Notice

Every effort was made to ensure that the information in this manual was accurate at the time of printing. However, information is subject to change without notice, and VIAVI reserves the right to provide an addendum to this manual with information not available at the time that this manual was created.

Copyright

© Copyright 2019 VIAVI Solutions Inc. All rights reserved. VIAVI and the VIAVI logo are trademarks of VIAVI Solutions Inc. (“VIAVI”). All other trademarks and registered trademarks are the property of their respective owners. No part of this guide may be reproduced or transmitted, electronically or otherwise, without written permission of the publisher.

Copyright release

Reproduction and distribution of this guide is authorized for Government purposes only.

Terms and conditions

Specifications, terms, and conditions are subject to change without notice. The provision of hardware, services, and/or software are subject to VIAVI standard terms and conditions, available at www.viavisolutions.com/terms.

Specifications, terms, and conditions are subject to change without notice. All trademarks and registered trademarks are the property of their respective companies.

Federal Communications Commission (FCC) Notice

This product was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this product in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

The authority to operate this product is conditioned by the requirements that no modifications be made to the equipment unless the changes or modifications are expressly approved by VIAVI.

Laser compliance

This device is a class 1 laser product.

Industry Canada Requirements

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

WEEE and Battery Directive Compliance


This product, and the batteries used to power the product, should not be disposed of as unsorted municipal waste and should be collected separately and disposed of according to your national regulations. In the European Union, all equipment and batteries purchased from VIAVI after 2005-08-13 can be returned for disposal at the end of its useful life. VIAVI will ensure that all waste equipment and batteries returned are reused, recycled, or disposed of in an environmentally friendly manner, and in compliance with all applicable national and international waste legislation.

It is the responsibility of the equipment owner to return equipment and batteries to VIAVI for appropriate disposal. If the equipment or battery was imported by a reseller whose name or logo is marked on the equipment or battery, then the owner should return the equipment or battery directly to the reseller.

Instructions for returning waste equipment and batteries to VIAVI can be found in the Environmental section of VIAVI web site at . If you have questions concerning disposal of your equipment or batteries, contact VIAVI WEEE Program Management team at WEEE.EMEA@viavisolutions.com.

Technical Support

<table>
<thead>
<tr>
<th>Region</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>1.844.GO VIAVI / 1.844.468.4284</td>
</tr>
<tr>
<td>Latin America</td>
<td>+52 55 5543 6644</td>
</tr>
<tr>
<td>EMEA</td>
<td>+49 7121 862273</td>
</tr>
<tr>
<td>APAC</td>
<td>+1 512 201 6534</td>
</tr>
<tr>
<td>All Other Regions</td>
<td>viavisolutions.com/contacts</td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:customer.care@viavisolutions.com">customer.care@viavisolutions.com</a></td>
</tr>
</tbody>
</table>

Support hours are 7:00 A.M to 7:00 P.M. (local time for each office).
# Table of Contents

**Chapter 1: Getting started**

Which version of Observer is right for you? .......................................................... 12
Observer Standard ........................................................................................................ 16
Observer Expert .......................................................................................................... 16
How to install or upgrade the software ................................................................. 16
Minimum and recommended system specifications ........................................ 17
How to upgrade to Windows 10 .............................................................................. 18
How to install all versions ....................................................................................... 19
How to upgrade version 17 and later ................................................................. 19
How to upgrade version 16 and earlier ............................................................... 20
FAQ: Licensing and updating ............................................................................. 20
Capture card driver requirements ...................................................................... 22
Installing Windows updates and updating virus protection ........................................ 23
Virtual machine troubleshooting ........................................................................ 23
Cannot capture traffic using VMware ESX VM .................................................. 23
Experiencing BSOD when packet capture starts .............................................. 24
Overview of Observer ........................................................................................... 25
User interface ........................................................................................................... 26
Ports used by Observer Platform v17 and later .................................................... 27
Configuring Observer’s general settings .......................................................... 27
General tab ............................................................................................................... 28
Security tab ............................................................................................................. 29
Folders tab ................................................................................................................ 31
SNMP tab .................................................................................................................. 31
IPv6 tab .................................................................................................................... 32
Third Party Decoder tab ....................................................................................... 32
GeoIP Settings ......................................................................................................... 33
How to have Expert Probe managed by OMS........................................................................33
How to show and use older features (Classic Mode)..........................................................34
How to upgrade Expert Probe..................................................................................................34
How to retrieve a list of available Expert Probe versions.............................................35
How to download a version of Expert Probe................................................................35
How to install a version of Expert Probe..........................................................................36
Upgrade settings.......................................................................................................................36
Version numbering....................................................................................................................37

Chapter 2: Real-Time Statistics.................................................................................................39
Monitoring connection statistics..........................................................................................39
Discovering conversations between local devices and the Internet........................................39
Configuring the IP application list.......................................................................................41
Discovering conversations between local devices.............................................................41
Viewing real-time statistics per device..............................................................................41
Viewing a list of protocols seen on the network.................................................................42
Viewing wireless access point statistics...........................................................................42
Monitoring network load.......................................................................................................43
Viewing router utilization statistics....................................................................................43
Viewing bandwidth utilization.............................................................................................44
Viewing bandwidth utilization with a filter..........................................................................45
Wireless Access Point Load Monitor..................................................................................45
Viewing the distribution of packet sizes by station............................................................46
Discovering current top talkers on the network.................................................................46
Load testing the network.......................................................................................................47
Configuring your load test settings....................................................................................47
Viewing utilization history.....................................................................................................48
Tell me more about the Utilization History tool...............................................................48
Viewing real-time utilization...............................................................................................49
Viewing a summary of network activity.............................................................................49
Checking the health of your network..................................................................................49
Viewing network errors........................................................................................................49
Viewing network errors by device.....................................................................................50
Searching for wireless interference...................................................................................51
Ethernet errors tracked by Observer................................................................................53
Watching for packet storms...............................................................................................55
Understanding Real-time Statistics....................................................................................55
Monitoring your VLAN.........................................................................................................56
Viewing optional VLAN statistics....................................................................................57

Chapter 3: Network and Application Discovery....................................................................58
Building and saving an address book................................................................................58
Configuring a discovery method (optional).........................................................................58
Building an address book automatically..............................................................................59
Adding entries to the address book manually......................................................................59
Resolving DNS names..........................................................................................................60
Saving the address book.......................................................................................................61
## Chapter 5: Filtering

