Control Panel also automates storage management by deleting the oldest data before storage runs out. This maintains a multi-terabyte “sliding windows” of time within which you can review and decode traffic. It also allows for passive (in other words, virtual) probe instances, which allow users to have their own instances (and security credentials) without duplicating data collection or storage.

You can view the sliding window as a time line chart. Depending on what constraint are in effect and your display options determine what appears on the chart. By using time selection sliders and other options, you can quickly acquire and analyze the packets by clicking the Analyze button. This opens the standard packet decode and analysis window. From there you can view packets, save them, and perform further filtering if desired.
Setting a schedule for when data captures should occur

One way to ensure you always have timely packet captures is to schedule them. For example, you may want to automatically start a packet capture at the beginning of business hours each day; you can accomplish this by scheduling your packet captures accordingly.

Scheduled packet captures only tell Observer when to automatically begin and end a packet capture. The true length of capture time still depends on the size of your capture buffer; after it fills, you are no longer capturing packets. In effect, all scheduled packet captures automatically end in one of two ways: the capture buffer becomes full or the capture ends at the scheduled time.

To schedule packet captures to begin at preset times, complete the following steps:

2. Click the Settings button. The GigaStor Settings window appears.
3. Click the Schedule tab.
4. Select one of the following scheduling types. For the GigaStor active instance you should choose “Always” unless you have a specific reason to choose a different option.
   - No scheduling—captures are never scheduled
   - Always—capture runs at all times
   - Daily at specified times—capture runs at same time each day
     You must specify a capture begin and end time by clicking the Add button for each day you select. Multiple time intervals are configurable, per day, if the times do not conflict.
5. In the Reserve scheduling for section, select GigaStor and click OK. You may receive a notice about scheduling reservation. If you do, click Yes to change the scheduling.
6. Click OK to confirm and save your changes

Trimming data from your captures for space or privacy

Typically, packet headers contain the most useful information because they contain routing information and protocol information. The packet payload counterpart, however, is sometimes wasteful to collect because most troubleshooting is done just with the header.

Under these circumstances, you may want to truncate most payload data from the packet header(s). In Observer, the result is a partial packet capture.

Some benefits of partial packet captures include:

- Smaller capture sizes
  - More overall storage space for packet captures
  - Greatly increases the effective storage size of a GigaStor (or other capture buffer)
- Performance metrics remain intact
- Increased overall privacy
- Least resource intensive capturing

Some disadvantages of partial packet captures include:

- Not all network traffic is stored to disk
  - Forensics may be hindered without full payload data
  - Data stream reconstruction may not work
To configure the GigaStor probe to trim all packet data beyond the first 64-bytes, choose Capture > Packet Capture > Settings > Capture Options tab, and enable Capture Partial Packets (Bytes).

1. In the Observer analyzer, choose Capture > GigaStor Control Panel.
2. Click the Settings button.
3. Click the General Options tab. See Table 50 for a description of each field of the GigaStor General Options tab.
4. Enable the Capture partial packets option and choose how many bytes to include in the capture. The rest of the packet beyond what you define is excluded and is not saved to disk.

   It is possible to decrease or increase the default 64-byte partial packet capture size. Click the Change Size button to set a custom value. From then on, each packets' bytes following the target value are discarded from capture.

Password protecting the ability to change partial packet capture size

Password protecting this option helps ensure your partial captures remain partial, saving you disk space and enhancing data subject privacy because payload is not recorded in full.

1. To password protect the ability to change partial packet capture size, in the Observer analyzer, choose Options > Security tab, and enable Require a Password to Change Partial Packet Capture Size.

Differences between statistics and packets

Observer uses packets and statistics about your traffic to provide you with information about your network. This topic describes why each is useful and why there may appear to be discrepancies between a statistical view and the actual packets.

At times you may notice what appears to be a discrepancy between what you see in the GigaStor Control Panel and what you see when you are analyzing packets in a selected time frame. The difference stems from the fact that the GigaStor Control Panel displays statistics based on a sample of the packets seen, but when you are analyzing a specific time frame you are viewing all of the actual packets.

The GigaStor uses samples for a couple of reasons. First, it is more efficient to sample large sets of data rather than to process each data point individually. Network traffic is ideally suited for statistical sampling. Second, statistics serve a different role than actual packets. Statistics are intended to give you an indication of what is happening with your network. If the statistics indicate you may have an issue, then you can use the actual packets saved in your GigaStor to further analyze the traffic.

By default the GigaStor uses a dynamic sampling ratio for statistics. This can be changed in the GigaStor Control Panel > Settings > General tab to a fixed sampling ratio of 1, 100, or whatever you wish.

Using dynamic sampling allows the GigaStor to make decisions about how sampling for statistics should be accomplished. The GigaStor makes its decisions based on the amount of memory available in the statistics queue buffer and the amount of packets coming into the Gen2 card. All statistical processing is handled in the statistics queue buffer (stored in RAM) and the size of this buffer is very significant for probe instances providing statistics information.

If you set GigaStor Packet Sampling to a fixed sampling ratio, the GigaStor collects its statistics based on your sampling ratio regardless of available system resources and traffic to the capture card. If, for example, you have the ratio set to 1, you are telling the GigaStor to sample every single packet that it sees. This has a potential negative side effect—especially in very high traffic conditions—because there could be a significant impact on the GigaStor’s processing resources (either write-to-disk or read-from-disk), thereby slowing other processes
active at the same time. The potential advantage is that your statistics will more closely resemble what you see in actual packet analysis, but may not exactly match it.

There are millions and millions of packets traversing your network. Over a long enough time frame the statistics are going to be equally valid if you sample every 10 or 100 or 1000 packets rather than every single packet. Again, statistics sampling does not prevent you from clicking the Analyze button to view the actual packets the GigaStor captured with no sampling at all.

This explains why you might see more stations in Top Talkers within Decode and Analysis than in IP pairs on the GigaStor Control Panel. Usually, the risk of packet loss significantly outweighs any discrepancy between the statistics in the GigaStor Control Panel and the actual packets it captured.

Understanding GigaStor indexing

This section describes how the GigaStor captures packets and indexes them for statistics.

Indexing is an important part of how the GigaStor is able to be as efficient as it is. A brief synopsis of indexing in the GigaStor is this:

- All captured packets are written to disk. None of the settings in the GigaStor Control Panel control what is written to disk in any way.
- Indexing is not used for packet capture. It is only for statistics.
- GigaStor Control Panel > Settings > Capture and Analysis options tells the GigaStor which packets to index for statistics.
- GigaStor Control Panel > Settings > Collect and Show GigaStor Indexing Information by tells GigaStor how many entries it can use every 15 seconds. After the maximum number of entries for a 15 second period is reached, new data that was not already being indexed is not indexed for that 15 second period; however, packets that were already being indexed continue to be indexed during that 15 second period.
- Every 15 seconds the GigaStor writes all indexed data for 15 second interval that was just indexed. The indexed data is cleared from memory and indexing of the next 15 seconds begins.
- Previously indexed data has no effect on any other 15 second interval, except for the need to see the SYN-SYN/ACK-ACK to begin collecting “new” server data. This means that if in one 15 second period the maximum number of entries was reached and a new conversation was started that continues into the next 15 second interval, there is nothing that prevents the subsequent 15 second interval from beginning to index the new conversation that was not indexed in the previous 15 second interval.
- When GigaStor Control Panel > Settings > Enable Intelligent TCP protocol determination is enabled, a SYN-SYN/ACK-ACK is required. After the GigaStor sees a SYN-SYN/ACK-ACK for a server, it no longer needs to see the SYN-SYN/ACK-ACK to collect data from that server on the port that it saw the SYN-SYN/ACK-ACK. If for any reason the GigaStor probe is not running, it needs to see the SYN-SYN/ACK-ACK to index data. If GigaStor Control Panel > Settings > Enable Intelligent TCP protocol determination is unchecked, the GigaStor does not need to see the SYN-SYN/ACK-ACK to ever index data.

For more details about indexing in the GigaStor continue reading the rest of this section.

Every 15 seconds the GigaStor writes indexed, statistical data into a GigaStor.ometa file on the D: drive. It contains only statistical (indexed) information “collected” by the GigaStor. This file and the statistics it contains have no relationship to what packets are written to disk. When the capture card sees any packet, it is immediately timestamped and passed to the GigaStor buffer. The GigaStor writes all packet data to disk regardless of whether a packet is indexed.

Also on the D:\ drive are a number of .odat files. These files contain the actual packets that are written to disk and used for analyzing.

The GigaStor does not index every single packet. There are a number of factors that result in a packet not being indexed. Anything you see in the GigaStor Control Panel should be used for reference, not as absolute numbers. For absolute numbers, you must analyze the packets and view them in the Decode pane.
At the beginning of each 15 second period (the 15 seconds is not based on the system time clock period, but on timestamps from the captured packets) the GigaStor takes all of the indexed data that it has and writes it into the GigaStor.ometa file. The GigaStor then clears out the statistical memory that was used for indexing during the 15 second collection period and begins analyzing the next 15 seconds for statistical data. After a packet has been analyzed, it is written to disk. If for some reason a packet is skipped, it is written to disk before the next packet is analyzed.

Again, not every packet is indexed. This does not mean that if a packet is not indexed, that it is not written to disk. The GigaStor writes every packet to disk, even if it is not indexed. If there are 1,000,000 packets that come in during a 15 second period, and the GigaStor only analyzes 85,000, it will still write 1,000,000 packets to the hard drive.

If the Screen Resolution in the GigaStor Control Panel is set to less than 15 seconds, the GigaStor does not use the index file (GigaStor.ometa) to see what was indexed because the time frame is smaller than 15 seconds. Instead it reads the data that is written to disk in the .odat file to produce the reports and not the indexed data.

The indexed, statistical information that comes from the indexed data is not 100% accurate when compared to packet capture. More importantly, it is not intended to be. It is, however, statistically accurate.

When the GigaStor attempts to analyze a packet to index, it does not analyze the packet if the packet is being analyzed by a different portion within Observer, such as Network Trending. Network Trending analyzes data for its own purpose. If a packet is being analyzed by Network Trending at the time the GigaStor wants to analyze the packet, the GigaStor skips the packet and goes to the next packet. The packet is written to disk, it is just not indexed.

After 15 seconds, the GigaStor starts over, so everything is cleared out and it all starts from zero entries per index data table, but the GigaStor does keep track of which devices it classified as servers. For instance, if in one 15 second period, the GigaStor sees a SYN-SYN/ACK-ACK and determines that port 8080 on 10.0.0.1 is a server, in the next 15 second period, the GigaStor does not require a SYN-SYN/ACK-ACK to know that port 8080 on 10.0.0.1 is a server. It already knows and continues indexing any 10.0.0.1 8080 as the server. The indexing of server 10.0.0.1 on port 8080 requires that either you establish 8080 as a known protocol or you have disabled the GigaStor Control Panel > Settings > Intelligent TCP Determination option. However, depending on which options are enabled and disabled, the GigaStor may completely ignore 10.0.0.1 on 8080 from being indexed.

Exporting GigaStor data for archiving

You can export your GigaStor-collected data on a scheduled basis. Use the Export tab to configure when and to where your data is saved or to manually export your data. You can manually export your GigaStor data in several file formats or you can schedule Observer to export the data.

Part of what makes the GigaStor searches so quick is that the data is indexed. Any data that is exported to a file is saved, but unindexed. The data remains in the indexed GigaStor file until it is overwritten. The exported data is always available and means you will still have access to the saved packet data, but you must load the capture file into the analyzer before you can search it. Having a good naming convention can help you find your files later.

Note: This process should be completed on the GigaStor probe itself by having the software running in Observer analyzer mode rather than Expert Probe. See Switching between the probe and analyzer user interfaces on page 256. This may require that you use Remote Desktop to access the system.

1. Redirect the probe instance to the local analyzer if it is not already connected to it. See Connecting to a probe instance from an Observer analyzer.
2. Choose Capture > GigaStor Control Panel.
3. Click the Settings button to open the GigaStor Settings dialog.
4. Click the Export tab.
5. Choose how you want to export the data and in which format (bfr, pcap, or cap). You can choose to schedule the export so that it happens automatically, or you can choose to manually export the data on an “as needed” basis.

6. (Optional) Choose if you want to have Observer write a progress status every 30 seconds to the Log window.

**Configuring your GigaStor**

Your GigaStor probe can be configured in many different ways and tuned for your environment.

### Defining your subnets in GigaStor

You can specify subnet properties for the GigaStor to allow for statistical aggregation of devices within the Statistics tabs in GigaStor Control Panel.

2. Click the Settings button.
3. Click the Subnet tab.
4. Use the Add, Delete, Modify, and Delete All buttons to configure the subnet settings for the GigaStor. When you define subnets in the GigaStor Control Panel, the Observer analyzer adds that subnet information to its index files. All future data analyzed will have subnet filtering readily available as well as statistical data. On the IP Stations tab you see your subnets and you can perform statistical analysis based on subnets.

   When you analyze data from captures with index files without any subnets defined, there will be no subnet available in the IP stations tab even if the analyzed data includes some index files with the new subnet information.

### Tracking individual analysis ports

When using the Gen2 capture card in your GigaStor, you can track statistical information per physical port. Data captured by the Gen2 capture card is indexed to show on which port the data arrived. You can further choose to use physical ports to filter statistics. This means that information on the Statistics tab at the bottom of the GigaStor Control Panel is dependent on which physical ports are selected.

**Note:** If you are using virtual adapters on your Gen2 capture card in your GigaStor probe, you should not attempt to analyze the packets on a per-port basis.

2. Click the Settings button.
3. Click the General Options tab. See Table 50 for a description of each field of the GigaStor General Options tab.
4. Enable these two options:
   - Track statistics information per physical port
   - Use physical port selections to filter statistics

### Configuring the packet capture and GigaStor buffer size

Allows you to set the amount of RAM that Observer will dedicate to the capture buffer cache for this instance. This configuration value has been pre-set for optimum performance given a single active GigaStor monitoring instance. The default settings allows enough memory to set up a number of passive GigaStor instances.
If you wish to run multiple active monitoring instances to watch multiple links or networks, you can decrease the capture buffer size dedicated to GigaStor collection, which frees some memory for creating other probe collection instances. Inadequate memory allocation to GigaStor collection can affect performance and result in dropped packets during high load periods.

A GigaStor Instance can be as large as the physical memory installed on your system after subtracting the memory dedicated to Windows and other probe instances.

To change the allocation for this probe instance, click the Configure button, which will display the probe instance, Memory and Security Administration dialog.

In all cases, the actual buffer size (Max Buffer Size) is also reduced by 7% for memory management purposes. Should you try to exceed the Max Buffer Size an error dialog will be displayed indicating the minimum and maximum buffer size for your Observer (or probe) buffer.

### Generating NetFlow records from the GigaStor’s NetFlow Agent

The GigaStor probe has the ability to publish any NetFlow flows generated by its network adapter using the NetFlow Agent, including flows from any virtual adapter on the Gen2 card. The data outputs for NetFlow are sent to a NetFlow collector for further analysis.

All NetFlow flows generated by the GigaStor probe are template-based using the Cisco NetFlow v9 templates. See the [Cisco documentation](#) for details about the NetFlow flow-based record formats and what is contained in the flow records. The GigaStor generates the flows adhering to the NetFlow v9 standards.

Only NetFlow version 9 and higher 10 (also known as IPFIX) are supported by the NetFlow Agent.

2. Click the Settings button to open the GigaStor Settings dialog.
3. Click the NetFlow Agent tab.
4. Select Enable NetFlow Agent option.
5. In the Destinations section, click Add and type the IP address of the system with your NetFlow collector. By default port 9996 is used for NetFlow. Change it if needed.
6. Enable the various data outputs and how frequently you want the template published. The GigaStor collects the datagram information continuously and publishes it every 15 seconds (the GigaStor’s fixed collection interval).

   is now configured to publish NetFlow records to the NetFlow collector of your choice. This could also be a GigaStor probe.

7. To view the NetFlow records in the GigaStor Control Panel, choose **File > Load and Analyze** Observer Capture Buffer. Find the buffer file you want and open it.
8. The buffer opens to the Decode and Analysis tab. Click the Decode tab.
9. Search the buffer for the records that interest you. Figure 93 shows how the Observeranalyzer displays captured NetFlow records and what the NetFlow templates format is for that record. See the [Cisco documentation](#) for details about the NetFlow records, templates, and formats.
Configuring options for the GigaStor charts, graphs, and reports

Detailed Chart tab

This tab lets you choose the appearance, colors, and scale of the Detail chart. The Detail chart is the top graph of the GigaStor Control Panel.

2. Click the Settings button.
3. Click the Detailed Chart tab.
4. Choose the appearance settings you want for the Detail Chart.
GigaStor Outline

This tab lets you choose the appearance, colors, and scale of the Outline Chart. The Outline chart is the bottom graph in the upper portion of the GigaStor Control Panel.

1. Choose **Capture > GigaStor Control Panel**.
2. Click the Settings button.
3. Click the Outline Chart tab.
4. Choose the appearance settings you want for the Outline Chart.

Capture Graph tab

This tab lets you choose the appearance, colors, and scale of the Capture Graph. The Capture chart is the graph on the bottom right of the GigaStor Control Panel.

1. Choose **Capture > GigaStor Control Panel**.
2. Click the Settings button.
3. Click the Capture Graph tab.
4. Choose the appearance settings you want for the Capture Graph.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>allows you to select which item will be configured.</td>
</tr>
<tr>
<td>Item color</td>
<td>allows you to select the color of the display item.</td>
</tr>
<tr>
<td>Item plot</td>
<td>allows you to select the item to be displayed as Lines or Bars. This will only be active if Lines is selected in the Item plot.</td>
</tr>
<tr>
<td>Item line thickness</td>
<td>allows you to select the thickness of the displayed item (in pixels).</td>
</tr>
<tr>
<td>Graph Times</td>
<td>allows you to set how the X axis will be displayed. Clock time will show times using a 24-hour clock (i.e., the current time). Relative time will display times from the start of the activation of the mode.</td>
</tr>
</tbody>
</table>

Statistics Lists tab

Observer tracks and makes many statistics available to you. You can control how those statistics are displayed for your GigaStor. This tab lets you customize how MAC address, IP address, IP Pair, and port information are displayed in the various constraint tab statistical listings.

1. Choose **Capture > GigaStor Control Panel**.
2. Click the Settings button.
3. Click the Statistics Lists tab.
4. Choose how you want the statistics to be displayed.

Monitoring and maintaining the GigaStor RAID array

There is very little that must be done with the RAID other than to install the drives and, if you wish, monitor the drives in the RAID array.
To maintain your GigaStor, you may want to

- Get e-mail notifications if a drive in the RAID array is failing.
- Clean up disks to maintain performance.
- Get e-mail notifications if a drive in the RAID array is failing.
- Clean up disks to maintain performance.

**Monitoring the RAID drives through e-mail notifications**

The RAID array is built at the factory and then the drives are removed and packaged separately to minimize the risk of hardware damage during shipping.

Network Instruments does not recommend you attempt to do anything with the RAID without contacting its Support department. You could lose some or all data on the array.

Network Instruments uses a third party monitoring tool to monitor the RAID array. It is developed by Areca. You can be notified by e-mail if there is an issue with the array.

1. Choose Start > All Programs > Areca Technology Corp > ArcHttpSrvGui > Areca HTTP Proxy Server GUI. The program starts. You should see something similar to Figure 94.

Figure 94: Areca RAID application

2. Select Controller#01 and click Launch Browser. If the controller is not running, click the Start button then launch the browser. The Areca RAID application attempts to connect to its web server.

3. Type the user name and password. The default user name is **admin**. There is no default password. Click OK to open the browser.

   In the browser you can see the RAID set, IDE channels, Volume, and capacity.

4. Along the left, click System Controls to expand the list and click Alert By Mail Config. This opens the page for you to add your contact information.
5. Complete the page with the details for your SMTP server and users to be notified.

Figure 95: RAID array e-mail notification

6. Close the web browser and minimize the Areca application to the task bar.

Cleaning the disk to maintain write performance

As the GigaStor RAID array is filled and refilled, disk fragmentation can occur over time. Rather than running a time-consuming system-level disk fragmentation utility, you can automatically delete all of the data files that store probe instance data. When disk writes begin again on a clean disk, the files are written contiguously until the disk fills.

Clean the disk whenever system performance seems to be slowing down. To prevent disk write performance from degrading, perform the cleanup on a schedule. For heavily used GigaStor probes (over 50% utilization), perform this operation twice a month. For more lightly used GigaStor probes (5-10% utilization), cleaning every two months is sufficient.

Before cleaning the disk, ensure you have identified and saved any data of interest or you will lose the data. See Exporting GigaStor data for archiving on page 293.

To clean the GigaStor RAID array:

1. Select the active probe instance and then choose Capture > GigaStor Control Panel. You cannot clean the array from a passive probe instance.

2. Choose Tools > Delete All Instance Capture Data.
Mining data from your GigaStor

Retrieving data from GigaStor and analyzing it is a primary function of the GigaStor Control Panel. You can use the information in the packet capture to identify numerous network conditions. By using filters and a specific analysis type, you can hone in on the exact information you want.

You have different options when you want to analyze captured data. You can analyze the data:

- Without any filters.
- With filters from the Observer filter editor.
- With filters from the GigaStor Control Panel.
- By combining filters from the GigaStor Control Panel and the Observer filter editor.

Table 51 on page 300 describes the different options available on the GigaStor Analysis Options screen that appears when you click the Analyze button on the GigaStor Control Panel.

All packets captured by the probe are time stamped immediately as it is seen by the capture card interface and then passed to the capture buffer. This ensures the most accurate timestamp.