- Pre-filtering your packet captures .................................................. 87
- Tell me how to filter by protocol ....................................................... 88
- Tell me how to filter by pattern ......................................................... 89
- Activating and deactivating filters .................................................... 93
- How to chain filter rules using logical operators ............................. 93
- Post-filtering your packet captures .................................................. 94
- Enabling command-line filtering ...................................................... 95

---

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>87</td>
</tr>
<tr>
<td>73</td>
</tr>
<tr>
<td>61</td>
</tr>
<tr>
<td>61</td>
</tr>
<tr>
<td>62</td>
</tr>
<tr>
<td>62</td>
</tr>
<tr>
<td>62</td>
</tr>
<tr>
<td>63</td>
</tr>
<tr>
<td>65</td>
</tr>
<tr>
<td>65</td>
</tr>
<tr>
<td>66</td>
</tr>
<tr>
<td>67</td>
</tr>
<tr>
<td>68</td>
</tr>
<tr>
<td>68</td>
</tr>
<tr>
<td>68</td>
</tr>
<tr>
<td>69</td>
</tr>
<tr>
<td>69</td>
</tr>
<tr>
<td>70</td>
</tr>
<tr>
<td>70</td>
</tr>
<tr>
<td>71</td>
</tr>
<tr>
<td>71</td>
</tr>
<tr>
<td>72</td>
</tr>
<tr>
<td>73</td>
</tr>
<tr>
<td>75</td>
</tr>
<tr>
<td>76</td>
</tr>
<tr>
<td>77</td>
</tr>
<tr>
<td>78</td>
</tr>
<tr>
<td>79</td>
</tr>
<tr>
<td>79</td>
</tr>
<tr>
<td>80</td>
</tr>
<tr>
<td>81</td>
</tr>
<tr>
<td>82</td>
</tr>
<tr>
<td>82</td>
</tr>
<tr>
<td>83</td>
</tr>
<tr>
<td>83</td>
</tr>
<tr>
<td>84</td>
</tr>
<tr>
<td>84</td>
</tr>
<tr>
<td>85</td>
</tr>
<tr>
<td>85</td>
</tr>
<tr>
<td>87</td>
</tr>
</tbody>
</table>

---

**Table of Contents (19 Feb 2020) — Archive/Non-authoritative version | 5**
Chapter 6: Decodes

Decoding network traffic................................................................. 100
I have a packet capture to analyze. What file formats can Observer load? 101
Opening files from unknown locations............................................. 101
Private key locations per server...................................................... 102
Decoding encrypted network traffic................................................. 103
Decoding NetFlow or sFlow streams............................................... 106
Replaying a packet capture............................................................. 107
Working with packets..................................................................... 108
Using the Decode pane................................................................. 110
Saving a packet capture................................................................. 112
Searching for a specific packet...................................................... 113
Filtering your saved packet capture.............................................. 114
Processing NetFlow or sFlow data.................................................. 114
Packet View Settings..................................................................... 115
Configure SNMP MIBs................................................................... 115
General......................................................................................... 115
Protocol Colors............................................................................ 117
Protocol Forcing........................................................................... 117
Summary....................................................................................... 117
TCP/UDP/SCTP Application Colors................................................ 117

Chapter 7: Expert Analysis

Preparing expert decoding techniques.......................................... 118
Using the Expert Analysis feature................................................ 119
Configuring global settings......................................................... 121
What is goodput?........................................................................ 122
Network delay calculation............................................................ 122
Response time calculation............................................................ 123
Using Expert Summary............................................................... 123
Using Time Interval Analysis....................................................... 124
Using Server Analysis................................................................. 125
Using End-to-End Analysis.......................................................... 125
Using “What-if” modeling........................................................... 126
Reconstructing TCP data streams................................................ 128
Tell me more about stream reconstruction.................................... 129
Using Connection Dynamics....................................................... 129
Tell me more about the Connection Dynamics tool.................... 130
What are skipped packets, and why are they appearing?............ 131
Configuring expert thresholds...................................................... 132
Tell me more about expert thresholds......................................... 133
Using MultiHop Analysis........................................................... 133
Tell me more about the MultiHop Analysis tool......................... 135
Quickly using MultiHop Analysis............................................... 135
Configuring MultiHop Analysis settings...................................... 136
Troubleshooting synchronization errors ................................................................. 138
How to use IP mapping in MultiHop Analysis ............................................................ 139

**Chapter 8: Alarms** ................................................................................................. 140
Configuring and using alarms ..................................................................................... 140
   Enabling probe instance alarms .................................................................................. 140
   Enabling individual alarms ......................................................................................... 141
   Creating filter-based alarms ....................................................................................... 142
   Resetting statistical alarms ....................................................................................... 143
Customizing triggers and actions ................................................................................. 144
   Customizing alarm triggers ....................................................................................... 144
   Customizing alarm actions ....................................................................................... 144
Sharing alarms with others ......................................................................................... 145
   How to export alarms ............................................................................................... 145
   How to import alarms .............................................................................................. 146

**Chapter 9: Security and Privacy** .......................................................................... 147
Security, privacy, and regulatory compliance ................................................................. 147
   Configuring user accounts for secure access .............................................................. 148
Sharing packet captures with third-parties .................................................................... 148
   Password protecting the ability to change partial packet capture size ....................... 149
   Trimming data from your captures .......................................................................... 149
How to encrypt captured data at rest ........................................................................... 150
Understanding the certificate trust model ..................................................................... 153
   How to view certificates ......................................................................................... 154
   How to change the trust of a certificate .................................................................... 154
Certificates and how they are used .............................................................................. 154

**Chapter 10: Network Trending** ............................................................................. 155
Understanding the Network Trending tool ................................................................... 155
   Does network trending have any limitations? ............................................................. 156
Understanding Application Performance Analysis ......................................................... 156
   How to configure Application Performance Analysis ................................................. 157
Understanding Application Transaction Analysis .......................................................... 160
   Analyzing servers and applications using ATA ........................................................ 161
   Importing or exporting a server profile .................................................................... 162
   Global Settings ........................................................................................................ 163
   ATA is reporting inaccurate values ........................................................................ 164
Collecting network trending data ................................................................................. 165
   Viewing network trending data .............................................................................. 165
   Deleting your network trending data files ............................................................... 165
Configuring your network trending settings ............................................................... 166
   Choosing your network trending types .................................................................... 167
   Scheduling your network trending data collection ................................................... 169
   How to determine disk space requirements for network trending .......................... 170
   How to reduce the disk space consumed by network trending files ........................ 170
   How to change where network trending is stored .................................................... 171
   Adding specific servers to network trending .......................................................... 171
Table of Contents (19 Feb 2020) — Archive/Non-authoritative version