**Table 51: GigaStor Analysis Options**

<table>
<thead>
<tr>
<th>This option…</th>
<th>Allow you to do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis Time Range</td>
<td>Shows the start and end time of the time range you selected in the Detail Chart. You can change the time here if you wish.</td>
</tr>
<tr>
<td><strong>Analysis Options</strong></td>
<td></td>
</tr>
<tr>
<td>Analyze all data (no filtering)</td>
<td>Takes all packets in the selected time frame on the Detail Chart and analyzes it using the analysis type chosen at the bottom of the screen, but without using any filter. See Analyzing data without any filters on page 304.</td>
</tr>
<tr>
<td>Select an existing filter</td>
<td>Takes all packets in the selected time frame on the Detail Chart and analyzes it using the analysis type chosen at the bottom of the screen and applies the filter you select (after clicking OK). See Analyzing data with filters from the Observer filter editor on page 304.</td>
</tr>
<tr>
<td>Filter using selected GigaStor entries</td>
<td>Takes all packets in the selected time frame on the Detail Chart and creates a one-time use filter for you using the options you chose from the Mac Stations, IP Stations, IP Pairs or any of the other tabs in the GigaStor Control Panel. See Analyzing data by combining GigaStor Control Panel and Observer filters on page 305</td>
</tr>
<tr>
<td>This option...</td>
<td>Allow you to do this...</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>4G LTE Device by IMSI</td>
<td>Takes all packets in the selected time from on the Detail Chart and allows you to choose the Device IMSI and whether control plane and user plane packets are included in the analysis.</td>
</tr>
<tr>
<td>VoIP and Videoconferencing calls by SIP tag</td>
<td>Takes all of the packets in the selected time frame on the Detail Chart and allows you to extract VoIP and videoconferencing calls based on a SIP tag. For further details about the Settings, see How to extract VoIP and video calls from your GigaStor on page 168.</td>
</tr>
<tr>
<td>Reorder and filter based on trailer timestamp</td>
<td>Some switch aggregators add their own timestamp to packets and can cause packets to have a different order than they were actually seen by the GigaStor. If selected, Observer reorders and filters packets based on the timestamp information from the switch aggregator you chose from the list instead of from the GigaStor. This is limited to post capture analysis only, and does not affect real-time analysis, triggers and alarms, or trending analysis. If you save a packet capture after it has been reordered using this option, the packets are saved in the reordered series. If you load a saved, reordered packet capture, then analysis is based on the reordered time frames and not the time stamps from the GigaStor.</td>
</tr>
<tr>
<td>Include Expert information in analysis filter</td>
<td>Expert Information packets provide context of network conditions during the time that the traffic was captured. The expert frames may provide you insight into what was happening that may have influenced a condition within a packet capture you are analyzing.</td>
</tr>
<tr>
<td>Display selected filter before starting analysis</td>
<td>Allows you to view the filter before Observer begins analyzing the packet capture. For example, you might choose this option if you have already used the filter and the output is has excluded traffic you were expecting. By displaying the filter, you can inspect it to see why it may excluding the traffic.</td>
</tr>
</tbody>
</table>

**Analysis Type**

<table>
<thead>
<tr>
<th>Analysis Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expert analysis and decode</td>
<td>Along with the packet decode, this provides Observer's advanced expert analysis, such as protocol analysis, top talkers, Internet Observer, Application Transaction Analysis, VLAN information, and Forensic Analysis using Snort. Use this option if you want to deep dive into the packets with ability to view common services and applications, response performance by severity, port-based protocols with slow response, network and application problems with local traffic and WAN/Internet traffic distinction, and more.</td>
</tr>
<tr>
<td>Decode without expert analysis</td>
<td>Provides a packet decode without any of the insight of expert features listed above.</td>
</tr>
<tr>
<td>FIX analysis</td>
<td>Used in conjunction with a FIX analysis profile, the results are displayed on the FIX Analysis tab in the GigaStor Control Panel. See Analyzing FIX transactions on page 323. Use this option if you need to see the raw FIX protocol packets and headers, highlight just the FIX data, filter a trade by order ID for further analysis, or to validate a specific transaction.</td>
</tr>
<tr>
<td>Forensic analysis</td>
<td>Allows you to choose a profile where you have defined which Snort rules you want to use. The results are displayed on the Forensic Analysis tab in the GigaStor Control Panel. If you chose “Expert analysis and decode” and decided you also wanted to do forensic analysis, you could do that by clicking the Forensic Analysis tab, which prompts you for a profile. Use this option if you need to scan high-volume packet captures for intrusion signatures and other traffic patterns that can be specified using the familiar Snort rule syntax. You can enforce your “acceptable use” policies, fight industrial espionage, and assist with government...</td>
</tr>
<tr>
<td>This option...</td>
<td>Allow you to do this...</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>regulations like Sarbanes Oxley or HIPPA requirements. Using network forensics you can provide pre-intrusion tracking and identification while delivering a paper trail after any intrusion. Or you can perform network troubleshooting using root-cause analysis and identify network problems that have been around awhile. See Examining your network traffic with forensic analysis on page 306.</td>
<td></td>
</tr>
<tr>
<td>Microburst analysis</td>
<td>Analyzes the selected time frame for any microbursts (as defined in the Microburst Analysis Settings dialog) and displays the results in the Microburst Analysis tab of the GigaStor Control Panel. This is an easier way to find microbursts across a much longer time frame than using the Detail Chart where the longest time frame that can be analyzed is 15 minutes. Use this option if you need to monitor applications that are sensitive to microbursts, such as financial, audio, video, or multicast applications. See Searching for microbursts on page 313.</td>
</tr>
<tr>
<td>Trading Multicast analysis</td>
<td>Analyzes the selected time frame for trading multicast streams issues on your network specifically related to stock exchanges. The streams can be analyzed for tracking UDP sequence numbers, multiple protocol data units (PDUs) within a UDP packet, and stream type or ID. Use this option if you want to analyze any of the Trading Multicast streams Observer supports.</td>
</tr>
<tr>
<td>IPTV analysis</td>
<td>Analyzes the selected time frame for IPTV traffic on your network. IPTV is configured by providing the multicast stream IP (or range of IPs) and, optionally, the UDP ports used to transport the content, along with the receive capabilities of the devices consuming the IPTV feeds. These settings allow Observer to identify IPTV traffic of interest (the IP and UDP ports) and to accurately calculate metrics about the quality of the feed for the endpoints, such as MDI, by providing the Delay Factor and Media Loss Rate information.</td>
</tr>
<tr>
<td>4G LTE analysis</td>
<td>Analyzes the captured 4G LTE traffic from the selected time frame. The 4G traffic can be filtered by IMSI and you can choose to exclude devices rejected from your 4G LTE network. Use this option if you want to analyze 4G LTE traffic for control or data plane issues or to isolate a specific end user’s quality issues. See How to analyze 4G LTE traffic from your GigaStor on page 320 for more details.</td>
</tr>
<tr>
<td>Multiple GigaStor analysis</td>
<td>Combines and analyzes data streams from two or more active probe instances. The active probe instances are typically from multiple GigaStor probes, but can also be from the same GigaStor probe. Use this option if your GigaStor probes captured the same data from two or more perspectives and you want to compare them using MultiHop Analysis. The MultiHop Analysis can be based on IP, IP Pair, IP port, or a filter. Or use it when two or more perspectives are capturing different parts of the same communication (one send and the other receive; or 50% of the connections to an application on one and 50% on the other) and you want to combine the data to get a complete picture of the communication. This might be due to the way traffic was routed (and eventually captured) or part of an architectural decision to load balance the traffic across multiple physical capture appliances.</td>
</tr>
<tr>
<td>Third Party Decoder</td>
<td>Observer allows you to use other software to view packet decodes if you wish, although Observer’s expert information is not available. You might do this because the other tool’s interface or workflow. This option is only available if the Third Party Decoder option has already been enabled in Options &gt; Observer General Options &gt; Third Party Decoder. By default the menu text is “Decode Capture File using Wireshark,” but is completely configurable. See Third Party</td>
</tr>
</tbody>
</table>
Selecting a time frame to analyze

The GigaStor Control Panel has two graphs along the top: a Detail Chart and below it a Outline Chart. The Detail chart shows a shorter time frame. The Outline Chart shows a longer time frame with the Detail Chart being a portion of time from within Outline Chart.

You can configure the resolution of Detail Charts by clicking the “Screen resolution” option and using the slider to pick a time resolution. It can be anything from 8 hours/8 weeks so that you can see longer term trends to as short as 10 nanoseconds/500 nanoseconds to focus on specific issues. At the shorter time resolutions you can enable microburst analysis. The “Data type” list specifies what type of data appears in the Detail Chart.

You can configure the amount of time shown on the Outline Chart by right-clicking it and choosing “Outline Time Resolution.” It is measured in multiples of the Detail Chart. You may also choose to show packets or load in the chart.

If you know the time when something occurred that you want to investigate, you can jump to that time by right-clicking the Detail Chart and choosing “Go to Specific Time.”

The FIFO/sampling/cpu gauge on the right side tracks how well GigaStor’s disk hardware is keeping up with the current trafficload. Its data is only for the active GigaStor instance (the data always reads “0” for passive GigaStor instances) and indicates the following:

- FIFO – shows how efficiently the probe is processing and monitoring packets
- Sampling – indicates the ratio of how many packets are being sampled/processed compared to the number of packets witnessed. It is shown as: \(1/sampling\, divider\)
- CPU – How much CPU the probe is using to sample packets

If the FIFO gauge shows 90% or greater, you should consider reducing the load using one or more of the following methods:

- Allocate more memory to the GigaStor instance.
- Activate partial packet capture or reduce the size of portion captured.
- Activate dynamic sampling, or increase the fixed sampling ratio.

<table>
<thead>
<tr>
<th></th>
<th>10%</th>
<th>50%</th>
<th>90%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits/sec in Interval</td>
<td>1,000,000</td>
<td>5,000,000</td>
<td>9,000,000</td>
</tr>
<tr>
<td>Bytes/sec in Interval</td>
<td>124.476</td>
<td>617,826</td>
<td>1,111,176</td>
</tr>
<tr>
<td>Bytes/sec in Interval with IFG</td>
<td>125,000</td>
<td>625,000</td>
<td>1,125,000</td>
</tr>
<tr>
<td>Megabytes/sec</td>
<td>0.119</td>
<td>0.596</td>
<td>1.073</td>
</tr>
<tr>
<td># of packets/Interval</td>
<td>82</td>
<td>407</td>
<td>732</td>
</tr>
<tr>
<td>Max # of microbursts in Interval</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Max bits of duration from Utilization Threshold</td>
<td>100,000</td>
<td>500,000</td>
<td>900,000</td>
</tr>
<tr>
<td># of bits per Duration for microburst</td>
<td>50,000</td>
<td>250,000</td>
<td>450,000</td>
</tr>
</tbody>
</table>
Analyzing data without any filters

1. Select a time frame you want to analyze. See Selecting a time frame to analyze.
2. Click the Update Reports button to get the latest data from the time frame selected. This is unnecessary if you have “Auto-update GigaStor chart on statistics tab or selection change” in the GigaStor Settings. See Setting GigaStor’s basic options.
3. Click the Analyze button. The GigaStor Analysis Options window opens.
4. Select “Analyze all traffic in the analysis interval” and click OK.

Your unfiltered data appears in a new “Decode and Analysis” tab.

Analyzing data with filters from the Observer filter editor

1. Select a time frame you want to analyze. See Selecting a time frame to analyze.
2. Click the Update Reports button to get the latest data from the time frame selected. This is unnecessary if you have “Auto-update GigaStor chart on statistics tab or selection change” in the GigaStor Settings. See Setting GigaStor’s basic options.
3. Click the Analyze button. The GigaStor Analysis Options window opens.
5. Choose one or more filters that you want to use and click OK.

Your filtered data appears in a new “Decode and Analysis” tab.

Analyzing data with filters from the GigaStor Control Panel

You may want to filter the data that is shown on the Detail Graph. You can do so with the filters section of the GigaStor Control Panel. You can filter data from MAC Stations tab, IP Stations tab, IP Pairs tab, and more.

One example where you might use this is if you have strange traffic (perhaps a virus) on your network that you want to identify or isolate. By selecting a station from IP Stations tab and an application from the TCP Applications tab, you can select the “Combine tabs for detailed chart pre-filter” to generate a specific report. Using this report you can understand the general pattern of activity of the strange traffic so that you can conduct further analysis using packet decodes.

If you are using the Ethernet Physical Port filter in conjunction with other filters, in the GigaStor Control Panel > Settings > General Options tab, you must enable the “Use physical port selections to filter statistics” option otherwise the combined filter will not work as you expect.

1. Select a time frame you want to analyze. See Selecting a time frame to analyze.
2. Click the Update Reports button to get the latest data from the time frame selected. This is unnecessary if you have “Auto-update GigaStor chart on statistics tab or selection change” in the GigaStor Settings. See Setting GigaStor’s basic options.
3. Click the IP Stations tab (or any statistics tab to the right of the Summary tab).
4. Select one or more stations. This creates and opens a GigaStor Control Panel filter.
5. Click other tabs and choose what entries you want to add to your filter, such as an application from the TCP Applications tab. When selecting options from different tabs a filter is built, and it uses a logical AND to build it.

6. Click the Update Chart button. This refreshes the Detail Chart using the filter you built.

You have filtered data in the GigaStor Control Panel, which may suffice. You can also choose to further analyze the data. See Analyzing data by combining GigaStor Control Panel and Observer filters on page 305.

Analyzing data by combining GigaStor Control Panel and Observer filters

If you chose “Create analysis filter using checked GigaStor entries” and do not have any data or do not have the data you expected, it may be because you applied too many filters. Try the “Analyze all traffic in the analysis interval” option instead.

1. Complete the procedure in Analyzing data with filters from the GigaStor Control Panel.
2. After you have a filtered chart, click the Analyze button. The GigaStor Analysis Options window opens.
3. Because you are analyzing data with checked GigaStor entries, you have two choices:
   # Analyze all traffic in the analysis interval—Uses the filtered data as-is and analyzes it.
   # Create analysis filter using checked GigaStor entries—Creates a second filter and applies it to the already filtered data.
4. Click OK.

Your filtered data appears in a new “Decode and Analysis” tab.

Analyzing multiple GigaStor probe instances from one GigaStor Control Panel

Combining the data of multiple GigaStor probe instances into one GigaStor Control Panel allows for quick and easy isolation of information.

One example where you might use this is if you need to find information but are unsure which GigaStor probe instance to query. Instead, you can combine the data of any GigaStor probe instances you have access to and perform just one query.

**Note:** The GigaStor Control Panel must be open for every GigaStor probe instance you want to combine for analysis.

To analyze multiple GigaStor probe instances from one GigaStor Control Panel:

1. Choose Capture > GigaStor Control Panel

---

**Figure 97: GigaStor Control Panel filter**

- Click other tabs and choose what entries you want to add to your filter, such as an application from the TCP Applications tab. When selecting options from different tabs a filter is built, and it uses a logical AND to build it.
- Click the Update Chart button. This refreshes the Detail Chart using the filter you built.

You have filtered data in the GigaStor Control Panel, which may suffice. You can also choose to further analyze the data. See Analyzing data by combining GigaStor Control Panel and Observer filters on page 305.

Analyzing data by combining GigaStor Control Panel and Observer filters

If you chose “Create analysis filter using checked GigaStor entries” and do not have any data or do not have the data you expected, it may be because you applied too many filters. Try the “Analyze all traffic in the analysis interval” option instead.

1. Complete the procedure in Analyzing data with filters from the GigaStor Control Panel.
2. After you have a filtered chart, click the Analyze button. The GigaStor Analysis Options window opens.
3. Because you are analyzing data with checked GigaStor entries, you have two choices:
   # Analyze all traffic in the analysis interval—Uses the filtered data as-is and analyzes it.
   # Create analysis filter using checked GigaStor entries—Creates a second filter and applies it to the already filtered data.
4. Click OK.

Your filtered data appears in a new “Decode and Analysis” tab.

Analyzing multiple GigaStor probe instances from one GigaStor Control Panel

Combining the data of multiple GigaStor probe instances into one GigaStor Control Panel allows for quick and easy isolation of information.

One example where you might use this is if you need to find information but are unsure which GigaStor probe instance to query. Instead, you can combine the data of any GigaStor probe instances you have access to and perform just one query.

**Note:** The GigaStor Control Panel must be open for every GigaStor probe instance you want to combine for analysis.

To analyze multiple GigaStor probe instances from one GigaStor Control Panel:

1. Choose Capture > GigaStor Control Panel

---
2. Click Tools.
3. Click Select GigaStors for Combined Indexing.
4. Choose two or more probe instances and click Apply.
   If a particular GigaStor probe instance is not listed, ensure the GigaStor Control Panel for that instance is open and try again.
5. Click Update Reports to start combining index data.
6. After the process completes, the currently open GigaStor Control Panel is showing a real-time aggregate of multiple GigaStor probe instances.

After completing this task:

Simply use the combined GigaStor Control Panel the same way as a non-combined GigaStor Control Panel. See Using the GigaStor Control Panel on page 284 for details.

**Examining your network traffic with forensic analysis**

Network forensics is the idea of being able to resolve network problems through captured network traffic. Previous methods of network forensics required you to be able to recreate the problem. Using the GigaStor you do not have to recreate the problem — you already have the captured packets. Instead of reacting to a problem, you can use network forensics to proactively solve problems.

You might need network forensics because of company policy or because of governmentally-mandated compliance. You can enforce your “acceptable use” policies, fight industrial espionage, and assist with government regulations like Sarbanes Oxley or HIPPA requirements. Using network forensics you can provide pre-intrusion tracking and identification while delivering a paper trail after any intrusion. Or you can perform network troubleshooting using root-cause analysis and identify network problems that have been around awhile.

Forensic Analysis, exclusive to the GigaStor version of Observer, is a powerful tool for scanning high-volume packet captures for intrusion signatures and other traffic patterns that can be specified using the familiar Snort rule syntax. You can obtain the rules from [http://www.snort.org](http://www.snort.org).

Snort is an open source network intrusion detection system (NIDS). Snort’s rule definition language is the standard way to specify packet filters aimed at sensing intrusion attempts.

Snort rules imported into Observer operate much like Observer’s expert conditions, telling Observer how to examine each packet to determine whether it matches specified criteria, triggering an alert when the criteria is met. They differ from expert conditions in that they only operate post-capture, and the rules themselves are text files imported into Observer.

**Importing Snort rules**

After getting the Snort rules from [http://www.snort.org](http://www.snort.org), follow these steps to import them into Observer.

1. In Observer, choose Capture > GigaStor Control Panel > Forensic Analysis tab.
2. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.
3. Choose your profile and click Edit. The Forensic Settings window opens.
4. At the bottom of the window, click the Import Snort Files button.
5. Locate your Snort rules file and click Open. Close all of the windows. After you import the rules into Observer you are able to enable and disable rules and groups of rules by their classification as needed.

Observer displays a progress bar and then an import summary showing the results of the import. Because Observer’s forensic analysis omits support for rule types and options not relevant to a post-capture system, the import summary will probably list a few unrecognized options and rule types. This is normal, and unless you are debugging rules that you wrote yourself, can be ignored.

6. To use the Snort rules you just imported, right-click anywhere on the Forensic Analysis tab and choose Analyze from the menu.

Analyzing packets using Snort rules

To analyze packets using Snort rules, you must first import the rules into Observer. See Importing Snort rules on page 306.

1. In Observer, choose Capture > GigaStor Control Panel > Forensic Analysis.

2. Right-click anywhere on the Forensic Analysis tab and choose Analyze from the menu.

    applies the rules and filters to the capture data and displays the results in the Forensics Summary tab. A new tab is also opened that contains the decode.

| Forensic Analysis tab | It is important to examine the preprocessor results to ensure that time-outs and other maximum value exceeded conditions haven’t compromised the analysis. If you see that preprocessors have timed out on hundreds of flows and streams, you may want to adjust preprocessor settings to eliminate these conditions. Intruders often attempt to exceed the limitations of forensic analysis to hide malicious content. The right-click menu lets you examine the rule that triggered the alert (if applicable). It also lets you jump to web-based threat references such as bugtraq for further information about the alert. These references must be coded into the Snort rule to be available from the right-click menu. |
| Forensic Analysis Log tab | The Forensic Analysis Log comprehensively lists all rule alerts and preprocessor events in a table, letting you sort individual occurrences by priority, classification, rule ID, or any other column heading. Just click on the column heading to sort the alerts by the given criteria. The right-click menu lets you examine the rule that triggered the alert (if applicable). It also lets you jump to web-based threat references such as bugtraq for further information about the alert. These references must be coded into the Snort rule to be available from the right-click menu. You can also jump to the Decode display of the packet that triggered the alert. |

Creating a Forensic Settings profile

Forensics profiles provide a mechanism to define and load different pairings of settings and rules profiles. Settings profiles define pre-processor settings that let you tune performance; rules profiles define which forensic rules are to be processed during analysis to catch threats against particular target operating systems and web servers. Because Observer performs signature matching on existing captures rather than in real time, its preprocessor configuration differs from that of native Snort. When you import a set of Snort rules that includes configuration settings, Observer imports rules classifications, but uses its own defaults for the preprocessor settings.

There is a difference between enabling the preprocessor and enabling logs for the preprocessor. For example, you can enable IP defragmentation with or without logging. Without logging, IP fragments are simply
reassembled; only time-out or maximum limit reached messages are noted in the Forensics Log and in the Forensic Analysis Summary window. If logging is enabled, all reassembly activity is displayed in the Forensics Log (but not displayed in the Forensic Analysis Summary).

1. In Observer, choose Capture > GigaStor Control Panel > Forensic Analysis tab.

2. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.

3. Choose your profile and click Edit. The Forensic Settings window opens.

4. From the Forensic Settings window, complete the following:
   
   # Import Snort rules
   # Define Forensic Settings.
   # Define Rule Settings—Select the rules you want to enable.

5. Close all of the windows, then right-click anywhere on the Forensic Analysis tab and choose Analyze from the menu.

   applies the rules and filters to the capture data and displays the results in the Forensics Summary tab.

   The top portion of the Rules window lists the rules that were imported, grouped in a tree with branches that correspond to the files that were imported.

   Rule classifications offer another level of control. Check the “Rules must also match rule classifications” box to display a list of defined rule classifications. Classifications are defined at import time by parsing the Snort config classification statements encountered in the rule set. Rules are assigned a classification in the rule statement’s classtype option.

   Select the rule classification(s) you want to enable. If classification matching is enabled, a rule and its classification must both be enabled for that rule to be processed. For example, suppose you want to enable all policy violation rules: simply right-click on the rule list, choose Enable all rules, and then enable the policy violation classification.

Table 52: Forensic Settings options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings Profile</td>
<td>Settings Profiles provide a mechanism to save and load different preprocessor settings, and share them with other Observer analyzers.</td>
</tr>
<tr>
<td>IP Flow</td>
<td>Packets belong to the same IP flow if they share the same layer 3 protocol, and also share the same source and destination addresses and ports. If this box is checked, forensic analysis identifies IP flows (also known as conversations), allowing Snort rules to isolate packets by direction and connection state via the flow option. If this pre-processor is disabled, flow keywords are ignored, but the rest of the rule is processed. The remaining settings allow you to throttle flow analysis by limiting the number of flows tracked, and by decreasing the time window within which a flow is considered active.</td>
</tr>
<tr>
<td>IP Defragmentation</td>
<td>Some types of attacks use packet fragmentation to escape detection. Enabling this preprocessor causes forensic analysis to identify and reconstruct fragmented packets based on the specified fragment reassembly policy. Rules are then run against the reconstructed packets during forensic analysis. The fragment reassembly policy mimics the behavior of various operating systems in what to do when ambiguous fragments are received. Choose the policy to match the OS of the server (or servers) being monitored. If the buffer contains traffic targeting hosts with different operating systems, use post-filtering to isolate the traffic before forensic analysis so that you can apply the correct policy.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Defragmentation Policy is:</td>
<td>BSD=AIX, FreeBSD, HP-UX B.10.20, IRIX, IRIX64, NCD Thin Clients, OpenVMS, OS/2, OSF1, SunOS 4.1.4, Tru64 Unix, VAX/VMS</td>
</tr>
<tr>
<td>Last data in=</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>BSD-right=</td>
<td>HP JetDirect (printer)</td>
</tr>
<tr>
<td>First data in=</td>
<td>HP-UX 11.00, MacOS, SunOS 5.5.1 through 5.8</td>
</tr>
<tr>
<td>Linux=</td>
<td>Linux, OpenBSD</td>
</tr>
<tr>
<td>Solaris=</td>
<td>Solaris</td>
</tr>
<tr>
<td>Windows=</td>
<td>Windows (95/98/NT4/W2K/XP)</td>
</tr>
<tr>
<td>Refer to</td>
<td><a href="http://www.snort.org">http://www.snort.org</a></td>
</tr>
</tbody>
</table>

TCP Stream Reassembly

Another IDS evasion technique is to fragment the attack across multiple TCP segments. Because hackers know that IDS systems attempt to reconstruct TCP streams, they use a number of techniques to confuse the IDS so that it reconstructs an incorrect stream (in other words, the IDS processes the stream differently from that of the intended target). As with IP fragmentation, forensic analysis must be configured to mimic how the host processes ambiguous and overlapping TCP segments, and the topology between attacker and target to accurately reassemble the same stream that landed on the target. Re-assembly options are described below:

TCP Stream Reassembly (Continued)

Log preprocessor events—Checking this box causes forensic analysis to display all activity generated by the TCP stream assembly preprocessor to the log.

Maximum active TCP streams tracked—If this value is set too high given the size of the buffer being analyzed, performance can suffer because of memory consumption. If this value is set too low, forensic analysis can be susceptible to denial of service attacks upon the IDS itself (i.e., the attack on the target is carried out after the IDS has used up its simultaneous sessions allocation).

Drop TCP streams inactive for this duration—A TCP session is dropped from analysis as soon as it has been closed by an RST message or FIN handshake, or after the time-out threshold for inactivity has been reached. Exercise caution when adjusting the time-out, because hackers can use TCP tear-down policies (and the differences between how analyzers handle inactivity vs. various operating systems) to evade detection.

TTL delta alert limit—Some attackers depend on knowledge of the target system's location relative to the IDS to send different streams of packets to each by manipulating TTL (Time To Live) values. Any large swing in Time To Live (TTL) values within a stream segment can be evidence of this kind of evasion attempt. Set the value too high, and analysis will miss these attempts. Setting the value too low can result in excessive false positives.

Overlapping packet alert threshold—The reassembly preprocessor will generate an alert when more than this number of packets within a stream have overlapping sequence numbers.