<table>
<thead>
<tr>
<th>Chapter 11: VoIP and Teleconferencing</th>
<th>175</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collecting VoIP or video conferencing trending data</td>
<td>175</td>
</tr>
<tr>
<td>Importing and exporting VoIP or video conferencing settings</td>
<td>176</td>
</tr>
<tr>
<td>Analyzing VoIP or video conferencing traffic</td>
<td>177</td>
</tr>
<tr>
<td>How to extract VoIP and video calls from your GigaStor</td>
<td>178</td>
</tr>
<tr>
<td>VoIP MOS</td>
<td>179</td>
</tr>
<tr>
<td>VoIP R-Factor</td>
<td>179</td>
</tr>
<tr>
<td>Configuring network trending settings for VoIP or video conferencing</td>
<td>180</td>
</tr>
<tr>
<td>General tab</td>
<td>181</td>
</tr>
<tr>
<td>MOS tab</td>
<td>181</td>
</tr>
<tr>
<td>Device IP Addresses tab</td>
<td>183</td>
</tr>
<tr>
<td>Caller ID Determination tab</td>
<td>184</td>
</tr>
<tr>
<td>IP Range Filters tab</td>
<td>184</td>
</tr>
<tr>
<td>Enabling VoIP alarms</td>
<td>185</td>
</tr>
<tr>
<td>VoIP Top 10 best practices</td>
<td>186</td>
</tr>
<tr>
<td>Network Jitter and Delay</td>
<td>187</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>188</td>
</tr>
<tr>
<td>Managing VoIP Quality</td>
<td>188</td>
</tr>
<tr>
<td>VoIP terminology</td>
<td>189</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12: Reports</th>
<th>192</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up email notifications</td>
<td>192</td>
</tr>
<tr>
<td>Setting up text message notifications</td>
<td>192</td>
</tr>
<tr>
<td>Setting up pager notifications</td>
<td>193</td>
</tr>
<tr>
<td>Sending a page</td>
<td>194</td>
</tr>
<tr>
<td>Viewing the Paging Server logs</td>
<td>194</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13: Probes and Probe Instances</th>
<th>195</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing Probes</td>
<td>195</td>
</tr>
<tr>
<td>What is a probe instance?</td>
<td>196</td>
</tr>
<tr>
<td>Which software probe is right for you?</td>
<td>198</td>
</tr>
<tr>
<td>How probes work with switches</td>
<td>200</td>
</tr>
<tr>
<td>How a probe uses RAM</td>
<td>201</td>
</tr>
<tr>
<td>Packet capture buffer and statistics buffer</td>
<td>202</td>
</tr>
<tr>
<td>Running Observer without reserved memory</td>
<td>203</td>
</tr>
<tr>
<td>Running Observer with reserved memory</td>
<td>205</td>
</tr>
<tr>
<td>How packet capture affects RAM</td>
<td>207</td>
</tr>
<tr>
<td>How to allocate the reserved RAM</td>
<td>208</td>
</tr>
<tr>
<td>Recommendations for the VIAVI capture cards</td>
<td>209</td>
</tr>
<tr>
<td>Troubleshooting common issues</td>
<td>209</td>
</tr>
<tr>
<td>Troubleshooting a slow probe system</td>
<td>210</td>
</tr>
<tr>
<td>A probe is not connecting to the analyzer or vice versa</td>
<td>211</td>
</tr>
<tr>
<td>No network adapter available</td>
<td>211</td>
</tr>
<tr>
<td>Integrated adapters report all sent packets with bad TCP checksum</td>
<td>212</td>
</tr>
<tr>
<td>“No VLAN” shown while using a Gigabit NIC</td>
<td>212</td>
</tr>
<tr>
<td>VLAN Statistics tool is not working</td>
<td>213</td>
</tr>
</tbody>
</table>
Using Discover Network Names on a Layer 3 switch that uses VLANs....................214
Suspected NAT or VPN issues.............................................................................................. 215
Running Observer passively affects NetFlow................................................................. 215
Daylight Savings Time............................................................................................................215
Configuring Cisco 6xxx switches using a SPAN port to a full-duplex Gigabit
Probe........................................................................................................................................... 216

Chapter 14: Expert Probe Software..........................................................................217
How to install or upgrade the software.............................................................................217
Comparing software probe features..................................................................................218
Minimum and recommended system specifications......................................................... 220
How to upgrade to Windows 10......................................................................................... 221
How to install all versions.................................................................................................... 221
How to upgrade version 17 and later................................................................................222
How to upgrade version 16 and earlier............................................................................222
Capture card driver requirements...................................................................................... 223
Installing the wireless NIC driver on Windows 7/Vista................................................ 223
Installing a third-party USB wireless adapter................................................................. 224
Installing Windows updates and updating virus protection............................................ 225
Upgrading the probe software............................................................................................226
Upgrading the probe software directly........................................................................... 226
FAQ: Licensing and updating............................................................................................. 226
Backing up your GigaStor settings.................................................................................... 228
Creating a probe instance................................................................................................... 230
Creating GigaStor active and passive probe instances.................................................... 231
Creating and configuring an MPLS probe instance......................................................... 232
How to use additional storage volumes on the GigaStor active instance.............. 232
Connecting to a Probe.......................................................................................................... 233
How to change the monitored network adapter............................................................ 233
Connecting to a probe for the first time from Observer................................................. 233
Connecting the Multi Probe or Expert Probe to an Observer.................................... 234
Connecting to a probe instance from an Observer analyzer...................................... 234
Connecting the probe to an Observer.............................................................................. 235
Redirecting a probe instance............................................................................................ 235
Configuring a probe’s name and other probe options...................................................... 237
Customizing statistics and capture buffers for probe instances............................... 238
Configuring probes to collect data even when not connected to an analyzer.............. 239
Setting the probe’s time clock synchronization settings.............................................. 239
Configuring connections to multiple NICs or Observer.............................................. 239
Setting the total system memory reserved for probes.................................................. 240
Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics
sampling................................................................................................................................. 240
Probe Properties field-level descriptions......................................................................... 241
Understanding the Packet Broker Integration tab......................................................... 245
Dynamic traffic management............................................................................................. 245
Contextual visibility............................................................................................................... 246
How to configure packet broker integration.................................................................... 247
How to encrypt captured data at rest..................................................................................250
Using the Probe..................................................................................................................253
   Using the Expert Probe software..................................................................................253
   VoIP Expert, Application Performance Analysis, and Application Transaction Analysis ...................................................................... 254
Switching between the probe and analyzer user interfaces...................................... 254
Enabling Network Trending and setting which statistics are collected................. 255
Monitoring a wireless access point................................................................................. 255
Using the probe as a virtual TAP......................................................................................256
   When to use a virtual TAP............................................................................................257
Configuring VMware ESX Server....................................................................................262
   How to assign physical ports to probe instances.......................................................264
Using the NetFlow features in Observer........................................................................267
   Creating a NetFlow collector or NetFlow Trending collector................................267

Chapter 15: GigaStor Control Panel......................................................................... 269
Getting started using your GigaStor.....................................................................................269
   What is the GigaStor?........................................................................................................ 271
   Differences between GigaStor Software Edition and GigaStor.................................... 272
   Using the GigaStor Control Panel...............................................................................274
   Non-GigaStor-specific settings......................................................................................276
   Setting the GigaStor general options...........................................................................276
   Understanding GigaStor protocol and port settings....................................................280
   Capturing packets with the GigaStor............................................................................281
      Setting a schedule for when data captures should occur...........................................282
      Trimming data from your captures for space or privacy........................................282
      Password protecting the ability to change partial packet capture size...................283
      Differences between statistics and packets..............................................................283
   Understanding GigaStor indexing................................................................................... 284
   Exporting GigaStor data for archiving..........................................................................286
Configuring your GigaStor........................................................................................................ 287
   Defining your subnets in GigaStor...............................................................................287
   Tracking individual analysis ports..............................................................................287
   Configuring the packet capture and GigaStor buffer size..........................................288
   How to change the GigaStor storage directory or drive.............................................288
Configuring options for the GigaStor charts, graphs, and reports.............................289
   Statistics Lists tab........................................................................................................ 289
Mining data from your GigaStor............................................................................................. 289
   Selecting a time frame to analyze.................................................................................292
   How to reorder packets based on a trailer timestamp.................................................292
   Analyzing data without any filters............................................................................. 294
   Analyzing data with filters from the Observer filter editor.........................................294
   Analyzing data with filters from the GigaStor Control Panel.....................................295
   Analyzing data by combining GigaStor Control Panel and Observer filters......... 296
   Analyzing multiple GigaStor probe instances from one GigaStor Control Panel........ 296
   Understanding GigaStor accelerated analysis..............................................................297
Filter elements that support accelerated analysis..................................................298
Examining your network traffic with forensic analysis..............................................298
Importing Snort rules...............................................................................................299
Analyzing packets using Snort rules.................................................................299
Creating a Forensic Settings profile......................................................................300
Using network forensics to track a security breach...............................................305
Using network forensics to track acceptable use or compliance..............................306
Searching for microbursts.......................................................................................306
Using the Microburst Analysis tab in the GigaStor Control Panel..........................308
Using the Detail Chart only....................................................................................308
Reconstructing streams of HTTP, VoIP, and more.................................................311
Defining what can be recreated in Stream Reconstruction.....................................312
How to extract VoIP and video calls from your GigaStor........................................312
Using Observer in financial firms.........................................................................313
Analyzing FIX transactions....................................................................................315
Configuring a FIX profile.......................................................................................315
Troubleshooting the GigaStor Control Panel.........................................................316
GigaStor Control Panel option is grayed out.........................................................316
GigaStor is full or does not have the history you expect..........................................317
TCP applications are not appearing in the GigaStor Control Panel........................317
Loading decodes in Observer is slow.....................................................................317
Chapter 16: Backups and Restoring......................................................................318
Configuring a FIX profile.......................................................................................318
Sharing alarms with others....................................................................................319
How to import alarms............................................................................................319
How to export alarms............................................................................................319
Sharing application definitions with others.........................................................320
How to export application definitions.................................................................320
How to import application definitions.................................................................320
Private key locations per server...........................................................................321
Microsoft Lync Server..........................................................................................321
Apache Web Server..............................................................................................321
Windows IIS Web Server.......................................................................................322
Non-encrypted private key file...............................................................................322
Encrypted private key file......................................................................................322
Importing and exporting VoIP or video conferencing settings...............................323
Restoring the default application list......................................................................323
How to restore TCP application definitions.........................................................323
How to restore UDP application definitions.........................................................323
Importing or exporting a server profile.................................................................324
Creating a Forensic Settings profile.......................................................................324
Index......................................................................................................................331
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>
<thead>
<tr>
<th></th>
<th>Standard</th>
<th>Expert</th>
<th>Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packet Capture</strong></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(page 82)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Packet Decode</strong></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(page 100)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Real-Time Packet Captures &amp; Decode</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><em>Automated Packet Captures</em></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><em>Nanosecond Resolution</em></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><em>Financial Protocol Support</em></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Filters (page 87)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Find Virus and Hack Signatures</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Statistical Drill Down</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarms (page 140)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Custom Alarm Triggers (page 144)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Error Tracking (page 53)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Real-Time Statistics (page 39)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><em>Top Talkers</em> (page 46)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><em>Bandwidth Utilization</em></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>VLAN Analysis (page 57)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Internet Activity (page 39)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Wireless Analysis (page 42)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><em>IP Pair Statistics</em></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Protocol Distribution (page 42)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>64 &amp; 32-bit applications (page 16)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Network Trending/Reporting (page 155)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><em>Comparison Reports</em></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><em>Ready-Made Reports</em></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Version 1</td>
<td>Version 2</td>
<td>Version 3</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>Custom Reports</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Report Scheduler</strong></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>IPv6 Support (page 32)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trace File Aggregation (page 81)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SRTP Support</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Integrated reporting with Apex</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Application Analysis Trending (page 156)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Stream Reconstruction (page 128)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Web pages</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Instant messages</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>HTTP-transferred files</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Expert Analysis (page 119)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Over 600 Experts</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Expert Summary</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Network Delay (page 122)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Connection Dynamics (page 129)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>MultiHop Analysis (page 133)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>&quot;What-If&quot; Analysis (page 126)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Application Analysis (page 161)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Citrix</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>FIX</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>MS Exchange</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
### Which version of Observer is right for you?