Process only established streams—Check this box if you want analysis to recognize streams established during the given packet capture.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Reconstruct Client to Server streams**—Check this box to have analysis actually reconstruct streams received by servers.  
Reconstruct Server to Client streams—Check this box to have analysis actually reconstruct streams received by clients.  
Overlap method—Different operating systems handle overlapping packets using one of these methods. Choose one to match the method of the systems being monitored. |
| **TCP Stream Reassembly** (Continued) | Reassembly error action—Discard and flush writes the reassembled stream for analysis, excluding the packet that caused the error. Insert and flush writes the reassembled stream, but includes the packet that caused the error. Insert no flush includes the error-causing packet and continues stream reassembly.  
Reassembled packet size threshold range—Some evasion strategies attempt to evade detection by fragmenting the TCP header across multiple packets. Reassembling the stream in packets of uniform size makes this easier for attackers to slip traffic past the rules, so forensic analysis reassembles the stream using random packet sizes. Here you can set the upper and lower limits on the size of these packets.  
Reassembled packet size seed value—Changing the seed value will cause forensic analysis to use a different pattern of packet sizes for stream reassembly. Running the analysis with a different seed value can catch signature matches that would otherwise escape detection.  
Port List—Enabling the Port List option limits analysis to (or excludes from analysis) the given port numbers. |
| **HTTP URI Normalization** | Many HTTP-based attacks attempt to evade detection by encoding URI strings in UTF-8 or Microsoft %u notation for specifying Unicode characters. This preprocessor includes options to circumvent the most common evasion techniques. To match patterns against the normalized URIs rather than the unconverted strings captured from the wire, the VRT Rules use the uricontent option, which depends on this preprocessor. Without normalization, you would have to include signatures for the pattern in all possible formats (using the content option), rather than in one canonical version.  
Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the HTTP preprocessor to the log, but not the Forensic Summary Window.  
Maximum directory segment size—Specifies the maximum length of a directory segment (i.e., the number of characters allowed between slashes). If a URI directory is larger than this, an alert is generated. 200 characters is reasonable cutoff point to start with. This should limit the alerts to IDS evasions.  
Unicode Code Page—Specify the appropriate country code page for the traffic being monitored.  
Normalize ASCII percent encodings—This option must be enabled for the rest of the options to work. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because such encoding is considered standard, logging occurrences of this is not recommended.  
Normalize percent-U encodings—Convert Microsoft-style %u-encoded characters to standard format. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>such encoding is considered non-standard (and a common hacker trick), logging occurrences of this is recommended. Normalize UTF-8 encodings—Convert UTF-8 encoded characters to standard format. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because Apache uses this standard, enable this option when monitoring Apache servers. Although you might be interested in logging UTF-8 encoded URIs, doing so can result in a lot of noise because this type of encoding is common. Normalize UTF-8 encodings—Convert UTF-8 encoded characters to standard format. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because Apache uses this standard, enable this option when monitoring Apache servers. Although you might be interested in logging UTF-8 encoded URIs, doing so can result in a lot of noise because this type of encoding is common. Lookup Unicode in code page—Enables Unicode codepoint mapping during preprocessing to handle non-ASCII codepoints that the IIS server accepts. Normalize double encodings—This option mimics IIS behavior that intruders can use to launch insertion attacks. Normalize bare binary non ASCII encodings—This an IIS feature that uses non-ASCII characters as valid values when decoding UTF-8 values. As this is non-standard, logging this type of encoding is recommended. Normalize directory traversal—Directory traversal attacks attempt to access unauthorized directories and commands on a web server or application by using the <code>./</code> and <code>/../</code> syntax. This preprocessor removes directory traversals and self-referential directories. You may want to disable logging for occurrences of this, as many web pages and applications use directory traversals to reference content. Normalize multiple slashes to one—Another directory traversal strategy is to attempt to confuse the web server with excessive multiple slashes. Normalize Backslash—This option emulates IIS treatment of backslashes (i.e., converts them to forward slashes). ARP Inspection Ethernet uses Address Resolution Protocol (ARP) to map IP addresses to a particular machine (MAC) addresses. Rather than continuously broadcasting the map to all devices on the segment, each device maintains its own copy, called the ARP cache, which is updated whenever the device receives an ARP Reply. Hackers use cache poisoning to launch man-in-the-middle and denial of service (DoS) attacks. The ARP inspection preprocessor examines ARP traffic for malicious forgeries (ARP spoofing) and the traffic resulting from these types of attacks. Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the ARP Inspection preprocessor to the log, but not the Forensic Summary Window. Report non-broadcast requests—Non-broadcast ARP traffic can be evidence of malicious intent. Once scenario is the hacker attempting to convince a target computer that the hacker’s computer is a router, thus allowing the hacker to monitor all traffic from the target. However, some devices (such as printers) use non-broadcast ARP requests as part of normal operation. Start by checking the box to detect such traffic; disable the option only if analysis detects false positives. Telnet Normalization Hackers may attempt to evade detection by inserting control characters into Telnet and FTP commands aimed at a target. This pre-processor strips these codes, thus normalizing all such traffic before subsequent forensic rules are applied. Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the Telnet Normalization preprocessor to the log, but not the Forensic Summary Window.</td>
</tr>
</tbody>
</table>
### Field Description

**Port List**—Lets you specify a list of ports to include or exclude from Telnet pre-processing. The default settings are appropriate for most networks.

**Variable Name**

A scrollable window located below the preprocessor settings lists the variables that were imported along with the Snort rules. Variables are referenced by the rules to specify local and remote network ranges, and common server IP addresses and ports. You can edit variable definitions by double-clicking on the variable you want to edit.

The VRT Rule Set variable settings (and those of most publicly-distributed rule sets) will work on any network without modification, but you can dramatically improve performance by customizing these variables to match the network being monitored. For example, the VRT rules define HTTP servers as any, which results in much unnecessary processing at runtime.

Address variables can reference another variable, or specify an IP address or class, or a series of either. Note that unlike native Snort, Observer can process IPv6 addresses.

Port variables can reference another variable, or specify a port or a range of ports. To change a variable, simply double-click the entry. The Edit Forensic Variable dialog shows a number of examples of each type of variable which you can use as a template when changing values of address and port variables.

### Using network forensics to track a security breach

It goes without saying that you have a firewall and other perimeter defenses in place to ward off intruders. But sometimes those can be defeated by unique attacks from the outside, and they do not fend off any internal attacks. Existing security deployments look for known threats or vulnerabilities and miss the new, unknown threats. Use the Forensic Analysis tab to find all of these and to research and identify sources of “zero-day attack.”

Imagine the following scenario: Over the weekend seemingly random security anomalies began to attack your DMZ. Your intrusion protection system (IPS) detected and repelled these attacks. During the same time frame and unknown to the IPS/IDS, a brute force attack occurred and was successful against the default “Admin” account on your VPN concentrator. After they were beyond your perimeter, which was accomplished using a created VPN account, Trojan applications installed remote control utilities and keystroke loggers. Subsequent malicious activity using these utilities occurred against other internal systems.

How do you identify what happened and when it happened? How do you identify who was affected?

1. Isolate the time frame over the weekend where you noticed the attacks against your DMZ. Collect all of the internal activity over the next few days. Select the time in the Detail Chart of the GigaStor Control Panel from where you noticed the attacks and the next few days. Change the time resolution, if necessary, to zoom out (or in) so that you have the data highlighted. See Selecting a time frame to analyze.

2. Using current Snort rules, click the Analyze button. See Importing Snort rules.

3. Search the decoded packets for possible exploits, internal denial-of-service attacks, and key logging.

4. If you find anything suspicious, navigate into the individual frames to isolate data that was transferred under false pretenses.

5. Use Connection Dynamics in Observer to track the path that the intruder took across your network. Identify all infrastructure systems that were affected and potentially compromised.
Using network forensics to track acceptable use or compliance

Note: Stream reconstruction (including VoIP) is illegal in some jurisdictions and may be disabled by Network Instrumentsto comply with those laws.

Your company likely has an “acceptable use” policy for its network. As a network administrator, you may be asked to track a specific person's internet use. The challenge of tracking web user activity is that it can provide domain names and URL information but cannot show what exact content was being displayed at the time. If those sites cease to exist or change their content, providing adequate documentation is nearly impossible.

The solution is to record the traffic in its entirety, which offers the ability to view the transactions, and also to reconstruct the original stream of data.

1. Isolate the time frame where you suspect the person was misusing the network. See Selecting a time frame to analyze.
2. Click the IP Stations tab and find the address of the user you are tracking. Select the address. This creates a filter.
3. Click Update Chart. This updates the Detail Chart and shows you all of the traffic from the address.
4. You can further filter the chart and reports by selecting specific traffic types (for example, HTTP, SMTP, Telnet, and so on).
5. Analyze the data using one of the options described in Mining data from your GigaStor. This opens your data in the Decode tab in the Observer analyzer.
6. Assuming the data is HTTP, select a packet in the Decode tab and right-click. Choose TCP Dump (HTTP) from the menu. This analyzes the data and opens it in the Expert tab.
7. Scroll through the decoded packets. Click the “ReconstructedPage.html” files to see the web page as it looked when the user saw it.

This same process can be used for replaying VoIP calls or capturing e-mail and instant messaging to ensure your company’s “acceptable use” policy is being followed.

Searching for microbursts

For a computer network, a microburst is an unusually large amount of data in a short time frame that saturates your network and adds to latency. These bursts are seen as a spike over normal traffic when viewed on a graph. They are usually less than one millisecond long (or even shorter), and they typically occur during high traffic volume, such as after a major news event or announcement when many people are using the network simultaneously.

Note: Microbursts occur in every network, but are also very environment-specific. What may be a microburst for one company may be considered acceptable traffic for another. Given that many applications have error checking and retransmission algorithms, and that microbursts are so short that connectivity for most applications is not affected, microbursts are not a concern for many network engineers. However, some applications are more sensitive to microbursts, such as financial, audio, video, or multicast applications. The financial industry is especially keen about microbursts and reducing the effect of microbursts on their network. This section is written with a network administrator for a financial company as the primary audience, but any network administrator interested in microbursts should find the information useful.

You might have microburst issues if your latency is creeping into the tens of milliseconds (or doubling your previous baseline). Your brokers may know something is awry because revenue is dropping. Revenue is
dropping because your broker’s trades are executed just behind others beating them to the market, thereby getting a better price and more revenue. All of this will occur and neither your brokers nor you may even be aware the microbursts are occurring.

Almost half of all trades executed globally are initiated and completed by computers, not humans. Since computers are reacting to price fluctuations, when a microburst occurs, packets are dropped, which causes them to be transmitted and that takes several milliseconds—nearly doubling the time to complete the transaction. A 1-millisecond advantage in trading applications can be worth $100 million a year to a major brokerage firm.\footnote{Information Week, April 21, 2007.}

To prevent data loss because of microbursts, design your network so that its capacity can withstand the highest possible burst of activity in whatever a time frame you deem important (perhaps millisecond). Adding additional switches or load-balancers to your network are a couple of possible solutions. This way the link will never be constantly busy for more than one millisecond at a time, and no data will be delayed on the link for more than one millisecond.

Another option is to smooth out any traffic or applications not sensitive to latency or jitter sharing the same link. Using these options, you can optimize your network for bandwidth efficiency, performance, or a combination of both depending on each application’s requirements.

Even after identifying and correcting for all issues in your network, you may still have problems with your Internet Service Provider. A study performed by Microsoft Research indicates that microbursts are more likely to occur at edge or aggregation links.\footnote{Microsoft Research, June 1, 2009.} Therefore, it may be necessary to also have your ISP optimize their flows to you.

Practically speaking, the capacity necessary to keep latency below one millisecond is normally much less than the peak one millisecond data rate. This is because many links use buffers to hold the traffic exceeding the link capacity until the buffer can be cleared. Assuming the system can clear the buffer queue quickly when the burst ends, microbursts are avoided because buffer capacity was created.

In the GigaStor Control Panel, a microburst occurs when 1) the maximum bits per duration interval based on the capture card speed and utilization threshold you define is reached, and 2) the interval contains at least two packets (full or partial).

There are a few different ways to search for microbursts using Observer.

1. Using triggers and alarms to inform you when microbursts occur. Customize your triggers and actions and choose Microbursts from the Alarms list.

2. Using the Microburst Analysis tab is the easiest way to analyze large chunks of time for microbursts and view the decoded packets.

3. Using Network Trending for microbursts. This option is different than the packet capture and decode option available through the Microburst Analysis tab. First, packet capture does not need to be running for Microburst trending to see any microbursts. Second, Microburst trending can also be pushed to Observer Reporting Server and aggregated with Microburst trending information from other probes in your network so that you have a fuller picture of where and when microbursts are occurring.

4. Using the Detail Chart. This method is limited to a 15 minute time frame on the Detail Chart.

**Using the Microburst Analysis tab in the GigaStor Control Panel**

To search for microbursts across a large time frame (greater than 15 minutes) you must use the Microburst Analysis tab.

The Microburst Analysis tab shows you the number of microbursts Observer found in the time frame you selected. You can see exactly when the microburst occurred, how many bytes where in the burst, and the network utilization when the burst occurred.
When you select a microburst, you can choose to see that slice of time on the Detail Chart or you can view the packet in the Decode pane.

You can select the Microburst Analysis Graph tab and see the found microbursts on a graph.

1. Select the probe instance and then choose Capture > GigaStor Control Panel.
2. Click the Microburst Analysis tab.
3. Highlight the data in the Detail Chart you want to analyze for microbursts and click Analyze. The GigaStor Analysis Options screen opens.
4. Choose whether you want any filters and select Microburst analysis in the Analysis Type section.
5. Define what a microburst is for your network and click OK. The results appear in the Microburst Analysis tab. For details, see Duration, Utilization threshold, and Full duplex. It may take a moment for the GigaStor Control Panel to process the data and display the results.

Using the Detail Chart only

The longest time frame that can be analyzed with the Detail Chart method is 15 minutes. You may be better off using the Microburst Analysis tab instead. See Using the Microburst Analysis tab in the GigaStor Control Panel on page 314.

Microburst analysis is easier to comprehend using bars instead of lines on the Detail Chart. Choose Settings > Detailed Chart and change the appearance to 2D Columns. Depending on your preferences, at times you may also wish to change the Y-axis scale to 100 when you are viewing the chart as Percent of duration Intervals with Microbursts.

When you change between the Percent and Number charts, the bars may not appear to change. If you look closely, you will notice that the numbers on the vertical axis change as does the title of the chart.

To enable microburst analysis and define what on your network qualifies as a microburst:

1. Select the probe instance and then choose Capture > GigaStor Control Panel.
2. Click the Screen resolution box, which opens the Microburst Analysis options.
3. Select Enable Microburst Analysis and choose your settings. When you make changes to these options, the Detail Chart changes. Sometimes it is a very subtle change. All of these options are interrelated. By changing any one of these settings, you change what is determined to be a microburst. When that changes, the graphs change. Change only one option at a time, then view your changes.
**Screen resolution (Interval/Total Time):** The screen resolution is two numbers that define the length of time shown in the Detail Chart. The first number is the interval length, which when looking at a bar chart, is each bar. The second number is the total time of all of the intervals on the chart, although if an interval does not have any bursts the interval will not have a bar. The interval is used along with Duration to determine how many chunks of time are theoretically possible. See Table 53 on page 317 for examples of how changing the interval may affect the Detail Chart.

**Duration:** The duration is length of time over which the burst is calculated. It must contain two or more packets (or partial packets) to be counted as a microburst. A single packet filling an entire duration interval does not count as a microburst. The shorter the time frame, the more bursts you may have because the length of time necessary to meet the threshold is shorter. Conversely, as you increase the length of time required for traffic to be considered a burst, fewer bursts will meet the duration threshold. This is why counts may change as you increase or decrease the duration. More of less traffic meets the duration threshold to be considered a microburst. See Table 53 on page 317 for examples of how changing the duration may affect the Detail Chart.

**Utilization threshold:** The utilization threshold is the percent of your capture card speed that must be met before a microburst can be determined to have occurred. The highest threshold allowed is 100%. The lowest threshold is 10%, although it is extremely rare that 100% is ever achieved. Ninety-nine percent utilization is not uncommon though. See Table 53 on page 317 for examples of how changing the Utilization threshold may affect the Detail Chart.

**Full Duplex / DTE / DCE:** Determines how the utilization threshold is calculated and what information is shown in the Detail Chart. These options are only available when the probe instance you are using is attached to a Gen2 capture card. We do not recommend attaching passive probe instances to the Gen2
capture card, so these options may not be available to you. In this case, your settings are Full Duplex + DTE + DCE are not available and cannot be changed.

**Full Duplex + DTE + DCE:** Each port on the capture card is considered independently from all others. The traffic is never combined between ports to meet a threshold. If you have a 4-port 1 Gb capture card, you have four independent 1 Gb connections.

A microburst is counted when the utilization on any one of the ports exceeds the utilization threshold, but only on that port. The threshold does not need to be met on all ports — just on one or more of them.

**Full Duplex + DTE:** Calculates and displays microbursts only on DTE ports. The DTE ports on the Gen2 capture card are the even numbered ports (2, 4, 6, 8).

**Full Duplex + DCE:** Same as Full Duplex + DTE, except for DCE links. The DCE ports are the odd numbered ports (1, 3, 5, 7).

**None selected:** When no options are selected, the ports are combined to create the maximum utilization threshold. If you have a 4-port 1 Gb capture card, you have one connection with a 4 Gb maximum utilization. (This is the opposite of Full Duplex + DTE + DCE where you have four independent 1 Gb connections.) For this reason, you will likely see fewer microbursts than when any of the Full Duplex options are selected because the utilization threshold is higher.

The Data type option is unavailable when doing Microburst analysis because Microburst analysis shows the number of times or percentage of time when a microburst occurs within a duration and utilization threshold. Because the charts show only microbursts and no other type of information, you cannot choose to show bytes, bits or packets for data type.

**Percent of duration intervals with microbursts:** The Detail Chart shows bursts as a percentage. It uses four variables to determine the percentage. Each bar (assuming your chart is configured to show bars instead of lines) represents one interval. Within each slice are smaller chunks of time, which are the durations (although they are not visible on the Detail Chart). The percentage is calculated by:

$$\text{Percent of duration intervals with microbursts} = \frac{\text{Screen resolution interval}}{\text{Duration}} \times 100\%$$

**Number of duration intervals with microbursts:** The Detail Chart shows the count of microbursts that occurred in each duration interval. There can only be one microburst per duration interval. This number is also used to calculate the percent of duration intervals with microbursts.

[Table 53 on page 317](#) shows how changing one variable changes the calculations and can affect what you see in your charts.

**Table 53: Changing interval, duration, or MB Utilization**

<table>
<thead>
<tr>
<th>Interval</th>
<th>Duration</th>
<th>MB Util</th>
<th>MB Util</th>
<th>MB Util</th>
</tr>
</thead>
<tbody>
<tr>
<td>ms</td>
<td>µs</td>
<td>10%</td>
<td>50%</td>
<td>90%</td>
</tr>
<tr>
<td>5 ms</td>
<td>100 µs</td>
<td>1,2,3</td>
<td>1,2,4</td>
<td>1,2,4</td>
</tr>
<tr>
<td>200 ms</td>
<td>10 ms</td>
<td>1,2,3</td>
<td>1,2,4</td>
<td>1,2,4</td>
</tr>
<tr>
<td>1 s</td>
<td>1 ms</td>
<td>1,3,4</td>
<td>1,3,4</td>
<td>1,3,4</td>
</tr>
</tbody>
</table>

| Bits/sec in Interval | 2,500,000 | 5,000,000 | 5,000,000 |
| Bytes/sec in Interval | 309,672 | 617,826 | 617,826 |
Reconstructing streams of HTTP, VoIP, and more

Note: Stream reconstruction (including VoIP) is illegal in some jurisdictions and may be disabled by Network Instruments to comply with those laws.

The process of capturing and reconstructing traffic is pretty much the same regardless of traffic type. Use these steps to reconstruct the stream. The process described here is for reconstructing HTTP, but the process is the same for other applications, except in step 6 you would choose the appropriate menu option.

1. Isolate the time frame in the Detail Chart you want to analyze. See Selecting a time frame to analyze.
2. (Optional) Using the various Statistics tabs, select IP Stations tab and choose the station(s) you want to isolate. This creates a filter.
3. Click Update Chart. This updates the Detail Chart and shows you all of the traffic from the address.
4. You can further filter the chart and reports by selecting specific traffic types (for example, HTTP, SMTP, Telnet, and so on).
5. Analyze the data using one of the options described in Mining data from your GigaStor. This opens your data in the Decode tab in the Observer analyzer.
6. Assuming the data is HTTP, select a packet in the Decode tab and right-click. Choose TCP Dump (HTTP) from the menu. This analyzes the data and opens it in the Expert tab.

7. Scroll through the decoded packets. Click the “ReconstructedPage.html” files to see the web page as it looked when the user saw it.

Defining what can be recreated in Stream Reconstruction

**Note:** Stream reconstruction (including VoIP) is illegal in some jurisdictions and may be disabled by Network Instruments to comply with those laws.

For security or privacy reasons or because of company policy, you may need to limit what the GigaStor probe can recreate through its stream reconstruction feature.

2. Click the Settings button.
3. Click the Stream Reconstruction tab.
4. Choose which content streams you would like to be able to reconstruct and have appear on the Stream Reconstruction tab of the GigaStor Control Panel.
5. Choose whether to limit stream reconstruction by specific subnets.

How to extract VoIP and video calls from your GigaStor

VoIP and videoconferencing calls can be extracted from a GigaStor if you know the approximate time the events occurred.

Prerequisite(s):

You must understand how to select a time frame from your GigaStor. See ../observer/voip_and_video_sip_extraction.html.

**Note:** This process is only compatible with SIP data.

Locating and extracting SIP-based voice and video data from your GigaStor is a straightforward task. All of the SIP setup and teardown packets are extracted along with any payload, such as audio and video, to ensure you retrieve complete sessions. This includes all person-to-person audio calls and videoconferencing as well as conference calls and conference video where multiple endpoints are present. And endpoint could be a person holding a handset, wearing a headset, or a line that is open for hold music or for recording.

To extract VoIP and videoconferencing calls from your GigaStor:

1. Select a time frame you want to analyze.
2. Click the Update Reports button to get the latest data from the time frame selected.
   
   This step is unnecessary if Auto-update GigaStor chart on statistics tab or selection change is enabled in the GigaStor settings. See ../observer/non_gigastor_specific_settings.html.

3. Click the Analyze button.
4. In the Analysis Options section, choose VoIP and Videoconferencing calls by SIP tag. Click the Settings option and choose your call search criteria.
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A --&gt; (ANY)</td>
<td>Extract call(s) where pattern A is in the SIP “From” field.</td>
</tr>
<tr>
<td>A &lt;-- (ANY)</td>
<td>Extract call(s) where pattern A is in the SIP “To” field.</td>
</tr>
<tr>
<td>A &lt;-&gt; (ANY)</td>
<td>Extract call(s) where pattern A is in the SIP “From” or “To” field.</td>
</tr>
<tr>
<td>A &lt;-&gt; B</td>
<td>Extract call(s) where pattern A and pattern B is in either the SIP “From” or “To” field.</td>
</tr>
<tr>
<td>A --&gt; B</td>
<td>Extract call(s) with pattern A in the SIP “From” field and pattern B is in a SIP “To” field.</td>
</tr>
<tr>
<td>Call-ID</td>
<td>Extract call(s) with the specified pattern in the SIP “Call-ID” field.</td>
</tr>
</tbody>
</table>

5. (Optional) Enable one or more search pattern modifiers:

   - Use regular expression(s)—Perl 5 regular expressions. For details and examples, see [http://www.regular-expressions.info/tutorial.html](http://www.regular-expressions.info/tutorial.html)
   - Match case—case sensitive search

6. Type a string for the GigaStor to search for in the Call-ID Pattern.

7. Choose one of the result options:

   - Stop searching when one matching call is found. This provides you the results more quickly, but the tradeoff is that if the endpoints identified by search criteria had multiple separate calls within the timeframe selected, only the first call is extracted and any subsequent calls are excluded.
   - Search for all matching calls within the GigaStor analysis time range (up to the filtering limit).

8. Click OK to save your settings.

9. Choose your analysis type. The options are described in ../observer/analyzing_data_by_combining_gigastor_control_panel_and_observer_filters.html.

   - Expert analysis and decode
   - Decode without expert analysis
   - Third party decoder

If your search pattern found results, the results are displayed in a new tab and can be further analyzed.

### How to analyze 4G LTE traffic from your GigaStor

You can isolate subscribers by IMSI or IMEI across eNodeB, SGW, or PWG using various communication paths such as S1-MME, S1-U, S11, S5, or X2.

Prerequisite(s):

You must understand how to select a time frame from your GigaStor. See Selecting a time frame to analyze on page 303.

Your LTE environment likely has hundreds or thousands of matrix switches. It is impractical to monitor all of them simultaneously. Most likely, you are likely using the GigaStor as a reactive tool to subscriber complaints. After connecting the matrix switch to the GigaStor and collecting LTE traffic, you can analyze it to determine the problem.
1. Select a time frame you want to analyze.
2. Click the Analyze button.
3. In the **Analysis Options** section, choose your filter type. For details about the filter types, see Table 51.
4. In the Analysis Type list, choose **4G LTE analysis**.
5. Click **Settings**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard rejected devices</td>
<td>Allows you to include or exclude devices rejected by your LTE environment. There may be any number of reasons a device may be rejected, such as the device is not a subscriber because the device is not compatible with your network or because the device's owner has not paid their bill. Whether a device is rejected is not controlled by Observer, but rather by your LTE environment. If you are using the 4G LTE memory configuration for the probe instance, its default value is to show 50,000 devices. It is possible that rejected devices may take up a large portion of the 50,000 devices. You may want to either choose to discard rejected devices or increase the number of tracked devices. This is set in <strong>Fine-tuning the statistical buffer</strong>.</td>
</tr>
<tr>
<td>Filter IMSI</td>
<td>Allows you to filter for a specific IMSI. Provide the IMSI or a portion of the IMSI for which you want to filter.</td>
</tr>
<tr>
<td>First/Last time seen display resolution</td>
<td>Allows you to choose whether the display resolution is 1 millisecond, 1 microsecond, or 1 nanosecond.</td>
</tr>
<tr>
<td>Display date</td>
<td>Adds the date to the analysis output.</td>
</tr>
</tbody>
</table>

6. Click OK to save your settings.
7. Click OK to search the GigaStor for the 4G LTE traffic.

**Analyzing 4G LTE traffic**

By viewing the link between signaling and sessions on the data and user planes or by viewing detailed information on each session, including subscriber, service area, cell site, network element, handset type, error codes and session status, you will have excellent insight into your LTE network status.

Long Term Evolution (LTE) leverages the power of an IP infrastructure to significantly increase the performance of mobile communications. Observer provides end-to-end tracking of flow and control data services of LTE mobile communications and protocols. Carriers shifting to IP-based networks have complete visibility across all points of their LTE infrastructure from the tower to the core.

*Figure 99 on page 322* shows a user's mobile device connecting to eNodeB towers using radio frequency. The MMEs manage the control planes that connect with the Evolved Packet Core for authorization and authentication by using the HHS. The user plane is also handled separately by the MMEs for communication such as web browsing, e-mail, call set up, VoLTE, and, in some environments, private networks. After a user device is authenticated and connection established, the SGW manages the connection. As the user's device moves from eNodeB to eNodeB that handoff is handled using X2.
A GigaStor probe can capture and track all of a device's network traffic in your LTE environment after the device connects to an eNodeB. You can get comprehensive subscriber analysis as well as have a logical workflow for problem resolution. By analyzing the LTE traffic from a GigaStor probe, you can see a summary of all devices or filter to a specific device. Observer can:

- Show you detailed subscriber session use and error reporting including those associated with authentication, rejection, connectivity, handover, or application
- Filter subscribers by IMSI
- Provide real-time and post-event analysis of individual subscriber activities and session irregularities as well as bandwidth utilization for each interface
- Obtain metrics and visibility for all important interfaces within your LTE environment (eNodeB, X2, S1-U, S1-MME, S5-U, S6a, and S11), logically broken out by UE device, eNodeBs, MMEs, SGWs, PGWs and application tabs
- Provide subscriber and session level summaries by duration, throughput, handovers, errors, applications, and user (S1-U)/control (S1-MME, S11) planes
- Show multi-protocol support from the eNodeB access point through the EPC and beyond the PGW provides outstanding service knowledge related to all major applications such as authentication/authorization, web browsing, or any other customer facing apps including over-the-top (OTT)
- Show complete VoLTE analytics including, call setup and tear-down, replay capabilities, MOS, jitter, and packet loss metric

**Using Observer in financial firms**

In an environment where even nanoseconds matter, a GigaStor allows you to identify when an anomaly in your network occurs and alerts you to it so that you can resolve it quickly.

If you are a network administrator in a financial or trading firm, small amounts of time can mean the difference between making or losing money or making money versus making a lot of money. Your networks must be fast, and your trading algorithms must be running as efficiently as possible with no data loss on your network. In addition to the in-depth network troubleshooting features, the GigaStor has several components designed with your business in mind:
GigaStor probe: The GigaStor probe is a high-performance capture-based network appliance that is extremely fault tolerant with redundant, high efficiency cooling. It captures both packet and flow-based traffic for long-term retention of raw, indexed data. Having this data allows you rapid event analysis of errors and anomalies. It can sustain full-duplex wire speed capture and write-to-disk.

GPS time synchronization: With the GigaStor probe connected to the optional GPS antenna, the time on the Gen2 capture card is based on atomic clock sources. The clock updates every second and is within 150 nanoseconds of GPS/UTC time. This ensures remarkably accurate timing without concern for clock drift (gain or loss).

Trading Multicast analytics: Multicast is used in trading firms to deliver information on pricing, volume, and more. Getting this information as fast as possible is critical because it affects profits. Therefore, multicast streams use connectionless UDP rather than the connection-oriented TCP protocol to traverse the network. UDP has little overhead in comparison to TCP (like the three-way handshake). Hence, it is much faster and more efficient for traversing the network. However, UDP also has weaknesses that can have seriously negative implications for the trading network. Packets can be lost, arrive out of order, and/or be corrupted. Data is not retransmitted when this occurs with UDP, and even if it were, given the high speed of today’s trading, it would likely be too late. When any of these occur, it directly impacts trade execution. No data can mean that no trade or the wrong trade is placed. To partially overcome this weakness with UDP, multicast streams almost always use sequence numbers within their payload to allow detection of these events. As a network administrator in a trading firm, you likely monitor these sequence numbers quite closely looking for gaps in the numbers. In Observer, you are able to create custom feed definitions to monitor for missing sequence numbers if you are not using BATS, CME, Edge feed, JSE feed, LSE, Mold UDP 64, SIAC, FIX Fast. In addition to gap sequence detection and alarming, Observer can perform proximity analysis near anomalous events. What was occurring when the gap was detected? Proximity analysis shows you what was occurring on your network at or around the time the anomaly was detected. When a multicast gap is detected you want to quickly understand what may have caused it.

Microburst intelligence: A microburst is an unusually large amount of data in a short time frame that saturates your network and adds to latency. Excessive microbursts, even in duration or utilization impact multicast streams and/or trading activity. You want to swiftly locate the time and cause of these microbursts, but given the enormous amount of data that crosses your network, this process can be difficult. With a GigaStor probe, the microburst analysis is fully automated after you define duration and utilization thresholds. You can sort through hours of collected data, alarm when thresholds are exceeded, and report on trends. You can rapidly correlate microbursts to degraded response time. Using the trending reports you can proactively address trends before they impact performance.

FIX capabilities: FIX is a transport protocol used between trading companies. It contains what kind of trades are occurring (buy or sell), who is doing the trading, what the order ID is. Observer has full decode support for FIX (4.2, 4.4) along with support for all of the most significant FIX commands. If you need extended capabilities for monitoring FIX beyond what is available in Observer, you can create customized profiles. Using its FIX analytics, Observer can quantify execution times with transaction-by-transaction analysis and send alarms when specific conditions are met. You can use filters to parse vast amounts of traffic quickly by trading station, time, and many other parameters.

Analyzing FIX transactions

The Financial Information eXchange (FIX) protocol is an electronic communications protocol used for international real-time exchange of information related to the securities transactions and markets.

If you need visibility into the FIX protocol you must be able to see and use the raw packet data in the area above the header. The GigaStor probe provides you access to it.

Use the FIX Analysis tab in the GigaStor Control Panel to highlight only FIX data and to select of the timeframe in question. The capability to filter on a trade by order ID for further analysis or to validate a specific transaction can be accomplished from this point. Use the filtering available in the GigaStor Control Panel to identify specific issues with a FIX transaction. And, finally, graph a response time graph for those transactions.
Outside of the GigaStor Control Panel, these other areas may be valuable for you when you are analyzing FIX transactions:

- **Decode and Analysis in Observer**—Allows you to decode and analyze the raw FIX information and presents it in an easy to read format. In the Decode and Analysis tab you can use filters and do post-capture analysis on specific FIX transactions that have issues.

- **Application Transaction Analysis in Observer**—Examines all transactions related to FIX even those beyond layer 4 into the application layer. Information about the transactions of applications for each request and the type of request are tracked. View a graph of response time and application error conditions or request and response results. ATA performs in-depth application analysis of each request or type of request by examining important information within the payload. This information typically involves massive amounts of data often best viewed in graphical format to more easily spot trends or patterns.

- **Baseline and trending reports in Observer or Observer Reporting Server**—Using Application Transaction Analysis you can create reports on all FIX statistics for capacity planning. If you have numerous probes from which you want FIX transactions aggregated and analyzed, then use Observer Reporting Server (sold separately).

### Configuring a FIX profile

Observer uses profiles to analyze FIX data. Default profiles are in three main categories: pre-trade, trade, and post-trade. Within each category, there are numerous variants that allow you to focus on a specific trade type, such as "Pre-trade: Quote Negotiation." You can use the settings described here to edit, create, import, or export a FIX profile.

**Table 54: FIX Settings**
<table>
<thead>
<tr>
<th>This option...</th>
<th>Allow you to do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIX Profile</td>
<td>Lists the name of the current profile. The current profile is the rest of the dialog window, including the General Settings and the Type/Message.</td>
</tr>
<tr>
<td>Edit</td>
<td>Use this button to rename, add a new, or delete a profile. If you have numerous GigaStor probes where you want to use the same FIX analysis options, modify or create the profiles on one system, export them, and import them into the other GigaStor probes.</td>
</tr>
<tr>
<td>Import</td>
<td>Use this button to import FIX profiles that was created and exported from another Observer analyzer.</td>
</tr>
<tr>
<td>Export</td>
<td>Use this button to export a FIX profile.</td>
</tr>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum tracked requests</td>
<td>Lists the maximum number of requests to be tracked during the time frame selected in the Detail Chart. The default is 1000 requests. Typically, 1000 requests should be sufficient to provide the information you seek. If it is not, you may increase or decrease it. By increasing the amount of requests, the amount of system resources needed to analyze the requests is also increased, which means the analysis will take longer to complete.</td>
</tr>
<tr>
<td>Ignore duplicate requests</td>
<td>If selected, duplicate requests are ignored. This is the default setting. If unchecked, duplicate requests may be present in the analysis and reduces the number of unique requests in the tracked requests.</td>
</tr>
<tr>
<td>Maximum displayed results</td>
<td>Defines the maximum number of results to display in the GigaStor Control Panel for the fastest or slowest responses.</td>
</tr>
<tr>
<td>Track not responded requests within</td>
<td>Amount of time used as the threshold that the GigaStor should wait for a response to a request before discarding the request from its analysis data set. If you want only requests that have received a response, uncheck this option.</td>
</tr>
<tr>
<td><strong>Track/Type/Message</strong></td>
<td>Type and Message are options defined in the FIX protocol specification. If Track is selected, the FIX transaction type will be part of this analysis profile. All untracked options are ignored for this profile.</td>
</tr>
</tbody>
</table>

**Troubleshooting your GigaStor configuration**

**GigaStor Control Panel option is grayed out**
If the Capture > GigaStor Control Panel option is grayed out and unavailable, one of two things has likely occurred.

- You are not looking at a probe instance (passive or active) from the GigaStor probe. Verify you are using a probe instance for the GigaStor probe. If you are, then consider the next option.
- You are viewing a Packet Capture instead of the GigaStor Control Panel. You can only view one or the other. You cannot view both simultaneously. Close the Packet Capture window, then choose Capture > GigaStor Control Panel.

Now that you are viewing the GigaStor Control Panel, you may want to change your packet capture scheduling and ensuring that you do a “GigaStor” capture rather than a packet capture.
GigaStor is full or does not have the history you expect

Your GigaStor has several terabytes of hard drive space to capture your network’s traffic. The GigaStor probe will save data until its drives are full, then one of two things will happen. The GigaStor will stop capturing packets and saving them to disk or it starts overwriting the oldest data first so that you have a rolling window of capture. The option that controls how the GigaStor behaves in the Settings—General Options tab.

If you do not have as much history as you think you should, then consider:

- Pre-filtering your captures. Although this will provide more space for your captures, by definition you are excluding some traffic. The traffic you exclude may be just the traffic you need to analyze at some point.
- Capturing only partial packets. If you do not need to analyze the payload of every packet, then consider capturing the headers of packets.
- Purchasing a larger capacity GigaStor probe.

TCP applications are not appearing in the GigaStor Control Panel

If the GigaStor Control Panel is not displaying all of the applications you expect to see, ensure the “Limit to ports defined in Protocol Definitions” in Settings >General is unchecked.

Loading decodes in the Observer analyzer is slow

If your Observer analyzer is taking a long time to load a decode from a GigaStor probe, you may be attempting to mine too much data. To improve performance, use filters to limit the packets you want to decode, shorten the time frame you are mining, or both.

Loading decodes may also be impacted if you are using the “data capture time slice” feature, which ensures that the GigaStor’s write performance takes priority over mining performance. The default setting is that writing and reading have the same priority.

A RAID array drive is failing or has failed

It is necessary to have realistic expectations of component maintenance; specifically the individual disk drives that make up the GigaStor RAID array. Our engineering methods prioritize reliability and performance. There are many processes involved, from sourcing the best server-grade drives available to being consistent with burn-in to tracking reliability.

A disk drive has a life span, but as with anything electro-mechanical, it is impossible to predict. A Mean Time Before Failure (MTBF) number is supplied with the drive. The MTBF is 750,000 hours to 85 years on one of the drives we use (Seagate Barracuda 1T). Studies done by Carnegie Mellon, Google, Inc., and others suggest similar results. The bottom line is the drives in your GigaStor probably will not last 85 years.

There are two types of drive failure:

- Soft error: an error sent by the drive to the RAID controller, serious enough for it to be removed from the array
- Hard error: a physical drive failure (completely inoperable)
We recommend configuring the e-mail notification option in the RAID controller setup. This will notify the GigaStor administrator (and up to four others) of the drive status.

For soft errors, most of the time reinserting the drive will bring it back into the array. The error generally has to do with the drive having mapped some bad sectors, which is fairly common. If this event happens, we recommend replacing the drive from inventory and shipping the problem drive back for testing and replacement per your hardware maintenance arrangements that are in place. However, in many cases, the drive can run for years after being reinserted into the system. Unfortunately there is no way to know this ahead of time. If you choose to reinsert the drive, please log the failure with Support so if it happens again with the same drive, it can be replaced.

If a hard error is detected, the drive does not operate and requires replacement. It is critical to have at least one spare new drive on hand, and probably more than one. In general, we recommend that for every eight hard drives in your GigaStor probe that you have one replacement drive.

<table>
<thead>
<tr>
<th>Unit</th>
<th>Number of recommended spare drives</th>
<th>Hours to rebuild array</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigaStor 4T (8 drives)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>GigaStor 8T or 12 T (8 drives)</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>GigaStor 16T (16 drives)</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>GigaStor 32T (32 drives)</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>GigaStor 48T (48 drives)</td>
<td>5</td>
<td>12</td>
</tr>
</tbody>
</table>

RAID5 tolerates one drive failing, and can operate in a degraded state. When the drive is replaced, it starts to rebuild. How long the rebuild takes depends on the array size and whether it needs to write new data at the same time. If a second drive fails during the rebuild, the array is broken and must be recreated.

Your packet captures are available on a GigaStor running in a degraded mode, but are lost on a GigaStor with two bad drives at the same time (and also if the second drive fails during the time the first drive is rebuilding). From the time when the first bad drive is swapped until it has completed the rebuild period, your captured data is at risk.

There is an option to set aside one of the drives in the array to be allocated as a hot spare, and have 15 available for capture. Then if a drive fails, the controller automatically notifies you, and then includes the hot spare into the array. You lose storage overall, because that spare drive is not available, but the drive swap is handled automatically.

The optimal redundancy is two identical GigaStor s capturing the same set of traffic. If this is not practical, the next best option might be having a smaller GigaStor capturing the same set of traffic. Then if the first GigaStor has a drive failure followed quickly by another, your packet buffers would still be instantly available. Use filters to limit the captures to only the most critical traffic to extend the troubleshooting time available. The point is simply to have a backup plan to address even this unlikely drive-failure scenario.

**Related Topics**

- Building and saving an address book on page 36
- Selecting a time frame to analyze on page 303
- Understanding GigaStor indexing on page 292
- Analyzing data with filters from the GigaStor Control Panel on page 304
- Customizing statistics and capture buffers for probe instances on page 241
- Setting GigaStor’s basic options on page 286
- Using the Decode pane on page 87
- How a probe uses RAM on page 267
Discovering server applications on the network on page 39
 Differences between statistics and packets on page 291
 Getting started using your GigaStor on page 282
 Monitoring the RAID drives through e-mail notifications on page 298
 Cleaning the disk to maintain write performance on page 299
 Analyzing data without any filters on page 304
 Analyzing data with filters from the Observer filter editor on page 304
 Analyzing data with filters from the GigaStor Control Panel on page 304
 Analyzing data by combining GigaStor Control Panel and Observer filters on page 305
 Searching for microbursts on page 313
 Customizing statistics and capture buffers for probe instances on page 241
 Trimming data from your captures for space or privacy on page 290
 Setting GigaStor's basic options on page 286
 Using the Decode pane on page 87
 Using the Decode pane on page 87
 Using the Decode pane on page 87
 Customizing triggers and actions on page 118
 Using the Microburst Analysis tab in the GigaStor Control Panel on page 314
 Choosing your network trending types on page 158
 Using the Detail Chart only on page 315
 Mining data from your GigaStor on page 300
 How to extract VoIP and video calls from your GigaStor on page 168
 Tweaking the statistics memory configuration on page 274
 What is Application Transaction Analysis? on page 152
 Network Trending on page 146
 Decoding network traffic on page 77
Configuring a FIX profile

Observer uses profiles to analyze FIX data. Default profiles are in three main categories: pre-trade, trade, and post-trade. Within each category, there are numerous variants that allow you to focus on a specific trade type, such as "Pre-trade: Quote Negotiation." You can use the settings described here to edit, create, import, or export a FIX profile.

**Table 55: FIX Settings**

<table>
<thead>
<tr>
<th>This option...</th>
<th>Allow you to do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIX Profile</td>
<td>Lists the name of the current profile. The current profile is the rest of the dialog window, including the General Settings and the Type/Message.</td>
</tr>
<tr>
<td>Edit</td>
<td>Use this button to rename, add a new, or delete a profile. If you have numerous GigaStor probes where you want to use the same FIX analysis options, modify or create the profiles on one system, export them, and import them into the other GigaStor probes.</td>
</tr>
<tr>
<td>Import</td>
<td>Use this button to import FIX profiles that was created and exported from another Observer analyzer.</td>
</tr>
<tr>
<td>Export</td>
<td>Use this button to export a FIX profile.</td>
</tr>
</tbody>
</table>

**General Settings**

- **Maximum tracked requests**: Lists the maximum number of requests to be tracked during the time frame selected in the Detail Chart. The default is 1000 requests. Typically, 1000 requests should be sufficient to provide the information you seek. If it is not, you may increase or decrease it. By increasing the amount of requests, the amount of system resources needed to analyze the requests is also increased, which means the analysis will take longer to complete.

- **Ignore duplicate requests**: If selected, duplicate requests are ignored. This is the default setting. If unchecked, duplicate requests may be present in the analysis and reduces the number of unique requests in the tracked requests.
<table>
<thead>
<tr>
<th>This option...</th>
<th>Allow you to do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum displayed</td>
<td>Defines the maximum number of results to display in the GigaStor Control Panel for the fastest or slowest responses.</td>
</tr>
<tr>
<td>results</td>
<td></td>
</tr>
<tr>
<td>Track not responded</td>
<td>Amount of time used as the threshold that the GigaStor should wait for a response to a request before discarding the request from its analysis data set. If you want only requests that have received a response, uncheck this option.</td>
</tr>
<tr>
<td>requests within</td>
<td></td>
</tr>
<tr>
<td>Track/Type/Message</td>
<td>Type and Message are options defined in the FIX protocol specification. If Track is selected, the FIX transaction type will be part of this analysis profile. All untracked options are ignored for this profile.</td>
</tr>
</tbody>
</table>

**Sharing alarms with others**

Observer alarms can be shared using the included import and export functions. Sharing is useful for making your alarms uniform across multiple installations, and it can even be used as a backup tool. This section describes the exporting and importing processes.

**How to import alarms**

To import alarms, you need access to an exported *.ALM file. You must bring this file back into Observer using the import process described here:

1. Click the Alarms Settings button, near the bottommost portion of the Observer window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Click the Import Alarms button.
5. Navigate to, and select, your file; click Open.

You successfully imported an alarm file. The alarms contained within are now part of your local collection, including the triggers and actions associated with each alarm.

**How to export alarms**

To share alarms, the alarms must first be saved to a file. Create your file by following this export process:

1. Click the Alarms Settings button, near the bottommost portion of the Observer window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Select each alarm you want to export.
5. Click the Export Checked Alarms button.
6. Give your file a name, and click Save.

You successfully exported your alarms to an *.ALM file. You can now share this file with other Observer installations or keep it as a backup copy.
Sharing application definitions with others

Application definitions can be shared using the included import and export functions. Sharing is useful for making your application definitions uniform across multiple installations, and it can even be used as a backup tool. This section describes the exporting and importing processes.

How to export application definitions

To share application definitions with other users, you must first save them to a file. Create your file by following this export process:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click any one of the applications definitions tabs (not the Server Application Discovery tab itself) to ensure one of these tabs has focus.
3. Click **Tools**, and click **Export Current Application Definitions**. The Export Application Definitions dialog appears.
4. Select the groups of definitions you want to export, and click **Export**.
5. Type a name for your file, and click **Save**.

You successfully exported your application definitions to a *.protodefs file. You can now share this file with other users and installations, or keep it as a backup copy.

How to import application definitions

Prerequisite(s):

To import application definitions, you need access to an exported *.protodefs file. See **Exporting app definitions on page 46** for details.

To import application definitions, follow the import process:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click any one of the applications definitions tabs (not the Server Application Discovery tab itself) to ensure one of these tabs has focus.
3. Click **Tools**, and click **Import Application Definitions**.

    The Open file dialog appears.

4. Locate and select the *.protodefs file that you want to import, and click **Open**. The Import Application Definitions dialog appears.
5. Select the protocols to import and the importing behavior.

You successfully imported application definitions. The definitions you import are now part of your local collection.

How to export report data to XML

Sometimes it is advantageous to bring report data out of its native format and into third-party tools. If needed, you can accomplish this by exporting your report data to XML.

Your can generate hundreds of reports, all of which can be configured as you need and provide you visibility and analytics about your network. After creating a report, there may be times where you want the data from only part of a report so you can store the data elsewhere or manipulate it using another tool. Using settings only available from the report in your web browser, you can access the data on a report.

You can access report content in its raw format and then process the data with your tools. Just some of the raw data you can access includes SLA measurements for use in a MOM, security alerting inside a SIEM, or compliance monitoring data.

Unlike nearly every task described in this guide, which describes using the user interface to configure reports, this feature is only available after the report is created and you are viewing it in your web browser.

To export your report data to XML:

1. Open a web browser and type the following URL: http://Observer/Observer where Observer is the host name or IP address of the system running Observer.

2. In the upper left, ensure the desired probe instance is selected from the list.

3. Click Settings in the upper right. The Report Settings page opens.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Report Element Link when clicking on the report element title bar</td>
<td>Used for embedding report elements in a third-party tool. This allows you to click the title bar of any report element (graph, table, etc.) and obtain a link to that element and then embed the link in your tool. Hover your mouse over an element title and click it. This opens a pop up window from which you can open the element in another browser window or use in your third party tool. The report (or report element — table, graph, etc.) you selected is processed and displayed in your third</td>
</tr>
</tbody>
</table>
Private key locations per server

Microsoft Lync Server

Microsoft Lync Server encrypts all of its VoIP traffic, including the call set up process. To decrypt a Microsoft Lync server conversation, you must have the security certificate and Observer must see the telephone’s power up.

By default, the Lync Server key is not exportable. You must create an exportable key for Observer to use. Getting the Lync Server key is similar to that for the IIS Web Server. See Windows IIS Web Server on page 79.

Apache Web Server

Perform a search for the file with the name “server.key”. Check the format of the server.key file to ensure it is not an encrypted private key file. See Example of an encrypted private key file on page 80.

However, if the private key file is encrypted, the private key file must be decrypted using the openSSL command line tool and the password that was used to encrypt it. This utility can be obtained by following an appropriate link as follows:

- [http://www.openssl.org](http://www.openssl.org)

- For Windows compatible versions, use a search engine to search for the terms “Download,” “Win32,” and “OpenSSL”.

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>party dashboard. This report is from the source which it was generated, including any associated data sources and filters applied. In the URL, you may see a start time and end time for the report. This happens when you generate the report using a fixed time criteria. These fields are in epoch and can be modified within the URL to provide the report on whatever fixed time period you wish.</td>
<td></td>
</tr>
<tr>
<td>Show XML Export button</td>
<td>Allows the user to manually export the XML of a report (in its entirety, including all elements) to a XML file. An “XML Export” button appears at the top right. Click the button to generate an XML file which is saved to your hard drive. Use the XML file as you wish.</td>
</tr>
<tr>
<td>Show XML Report Link button</td>
<td>Similar to the Show XML Export button, but instead of needing to click the button to generate the XML, you can generate the URL once and then use the XML data request URL in your third party tool. The resulting XML will be for the entire report, including all elements. Similar to the “Show Report Element Link…”, the start and end times can be modified if using fixed time periods, and all business group sources and filters will apply.</td>
</tr>
</tbody>
</table>
After obtaining the OpenSSL command line utility, the private key file can be decrypted using the following command (choose the appropriate locations for the input and output files):

```
openssl rsa -in server.key -out UnencryptedKey.key [enter passphrase]
```

You can now use the newly created output key, in Observer, to successfully decrypt and analyze encrypted network traffic.

**Windows IIS Web Server**

Windows does not contain a searchable private key file. The key file must be extracted from the website server certificate, and the server certificate must contain the private key file. Use the following Microsoft Support document to export your server certificate and private key to a single .pfx file: [http://support.microsoft.com/kb/232136](http://support.microsoft.com/kb/232136) (How to back up a server certificate in Internet Information Services).

After you successfully export the .pfx file (PKCS #12), you must obtain the OpenSSL utility. This utility can be obtained by following an appropriate link as follows:

- [http://www.openssl.org](http://www.openssl.org)
- For Windows compatible versions, use a search engine to search for the terms “Download,” “Win32,” and “OpenSSL”.

With a valid .pfx server certificate backup file and the openssl utility, the following command should be used (choose the appropriate locations for the input and output files):

```
openssl pkcs12 -nodes -in c:\mycertificate.pfx -out c:\server.key
```

You can now use the newly created output key, in Observer, to successfully decrypt and analyze encrypted network traffic.