#### Chapter 1: Getting started

<table>
<thead>
<tr>
<th>Feature</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MS Networking (SMB)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Oracle</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>POP3</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>SMTP</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>SQL</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Telnet</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>VoIP</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>URL-Based Tracking</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>VoIP Analysis</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Call Detail Records</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Aggregate Call Summaries</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Over 70 VoIP metrics</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Over 50 VoIP Experts</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>QoS Metrics</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>MOS, R-Factor</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>SRTP support</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>VoIP Systems Supported</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Avaya</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Cisco</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Mitel</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Nortel</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Siemens</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>ShoreTel</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>MPLS Monitoring</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>SSL decryption</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>NetFlow Collector</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Video monitoring</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Video metrics</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>End-user experience monitoring</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Third-party decode and analysis</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>LTE Support</strong></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>SNMP Device Management</strong></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>RMON Support</strong></td>
<td></td>
<td>X</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.

How to install or upgrade the software

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

Prerequisite(s):

♦ An administrator account is required to install and run any version of Observer or probe software except Observer Expert Console Only (ECO). Observer ECO requires an administrator account just for installation; a standard user account can be used for running Observer ECO.

♦ 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. VIAVI sells hardware probes that are guaranteed to keep up with heavy loads. See the Observer Platform 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 (page 256).

Caution: See the important information in How to upgrade to Windows 10 (page 18) if you want to upgrade the operating system!

1. Ensure your system meets the minimum requirements.
   See Minimum and recommended system specifications (page 17).

2. Choose one of the following:
How to install or upgrade the software

Chapter 1: Getting started

- How to install all versions (page 19)
- How to upgrade version 17 and later (page 19)
- How to upgrade version 16 and earlier (page 20)

After completing this task:

- License your software. See FAQ: Licensing and updating (page 20).
- If you are using a wireless network adapter to capture traffic, see Installing the wireless NIC driver on Windows 7/Vista (page 223).
- If you are using a USB wireless network adapter to capture traffic, see Installing a third-party USB wireless adapter (page 224).
- If you use Observer on a virtual machine and network traffic cannot be captured or BSODs (bluescreens) are occurring, see Virtual machine troubleshooting (page 23).

Minimum and recommended system specifications

If you are installing the software on your own hardware or a virtual machine, these are the minimum and recommended specifications for a production environment.

Table 2. Observer Expert Console Only (ECO)

<table>
<thead>
<tr>
<th>Processor / CPU</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dual core Pentium class processor</td>
<td>Quad core Pentium class processor</td>
</tr>
<tr>
<td>RAM¹</td>
<td>2 GB RAM</td>
<td>8 GB RAM</td>
</tr>
<tr>
<td>Operating system²</td>
<td>64-bit Operating System Windows 7 or newer</td>
<td>64-bit Operating System Windows 7 or newer</td>
</tr>
<tr>
<td>Network Card</td>
<td>Server-class</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. See Supported Operating Systems (page 18) for a full list of supported operating systems.

Table 3. Observer or GigaStor Software Edition in a virtual server

<table>
<thead>
<tr>
<th>Processor / CPU</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Four core</td>
<td>Six core Intel</td>
</tr>
<tr>
<td>RAM¹</td>
<td>Minimum 16 GB (8 GB for Observer and 8 GB for the operating system)</td>
<td>64 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>Packet capture - Hardware: Determined by your product</td>
<td>Same</td>
</tr>
<tr>
<td></td>
<td>Network trending: See How to determine disk space requirements for network trending (page 170).</td>
<td></td>
</tr>
<tr>
<td>Operating system²</td>
<td>64-bit Operating System Windows 7 or newer</td>
<td>64-bit Operating System Windows 7 or newer</td>
</tr>
<tr>
<td>Network Card</td>
<td>Virtualized network adapter</td>
<td>Intel server-class</td>
</tr>
</tbody>
</table>
How to install or upgrade the software

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. See Supported Operating Systems (page 18) for a full list of supported operating systems.

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 (page 22).

Current compatibility and incompatibility of virtual machines with the GigaStor Software Edition (GSE) is described in this list:

- VMWare ESXi Server
  - ESXi 5.0 and higher is compatible with GSE.
- VMWare Workstation Pro is not supported with GSE
- Microsoft Hyper-V may function but is not supported with GSE

Supported Operating Systems

Your product must be installed on one of these operating systems to receive assistance from Technical Support.

<table>
<thead>
<tr>
<th>Product name</th>
<th>64-bit Windows</th>
<th>32-bit Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 (SP1 or higher) or newer</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008 R2 Enterprise, Standard, Web (SP1 or higher) or newer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 7 (SP1 or higher) or newer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How to upgrade to Windows 10

Due to the way Microsoft has designed its Windows® 10 operating system upgrade feature, Expert Probe will not function if you upgrade your operating system from Windows 7, Vista or Windows 8 to Windows 10 without first uninstalling Expert Probe.

This information does not apply if you:

- Already uninstalled Expert Probe.
- Are installing Windows 10 rather than upgrading to it.
- Are already using Windows 10.
- Are upgrading using the Observer Platform OS Upgrade product because it replaces the operating system rather than upgrading it. Additionally, it uses Windows Server 2012 R2.

Note: Unfortunately, if you have already upgraded the operating system and Expert Probe was not uninstalled prior to upgrading to Windows 10, the only path to recovery is to reinstall the operating system. Back up (page 228) any Expert Probe files on the operating system, reinstall the operating system, then install Expert Probe and restore its files.
To upgrade a system with Expert Probe to Windows 10:

1. Back up your settings.
3. Upgrade your operating system.
4. Install the Expert Probe software.
5. Restore your settings from step 1 using whatever method is best for you. 

Expert Probe is now available to use on Windows 10.

How to install all versions

Use this procedure to install all versions of the software.

Prerequisite(s):

An administrator account is required to install and run any version of Observer or probe software except Observer ECO. Observer ECO requires an administrator account just for installation; a standard user account can be used for running Observer ECO.

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

   http://update.viavisolutions.com/latest/ObserverSetupx64.exe

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.

How to upgrade version 17 and later

Version 17 allows you to upgrade directly from within Observer or from OMS (if used).

If OMS is not controlling Observer, then do the following in Observer:

- Click the File tab, and click Info > Update Observer.

If OMS is controlling Observer:

- See How to manage software versions using OMS.