**Example of a non-encrypted private key file**

A normal, non-encrypted private key file should contain text of the following format. Notice the absence of a “Proc-Type: ENCRYPTED” header. A file of this format is usable by Observer.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD7uhNymd6WCOQRhQ0rp5zs4FEmX2rKtm0dmTf44SVaGvFLF1vakeOFY/sfE4aa2u0NcFcbFaSzw3IzWumu4sCtqtvb8Zil+13VCdyR+2SRx9GBuSnoL/6P1I6m+C0gHq6g0ILoiTAJnY+MOEC2kbMkljPVUOEX9IEG0AQIDAQABAOGFQ0YogWEVqQRpWZWNY6XnJKxVGBGcZrPDrWfgC0/ITXyULt12I47QLd+ni-----END RSA PRIVATE KEY-----
```

**Example of an encrypted private key file**

An encrypted private key file may have the following format, which indicates that the private key file obtained contains an RSA Private Key, where the text for the key itself is encrypted. A file in this format will generate an error dialog stating “Error Loading the Private Key File!” You must decrypt this key file before it will function.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,7BC....
JHQ8U0pDbeFM9h2jZSmuugxdqOa2qg/MiX43Xa4Es6nKmzu9oI/ZfpIdAHi8qtsDm2sBQR1XD9AXeIry+0tGZibUaphQEsvI995FWUsh8N9dVumsgykmMXsNd7tKBHio/VVSAAD9bV3db15bMwMnP+YC3S90GAK4ZRIqHRQ94fd/ZAvP8kV9i1wCmX6sFWNBLGkFlL9qkyr+OOQqlrAyZAB2UThGCJJetELFtV4mLmIaHdgD1cUqpJp==
```

334 | Observer® (pub. 17.Sept.13)
Importing and exporting VoIP or video conferencing settings

Settings for VoIP can be imported or exported into the Network Trending tool. Doing either is very useful depending on what you are trying to accomplish. For example, if you want to backup your settings or share your VoIP settings with other Observer installations, you should export your VoIP settings.

To import and/or export your VoIP settings, complete the following steps:
1. Choose **Trending/Analysis > Network Trending**. The Network Trending tool opens.
2. Click the Tools button.
3. Click Import or Export Settings. A file dialog appears, which allows you to complete the process.

Restoring the default application list

Under certain circumstances, it may be beneficial for you to restore the default application list. Doing so removes all of your custom or modified application definitions and returns your applications to default—exactly how the default installation would behave.

How to restore TCP application definitions

To restore the default TCP applications, complete the following steps:
1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click the TCP Application Definitions tab to ensure it has focus.
3. Click the Tools button, and click Restore Predefined TCP Applications. A confirmation prompt appears.
4. Click OK to confirm.
5. (Optional) Select Apply Changes Across All Probe Instances if you want to apply these changes to all probe instances.
6. Click OK to apply and save your changes.

Your TCP application definitions list is now restored.

How to restore UDP application definitions

To restore the default UDP applications, complete the following steps:
1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click the UDP Application Definitions tab to ensure it has focus.
3. Click the Tools button, and click Restore Predefined UDP Applications. A confirmation prompt appears. Click OK to confirm.
4. (Optional) Select Apply Changes Across All Probe Instances if you want to apply these changes to all probe instances.
5. Click OK to apply and save your changes. Your list is restored.
Importing and exporting Observer Alias (.adr) files

Observer Infrastructure can exchange alias lists with Observer. To import an alias list from (or export an alias list to) Observer, select Tools > Observer Integration > Import Alias list from (or Export alias List to...).

A file dialog is then displayed, allowing you to select the file to import (or supply a filename to export).

Alias list files must have the extension .adr for Observer and Observer Infrastructure to recognize them.

Importing or exporting a server profile

You can import or export servers that you monitor from one Observer analyzer to another. This can save time and reduce typing errors if you have several Observer analyzers which you want to have the same servers be analyzed for application transaction analysis.

Tip! You can also logically group server applications and switch between profiles quickly by choosing a profile from the Profiles list.

1. Choose Trending/Analysis > Application Transaction Analysis.
2. Click the Settings button to define any application servers you want to monitor.
3. Click the Import or Export button.

First you must define the server applications and then export the server to create the *.ata file that you can later import.

Creating a Forensic Settings profile

Forensics profiles provide a mechanism to define and load different pairings of settings and rules profiles. Settings profiles define pre-processor settings that let you tune performance; rules profiles define which forensic rules are to be processed during analysis to catch threats against particular target operating systems and web servers. Because Observer performs signature matching on existing captures rather than in real time, its preprocessor configuration differs from that of native Snort. When you import a set of Snort rules that includes configuration settings, Observer imports rules classifications, but uses its own defaults for the preprocessor settings.

There is a difference between enabling the preprocessor and enabling logs for the preprocessor. For example, you can enable IP defragmentation with or without logging. Without logging, IP fragments are simply reassembled; only time-out or maximum limit reached messages are noted in the Forensics Log and in the Forensic Analysis Summary window. If logging is enabled, all reassembly activity is displayed in the Forensics Log (but not displayed in the Forensic Analysis Summary).

1. In Observer, choose Capture > GigaStor Control Panel > Forensic Analysis tab.
2. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.
3. Choose your profile and click Edit. The Forensic Settings window opens.
4. From the Forensic Settings window, complete the following:
   # Import Snort rules
   # Define Forensic Settings.
Define Rule Settings—Select the rules you want to enable.

5. Close all of the windows, then right-click anywhere on the Forensic Analysis tab and choose Analyze from the menu.

This applies the rules and filters to the capture data and displays the results in the Forensics Summary tab. The top portion of the Rules window lists the rules that were imported, grouped in a tree with branches that correspond to the files that were imported.

Rule classifications offer another level of control. Check the “Rules must also match rule classifications” box to display a list of defined rule classifications. Classifications are defined at import time by parsing the Snort config classification statements encountered in the rule set. Rules are assigned a classification in the rule statement’s classtype option.

Select the rule classification(s) you want to enable. If classification matching is enabled, a rule and its classification must both be enabled for that rule to be processed. For example, suppose you want to enable all policy violation rules: simply right-click on the rule list, choose Enable all rules, and then enable the policy violation classification.

### Table 56: Forensic Settings options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings Profile</td>
<td>Settings Profiles provide a mechanism to save and load different preprocessor settings, and share them with other Observer analyzers.</td>
</tr>
<tr>
<td>IP Flow</td>
<td>Packets belong to the same IP flow if they share the same layer 3 protocol, and also share the same source and destination addresses and ports. If this box is checked, forensic analysis identifies IP flows (also known as conversations), allowing Snort rules to isolate packets by direction and connection state via the flow option. If this pre-processor is disabled, flow keywords are ignored, but the rest of the rule is processed. The remaining settings allow you to throttle flow analysis by limiting the number of flows tracked, and by decreasing the time window within which a flow is considered active.</td>
</tr>
<tr>
<td>IP Defragmentation</td>
<td>Some types of attacks use packet fragmentation to escape detection. Enabling this preprocessor causes forensic analysis to identify and reconstruct fragmented packets based on the specified fragment reassembly policy. Rules are then run against the reconstructed packets during forensic analysis. The fragment reassembly policy mimics the behavior of various operating systems in what to do when ambiguous fragments are received. Choose the policy to match the OS of the server (or servers) being monitored. If the buffer contains traffic targeting hosts with different operating systems, use post-filtering to isolate the traffic before forensic analysis so that you can apply the correct policy. Defragmentation Policy is: BSD=AIX, FreeBSD, HP-UX B.10.20, IRIX, IRIX64, NCD Thin Clients, OpenVMS, OS/2, OSF1, SunOS 4.1.4, Tru64 Unix, VAX/VMS Last data in=Cisco IOS BSD-right=HP JetDirect (printer) First data in=HP-UX 11.00, MacOS, SunOS 5.5.1 through 5.8 Linux=Linux, OpenBSD Solaris=Solaris Windows=Windows (95/98/NT4/W2K/XP)</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Refer to** [http://www.snort.org](http://www.snort.org) **for more detailed version-specific information.** The remaining options allow you to enable logging of alerts and reconstruction progress, limit the number of active packet fragments to track, and change the length of fragment inactivity that causes the fragment to be dropped from analysis.

### TCP Stream Reassembly

- **Another IDS evasion technique is to fragment the attack across multiple TCP segments.** Because hackers know that IDS systems attempt to reconstruct TCP streams, they use a number of techniques to confuse the IDS so that it reconstructs an incorrect stream (in other words, the IDS processes the stream differently from that of the intended target). As with IP fragmentation, forensic analysis must be configured to mimic how the host processes ambiguous and overlapping TCP segments, and the topology between attacker and target to accurately reassemble the same stream that landed on the target. Re-assembly options are described below:

- **Log preprocessor events**—Checking this box causes forensic analysis to display all activity generated by the TCP stream assembly preprocessor to the log.

- **Maximum active TCP streams tracked**—If this value is set too high given the size of the buffer being analyzed, performance can suffer because of memory consumption. If this value is set too low, forensic analysis can be susceptible to denial of service attacks upon the IDS itself (i.e., the attack on the target is carried out after the IDS has used up its simultaneous sessions allocation).

- **Drop TCP streams inactive for this duration**—A TCP session is dropped from analysis as soon as it has been closed by an RST message or FIN handshake, or after the time-out threshold for inactivity has been reached. Exercise caution when adjusting the time-out, because hackers can use TCP tear-down policies (and the differences between how analyzers handle inactivity vs. various operating systems) to evade detection.

- **TTL delta alert limit**—Some attackers depend on knowledge of the target system’s location relative to the IDS to send different streams of packets to each by manipulating TTL (Time To Live) values. Any large swing in Time To Live (TTL) values within a stream segment can be evidence of this kind of evasion attempt. Set the value too high, and analysis will miss these attempts. Setting the value too low can result in excessive false positives.

- **Overlapping packet alert threshold**—The reassembly preprocessor will generate an alert when more than this number of packets within a stream have overlapping sequence numbers.

- **Process only established streams**—Check this box if you want analysis to recognize streams established during the given packet capture.

- **Reconstruct Client to Server streams**—Check this box to have analysis actually reconstruct streams received by servers.

- **Reconstruct Server to Client streams**—Check this box to have analysis actually reconstruct streams received by clients.

- **Overlap method**—Different operating systems handle overlapping packets using one of these methods. Choose one to match the method of the systems being monitored.

### TCP Stream Reassembly (Continued)

- **Reassembly error action**—Discard and flush writes the reassembled stream for analysis, excluding the packet that caused the error. Insert and flush writes the...
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reassembled stream, but includes the packet that caused the error. Insert no flush includes the error-causing packet and continues stream reassembly.</td>
<td></td>
</tr>
<tr>
<td>Reassembled packet size threshold range—Some evasion strategies attempt to evade detection by fragmenting the TCP header across multiple packets. Reassembling the stream in packets of uniform size makes this easier for attackers to slip traffic past the rules, so forensic analysis reassembles the stream using random packet sizes. Here you can set the upper and lower limits on the size of these packets.</td>
<td></td>
</tr>
<tr>
<td>Reassembled packet size seed value—Changing the seed value will cause forensic analysis to use a different pattern of packet sizes for stream reassembly. Running the analysis with a different seed value can catch signature matches that would otherwise escape detection.</td>
<td></td>
</tr>
<tr>
<td>Port List—Enabling the Port List option limits analysis to (or excludes from analysis) the given port numbers.</td>
<td></td>
</tr>
</tbody>
</table>

### HTTP URI Normalization

Many HTTP-based attacks attempt to evade detection by encoding URI strings in UTF-8 or Microsoft %u notation for specifying Unicode characters. This preprocessor includes options to circumvent the most common evasion techniques. To match patterns against the normalized URIs rather than the unconverted strings captured from the wire, the VRT Rules use the uricontent option, which depends on this preprocessor. Without normalization, you would have to include signatures for the pattern in all possible formats (using the content option), rather than in one canonical version.

Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the HTTP preprocessor to the log, but not the Forensic Summary Window.

Maximum directory segment size—Specifies the maximum length of a directory segment (i.e., the number of characters allowed between slashes). If a URI directory is larger than this, an alert is generated. 200 characters is a reasonable cutoff point to start with. This should limit the alerts to IDS evasions.

Unicode Code Page—Specify the appropriate country code page for the traffic being monitored.

Normalize ASCII percent encodings—This option must be enabled for the rest of the options to work. The second check box allows you to enable logging when such encoding is encountered during preprocessing. BEcause such encoding is considered standard, logging occurrences of this is not recommended.

Normalize percent-U encodings—Convert Microsoft-style %u-encoded characters to standard format. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because such encoding is considered non-standard (and a common hacker trick), logging occurrences of this is recommended.

Normalize UTF-8 encodings—Convert UTF-8 encoded characters to standard format. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because Apache uses this standard, enable this option when monitoring Apache servers. Although you might be interested in logging UTF-8 encoded URIs, doing so can result in a lot of noise because this type of encoding is common.

Lookup Unicode in code page—Enables Unicode codepoint mapping during preprocessing to handle non-ASCII codepoints that the IIS server accepts.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normalize double encodings—</td>
<td>This option mimics IIS behavior that intruders can use to launch insertion attacks. Normalize bare binary non ASCII encodings—This an IIS feature that uses non-ASCII characters as valid values when decoding UTF-8 values. As this is non-standard, logging this type of encoding is recommended. Normalize directory traversal—Directory traversal attacks attempt to access unauthorized directories and commands on a web server or application by using the // and ../ syntax. This preprocessor removes directory traversals and self-referential directories. You may want to disable logging for occurrences of this, as many web pages and applications use directory traversals to reference content. Normalize multiple slashes to one—Another directory traversal strategy is to attempt to confuse the web server with excessive multiple slashes. Normalize Backslash—This option emulates IIS treatment of backslashes (i.e., converts them to forward slashes).</td>
</tr>
<tr>
<td>ARP Inspection</td>
<td>Ethernet uses Address Resolution Protocol (ARP) to map IP addresses to a particular machine (MAC) addresses. Rather than continuously broadcasting the map to all devices on the segment, each device maintains its own copy, called the ARP cache, which is updated whenever the device receives an ARP Reply. Hackers use cache poisoning to launch man-in-the-middle and denial of service (DoS) attacks. The ARP inspection preprocessor examines ARP traffic for malicious forgeries (ARP spoofing) and the traffic resulting from these types of attacks. Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the ARP Inspection preprocessor to the log, but not the Forensic Summary Window. Report non-broadcast requests—Non-broadcast ARP traffic can be evidence of malicious intent. Once scenario is the hacker attempting to convince a target computer that the hacker’s computer is a router, thus allowing the hacker to monitor all traffic from the target. However, some devices (such as printers) use non-broadcast ARP requests as part of normal operation. Start by checking the box to detect such traffic; disable the option only if analysis detects false positives.</td>
</tr>
<tr>
<td>Telnet Normalization</td>
<td>Hackers may attempt to evade detection by inserting control characters into Telnet and FTP commands aimed at a target. This pre-processor strips these codes, thus normalizing all such traffic before subsequent forensic rules are applied. Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the Telnet Normalization preprocessor to the log, but not the Forensic Summary Window. Port List—Lets you specify a list of ports to include or exclude from Telnet pre-processing. The default settings are appropriate for most networks.</td>
</tr>
<tr>
<td>Variable Name</td>
<td>A scrollable window located below the preprocessor settings lists the variables that were imported along with the Snort rules. Variables are referenced by the rules to specify local and remote network ranges, and common server IP addresses and ports. You can edit variable definitions by double-clicking on the variable you want to edit. The VRT Rule Set variable settings (and those of most publicly-distributed rule sets) will work on any network without modification, but you can dramatically improve performance by customizing these variables to match the network being monitored.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>monitored. For example, the VRT rules define HTTP servers as any, which results in much unnecessary processing at runtime. Address variables can reference another variable, or specify an IP address or class, or a series of either. Note that unlike native Snort, Observer can process IPv6 addresses. Port variables can reference another variable, or specify a port or a range of ports. To change a variable, simply double-click the entry. The Edit Forensic Variable dialog shows a number of examples of each type of variable which you can use as a template when changing values of address and port variables.</td>
<td></td>
</tr>
</tbody>
</table>

**Importing Snort rules**

After getting the Snort rules from [http://www.snort.org](http://www.snort.org), follow these steps to import them into Observer.

1. In Observer, choose Capture > GigaStor Control Panel > Forensic Analysis tab.
2. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.
3. Choose your profile and click Edit. The Forensic Settings window opens.
4. At the bottom of the window, click the Import Snort Files button.
5. Locate your Snort rules file and click Open. Close all of the windows. After you import the rules into Observer you are able to enable and disable rules and groups of rules by their classification as needed.

   Observer displays a progress bar and then an import summary showing the results of the import. Because Observer’s forensic analysis omits support for rule types and options not relevant to a post-capture system, the import summary will probably list a few unrecognized options and rule types. This is normal, and unless you are debugging rules that you wrote yourself, can be ignored.

6. To use the Snort rules you just imported, right-click anywhere on the Forensic Analysis tab and choose Analyze from the menu.
Chapter 20: Supported Protocols

Protocols supported by Observer

The following list is current at the time of publication.

For the most complete and up-to-date protocol list, always visit:

http://www.networkinstruments.com/protocols

29West - LBT-TCP
29West - LBT-RM
29West - LBT-RU
29West - LBMC
29West - LBMR
3COM - MIP - Extensions to Mobile IP
3COM - NBP - Name Binding Protocol
3COM - NetBIOS - NetBIOS
802.11b, 802.11g and 802.11n wireless protocols.
802.11 - Management
802.11 - Control
802.11 - Data
802.11 - WEP - Wireless Encryption Protocol
802.11 - LWAPP (ports 12222, 12223)
802.11e - QoS for Wireless LANs
802.11i - TKIP - Temporal Key Integrity Protocol
802.11i - RSN - Robust Security Network
802.11a - Outdoor Channel Support - channels 149, 153, 157, 161, 165 (at 5.470-5.745GHz)
802.1Qad - Service VLAN Tag
802.1Qag - CFM - Connectivity Fault Management
802.1Qah - PBB - Provider Backbone Bridge
802.1x - PEAP - Protected EAP (draft-josefsson-pppext-eap-tls-eap-07)
802.1x - TLS - Transport Layer Security - RFC2246 and RFC3546
802.1x Port-Based Network Access Control - EAP over LANs (EAPOL)
AFS - Replication Server
AppleTalk
AppleTalk - AARP - Address Resolution Protocol
AppleTalk - ADSP - Data Stream Protocol
AppleTalk - AEP - Echo Protocol
AppleTalk - AFP - Filing Protocol
AppleTalk - ALAP - Link Access Protocol over WAN
AppleTalk - ASP - Session Protocol
AppleTalk - ATP - Transaction Protocol
AppleTalk - DDP - Datagram Delivery Protocol Phase 1 & 2
AppleTalk - ELAP - Ethernet Link Access Protocol
AppleTalk - NBP - Name Binding Protocol
AppleTalk - PAP - Printer Access Protocol
AppleTalk - RTMP - Routing Table Maintenance Protocol
AppleTalk - SoftTalk - Session Layer Protocol
AppleTalk - ZIP - Zone Information Protocol
ATM
ATM - SONET/SDH
Banyan VINES - ARP - Address Resolution Protocol
Banyan VINES - AS - Application Services
Banyan VINES - Echo - Echo
Banyan VINES - ICP - Internet Control Protocol
Banyan VINES - IP - Network Layer
Banyan VINES - IPC - Interprocess Communication Protocol
Banyan VINES - LLP - Link Layer Protocol
Banyan VINES - Matchmaker - Program to Program Communication
Banyan VINES - RTP - Routing Update Protocol
Banyan VINES - SMB - Server Message Block
Banyan VINES - SPP - Sequenced Packet Protocol
Cellular - 3GPP2
Cellular - A11
Cellular - A10
Cellular - SMPP - Short Message Peer-to-peer
Cellular - LTE - GTPv2-c - GPRS Tunneling Protocol version 2
Cellular - LTE - NAS - Non-Access-Stratum
Cellular - LTE - S1AP - S1 Application Protocol
Cellular - LTE - X2AP - X2 Application Protocol
Cisco - CDI - Cisco Device Identification
Cisco - CDP - Cisco Discovery Protocol
Cisco - CGMP - Cisco Group Membership Protocol
Cisco - DISL - Dynamic ISL
Cisco - DLSw - Data Link Switching
Cisco - DTP - Dynamic Trunking Protocol
Cisco - EIGRP - Enhanced Interior Gateway Routing Protocol
Cisco - ERSPAN - Enhanced Remote Switch Port Analyzer
Cisco - HSRP - Hot Standby Router Protocol (RFC2281)
Cisco - IGRP - Internet Gateway Routing Protocol
Cisco - ISL - Inter-Switch Link Protocol
Cisco - Netflow (v1-9)
Cisco - LEAP
Cisco - PVSTP+
Cisco - RUDP - Reliable UDP
Cisco - SLARP - Serial Line Address Resolution Protocol
Cisco - SLE - Cisco - Serial Link Encapsulation
Cisco - SSP - Skinny Station Protocol
Cisco - STUN - Serial Tunneling of SDLC header
Cisco - TDP - Tag Distribution Protocol over TCP
Cisco - VNTag
Cisco - VTP - Virtual Trunking Protocol
Cisco - VoIP - SGM - Skinny Gateway Message
Cisco - VoIP - SCCP - Skinny Client Control Protocol
Cisco - WIDS - Wireless IDS Protocol
Citrix - CGP - Common Gateway Protocol
Citrix - Decrypt "Light Encryption"
Citrix - Decompress "Reducer Version 2"
Citrix - Independent Computing ARchitecture (ICA) 3.0
Citrix - Name Enumerator
Citrix - Name Resolver
Citrix - Protocol Driver
Citrix - Scripting
Citrix - Seemless Windows Interface (VC)
Citrix - Speedbrowse
Citrix - SubDriver
Citrix - Thinwire1 (VC)
Citrix - Thinwire2 (VC)
Citrix - Transport Driver
Citrix - User Interface
Citrix - User Interface Extension
Citrix - Virtual Driver
Citrix - Winstation Driver
Citrix - Winstation Driver - Client Drive Mapping
Citrix - Winstation Driver - Speedbrowse
Citrix - Winstation Driver - Remote Windows Data (Thinwire)
DCE - Distributed Time Service Local Server
DCE - Distributed Time Service Provider
DCE - Name Service
DCE - RPC
DCE - Security ID Mapper
DCE/RPC - BOS Server
DCE/RPC - BUDB
DCE/RPC - BUTC
DCE/RPC - CDS Solicitation
DCE/RPC - Conversation Manager
DCE/RPC - Directory ACL Interface
DCE/RPC - Endpoint Mapper
DCE/RPC - Endpoint Mapper4
DCE/RPC - FLDB
DCE/RPC - FLDB UBIK TRANSFER
DCE/RPC - ICL RPC
DCE/RPC - Kerberos V (under TCP or UDP)
DCE/RPC - NCS 1.5.1 Local Location Broker
DCE/RPC - Operations between registry server replicas
DCE/RPC - Prop Attr
DCE/RPC - RS_ACCT
DCE/RPC - RS_BIND
DCE/RPC - RS_MISC
DCE/RPC - RS_PROP_ACCT
DCE/RPC - RS_UNIX
DCE/RPC - Registry Password Management
DCE/RPC - Registry Server Attributes Schema
DCE/RPC - Registry server propagation interface - ACLs.
DCE/RPC - Registry server propagation interface - PGO items
DCE/RPC - Registry server propagation interface - properties and policies
DCE/RPC - Remote Management
DCE/RPC - Repserver Calls
DCE/RPC - TokenServer Calls
DCE/RPC - UpServer
DECNet IV - CTERM - Command Terminal
DECNet IV - DAP - Data Access Protocol
DECNet IV - DECnet-DNS - Distributed Name Services
DECNet IV - DNAv4 - Digital Network Architecture v4
DECNet IV - DRP - DECnet Routing Protocol
DECNet IV - FOUND - Found
DECNet IV - LAT - Local Area Transport Protocol
DECNet IV - LANBridge (DEC Spanning Tree Protocol)
DECNet IV - MOP - Maintenance Operations Protocol
DECNet IV - NICE - Network Information & Control Exchange
DECNet IV - NSP - Network Services Protocol
DECNet IV - SCP - Session Control Protocol
DECNet IV - SMB - Server Message Block
DICOM - AC-PDU - DICOM Upper Layer Protocol
DICOM - P-DATA-PF - DICOM Upper Layer Protocol
DICOM - P-DATA-TF - DICOM Upper Layer Protocol
DICOM - PDV-Header - DICOM Upper Layer Protocol
DICOM - Message Control - DICOM Upper Layer Protocol
DICOM - A-RELEASE-RQ - DICOM Upper Layer Protocol
DICOM - A-ASSOCIATE-AC - DICOM Upper Layer Protocol
DICOM - DICOM Message Control Protocol
DICOM - DICOM Group Length
DICOM - DICOM Affected SOP Class
DICOM - C-SEND-RQ - DICOM Command Set
DICOM - C-SEND-RSP - DICOM Command Set (Command Field)
DICOM - DICOM Message ID
DICOM - DICOM Application Control Protocol
DICOM - DICOM Data Set Type Fields
DICOM - DICOM Status Fields
DICOM - DICOM Affected SOP Instance UIDs
DICOM - DICOM Associate RQ/AC
DICOM - DICOM Data Control
DICOM - JPEG - DICOM Presentation Protocol
DICOM - RQ/AC - DICOM Associate RQ/AC
FDDI - MAC - Media Access Control
FDDI - SMT - Station Management
FIBRE Channel - ISO/IEC 8802-2 LLC
FIBRE Channel - ISO/IEC 8802-2 LLC/SNAP
FIBRE Channel - iSCSI
FIBRE Channel - IPI-3
FIBRE Channel - SBCCS
FIBRE Channel - Fibre Channel Services
FIBRE Channel - FC-FG
FIBRE Channel - FC-XS
FIBRE Channel - FC-AL
FIBRE Channel - SNMP
FIBRE Channel - HIPPI - FP
FIBRE Channel - FCIP Fibre Channel Over IP
LAN - Ethernet - Non-802.3 Ethernet
LAN - FDDI - Fiber Distributed Data Interface
LAN - IEEE 802.3 - IEEE 802.3
LAN - IEEE 802.3x - IEEE 802.3 extensions
LAN - IEEE 802.5 - Token Ring
LAN - IEEE 802.5/MAC - Token Ring Media Access Control
LAN - IEEE 802.3 Slow Protocol OAM - Operations Administration and Maintenance
LAN - IEEE 802.3.ad - Link Aggregation Control Protocol
LAN - Ethernet Loopback
LAN - IEEE 802.11b - Management
LAN - IEEE 802.11b - Control
LAN - IEEE 802.11a - Management
LAN - IEEE 802.11a - Control
LAN - IEEE 802.11g - Management
LAN - IEEE 802.11g - Control
LLC - 802.1Q - Load-balanced switch-to-switch trunking on VLAN
LLC - ARM - Component of VIVID
LLC - ARM TLV - Component of VIVID
LLC - BME - Component of VIVID
LLC - CCP - Component of VIVID
LLC - CCP TLV - Component of VIVID
LLC - Ethernet - Ethernet Data Link Control
LLC - FNA - Fujitsu Network Architecture
LLC - IEEE 802.1 - Spanning Tree
LLC - IEEE 802.1p - VLAN - GARP GVRP GMRP
LLC - IEEE 802.1Q - Flow control
LLC - LLC - Logical Link Control
LLC - MPLS - Multi-Protocol Label Switching - Internet Draft
LLC - PPPoE - Point-to-Point over Ethernet
LLC - SNAP - Subnet Access Protocol
LLC - Token Ring MAC - Token Ring Medium Access Control
LLC - VIVID - System LAN Emulation
LLC - XTP - Xpress Transfer over Ethernet, Token-Ring, FDDI
Microsoft - DCOM - Distributed COM
Microsoft - DS - Datagram Service
Microsoft - NetBIOS - LAN Manager
Microsoft - NS - Name Service
Microsoft - NTLMSSP - NT Lan Manager Secure Socket Protocol
Microsoft - SMB - LAN Manager SMB
Microsoft - SS - Session Service
Microsoft - SMB Mailslot - SMB Mailslot
Microsoft - SMB Pipe - SMB Pipe
Microsoft - RPC SvcCtl - Microsoft RPC Service Control
Microsoft - RPC NETLOGON - Directory Service Functions
Microsoft - Directory Replication Service
Microsoft - Distributed File System
Microsoft - Distributed Link Tracking Server Service
Microsoft - Encrypted File System Service
Microsoft - LLMNR - Link Local Multicast Name Resolution
Microsoft - Local Security Architecture
Microsoft - Local Security Architecture (Directory Services)
Microsoft - MAPI (Exchange)
Microsoft - RPC Endpoint Mapper
Microsoft - RPC MGMT
Microsoft - Messenger Service
Microsoft - NetLogon
Microsoft - RPC NSPI
Microsoft - Registry
Microsoft - Security Account Manager
Microsoft - Server Service
Microsoft - Service Control
Microsoft - MS RPC SAMR
Microsoft - MS RPC SRVSVC
Microsoft - MS RPC SVCCTL
Microsoft - MS RPC WKSSVC
Microsoft - Spool Subsystem
Microsoft - Task Scheduler Service
Microsoft - Telephony API Service
Microsoft - Web Service Discovery
Microsoft - Windows Browser Protocol
Microsoft - Windows Lanman Remote API Protocol
Microsoft - Windows Logon Protocol
Microsoft - Workstation Service
MPLS - BGP-4 - Carrying Label Information in BGP-4
MPLS - CP - Label Encapsulation Protocol
MPLS - CR-LDP - Label Distribution Protocol
MPLS - DiffServ - Support of Differentiated Services
MPLS - ICMP - Internet Control Message for MPLS
MPLS - ICMPv6 - Internet Control Message Protocol for MPLS
MPLS - LDP - Label Distribution Protocol
MPLS - LSE - Label Stack Encoding
MPLS - RSVP ext - RSVP-TE - Internet Draft
NASDAQ - MoldUDP
NASDAQ - MoldUDP64
NASDAQ - OUCH
NASDAQ - SoupBin TCP
NASDAQ - UQDF - UTP Plan Quotation Data Feed
Nortel - IWF - Inter-Working Function
Nortel - SLPP - Simple Loop Prevention Protocol
Nortel - UNIStim
Novell - Diagnostic - Diagnostic
Novell - Diagnostic - Serialization
Novell - Diagnostic - Watchdog
Novell - Diagnostic - Broadcast Notification
Novell - Echo - Echo
Novell - Error - Error
Novell - IPX - Internet Packet Exchange
Novell - IPX - IPX under IP
Novell - NCP 2.x 3.x - Netware Core Protocols 2.x,3.x
Novell - NCP 4.x - Netware Core Protocols 4.x
Novell - NCP 5.x - Netware Core Protocols 5.x
Novell - NetBIOS - NetBIOS
Novell - NLSP - Novell Link State Protocol
Novell - Novell-5 - Netware Core Protocols
Novell - Packet Burst - Packet Burst
Novell - PEP - Packet Exchange Protocol
Novell - RIP - Routing Information Protocol
Novell - SAP - Service Advertising Protocol
Novell - SPX - Sequenced Packet Exchange
Novell - IPX NDS - Netware Directory Protocol
Oracle - NET8
Oracle - TNS - Transparent Network Substrate
Oracle - TDS - Oracle Tabular Data Stream
OSI - ACSE - Application Control Service Element
OSI - ASN.1 - Abstract Syntax Notation
OSI - CLNP - WAN/Connectionless Mode Network Service Protocol - ISO 8473
OSI - CLNS OSI - CMIP/CMISe - Common Management Information Protocol
OSI - COTP OSI - EISIS - Connectionless-Mode Network Service End System to Intermediate System - RFC 1195
OSI - FTAM - File Transfer Access and Management, MAP decode
OSI - IN - Inactive Network
OSI - ISIS - WAN/Intermediate-System to Intermediate-System - RFC 1195
OSI - ISIS ext - ISIS extensions for Traffic Engineering and Update
OSI - MMS - Manufacturing Messaging Service
OSI - MNLP - Mobile Network Location Protocol
OSI - NSAP - WAN/Connectionless-Mode Network Service Access Point - ISO 8348
OSI - Presentation - Presentation
OSI - ROSE - Remote Operation Service Element
OSI - RTSE - Reliable Transfer Service Element
OSI - Session - Session
OSI - TP0 - Transport Protocol class 0
OSI - TP1 - Transport Protocol class 1
OSI - TP2 - Transport Protocol class 2
OSI - TP3 - Transport Protocol class 3
OSI - TP4 - Transport Protocol class 4
OSI - X.400 - Electronic Mail
OSI - X.500 - Directory Services
PPP - BAC/BACP - Bandwidth Allocation Control Protocol
PPP - CCP - Compression Control Protocol
PPP - CHAP - Challenge Handshake Authentication Protocol
PPP - EAP - Extensible Authentication Protocol
PPP - IPXCP - IPX Control Protocol
PPP - L2TP - Layer 2 Tunneling Protocol
PPP - LCP - Link Control Protocol
PPP - MP - Multilink Protocol
PPP - NETBCP - NetBIOS Frames Control Protocol
PPP - PAP - Password Authentication Protocol
PPP - PPP - Point to Point Protocol
PPP - PPP w/HDLC - PPP with HDLC-like framing over SONET/SDH
PPP - BAC/BACP - Bandwidth Allocation Control Protocol
PPP - CCP - Compression Control Protocol
PPP - CHAP - Challenge Handshake Authentication Protocol
PPP - EAP - Extensible Authentication Protocol
PPP - IPXCP - IPX Control Protocol
PPP - L2TP - Layer 2 Tunneling Protocol
PPP - LCP - Link Control Protocol
PPP - MP - Multilink Protocol
PPP - NETBCP - NetBIOS Frames Control Protocol
PPP - PAP - Password Authentication Protocol
PPP - PPP - Point to Point Protocol
PPP - PPP w/HDLC - PPP with HDLC-like framing over SONET/SDH
SCTP
SCTP - DUA - ISDN Q.921 DPNSS 1/DASS 2 User Adaptation
SCTP - IUA - ISDN Q.921 User Adaptation Layer
SCTP - S1AP - S1 Application Protocol
<table>
<thead>
<tr>
<th>Protocol Type</th>
<th>Protocol Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCTP - x2AP</td>
<td>X2 Application Protocol</td>
</tr>
<tr>
<td>SCTP - M3UA</td>
<td>MTP3 User Adaptation Layer</td>
</tr>
<tr>
<td>SIGTRAN</td>
<td>M3UA - MTP3 User Adaptation Layer</td>
</tr>
<tr>
<td>SNA - DFC</td>
<td>SNA Session Layer Data Flow Control</td>
</tr>
<tr>
<td>SNA - DCAP</td>
<td>Document Content Architecture Protocol</td>
</tr>
<tr>
<td>SNA - DIAP</td>
<td>Document Interchange Architecture Protocol</td>
</tr>
<tr>
<td>SNA - DSP</td>
<td>Distributed Services Protocol</td>
</tr>
<tr>
<td>SNA - FSP</td>
<td>File Services Protocol</td>
</tr>
<tr>
<td>SNA - FMD</td>
<td>SNA Function Management</td>
</tr>
<tr>
<td>SNA - General Data Stream</td>
<td>SNA General Data Stream</td>
</tr>
<tr>
<td>SNA - Management Services</td>
<td>SNA Management Services</td>
</tr>
<tr>
<td>SNA - NCP</td>
<td>Network Control Protocol</td>
</tr>
<tr>
<td>SNA - NetBIOS</td>
<td>NetBIOS</td>
</tr>
<tr>
<td>SNA - Path Control</td>
<td>SNA Network Layer</td>
</tr>
<tr>
<td>SNA - PU 2.0</td>
<td>(Token Ring)</td>
</tr>
<tr>
<td>SNA - SCP</td>
<td>Session Control Protocol</td>
</tr>
<tr>
<td>SNA - SMB</td>
<td>Server Message Block</td>
</tr>
<tr>
<td>SNA - Transmission Control</td>
<td>SNA Transport Layer</td>
</tr>
<tr>
<td>SNA - FID1</td>
<td></td>
</tr>
<tr>
<td>SNA - FID2</td>
<td></td>
</tr>
<tr>
<td>SNA - FID3</td>
<td></td>
</tr>
<tr>
<td>SNA - FID4</td>
<td></td>
</tr>
<tr>
<td>SNA - FID5</td>
<td></td>
</tr>
<tr>
<td>SNA - FIDF</td>
<td></td>
</tr>
<tr>
<td>SNA - RH</td>
<td></td>
</tr>
<tr>
<td>SQL - SQL</td>
<td>SQL Database Functions</td>
</tr>
<tr>
<td>SQL - SQL/TDS</td>
<td>SQL Tabular Data Stream</td>
</tr>
<tr>
<td>Sun - BOOTPARAM</td>
<td>Boot Parameters</td>
</tr>
<tr>
<td>Sun - MOUNT</td>
<td>Mount</td>
</tr>
<tr>
<td>Sun - NFS - v2</td>
<td>Network File System - RFC1094</td>
</tr>
<tr>
<td>Sun - NFS - v3</td>
<td>Network File System - RFC1813</td>
</tr>
<tr>
<td>Sun - NFS - Mount v3</td>
<td>RFC1813</td>
</tr>
<tr>
<td>Sun - NFS - Lock Manager v4</td>
<td>RFC1813</td>
</tr>
<tr>
<td>Sun - NIS</td>
<td>Network Information Services</td>
</tr>
<tr>
<td>Sun - PCNFSD</td>
<td>PC Network File System</td>
</tr>
<tr>
<td>Sun - PMAP</td>
<td>Port Map - RFC1833</td>
</tr>
<tr>
<td>Sun - RLOCK</td>
<td>RLOCK</td>
</tr>
<tr>
<td>Sun - RPC v2</td>
<td>Remote Procedure Call - RFC1831</td>
</tr>
<tr>
<td>Sun - RSTAT</td>
<td>RSTAT</td>
</tr>
<tr>
<td>TCP/IP - AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>TCP/IP - ArcaBook Multicast</td>
<td></td>
</tr>
<tr>
<td>TCP/IP - ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>TCP/IP - BFD Control</td>
<td>Bidirectional Forwarding Detection Control</td>
</tr>
<tr>
<td>TCP/IP - BFD Echo</td>
<td>Bidirectional Forwarding Detection Echo</td>
</tr>
<tr>
<td>TCP/IP - BGMP</td>
<td>Border Gateway Multicast Protocol</td>
</tr>
<tr>
<td>TCP/IP - BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>TCP/IP - BGP-4</td>
<td>BGP version 4</td>
</tr>
<tr>
<td>TCP/IP - BGP-4 ext</td>
<td>BGP ASC</td>
</tr>
<tr>
<td>TCP/IP - BitTorrent</td>
<td></td>
</tr>
<tr>
<td>TCP/IP - BOOTP</td>
<td>BOOT Protocol</td>
</tr>
<tr>
<td>TCP/IP - BSD Syslog</td>
<td>Berkeley Software Distribution Syslog</td>
</tr>
<tr>
<td>TCP/IP - CAPWAP</td>
<td>Control And Provisioning of Wireless Access Points</td>
</tr>
<tr>
<td>TCP/IP - CIFS</td>
<td>Common Internet File System</td>
</tr>
<tr>
<td>TCP/IP - CME RLC</td>
<td>CME Market Data Platform RLC</td>
</tr>
<tr>
<td>TCP/IP - CPHA</td>
<td>Checkpoint High-Availability</td>
</tr>
</tbody>
</table>
TCP/IP - CQs - SIAC Consolidated Quotation System
TCP/IP - CTS - SIAC Consolidated Tape System
TCP/IP - DAAP
TCP/IP - DCE RCP - DCE Endpoint
TCP/IP - DHCP - Dynamic Host Configuration Protocol
TCP/IP - DHCPv6 - Dynamic Host Configuration Protocol v6
TCP/IP - DIAMETER (RFC 3588)
TCP/IP - DIFFSERV - Differentiated Services
TCP/IP - DirectEdge Multicast
TCP/IP - DSL - Dynamic ISL
TCP/IP - DISP - Dispatching for SNMP
TCP/IP - DLSw - Data Link Switching
TCP/IP - DNP3 - Distributed Network Protocol 3.0
TCP/IP - DNS - Domain Name Service
TCP/IP - DVRMPv3 - Distance Vector Multicast Routing Protocol
TCP/IP - EGP - Exterior Gateway Protocol
TCP/IP - EIGRP - Enhanced Interior Gateway Routing Protocol
TCP/IP - EtherIP - Ethernet over IP Tunneling
TCP/IP - Finger - User Information - RFC 1288
TCP/IP - FLAP/SNAC - AOL Instant Messenger
TCP/IP - FIX - Financial Information Exchange
TCP/IP - FTP - File Transfer Protocol
TCP/IP - GGP - Gateway to Gateway Protocol
TCP/IP - GIOP - General Inter-ORB Protocol
TCP/IP - GMRP - 802.1 GARP Multicast Registration Protocol
TCP/IP - GOPHER - File Retrieval
TCP/IP - GRE - Generic Routing Encapsulation
TCP/IP - GTP - GPRS (General Packet Radio Service) Tunneling Protocol
TCP/IP - GTPhv2 - GPRS Tunneling Protocol version 2
TCP/IP - HTTP - Hypertext Transfer Protocol
TCP/IP - HTTP 1.1 - Hypertext Transfer Protocol 1.1
TCP/IP - IAX2 (Inter-Asterisk eXchange version 2)
TCP/IP - ICMPv4 - Internet Control Message Protocol Version 4 - RFC 2060
TCP/IP - ICMPv6 - Internet Control Message Protocol Version 6 - RFC 2463
TCP/IP - ICMP RS - Internet Control Message Router Solicitation ICMP Router Discovery
TCP/IP - IGMP - Internet Gateway Routing Protocol
TCP/IP - IGMPv2 - Internet Group Management Protocol version 2
TCP/IP - IGMPv3 - Internet Group Management Protocol version - RFC 3376
TCP/IP - IGRP - Internet Gateway Routing Protocol
TCP/IP - IIOP - Internet Inter-ORB Protocol
TCP/IP - IMAP4 - Internet Message Access Protocol
TCP/IP - IP - Internet Protocol
TCP/IP - IP Compression
TCP/IP - IPCP - Internet Protocol Control Protocol
TCP/IP - IPFIX - Internet Protocol Flow Information eXport
TCP/IP - IPinIP - IP within IP
TCP/IP - IPv6 - Internet Protocol Version 6 - RFC 2460
TCP/IP - IPv6AUTH - Internet Protocol Version 6 Authentication Header - RFC 2402
TCP/IP - IRC - Internet Relay Chat
TCP/IP - ISAKMP - Internet Security Association and Key Management Protocol
TCP/IP - iSCSI
TCP/IP - ISO TSAP - ISO Transport Service Access Point
TCP/IP - Kerberos - RFC 1510
TCP/IP - Kerberos Passwords - RFC 3244
TCP/IP - LDAPv2 - LDAP Version 2
TCP/IP - LDAPv3 - LDAP Version 3 - RFC 2251
TCP/IP - LMP - Link Management Protocol over IP
TCP/IP - Lotus Notes
TCP/IP - LPD - Line Printer Daemon Protocol
TCP/IP - LPR - Line Printer Daemon Protocol Remote
TCP/IP - LPP - ISO Services
TCP/IP - LSE Infolect - London Stock Exchange Inforject
TCP/IP - M2PA - MTP2 - Peer-to-Peer Adapt Layer
TCP/IP - MBGP - Multi-protocol BGP
TCP/IP - MINET - Mitel IP Terminal
TCP/IP - MIP - Mobile IP
TCP/IP - MIP RT - Mobile IP Reverse Tunneling
TCP/IP - MobileIP
TCP/IP - MODBUS - Modicon BUS
TCP/IP - MOSPF - Multicast Open Shortest Path First
TCP/IP - MSDP - Multicast Source Discovery Protocol
TCP/IP - Multicast DNS
TCP/IP - Multicast PITCH - BATS Multicast PITCH
TCP/IP - MYSQL
TCP/IP - NetBIOS - NetBIOS over TCP/IP
TCP/IP - NNTP - Network News Transfer Protocol
TCP/IP - NTP - Network Time Protocol - RFC 1305
TCP/IP - ODSI CP - Optical Domain Service Interconnect Control Protocol
TCP/IP - ODSI SS Optical Domain Service Interconnect Signaling Specification
TCP/IP - OSPF - Open Shortest Path First
TCP/IP - OSPF ext - Open Shortest Path First
TCP/IP - OSPF v6 - OSPF for IPv6
TCP/IP - PIM-DM - Protocol Independent Multicast, Dense Mode
TCP/IP - PIM-SM - Protocol Independent Multicast, Sparse Mode
TCP/IP - POP2 - Post Office Protocol v2
TCP/IP - POP3 - Post Office Protocol v3 and extensions
TCP/IP - PPTP - Point to Point Tunneling Protocol
TCP/IP - PTP - Precision Time Protocol
TCP/IP - Profinet - IEC 61158 and IEC 61784
TCP/IP - RADIUS Accounting (obsoletes RFC2139)
TCP/IP - RADIUS Accounting Modifications for Tunnel Protocol Support
TCP/IP - RADIUS Attributes for Tunnel Protocol Support
TCP/IP - RADIUS Extensions
TCP/IP - RARP - Reverse Address Resolution Protocol
TCP/IP - REXEC - Remote Exec
TCP/IP - RIP - Routing Information Protocol
TCP/IP - RIP-2 - Routing Information Protocol v2
TCP/IP - RIPv6 - RIP for IPv6
TCP/IP - RLOGIN - Remote Login
TCP/IP - RLPR - Remote Print Routed Route daemon Protocol
TCP/IP - RSHHELL - Remote Shell
TCP/IP - RSRB - Remote Source Route Bridging Protocol
TCP/IP - RSVP - Resource Reservation Protocol
TCP/IP - RTSP - Real Time Streaming
TCP/IP - RWHO - Remote Who
TCP/IP - SCMG - SCCP Management
TCP/IP - SSDPv1 - Simple Service Discovery Protocol
TCP/IP - Shoutcast
TCP/IP - SIMPLE - MSN / SIP for Instant Messaging and Presentation Leveraging Extensions
TCP/IP - SLPv1 - Service Location Protocol
TCP/IP - SLPv2 - Service Location Protocol Version 2 (RFC 2608)
TCP/IP - SMB - Server Message Block
TCP/IP - SMBv2 - Server Message Block version 2
TCP/IP - SMPP - Short Message Peer to Peer v3.4
TCP/IP - SMTP - Simple Mail Transport Protocol
TCP/IP - SMTPS - SMTP over SSL/TLS
TCP/IP - SNMP - Simple Network Management Protocol
TCP/IP - SNMP-2 - Simple Network Management Protocol version 2
TCP/IP - SNMP-2c - Simple Network Management Protocol version 2c
TCP/IP - SNMP-3 - Simple Network Management Protocol version 3
TCP/IP - SNMP - All Objects and Object Types MIB descriptions listed by name if MIB is loaded
TCP/IP - SOCKS
TCP/IP - SSH - Secure Shell
TCP/IP - TACACS - Terminal Access Controller Access Control System
TCP/IP - TACACS+ - Terminal Access Controller Access Control System Extensions
TCP/IP - TCP - Transport Control Protocol
TCP/IP - TDMoIP - Time Division Multiplexing over IP
TCP/IP - TELNET - Telnet
TCP/IP - Teradata - NCR Teradata
TCP/IP - Teredo - Tunneling IPv6 over UDP through Network Address Translations
TCP/IP - TFTP - Trivial File Transfer Protocol
TCP/IP - TIMED - Time Daemon Protocol
TCP/IP - UDP - User Datagram Protocol
TCP/IP - VISA Cardnet
TCP/IP - VRRP - Virtual Router Redundancy
TCP/IP - VTP - Virtual Trunking Protocol
TCP/IP - WCCP - Web Cache Communication Protocol
TCP/IP - WebSphere MQ - IBM WebSphere MQ
TCP/IP - WMP-NSS
TCP/IP - X-Windows
TCP/IP - IPv6 - (All lower TCP/Data functions)
TCP/IP - ISO - 8583 (AMEX)
TCP/IP - UPD - London Stock Exchange
WAN - Ethertype - Ethertype
WAN - Frame Relay - Frame Relay
WAN - GR303 TMC - Q.931 on T1-GR-303-CORE
WAN - HDLC - High level Data Link Control
WAN - LAPB - Link Access Procedure Balanced
WAN - LAPD - D channel Link Access Protocol
WAN - LAPV - Link Access Protocol v5
WAN - LMI Annex A - Local Management Interface A
WAN - LMI Annex D - Local Management Interface D
WAN - LMI Original - Local Management Interface<
WAN - NODELOC - Node Location
WAN - PDU Bridged - Protocol Data Unit Bridged
WAN - RFC 1490/2427 - Frame Relay
WAN - SDLC - Synchronous Data Link Control
WAN - SLIP - Serial Line Interface Protocol
WAN - TOH - Transport OverHead
WAN - VoFR - Voice over Frame Relay
WAN - VoFR Annex C - Voice over Frame Relay Annex C
WAN - VoFR Annex E - Voice over Frame Relay Annex E
<table>
<thead>
<tr>
<th>Protocols supported by Observer</th>
<th>353</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN</strong> - VoFR Annex F - Voice over Frame Relay Annex F</td>
<td></td>
</tr>
<tr>
<td><strong>WAN</strong> - VoFR Annex G - Voice over Frame Relay Annex G</td>
<td></td>
</tr>
<tr>
<td><strong>WAN</strong> - VoFR Annex H - Voice over Frame Relay Annex H</td>
<td></td>
</tr>
<tr>
<td><strong>WAN</strong> - VoFR Annex I - Voice over Frame Relay Annex I</td>
<td></td>
</tr>
<tr>
<td><strong>WAN</strong> - X.25 - X.25</td>
<td></td>
</tr>
<tr>
<td><strong>WAN</strong> - X.25 - XOT - RFC1613</td>
<td></td>
</tr>
<tr>
<td><strong>WAN</strong> - Q.922 - Q.931/Annex D (Frame Relay)</td>
<td></td>
</tr>
<tr>
<td><strong>WAN</strong> - ISO8885 - X.75 - X.75</td>
<td></td>
</tr>
<tr>
<td><strong>WAN</strong> - MultiLink PPP</td>
<td></td>
</tr>
<tr>
<td><strong>Xerox/XNS</strong> - Echo - XNS - Echo</td>
<td></td>
</tr>
<tr>
<td><strong>Xerox/XNS</strong> - Error - XNS - Error</td>
<td></td>
</tr>
<tr>
<td><strong>Xerox/XNS</strong> - PEP - XNS - Packet Exchange Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>Xerox/XNS</strong> - RIP - Routing Information Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>Xerox/XNS</strong> - SPP - Sequenced Packet Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>Xerox/XNS</strong> - Xerox XNSldp</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - COPS - Common Open Policy Service for Packet Cable</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.225.0 Version 2 - RAS</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.225.0 Version 3 - Call signalling (Q.931/Q.932)</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.235 - Security and encryption for H-series multimedia terminals</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.245 Version 1 - Call Control for H.323 multimedia</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.245 Version 2 - Call signaling for H.323 logical channels</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.245 Version 3 - Call signaling for H.323 logical channels</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.245 Version 5 - Control Protocol for Multimedia Communication</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.248 MEGACO - ITU-T &amp; IETF carrier-class VoIP signaling (text and binary)</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.261 - Video CODEC used in H.323 - RFC2032</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.263 - Video CODEC for low bit rate communication - RFC2250</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H263-1998 - RFC2429, RFC3555</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H263-2000 - RFC2429, RFC3555</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.323v3 Annex E - Protocol for multiplexed call signaling transport E</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.323v3 Annex F - Protocol for multiplexed call signaling transport F</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - H.323v3 Annex G - Communication between administrative domains</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - Megaco - Media Gateway Control Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - MGCP - Media Gateway Control Protocol Version 1 - RFC 2705</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - NCS - PacketCable - Network-Based Call Signaling Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - Q.931 - Signaling for H.323</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - RAS (H.225.0 V1) - RAS for H.323</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - RTCP - Real-time Transport Control Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - RTP - Real-time Transport Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - SAP - Session Announcement Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - SDP - Session Description Protocol - RFC 2327</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - SGCP - Simple Gateway Control Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - SIP - Session Initiation Protocol - RFC 2543, RFC 3261</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - IAX VoIP - Nortel Unistim</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - Avaya CCMS</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - T.120/X.224 - DPMC</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - T.122 - DPMC</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - T.123 - DPMC</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - T.124 (GCC) - Generic Conference Control</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - T.125 - DPMC</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - T.126 (SI) - Multipoint Still Image and Annotation</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - T.127 (MBFT) - Multipoint Binary Transfer Protocol</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - T.128 (AS) - Multipoint Application Sharing</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - XGCP - Extended GCP</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - XoIP - Media over IP</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - CN - RFC3389</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong> - 1016 - RTP Audio Payload</td>
<td></td>
</tr>
</tbody>
</table>