The software is updated to the latest version.
How to upgrade version 16 and earlier

Upgrading version 16 uses the same procedure as installing the software. The process is different for version 17 and later.

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

   http://update.viavisolutions.com/latest/ObserverSetupx64.exe

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.

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.

How to license Observer and GigaStor

To license and activate a compatible GigaStor, Observer, or Probe:

1. Install and launch the application.

2. After launching the application in DEMO mode, click the Help menu and select License Observer.

3. Click the Enter Name button in the lower left corner.

4. Type into the Contact/Department and Company boxes exactly what is listed in your license document.

5. Click OK, and then click Accept on the confirmation dialog.

6. Ensure the Identification Number matches the number on your license document. If they do not match, click Re-Type Name? to correct any mistakes.

7. Type the license number, from your license document, into the License Number box.

8. Click OK.

You successfully licensed and activated your product.

If licensing and activating your product remains unsuccessful, please contact Technical Support.

How to update your license

If Observer or GigaStor is already licensed and you need to modify, update, or change that license, you can do so.
Prerequisite(s):
This task requires you have already licensed (page 20) your Observer or GigaStor.
This task cannot be completed if the license to your Observer or GigaStor is managed by OMS. Instead, refer to How to edit an asset license.

Updating your license refers to changing, editing, or updating the license that is already applied to your product. Some reasons for needing to do this can include:

- Activating a new license. The new license might provide different or increased functionality over your existing license, like increased data storage for a GigaStor Software Edition (GSE).
- Changing a license. Perhaps you accidentally applied the wrong license to your product and need to change it.

To update a license:
1. Click the File tab, and click Info > License Observer.
2. Click OK to confirm you want to re-license.
3. Type the license number, from your license document, into the License Number box.
4. Click the Re-Type Name? button in the lower left corner.
5. Type into the Contact/Department and Company boxes exactly what is listed in your license document.
6. Click OK, and then click OK on the confirmation dialog.

You successfully updated your license. Observer begins using the license the next time Observer is launched.

Close and restart Observer for the new license to take effect. You may need to coordinate a suitable time to do so if restarting would affect many users or significantly interrupt your data collection.

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.

Ensure you are licensing the correct version of Observer. License numbers are version-specific. License numbers work within equal major version numbers of the product only. For example, an 17.0 license can be used to activate 17.x versions but not 16.1, 16.0, 15.1, 15.0, etc.

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).

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 software version the license number applies to. If it does not, or you notice any other error, please call our support team for assistance.
Should I uninstall Observer before updating it?

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.

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 VIAVI 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.
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 anti-virus software, follow these guidelines:

- Ensure TCP ports 25901 and 25903 are open. All Observer Platform products communicate on these ports.
- Ensure UDP ports 25901 and 25903 are open if you use OMS.
- 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 anti-virus software.

Virtual machine troubleshooting

The hardware abstraction granted by virtual machines can interact with Observer Platform products in ways bare-metal systems cannot. This can sometimes lead to oddities, but these problems can be resolved.

Cannot capture traffic using VMware ESX VM

When using GigaStor Software Edition in a virtual machine, Observer cannot capture network traffic when Memory Hot Add is enabled.

When Memory Hot Add is enabled, Observer can see traffic as a blue line, but Observer cannot capture any traffic by manually starting packet capture or being set to always capture data. You can still reserve memory in Observer (for example: 12 GB of 16 GB), and Observer states that it has reserved 12 gigabytes of memory; however, Windows does not actually reserve the memory. Windows views all 16 GB of memory, from our example, as available to the operating system. The result of this behavior is that Observer cannot capture data.

A solution for this issue is to Disable memory hot add for this virtual machine in your virtual machine settings. The process for disabling memory hot add is described in How to disable memory hot add (page 23).

How to disable memory hot add

Memory hot add lets you add memory resources for a virtual machine while the machine is powered on.

Prerequisite(s):

- VMware Tools must be installed.
- The guest operating system supports memory hot add.
- The virtual machine uses hardware version 7 or later.
Follow the steps outlined in the vSphere Documentation.

Ensure **Disable memory hot add for this virtual machine** is selected in the VM properties.

This means the feature is disabled.

Figure 1: Disable memory hot add

![Figure 1: Disable memory hot add](image)

Memory hot add is now disabled. You should now be able to capture traffic.

**Experiencing BSOD when packet capture starts**

A blue screen of death (BSOD) can occur when Observer is installed on a virtual machine and packet capture begins.

In this case, the issue is specifically related to the Virtual Machine (VM) itself. The VM has been configured in a way that prevents Observer from using memory correctly, and this leads to a system BSOD when packet capture begins.

There are some options in the configuration details of your VM that have been found to resolve this issue. These include disabling hotplug options in your virtual machine settings. The process for disabling memory hot add and CPU hot plug is described in **How to disable hot plug VM features (page 24)**.

**How to disable hot plug VM features**

Hot plug features can interfere with Observer running inside a virtual machine. Disable them to avoid blue screen errors and crashes.

**Prerequisite(s):**

- VMware Tools must be installed.
The guest operating system supports Memory/CPU Hotplug.

- The virtual machine uses hardware version 7 or later.
- Follow the steps outlined in the vSphere Documentation.
- Select both Disable memory hot add for this virtual machine and Disable CPU hot plug for this virtual machine in the VM properties.

This means the features will be disabled on this virtual machine.

Figure 2: Disable hot plug options

Memory hot add and CPU hot plug features are now disabled. You should now be able to capture network traffic without experiencing a BSOD.

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.

Note: All Observer versions use the same set of TCP ports to communicate with Observer Platform probes. For more details, see Ports used by Observer Platform v17 and later (page 27).

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? (page 12).

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? (page 12).

The depth of features in Observer depends on which product license you purchased. For information about Observer licenses, see FAQ: Licensing and updating (page 20).

User interface

Observer, the software and its user interface, is described as the analyzer. The engine that makes traffic collection possible is the probe.

Observer (i.e., the Observer 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 Observer 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 their 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 Observer 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.
Ports used by Observer Platform v17 and later

Open inbound and outbound TCP 80, 443, and 25901 on your firewalls for Observer Platform products version 17 and later.