Protocols supported by Observer | 353
VoIP - G711/PCM
VoIP - PCMA - G711 A-law - RFC 3551
VoIP - G721 - RTP Audio Payload
VoIP - GSM - RTP Audio Payload - RFC3551
VoIP - G722 - RTP Audio Payload - RFC3551
VoIP - G723 - Payload 4 - G.723 (Audio Playback)
VoIP - G.723.1-5.3
VoIP - G723.1A-5.3
VoIP - G723.1A
VoIP - DVI4 - RTP Audio Payload - RFC3551
VoIP - LPC - RTP Audio Payload
VoIP - parityfec - RFC3009
VoIP - PCMA(G.711) - Payload 0 - G.711 PCMU u-law (Audio Playback)
VoIP - PCMU(G.711) - Payload 8 - G.711 PCMU A-law (Audio Playback)
VoIP - L8 - RFC3551
VoIP - L16 - RTP Audio Payload - RFC3551
VoIP - L20 - RFC3190
VoIP - L24 - RFC3190
VoIP - MPA - RTP Audio Payload - RFC3551, RFC2250
VoIP - MP4A-LATM - RFC3016
VoIP - mpa-robust - RFC3119
VoIP - G726
VoIP - G726-16 - RFC3551
VoIP - G726-24 - RFC3551
VoIP - G726-32 - RFC3551
VoIP - G726-40 - RFC3551
VoIP - G728 - RTP Audio Payload - RFC3551
VoIP - G729A - RTP Nortel Audio Payload (Audio Playback)
VoIP - G729B
VoIP - G729D - RFC3551
VoIP - G729E - RFC3551
VoIP - CeltB - RTP Video Payload - RFC2029
VoIP - JPEG - RTP Video Payload - RFC2435
VoIP - Nv - RTP Video Payload - RFC3551
VoIP - MPV - RTP Video Payload - RFC2250
VoIP - MP2T - RTP Audio/Video Payload - RFC2250
VoIP (FoIP) - T.30/T.38 Fax over UDP (H.323 Annex D)
VoIP - QCLEP VoIP - rtx - RFC-ietf-avt-rtp
VoIP - AMR - RFC3267
VoIP - AMR-WB - RFC3267
VoIP - DAT12 - RFC3190
VoIP - dsr-es201108 - RFC3557
VoIP - EVRC - RFC3558
VoIP - EVRC0 - RFC3558
VoIP - GSM-EFR - RFC3551
VoIP - RED - RFC2198, RFC3555
VoIP - red - RFC4102
VoIP - rtx - RFC-ietf-avt-rtp
VoIP - VDVI - RFC3551
VoIP - SMV - RFC3558
VoIP - SMV0 - RFC3558
VoIP - t140c - RFC4351
VoIP - t38 - RFC4612
VoIP - telephone-event - RFC2833
VoIP - tone - RFC2833
VoIP - t140 - RFC4103
VoIP - BMPEG - RFC2343, RFC3555
VoIP - BT656 - RFC2431, RFC3555
VoIP - DV - RFC3189
VoIP - MP1S - RFC2250, RFC3555
VoIP - MP2P - RFC2250, RFC3555
VoIP - MP4V-ES - RFC3016
VoIP - pointer - RFC2862
VoIP - raw - RFC4175
VoIP - SMPTE292M - RFC3497
VoIP - vc1 - RFC4425
VoIP - BV16 - RFC4298; BroadVo
VoIP - BV32 - RFC4298; BroadVo
VoIP - LRNB VoIP - LRWB
Other - Bridged Ethernet
Other - EIP - Extended Internet Protocol
Other - IKE - RFC2409
Other - IPsec - RFC2401
Other - DOI - Domain of Interpretation RFC 2407
Other - ESP - RFC2406
Other - AH - RFC 2402
Other - LLDP - Link Layer Discovery Protocol
Other - MNLP - Mobile Network Location Protocol
Other - PPP EAP TLS Authentication Protocol - RFC2716
Other - PPP LCP Internationalization Configuration Option - RFC2484
Other - PPP Extensible Authentication Protocol (EAP) - RFC2284
Other - sFlow
Other - Yahoo - Instant Messenger Protocol
Other - Yahoo - YMSG Messenger Protocol
Other - COPS (Common Open Policy Service)
Other - GSMP - General Switch Management Protocol
Other - VRRP (Virtual Router Redundancy Protocol)
Other - SNA over UDP Other - SCTP (Stream Control Transmission Protocol)
Chapter 21: Change Log

Recent Documentation Changes

In addition to fixing typographical and grammar errors, these changes were also made to the documentation:

July 19, 2013 Observer

- Added instructions for how to enable 256-bit AES encryption for at-rest captured data. See How to encrypt captured data on page 143.
- Added network port information that was originally listed in a separate publication. See Ports used by Network Instruments products on page 12.
- Added instructions for exporting web report data to XML or third-party tools. See How to export report data to XML on page 127.
- Added conceptual information about the "Track only new connections in each collection interval" setting. See What is Application Performance Analysis? on page 149.
- Added new information to the table listed in Choosing your network trending types on page 158, including a setting to automatically delete old trending data after a set length of days.
- Updated information for deleting trending data. See Deleting your network trending data files on page 157.
Recent Product Changes
### Numerics

- 25901 (port) 12, 12, 276, 281, 281
- 25903 (port) 12, 276, 281
- 32-bit 270, 270
- 3-D Pie/Chart Display Properties 57
- 3DES 136, 253
- 4G LTE 158
- 64-bit 257, 270, 270
- 64-bit, RAM 270
- 802.11 219, 219, 222, 226, 243
- 802.1Q 277

### Default

- 44, 279

### A

- about 163, 182, 210, 210
- access point statistics 22, 22, 24, 24
- activate and deactivate 71, 71
- active instance vs. passive instance 220
- Activity Display 33
- Activity Display tool 33
- adapter
  - see network adapter 24, 24
- see network adapter 24, 24
- adapter speed 243
- Adapter Speed tab 243
- Add Rename Filter Profile 66
- Add Report Element 130
- Add Server to Application Transaction Analysis - Add Server to Application Transaction Analysis 151
- Add/Edit Application Analysis Server 146
- Add/Edit Application Transaction Analysis Server 151
- Add/Edit Application Transactions Analysis Server 146
- Add/Edit Protocol Filter 66
- Add/Edit VoIP IP 173
- adding 46, 46
- adding derived definitions 46, 46
- adding MIBS 207
- address book 38
  - addresses, resolving 38, 38
- building 36, 36, 36, 36, 36
  - discovery method 36, 36
  - editing 38
  - entries, adding 37, 37, 38
  - importing 38, 38, 38
  - saving 36, 38, 38
  - using 39, 41, 130
  - using 41
- Address Filter 66
- address tables 233
- address, choosing 130
- addresses, resolving 38, 38
- administering 124
- administrator 249
- AES 138, 143, 239, 239, 251
- Agent Information Windows 194
- Agent Information Windows, SNMP 194
- agents 188, 188, 192, 194
- Alarm Settings 115
- alarms 120, 120, 120, 120, 120, 120, 120, 120, 120, 120, 175, 175, 222, 226, 275, 330, 330, 330, 330, 330, 330, 330, 330, 330
  - configuring 115, 115, 119
  - customizing 118, 118, 119, 119, 119, 119
  - enabling 115, 115, 116, 116
  - exporting 120, 120, 330, 330
  - filter-based, creating 117, 117
  - high latency 116
  - importing 120, 120, 330, 330
  - resetting 118, 118, 118
  - retransmissions, excessive 116
- VoIP 175, 175, 175
- alias files 336
- allocating 273
- Analysis Settings - Application Analysis Servers 146
- analyzer connection 276
- analyzing 306
- analyzing data 168, 168, 304, 304, 319, 319
- Anyone 249
- Anyone account 249, 249, 249, 276, 276
- Apache Web Server 79, 333
- Application Analysis 146
- Application Analysis - Define IP Range 146
- Application Analysis - Graph Properties 146
- Application Analysis Trending Specific 146
Application Definitions and Server Application Discovery
Settings 39
Application Discovery, Server 44
Application Performance Analysis 255

about 149
collection intervals 149
configuring 147
response time calculation 149
Application Discovery, Server 44

Application Performance Analysis 255

about 149
collection intervals 149
configuring 147
response time calculation 149
Application Discovery Analysis 151, 255

about 151, 152
response time calculation 152
Application Discovery Analysis - Graph Properties 151
Application Transaction Analysis Trending Specific - Servers 151
applications, analyzing 151, 163
applications, see server applications 44
applying 72, 72, 92
ArcaBook Multicast 44
archiving data 293
ARP inspection 307, 336
ARP Inspection, network forensics preprocessor 307, 336
as probe or analyzer 256
as Windows service 231
ATM 236, 236, 243, 244
ATM Address Filter 66
authentication 250
autoupgrade 239
Autoupgrade tab 231, 243
autoupgrading 239, 243

B
backup
installation 6, 232
backups 233
bad TCP checksums 277
troubleshooting 277
Bandwidth Utilization 24
Bandwidth Utilization - Full Duplex Display 24
Bandwidth Utilization tool 24, 24, 24
Bandwidth Utilization with Filter 24
best practices 220
BFR 17, 63, 63, 63, 63
BIOS memory hole 270
broadcast and multicast storms 33
broadcast traffic 237, 237, 237
buffer 268
buffer size 220, 294
buffer statistics 268
buffer, see capture buffer and statistics buffer 268
buffers 220, 222, 222, 222, 226, 226, 226, 270, 271

circular 58, 58
configuring 51, 57
replaying 84
bugtraq 307, 307
building 36, 36, 36, 36, 36

C
Calcule Cumulative Bytes 85
caller ID 174
CAP 63
Capture Application Transaction Analysis 151
capture buffer
32-bit Windows 268
64-bit Windows 268
FIFO 286
IP defragmentation 307, 336
Max Buffer Size 268
overwriting 286
physical ports 286
RAM limitations 268
size 268
TCP stream 307, 336
capture card
driver requirements 7, 228
capture card driver 7, 228
Capture Decode 87
capture decodes 243
Capture Graph 57
Capture Internet Observer 19
Capture Pairs (Matrix) 21
Capture Protocols 22
Capture Summary 28
Capture Top Talkers 25
Capture VLAN 35
captures
see packet captures 60
see packet captures 60
capturing 59
capturing packets 289
CAPWAP Control 44
CAPWAP Data 44
CDU 243
changing 237
changing NIC 237, 237, 237, 237, 237, 237
CIFS 152
CIR 115
circular 58, 58
Cisci 6xxx switches
troubleshooting 280
Cisco 6xxx switches 280
Cisco EAP/LEAP 256
clock synchronization 242
CME RLC 44
collecting data 242
Collecting Information in Charts, Lists, Forms, Tables and Traps 207
collection interval 265
collection intervals 149
collision test 279, 279
color codes 99
command line 73, 73
command line, enabling 73, 73
Committed Information Rate 115
Committed Information Rate (CIR) 249
common issues 274
common problems with 275, 276
Configure IP Application List for Internet Observer Statistics Dialog 19
Configure IP Application Ports Dialog 20
Configure IP Applications for Network Trending Reports Dialog 146
Configure IP Applications for Web Based Network Trending Reports Dialog 146
Expert Information 57
network trending folder 239
partial packets 59, 59, 59
probe name 239
configuring statistics memory 241
connecting 238
connecting to analyzer 238, 238, 238, 239, 242
Connection Dynamics 77
about 98
color codes 99
packet types 99
using 98
connections 19, 19, 19, 19, 21, 21, 21, 25
CPU 303
CRC-16 244
CRC-32 244
Create Network Trending Report 146
creating 59, 71, 129, 129, 131, 131, 132, 132
CSU 243
encapsulation 244, 244
Customizing SNMP Charts 202

D
D3 243
D3/E3/HSSI 243
DAAP 100
dashboard 10, 10
see Observer 10
see Observer 10
data analysis time slice 239, 239
data reconstruction 249
data transfer 255, 255, 255, 255
data, collecting 156, 156, 156, 163
data, deleting 157
data, viewing 157
daylight savings time 280
Daylight Savings Time 280, 280
decode API 217
decode DLLs, custom 84
decodes
keyboard shortcuts 89
decoding 77, 77, 80, 85, 91, 92, 92, 105, 167, 167, 167, 222, 222, 222, 226, 226, 226, 289, 307
expert analysis 77, 94, 98
configuring 93, 96, 96
summary view 97
using 101
expert thresholds
configuring 105, 105
geolocation 17
NetFlow 82, 92
packet captures 77, 77, 77, 77, 80, 91
encrypted 79, 79, 80, 80, 333, 333
reconstruction 100
sFlow 82, 92
user interface 85, 85, 87, 87
using third party decoder 17, 17
VoIP 167, 167
defining its purpose 273
definition 219
definitions, restoring 48, 335
deleting
 network trending data 157
denial of service 307, 336
derived application definitions 46
derived applications 13
Designing and Building Forms 205
Device Configuration 83
devices 40, 173
discovering 40, 40, 40, 41
DHCP 130, 130, 152
DHCPv6 152
Diameter 152
difference from packets 291
difference from statistics 291
disabling 113
Discover Network Names 279, 279, 279
VLANs 279
Discover Network Names (Address Book) 39
Discover Network Names Mode 39
Discover Network Names tool 36, 36
Discover SNMP Devices 40
discovering 39, 39, 39, 40, 40, 40, 41, 41, 201
discovery method 36, 36
Display Protocols for Selected Station 22
Display Stations sending Selected IP 77
DLCI Address Filter 66
DLCI CIR Setup 66
DLCIs 84
DLLs, custom decode 84
DMP 63, 77
DNS 37, 38, 38, 38, 38, 64, 152
DNS names
resolving 38
DNS resolution 239
driver error support 28
driver requirements 7, 7, 7, 228, 228, 228
drivers, wireless 229
DS3
fractionalized 244
DSU
encapsulation 244, 244
duplicate, removing 59, 78, 78, 97
dynamic 47

E
E1 243
WAN relay type 244
E3 243
fractionalized 244
EAP/LEAP 256
Edit Enumerated Value Dialog 182
Edit IP Application Port Dialog 19
Edit Pager Entry Dialog 77
Edit Probe Instance 269
Edit Probe User Account Dialog 77
Edit Statistics Memory Configuration 77
editing 38, 47
effects of packet capture 271
efficiency 142
elements, adding 130, 130, 131, 131, 132, 132, 132, 132, 133, 133
elements, filtering 134, 134
e-mail, via 125
E-Model 171
enabling 115, 115, 116, 116
ENC 63
encapsulation 243, 244, 244, 244, 244, 244, 244, 244, 244, 249, 249
encrypted 79, 79, 80, 80, 333, 333
encrypted traffic 80
encrypting data 249

3DES 136
AES 143, 251
see also security 143, 251
SNMP versions 158
encryption key 231, 239, 253, 253, 256, 276
encryption keys 231
End to End Server Analysis - MultiHop Analysis 102
End to End Server Analysis - Server Analysis 102
End to End Server Analysis Settings - Display - End to EndAnalysis 102
End to End Server Analysis Settings - Display - Response Time 102
End to End Server Analysis Settings - Display - Server Load 102
End to End Server Analysis Settings - Display - Utilization 102
End to End Server Analysis Settings - Files 102
End to End Server Analysis Settings - General 102
End to End Server Analysis Settings - Synchronization 102
End-to-End Analysis using 102
Expert Reconstruct Streams 77
Expert Server Analysis 77
expert summary 222, 226
Expert Summary 77
Expert TCP Dump 77
Expert TCP Events 77
expert thresholds
configuring 105, 105, 105, 105
Expert Thresholds (OSI Model) 105
Expert Time Interval Analysis 77
Expert UDP Events 77
Expert VoIP 77
Expert VoIP Analysis 77
Expert VoIP Events 77
Expert VoIP Settings - General 77
Expert VoIP Settings - MOS 77
Expert VoIP Settings - VoIP Summary Graph 170
Expert What-if Analysis 77
Expert Wireless Events 77
exporting 39, 39, 49, 49, 120, 120, 167, 330, 330, 331, 331, 335
alarms 120, 120, 120, 120, 120, 330, 330, 330, 330, 330, 330
protocol definitions 39
server applications 46, 49, 49, 331, 331
VoIP 167, 335
expressions 206

F

FDC 63
FDDI 63, 63, 63, 63, 77
FDDI Errors by Station 28
FDDI Vital Signs 28
feature suitability 59
Federal Information Processing Standards 135
Fibre Channel Vital Signs 28
FIFO 286, 303
FIFO gauge 303
files included 217
filter
Ethernet Physical Port 304
Filter Names 66
filter ports 286
filter-based, creating 117, 117
filtering 66
post-filters
applying 72, 72, 92
command line 73
command line, enabling 73
pre-filters
“exclude” rules 66
creating 66, 66, 71
exporting 66
importing 66
scope 71
pre-filters, scope 71
VoIP 167
filtering telephone numbers 167
filtering, physical 304
filters 249, 249, 265, 265, 304, 304, 305
activate and deactivate 71, 71
command line 73
command line, enabling 73
see also filtering 66
partial packets 59
Filters 66, 66
Find Packet 91
finding a specific time 303
FIPS 135, 135
firewall 12, 281
firewall, ports 276
FIX 87, 151, 152, 323
FIX protocol 323
forensic analysis 306, 307, 312, 313, 336
format
  XML 63
formats 63
  BFR 63
  CAP 63
  DMP 63, 77
  ENC 63
  FDC 63
  PCAP 63
  TRC 63
fractionalized 243, 244, 244, 244, 244
frame check sequence 243
frame checksum 243
frame relay 243
frame size 243
Frame too large 243
from multiple sources 60
from unknown sources 78, 78
FTP 47, 47, 47, 100, 105, 152
full-duplex 222, 226, 265, 265
full-duplex Ethernet 222, 226
G
  Gen2 26, 52
  Gen2 card
    filter ports 286
    full-duplex 265
    GPS 242
    passive probe instance 220
    performance 220
    ports 286
    probe instance warning 220
    recommendations 273
    statistics 286
    time synchronization 242
General tab 243
GeoIP Settings 17
geolocation 17, 17
getting started 282
Gigabit 222, 243
  jumbo frames 243
Gigabit tab 243
gigabytes 268, 268
GigaStor 138, 237, 255, 273
  AES 138, 239
  collision test 279
  data analysis time slice 239
  encryption 138, 239
Expert Probe 255
getting started 282
indexing 292
loss of data 298, 299
RAID array 297, 298
RAM 273
  recommendations 273
  reserved memory 273
traffic generation 279
virtual machine with 257
write performance 299
GigaStor capture 220, 222, 226
GigaStor Control Panel
  analyzing data 168, 168, 304, 304, 319, 319
  archiving data 293
  buffer size 294
  capturing packets 289
  configuring 286, 294
  filters 304, 304, 305
  finding a specific time 303
  FIX 323
  forensic analysis 306, 307, 312, 313, 336
  getting started 282
  mining data 300, 303
  NetFlow 295
  NetFlow Agent 295
  NetFlow collector 295
  Observer settings 285
  packet capture 290, 290, 290, 294
  ports 294
  privacy 290
  RAID maintenance 299
  reports 288
  scheduled capture 290
  security breach 312
  Snort 307, 336
  Snort rules 306, 307, 341
  stream reconstruction 318, 319
  subnets 294
  trimming data 290
  troubleshooting 305
  using 284
GigaStor Control PanelRAID, failing
  RAID, failing 325
  troubleshooting 325
GPS 242, 242
Graph Display Properties 77
Graph Display Properties - Graph Time 77
Graph Setup 131
H
  H.245 152
  H.248 152, 152
  H.323 77, 152
  hardware 269
  hardware acceleration 273
  hardware requirements 4, 225
  high latency 116
  high-volume 306
  HSSI 243, 244
  HSSI, fractionalized 243
HTTP 100, 152
I
  ICA 152
ICMP Expert 77
IIS Web Server, Windows 79, 333
IMAP 152
IMAP4 100
importing 38, 38, 39, 39, 45, 45, 49, 49, 49, 120, 120, 167, 330, 330, 331, 331, 331, 335

address book 38
alarms 120, 120, 120, 120, 330, 330, 330, 330, 330, 330
protocol definitions 39
server applications 49, 331
VoIP 167, 335
in a switched environment 224
included, files 217
indexing 292, 292
individual stations 21, 21, 21, 25
install MIBs 188
installation 6, 217, 232
Interface Properties 77
interface switching 222, 226
Internet Observer 19
Internet Observer Internet Patrol 19
Internet Observer IP Subprotocols View 19
Internet Observer Settings 19
Internet Observer tool 19, 19, 19
Internet Patrol 19
Internet Patrol - Pair Circle 19
IP address
   GigaStor 237
   IPv6 307, 336
   NAT 279
   statistics 297
   IP Calculator 39
   IP defragmentation 307, 336
   IP Discovery 39
   IP flow 307, 336
   IP Fragment Bits Filter 66
   IP Fragment Offset Filter 66
   IP mapping 110, 110, 110, 110
   IP masquerading, see NAT 279
   IP Pairs - Pair Circle 77
   IP precedence 243, 243
   IP Properties 77
   IP range 174
   IP Subnet Mask Calculator 39
   IP Subprotocols 77
   IPTV 158, 300
   IPv4 236, 236
   IPv4 Options Filter 66
   IPv4 TOS Precedence 59
   IPv6 16, 236, 236, 307, 307, 336, 336
   IPv6 Address representation 77
   IPv6 Flow Label 59
   IPv6 Options Filter 66
   IPv6 Traffic Class 59

J
   Jitter 77
   jumbo frames 243, 243, 243

K
   keyboard shortcuts 89

L
   LAPB 243
   laptop
      NICs 256
   using as probe 256
   wireless 256
Layer 3 Switch 279
LDAP 71, 71, 152
license 233
licenses
   redeeming 6, 232
   troubleshooting 6, 232
limitation 163
limitations 132, 132, 133, 151, 155, 155
limitations of 255
line frame 243
List Bar Display Properties 77
List Display Properties 77
load 23
   preprocess settings 307, 336
load, preprocessor 220
load, testing 26, 26, 26, 26, 26, 102
loading 63
local probe 9
Locator, Switch Station 39, 41
Log Window Settings - Event Filter 113
Log Window Settings - Log Files 112
logging 112
   disabling 113
loss of data 298, 299