<table>
<thead>
<tr>
<th>Port</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 80</td>
<td>Requests from product to VIAVI to see if a new version or update exists.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>Secure web server traffic, including trace extraction between Observer Apex and GigaStor.</td>
</tr>
<tr>
<td>TCP 8008</td>
<td>Default port for transfer of software upgrades.</td>
</tr>
<tr>
<td>TCP 25901</td>
<td>All intra-Observer Platform communication.</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:

- Click the File tab, and click **Options > 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 start and runtime options

The **Remember expert post-capture statistic data when switching tabs** field is only available when the product is installed on 64-bit systems because of memory limitations of 32-bit systems.

One option of note is: Enable port control via command line on capture card (xxxGig2010) capture cards. This option is only available for 1 Gb, 10 Gb, or capture cards released with version 15 or later. It will not work for any 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:;
```

**Purpose**
Sets the ports for the capture card to be on or off from a command line using NiDecodeApi.exe -VIRTADAPTER. Parameters must be separated by a semi-colon (;).

**Parameters**

- **C:** Specifies that the capture card is a either a 1, 10, or 40 Gb capture card. The options are:
  - C:oneGig2010
  - C:tenGig2010
  - C:fortyGig2010

- **V:** Specifies the virtual port adapter number. The capture card supports up to four virtual adapters. You may only specify one virtual adapter at a time.
  - V:1
  - V:2
  - V:3
  - V:4

- **P:** Specifies whether a port is on or off for a given virtual adapter.
  The capture 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 capture 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 Observer. Many of the options are used in conjunction with OMS, but some can be used by Observer by itself.

To view and change the security settings for an Observer, in Observer choose Options > Observer General Options > Security tab. Use the information in Table 4 (page 29) to configure the analyzer’s security and OMS options.

Table 4. 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 Observer. The user name can be stored locally if you are not using OMS, or maintained by OMS if the “Authenticate Observer login with OMS” 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 Observer with different user accounts, you must use OMS. Administrative Credentials—A local administrative user account that allows you to create a non-administrator account and to set security options for OMS.</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 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 “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 OMS.</td>
</tr>
<tr>
<td>Authenticate users (for redirected Probe instances)</td>
<td>Forces users to authenticate with OMS before using remote probes. User accounts belong to user groups in OMS 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 OMS” option.</td>
</tr>
<tr>
<td>Manage Observer / Probe license with OMS</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 OMS. 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 OMS and the analyzer or probe will take an available license when the analyzer or probe starts.</td>
</tr>
<tr>
<td>Get list of Probe Instances available</td>
<td>When selected all probe instances to which you the user has access to through group permissions set in OMS are available.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Option for redirection from OMS</strong></td>
<td>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 OMS</td>
<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 OMS.</td>
</tr>
<tr>
<td>Synchronize user protocol definitions through OMS</td>
<td>When selected you synchronize protocol definitions, including any derived applications definitions, automatically through OMS. 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 OMS and OMS 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>
</tr>
<tr>
<td>Primary/Secondary server</td>
<td>Provide the IP address of the primary OMS server. If you are also using a failover OMS 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 OMS thereby making your new version available to everyone else. When disabled, you can only get filters from OMS and upload your own. You cannot modify any filters you get from OMS. This option requires that you have the ability to share filters with OMS.</td>
</tr>
<tr>
<td>Authenticate Observer login with OMS</td>
<td>This option works in conjunction with the &quot;Require Observer Login&quot; option. This forces Observer to use OMS to authenticate users rather than Observer's local user list. A user list is maintained in OMS.</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 VIAVI 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 VIAVI 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><strong>Network Trending Folder</strong></th>
<th>The location for Observer to store Network Trending data.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Trending Viewer data size (in MB)</strong></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><strong>Folder for GigaStor and saving packets to disk</strong></td>
<td>The default save location for packet captures. Automatically generated files are also stored here, like packet capture data collected by GigaStor. The default directory for a GigaStor appliance is D:\DATA.</td>
</tr>
<tr>
<td><strong>SNMP Trending Folder</strong></td>
<td>The location for Observer Suite to store SNMP Trending data.</td>
</tr>
<tr>
<td><strong>Write SNMP Trending data to disk every N-minutes</strong></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><strong>Compiled SNMP MIB folder</strong></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><strong>SNMP Requests folder</strong></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.

| **Stop MIB compilation upon error in MIB source file** | If you want Observer to complete the compilation even though the source file contains errors, leave the box unchecked. |
| **Use as MIB source editor** | 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. |
| **Default SNMP version** | Allows you to select the default version of SNMP to use for new agents. You may also override this in the Agent Properties dialog. |
Request time-out period (sec) | Allows you to set the number of seconds that SNMP Management Console will wait for an agent to respond before resending a request.
---|---
Request retry count | Allows you to define how many times SNMP Management Console will re-send a request to an agent before timing out.
Max data buffer (x100K) for running charts | 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.
Max allowed RMON objects in MIB Walk | 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.
Repeat alarm notifications | Allows you to select the number of times that Observer should send out SNMP-related alarms when the alarm has been triggered.
Repeat trap notifications | 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.

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, 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
- Decimal. separated represents the address as 16 decimal octets, for example: 254.128.0.0.0.0.0.0.37.78.243.93.125.180.0.17

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 &quot;Decode Capture File using Wireshark,&quot; 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 Observer, 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 (page 80).</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 an incorrectly configured 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**.

**How to have Expert Probe managed by OMS**

If your organization uses OMS and wants Expert Probe to be a managed asset, you must integrate Expert Probe into OMS. Doing so allows functionality like user authentication and authorization, plus software version control.

**Caution:** By following these steps, Expert Probe will be managed by OMS. After the connection is made, you will be unable to disable the management within Expert Probe. Therefore, the only way to remove Expert Probe from being managed is to remove the asset from within OMS.

To change Expert Probe to be managed by OMS:

1. In the **System Settings** pane, click **Manage by OMS**.
2. Select **Manage Asset with OMS**.