M
   MAC address
      statistics 297
   MAC addresses 279
   Mac Header 236, 236
   MAC Properties 77
   macro graph, see Outline Chart 303
   Management Console 187, 187, 188, 188, 190, 210, 210
   Management Station 189
   man-in-the-middle 253
   man-in-the-middle, preventing 253
   matching between probe and analyzer 276
   Max Buffer Size 268
   Mean Opinion Score (VoIP Expert) 77
   megabytes 220
   MEGACO 152
   memory 269, 269
   memory allocation 241
   memory management 268
   memory tuning 268
   memory, see RAM 271
   Merge Two Packet Capture Buffers Dialog 63
   merging 63, 63, 63
   MIB 185
      see SNMP 185, 198
      see SNMP 185, 198
   MIB Compiler 182
   MIB Editor 182
      adding MIBS 207
      expressions 206
      install MIBs 188
      requests 195
      SNMP agents 195
      viewing MIBs 209
   MIB Editor, using 191, 195, 196, 198, 198, 199, 199, 199, 200, 202, 202, 203, 204, 204, 205, 207
   MIB Walker 182
   MIB Walker, using 208, 210
MIBs 182
micro graph, see Detail Chart 303
microburst analysis 303
microbursts, about 313, 313
microbursts, searching for 313
Microsoft 231
Microsoft Lync Server 79, 333
Microsoft Network Discovery 39
mining data 300, 303
mirror port 224
mirror port, see also SPAN ports 224
missing 62, 237, 276
missing from Observer 237
mobile devices, via 125, 125
Modify Observer Reserved Memory dialog 77
MOS 171
MOS Settings 77
moving through RAM 271
MPLS 222, 226, 235, 236, 243, 243
ATM 236
IPv4 236
IPv6 236
Mac Header 236
pseudowire word 236
MPLS Filter 66
Msft (Microsoft) Configuration 39
MSRPC 152
Multi Probe 222, 226, 226
changing NIC 237, 237
configuring 243, 243
connecting to analyzer 238
data transfer 255
limitations of 255
redirection 238
multicast 233
Multicast Pitch 44
MultiHop Analysis 105
configuring 108, 108
IP mapping 110, 110, 110, 110
synchronization method 108, 108
user offset 108, 110
using, quickly 108
Multiple Address Tables 39
Multiple Filters 66
multiple in a system 242

N
name, changing 239
naming 236
NAT 279, 279, 279
NetFlow 82, 82, 92, 222, 226, 243, 265, 279, 295
decoding 92
TAPs and 279
versions supported 265
NetFlow Agent 295
NetFlow collector 265, 295
NetFlow Device Configuration 83
NetFlow Trending collector 265
NetLive
about 163
limitation 163
trending on 163
network 26, 26, 28, 28, 28, 29, 29, 33
ers, 29
load 23
load, testing 26, 26, 26, 26, 26, 102
summary 28, 28
troubleshooting 28, 28, 28, 28
utilization 23, 24, 24, 24, 24, 27, 27, 27, 27
Network 1 probe instance 236
Network Activity Display Properties 33
network adapter
configuring 24
Gen2 26, 52
network adapter, see also NIC 237
network delay, calculation 97
Network Device Properties - Data Logging Tab 184
Network Device Properties - Description Tab 182
Network Device Properties - Notification Tab 184
Network Errors Settings 29
Network Instruments Management Server 239
Network Intrusion Detection 306, 306
network load 23, 26, 26, 26, 26
viewing 303
network masquerading, see NAT 279
Network Summary 28
Network Summary tool 28
network trending 170, 171, 222, 226, 256, 275
about 146, 151, 156
Application Performance Analysis
about 149
collection intervals 149
configuring 147
response time calculation 149
Application Transaction Analysis 152
applications, analyzing 151, 163
configuring 154, 158, 158, 163, 163
data, collecting 156, 156, 156, 163
data, deleting 157
data, viewing 151, 157
devices 173
enabling 166
filters 265
IP range 174
limitations 151, 155, 155
MOS 171
sampling divider 156, 265
scheduling 163
securing 249
server profiles 155, 336
settings 170, 171
VoIP 166, 170, 171, 171, 171, 173, 174
Network Trending 146, 233
Network Trending Application Analysis Settings 146
Network Trending Application Performance Analysis Settings
146
Network Trending Data Transfer Settings 146
network trending folder 239
Network Trending Internet Observer Settings 146
Network Trending Schedule 163
Network Trending Settings - General 146, 149
Network Trending Settings - MOS 77
Network Trending Settings - Protocols 146
Network Trending Settings - Subnet Ranges 146
Network Trending Time Settings 146
Network Trending URL Tracking Settings 146
Network Trending Viewer 157
Network Vital Signs tool 28
New MIB Object Dialog 207
New Trap Dialog 182
NFS 152
NIC 222, 226, 229
  broadcast traffic 237
  changing 237
  missing 237, 276
  missing from Observer 237
  multiple in a system 242
NICS 256
NIDS 306
NIMS 13, 13, 13, 13, 13, 13, 141, 222, 226, 229, 249, 250, 253
  SafeNet HSM 80
  synchronizing protocol definitions 39
NIProbe.exe 6, 232
NNTP 100
no network card 237
not connecting 276
notifications 125, 125, 125, 125, 126, 126, 126, 127, 127
Notify Probe User 59
Numeric Value Filter 66
O
Observer 137
  alias files 336
  dashboard 10, 10
  encryption 13, 137
  feature suitability 59
  no network card 237
  notifications 125, 125, 125, 126, 126, 126, 127, 127
  password protecting 140
  ports used 12, 281
  regulation compliance 135
  security 137
  supported protocols 342
  switching to probe 222, 226
  system requirements 4, 225
  user interface 9, 11
  web server 122
Observer General Options - folders 77
Observer General Options - IPv6 77
Observer General Options - Security 77
Observer General Options Tab 77
Observer settings 285
Observer Suite Custom Decode Kit
decode API 217
  installation 217
  using 216
  warranty 217
observer.exe 6, 232
OID
  see SNMP 189
  see SNMP 189
on Windows servers 183
OpenView 116
  options 239
OR filter example 71
OSI Layer 7 255
other codecs 100
overwriting 286
P
  packet 307, 336
    analyzing 306
    decoding 307
    sampling 286
  packet alert threshold 307, 336
  packet captures
    from unknown sources 78
  packet capture 243, 243, 271, 290, 290, 290, 294
    active instance vs. passive instance 220
    buffer 268
    daylight savings time 280
    decoding 222, 226, 289
    high-volume 306
    memory 269
    partial 303
    RAM 271
    reassembling 307, 336
    securing 249, 249
  Packet Capture on Multiple Instances Settings 60
  Packet Capture Options 57
  Packet Capture Schedule 60
  packet captures 57, 60, 60, 60, 77, 77, 77, 77, 80, 91, 141, 142
    configuring 51, 51, 57, 57, 58, 59, 60
      Expert Information 57
      partial packets 59, 59, 59
    creating 59
    decoding 77, 77, 80, 85, 91, 105
    efficiency 142
    encrypted 79, 79, 80, 80, 333, 333
    filtering 66
    from multiple sources 60
    from unknown sources 78
    loading 63
    merging 63, 63, 63
    replaying 84
    saving 63, 63, 90
    scheduling 60, 60
    security 142
    sharing 141
    synchronizing 108, 108, 110, 110
    timestamps 57
    transferring 61
    wireless 4, 225, 256
  packet filters 306
  packet fragmentation 307, 336
  packet headers, limiting captures to 286
  Packet Length Filter 66
  packet storms 33
  Packet Time Filter 66
  packet types 99
  Packet View Settings - Column Order 77
  Packet View Settings - Configure SNMP MIBs 77
  Packet View Settings - General 77
  Packet View Settings - Protocol Forcing 77
  Packet View Settings - Summary 77
  packets 25, 59
    capturing 59
    difference from statistics 291
    duplicate, removing 59, 78, 78, 97
    Expert Information 57
    Expert Information, excluding 57
    missing 62
    moving through RAM 271
    RAM 271
    saving 90
    searching for 91
    sizes 25
    skipped 100
  Paging Server Properties Dialog 126
paging service 126, 126
Pair Statistics (Matrix) 77
Pair Statistics Settings 77
Pair Statistics Settings - List 77
Pair Statistics Settings - Pair Circle 77
Pair Statistics Settings - Statistics Settings 77
Pair Statistics tool 21
partial 303
partial packet capture 249, 249
Partial Packet Capture for TCP/UDP Payload Filter 141
partial packets 59, 59, 59, 59
partial packets, saving 286
passive probe instance 220
password protecting 140
Pattern Filter 66, 67
PCAP 17, 63, 63, 63
PerfMon SNMP support 183
performance 220
permissions 249
Phone Pager Schedule 77
physical port indexing, see virtual adapters 282
physical ports 286
Ping Trace Route 43
Ping/Trace Route 43, 43
POP3 100, 152
port bonding 222, 226, 265
Port Filter 66
ports 44, 44, 47, 47, 47, 47, 286, 294
dynamic 47
filtering, physical 304
ports used 12, 281
Post Capture Filtering 72
post-filters
applying 72, 72, 92
command line 73
command line, enabling 73
prefilters
creating 66, 71
scope 71, 71
preprocess settings 307, 336
privacy 290
Probe administration, port required 12, 281
Probe Alarms Settings - Actions 118
Probe Alarms Settings - Alarm List 116
Probe Alarms Settings - Triggers 118
probe configuration 249
probe connection 276
probe instance 303
active 220, 268
active vs.passive 220
best practices 220
configuring 243
configuring statistics memory 241
collecting 238
classifying to analyzer 242
defining its purpose 273
definition of 220
memory allocation 241
memory tuning 268
naming 236
passive 220
redirecting 237
reserving memory 268
security 249
specifying NIC 242
probe instance warning 220
probe instances 249
redirecting 64, 64
user accounts 140
probe name 239
probe redirection 238
Probe redirection error 276
Probe Service Configuration Applet 256
probe, local 9
probes 59, 64, 136, 138
Adapter Speed tab 243
as Windows service 231
Autoupgrade tab 243
autoupgrading 239, 243
backing up 233
clock synchronization 242
collecting data 242
common problems with 275, 276
counting 239
connecting to analyzer 238, 239
D3/E3/HSSI 243
definition 219
encryption keys 231
Expert 138
General tab 243
Gigabit tab 243
hardware 269
hardware acceleration 273
in a switched environment 224
IP precedence 243
MPLS 236, 243
name, changing 239
not connecting 276
options 239
port bonding 265
see probe instances 64
protecting 231
running as Windows service 239
securing 136, 138, 249
security 64, 249
software, versions 222
SPAN ports 222
statistics sampling divider 243
switching to analyzer 222, 226
T1/E1 tab 243
updating 231
upgrading 231, 231
Virtual Adapters tab 243
virtual TAPs 257
VLAN access 276
WAN 243
wireless 243
Wireless 802.11 tab 243
see probe instances 64
promiscuous mode 4, 224, 225, 256, 257
protected memory 267, 269, 269, 269, 270, 271
protecting 231
protocol 152
Protocol Filters 66
protocol definitions 39, 39
exporting 39
importing 39
Protocol Definitions and Server Application Discovery 77
Protocol Distribution 22
Protocol Distribution Settings 22
Protocol Distribution Statistics 22
Q
QoS 243
Quality of Service (QoS) 77

R
RADIUS 152
RAID 220, 220
RAID array 297, 298
RAID maintenance 299
RAM 271, 271, 271, 273
  allocating 273
  buffer size 220
  effects of packet capture 271
  formula 268
  GigaStor 273
  limitations 268
  packet capture 220, 268
  probe instance 303
  see also buffer 268
  see also protected memory, user memory, and reserved
  memory 267
  recommendations 270
  reserving for Observer 242
  resizing 267
  statistics 268
  TCP stream reassembly 307, 336
  tuning 268
  used in Observer 267
  Windows 268
RAM limitations 268
RAM needed for busy networks 273
Random Access Memory, see also RAM 267
Real-time Transport Control Protocol 77
Real-time Transport Protocol 77
reassembling 307, 336
recommendations 270
Reconstruct Stream 249
reconstructing data 249
reconstruction 100
  see stream reconstruction 100
see stream reconstruction 100
reconstruction, stream 77, 100, 100
redirecting 64, 64, 237
redirecting, see probes 239
redirection 238, 238, 238, 238
registry 233
regulation compliance 135, 135
  see security 135
see security 135
Remote Probe Expert Analysis and Decode 77
Replay Packet Buffer 77
replaying 84
Report Filters 134
Report Setup - Layout 130
reports 124, 124, 124, 124, 124, 288
address, choosing 130
administering 122, 124
creating 122, 129, 129, 129, 130, 130, 131, 132, 132, 132, 133
elements, adding 130, 130, 131, 131, 132, 132, 132, 132, 132, 133
elements, filtering 134, 134
email, via 125
limitations 132, 132, 133
mobile devices, via 125, 125
scheduling 124
security 124, 124
settings 122
SNMP 122
viewing 122
web server, configuring 122, 122
requests 195
requirements, hardware/software 4, 225
Reserve Observer Memory 77
reserved memory 222, 226, 269, 269, 270, 270, 271, 271
  see also RAM 267
reserved memory from 222, 226
reserved memory in Observer 242
reserving for Observer 242
reserving memory 268
resetting 118, 118, 118
resizing 267
Resolve IP 39
resolving 38
resolving DNS names 38
response time calculation 149, 152
restoring 48, 48, 48, 48, 49, 49, 335, 335, 335, 335, 335, 335, 335
retransmissions, excessive 116
RFC1213
  see SNMP 40, 40
see SNMP 40, 40
RMON 224
RMON Extension Configuration 59
RMON Tables 77
Router Observer 23
Router Observer Settings 23
Router Observer tool 23
routers 23, 23, 23, 23
  statistics 23
RTCP 77
RTF Report Options 77
RTP 77
RTP RTCP Graph 77, 170
RTSP 100
rules profiles 307, 336
running as Windows service 239
running Observer or Probe 256

S
SafeNet HSM 80, 80
sampling 286
Sampling 303
sampling divider 265, 265, 275
  see network trending 156
Save Packet Capture 90
saving 36, 38, 38, 63, 63, 90, 90
saving packet captures 63
saving, formats 63
SCCP 152
scheduled capture 290
scheduling 60, 60, 124, 163
  packet captures 60, 60, 60
reports 124, 124
scope 71, 71
scripts 233
searching for 91
securing 136, 138, 249, 249, 249, 249
security 64, 124, 124, 137, 139, 140, 140, 140, 142, 222, 226, 249, 249, 249
Anyone account 249
authentication 250
encrypting data 249
equipment 136, 143, 251
equipment key 253, 276
filters 249
man-in-the-middle 253
matching between probe and analyzer 276
NIMS 250
Observer 137
packet captures 141, 142
partial packet capture 249
permissions 249
personal information 6, 232
probe configuration 249
probe instances 249
Probe redirection error 276
probes 59, 64, 136, 138
reconstructing data 249
regulation compliance 135
reports 124, 124, 124
user accounts 139, 140, 140, 140
users 249
VoIP 249
security breach 312
see also encryption 249
Select WEP Profile 90
Server Analysis
using 77, 77, 101, 101
Server Application Discovery 39, 39, 44
adding derived definitions 46, 46
definitions, restoring 48, 335
server applications 49, 49, 331, 331
adding 44, 46, 46
discovering 39, 39, 39
editing 47
exporting 39, 46, 49, 49, 49, 331, 331, 331
importing 39, 45, 45, 49, 49, 331, 331, 331
ports 44, 44, 47, 47, 47, 47, 47
restoring 48, 48, 48, 49, 49, 335, 335, 335, 335, 335
see also applications 44
server profiles 155, 336
Server Response Time Settings - General 149
Server Response Time Settings - Protocols 149
Server, Apache Web 79, 333
Server, Windows IIS Web 79, 333
service 239
services 256, 256
Set Local Probe Name 77
settings 171, 224
settings profiles 307, 336
sFlow 82, 82, 92, 222, 226, 243
decoding 92
Device Configuration 83
sFlow collector 267
sFlow, versions supported 265
sharing 141
Shoutcast 44, 100
signal strength 30
signal strength conversion 30
simultaneous 222, 226
Single Probe 222, 222, 222
Anyone account 249, 276
changing NIC 237, 237
configuring 243, 243
data transfer 255
redirection 238
security 249
VoIP 255
SIP 152, 173, 173
site survey 29
Size Distribution Settings 25
Size Distribution Statistics 25
Size Distribution Statistics tool 25
sizes 25
skipped 100
skipped packets 100
slow 235
slow probe system 275
SMB 152
SMTP 100, 125, 125, 152
Sniffer 63
SNMP 122, 224, 233
about 182, 210, 210
agents 188, 188, 192, 194
devices 40
discovering 40, 40, 40, 41
discovering 201
Management Console 187, 187, 188, 188, 190, 210, 210
Management Station 189
MIB 185
MIB Editor
adding MIBs 207
expressions 206
install MIBs 188
requests 195
SNMP agents 195
viewing MIBs 209
MIB Editor, using 191, 195, 196, 198, 198, 199, 199, 199, 199, 200, 202, 202, 203, 204, 204, 205, 207
MIB Walker, using 208, 210
on Windows servers 183
reports 122
traps 197, 207, 208, 208
SNMP Agent Information Windows 194
SNMP agents 195
SNMP General Options Tab 77
SNMP traps 116
SNMP Trending Data Manager 182, 182
SNMP versions 158
SNMP Walker 208
IP flow 307, 336
IPv6 307, 336
variable name 307, 336
SNORT 233
software probes 222, 231
software requirements 4, 225
software, versions 222
SPAN
VLANS 277
SPAN port 277
see also mirror port 224
SPAN ports 222
broadcast traffic 237
settings 224
software probes 222
see also mirror port 224
virtual machine 257
specifying NIC 242
SSL 80, 80, 80, 80, 80, 80, 85, 85
SSL, decrypting 80
SSL/TLS Decryption Parameters 77
Stations - Pair Circle 77
statistics 22, 22, 22, 23, 24, 24, 29, 243, 256, 268, 286, 297, 297
collection interval 265
connections 19, 19, 19, 19, 21, 21, 21, 25
difference from packets 291
errors 28, 29, 29
individual stations 21, 21, 21, 25
memory 269
network load 23
packet capture 243
packets 25
protocols 20, 22, 22, 22
RAM needed for busy networks 273
routers 23, 23, 23
sampling divider 265, 275
top talkers 25, 25, 25, 25
utilization 24, 24, 27, 28
VLAN 35, 35, 35
wireless 22, 22, 29, 29
statistics buffer 268, 268
Statistics Memory Allotment Page 77
statistics queue buffer 267, 269, 270, 271, 271, 273, 273
statistics sampling divider 243
stream reconstruction 77, 100, 100, 318, 319
other codecs 100
Stream Reconstruction 77
Subnet mask 59
Subnet Mask Calculator 43, 43
subnets 294
summary 28, 28
summary view 97
supported protocols 342, 342
Switch Station Locator 41
Switch Station Locator tool 39, 41, 41, 41
switches
discovering 41
switching to analyzer 222, 226
switching to probe 222, 226
synchronization 110, 242, 280
synchronization method 108, 108
synchronizing 108, 108, 110, 110
synchronizing protocol definitions 39
system load 286
system requirements 4, 225

T

T1 243
WAN relay type 244
T1/E1 tab 243
Table Column Setup 130
TAP
NetFlow 279
TAPs and 279
TCP 25901 12, 281
TCP 25903 12, 281
TCP Dump 249
TCP Expert 77
TCP stream 307, 336
TCP stream reassembly 307, 336
TCP/IP 279
TDS 152
Telnet 100, 152
termination 179
testing
network load 26, 26, 26, 26, 26
third party decoder 17
third-party capture card
driver requirements 7, 228
Time Interval Analysis
using 77, 101, 101
time synchronization 280
time synchronization 242, 242
timestamps 57
packet captures 57
Tivoli 116
TNS 152
Token Ring Errors by Station 29
Token Ring Vital Signs 28
Toolbar Setup 11
top talkers 25, 25, 25, 25
Top Talkers 33, 268
Top Talkers Statistics 25
Top Talkers tool 25, 25
top talkers, defined 25
topologies 219, 222, 226
802.11 219
Ethernet 219
ToS 243
traffic generation 279, 279
Traffic Generator 26
Traffic Generator Settings 26
Traffic Generator tool 26
transferring 61
transferring packet captures 61
see SNMP 208
traps 197, 207, 208, 208
see SNMP 208
TRC 63
trending
see network trending 151
trending on 163
triggers 222, 226, 275
trimming data 290
Triple DES 249, 253
see also encryption 249
troubleshooting 28, 28, 28, 28, 277, 280, 305, 325
analyzer connection 276
bad TCP checksums 277
broadcast and multicast storms 33
Cisco 6xxx switches 280
common issues 274
network 26, 26, 28, 28, 28, 29, 29, 33
packet storms 33
probe connection 276
slow probe system 275
VLAN Statistics tool 277, 277
VLAN visibility 279
TTL Hop Limit 59
udp 25903 12, 281
udp expert 77
update chart button 286
upgrading 231
observer 6, 232
upgrading, encryption keys 231
user accounts 139, 140, 140, 140, 140
security 139, 140, 140
user accounts/access permissions tab 122
user interface 9, 11, 85, 85, 87
see observer 9
user memory 267
user offset 108, 110
see user accounts 140
user permissions
see user accounts 140
users 222, 226, 249, 276
administrator 249
anyone 249
simultaneous 222, 226
using 39, 41, 77, 77, 101, 101, 101, 101, 101, 102, 102, 102, 102, 102, 102, 102, 102, 130, 216, 284
agent information windows 194
using as probe 256
using third party decoder 17, 17
using 41
using, quickly 108
utilization 23, 24, 24, 24, 24, 24, 24, 23, 27, 27, 27, 27, 27, 28
utilization history 27
utilization history tool 27
utilization thermometer mode 27
utilization thermometer tool 27
variable name 307, 336
versions supported 265
viewing 303
viewing mibs 209
virtual adapter 220, 243, 257, 265
virtual adapters 282
virtual adapters tab 243
virtual machine 4, 225, 257, 257, 257
virtual machine with 257
virtual nic 257
virtual tap 257
virtual tap 77
virtual tap settings dialog 77
virtual taps 257
virus protection 231
vlan 35, 35, 35, 277, 277
"no vlan" 277, 277
vlan access 276
vlan filter 66
vlan isl filter 66
vlan properties 35
vlan statistics 35, 277
vlan statistics tool 35, 277, 277
vlan visibility 279
vlans 277, 277, 279
discover network names 279
span port 277
vmoni 276
vmoni protocol analyzer 276
voip 77, 167, 167, 167, 167, 171, 171, 171, 173, 174, 175, 175, 175, 222, 226, 243, 249, 249, 249, 255, 255, 335, 335
alarms 175, 175
caller id 174
decoding 167, 167
exporting 167, 335
filtering telephone numbers 167
importing 167, 335
network trending 166, 170, 171
devices 173
ip range 174
mos 171
settings 171
terminology 179
voip rtp rtcp graph 77
voip settings - caller id 174
voip settings - device ip address 173
voip settings - general 171
voip settings - ip range filters 174
voip settings - mos score 171
vpn 279
wan 63, 63, 63, 108, 243, 243, 243
capsulation 249
fractionalized 243
security 249
wan alarms 115
wan conditions filter 66
wan load 33
wan port filter 66
wan relay type 244, 244
wan switch 39
wan type 244, 244
wan vital plot properties 28
wan vital signs 33
wan vital signs by dcli 28
warranty 217
web extension - configuring 122
web observer 21
web observer settings 21
web observer tool 21
web reporting custom reports 129
web reporting custom reports - add report 129
web reporting custom reports - add report element 122
web reporting custom reports - address filter setup 122
web reporting custom reports - address filters 122
web reporting custom reports - configure custom report 122
web reporting schedule 124
web reporting schedule - delivery 124
web reporting schedule - recipients 124
web reporting schedule - report 124
web reporting schedule - times 124
web reporting server options 122
web reporting user accounts 124
web reporting user accounts - edit user 124
web server 122
configuring 122
web server, apache 79, 333
web server, configuring 122, 122
web server, windows iis 79, 333
webSphere 152
What-if modeling
using 102, 102
Windows 229
  32-bit 233, 270
  64-bit 233, 257, 268, 270
registry 233
reserved memory from 222, 226
reserved memory in Observer 242
service 239
services 256, 256
Windows IIS Web Server 79, 333
Windows memory pool 269, 269
Windows protected memory 267
Windows updates 231
Windows, SNMP Agent Information 194
wireless 4, 22, 22, 22, 24, 29, 29, 29, 219, 222, 222, 226,
  226, 243, 243, 256, 256
  access point statistics 22, 22, 24, 24
  signal strength conversion 30
  site survey 29
Wireless 802.11 tab 243
wireless access point 256
Wireless Access Point Filter 66
Wireless Access Point Load Monitor 22
Wireless Access Point Settings 22
Wireless Access Point Settings - List 22
Wireless Access Point Statistics 22
Wireless Access Point Statistics tool 22
Wireless Channel Filter 66
Wireless Data Rate Filter 66
wireless driver 229
wireless interference 29
Wireless Network Errors by Station 29
wireless network, encryption key 256
wireless packets, raw 4, 225, 256
Wireless QoS 59
Wireless Signal Strength Filter 66
Wireless Site Survey 29
Wireless Site Survey - Channel Scan 29
Wireless Site Survey - Ctrl. Frames 29
Wireless Site Survey - Data Frames 29
Wireless Site Survey - Frame Types 29
Wireless Site Survey - General Info 29
Wireless Site Survey - Mgmt. Frames 29
Wireless Site Survey - Signal 29
Wireless Site Survey - Speeds 29
Wireless Site Survey tool 29
Wireless Vital Signs 28
Wireshark 17, 63
WMPNSS 100
Word Report Options 77
write performance 299

X
XML 63, 63

Symbols
"No VLAN" 277, 277