3. In the box, type the IP address or DNS name of the OMS server.
4. Type OMS administrator credentials into the **User Name** and **Password** boxes.
   
   The credentials must have permission to add new assets and/or licenses to OMS (depending on which is needed), or the asset must already be defined and the user must have access to the asset and a license number must be present.

If successful, Expert Probe should now be managed by OMS.

---

### How to show and use older features (Classic Mode)

Starting in version 17.3.0.0, some older features are hidden from view by default. You must turn on Classic Mode to show and use these older Observer features.

**Prerequisite(s):**

- ♦ 17.3.0.0 or higher
- ♦ Windows user account that can restart the Observer application
- ♦ Preparation for up to one minute of Observer downtime

**Tip!** Classic Mode is turned off by default.

An updated user interface was introduced in version 17.3.0.0 of Observer. The updated user interface places the most popular features in one area—the **Home** tab on the ribbon. Some of the older or less popular features were relocated to Classic Mode because of this change.

Turning on Classic Mode reveals a new tab on the ribbon: **Classic**. This tab provides access to older features.

1. Click the File tab, and click **Options > General Options**.
2. Ensure you are viewing the **General** tab, and then scroll down until you see the **Startup and runtime settings** list.
3. Select **Enable Classic Mode** in the **Startup and runtime settings** list.
   
   A confirmation message appears that says Classic Mode activates after the next restart of the Observer.
4. Restart the Observer application.

You turned on Classic Mode, so the **Classic** tab now shows on the ribbon.

---

### How to upgrade Expert Probe

New and past versions of Expert Probe software are made available to you directly from VIAVI. Use the Expert Probe upgrade tool to check for, download, or install a version of Expert Probe.
Prerequisite(s):
♦ Internet access to update.viavisolutions.com (port 80) is required on the system interacting with the VIAVI upgrade repository. This includes checking for upgrades and downloading upgrades.
♦ Proxy settings (page 36) can be used if direct Internet access is unavailable.

The Expert Probe upgrade tool allows you to:
♦ Check the VIAVI upgrade repository for old and new versions of Expert Probe.
♦ Download any available version of Expert Probe for offline installation.
♦ Install any available version of Expert Probe without needing to leave the Expert Probe interface.

How to retrieve a list of available Expert Probe versions
A listing of Expert Probe software versions to upgrade or downgrade to is available directly in Expert Probe. Connect to the VIAVI upgrade repository to retrieve the latest listing of available versions.

Note: Interacting with the upgrade repository requires web connectivity over TCP port 80 or 8008 (by default) on the Expert Probe system. This can be achieved with direct connectivity from OMS to the web or by configuring a proxy in the proxy configuration settings of OMS for downloads. The upgrade repository is hosted by VIAVI and no public mirrors are used.

To ensure your product is using the latest code available, always check the in-product update capability even if you have recently installed. It is strongly recommended that all product updates and upgrade are performed using the in-product update methods instead of installing the executable using Windows File Explorer.

To retrieve a list of available versions, click System > Update.

To retrieve a list of available versions:
1. Click the File tab, and click Info > Update Observer.

Expert Probe connects to the upgrade repository and displays the versions available for download. Release notes for each version are available for viewing.

How to download a version of Expert Probe
New or old versions of Expert Probe can be downloaded from the upgrade repository. Expert Probe is not automatically installed after downloading a version using this method. Instead, this method is suitable for scheduled installation or installation from Windows Explorer.

Tip! It is strongly recommended that you perform product updates using the in-product update method instead of installing with Windows File Explorer.
To download an available version of software for later installation, visit the repository and download any self-extracting setup executable:

1. Click the File tab, and click **Info > Update Observer**.
2. (Optional) Click the check for updates icon 🔄.
   
   **Example:** (Optional) Doing this ensures all available versions are shown.
3. Select an item by clicking it.
4. Click the download icon ✨.
   
   If not previously downloaded, the download begins, and you can view its transfer progress.

You successfully downloaded a software upgrade.

## How to install a version of Expert Probe

Installing a software upgrade downloads the self-extracting setup executable and immediately installs the upgrade.

**Note:** Firmware updates to the capture card are bundled with Observer software upgrades. During installation of an Observer software upgrade, any firmware updates available to your capture card will be applied.

To install a software upgrade:

1. Click the File tab, and click **Info > Update Observer**.
2. Select an item by clicking it.
3. Click the install icon 📦.
   
   The download begins, and you can view its transfer progress.
   
   After the download completes, the software upgrade begins installing.

You successfully installed the selected software upgrade. A notification appears if any errors occur during the upgrade.

## Upgrade settings

There are several settings that change the behavior of version upgrades.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatically check for upgrades</strong></td>
<td>If selected, Expert Probe periodically checks for upgrades. Scheduled transfers and installs rely on knowing if new versions exist. If cleared, users must manually check for available upgrades before any scheduled transfers or installs can occur.</td>
</tr>
<tr>
<td><strong>Show downgrade options</strong></td>
<td>If selected, any available downgrade versions are displayed in the available versions list. It is recommended to leave this cleared (disabled) if downgrading to previous versions is not desirable.</td>
</tr>
<tr>
<td><strong>Preferred speed (Kbps)</strong></td>
<td>Sets the preferred maximum transfer speed in kilobits per second. Use the value '0' to disable this bandwidth restriction.</td>
</tr>
<tr>
<td><strong>Use proxy server</strong></td>
<td>If selected, a proxy server is used for downloading upgrade versions.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>Sets which type of proxy server to connect to.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address or DNS name of the proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number accepting connections to the proxy server.</td>
</tr>
<tr>
<td>Username</td>
<td>Sets the user name expected by the proxy server for authentication.</td>
</tr>
<tr>
<td></td>
<td>Leave this box empty if authentication is not required.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets the password used to authenticate with the proxy server.</td>
</tr>
<tr>
<td></td>
<td>Leave this box empty if authentication is not required.</td>
</tr>
<tr>
<td>Edit Download</td>
<td>Schedules the download of available upgrade versions.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Downloaded versions will not automatically install unless an installation</td>
</tr>
<tr>
<td></td>
<td>schedule or upgrade policy allows it.</td>
</tr>
<tr>
<td>Edit Install</td>
<td>Schedules the installation of downloaded version upgrades.</td>
</tr>
<tr>
<td>Schedule</td>
<td>This setting affects version upgrades that are downloaded both automatically</td>
</tr>
<tr>
<td></td>
<td>or manually.</td>
</tr>
</tbody>
</table>

**Version numbering**

Observer Platform products use a four-field decimal scheme for product versions.

Figure 4: Version numbering scheme

### Version numbering scheme

17.1.3.2

<table>
<thead>
<tr>
<th>Portion of version number (17.1.3.2) — Major</th>
<th>Some defining characteristics¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major</td>
<td>Major version indicator. Full</td>
</tr>
<tr>
<td>Minor</td>
<td>platform version. Moving past</td>
</tr>
<tr>
<td>Build</td>
<td>this number requires a new license for your product (or products).</td>
</tr>
<tr>
<td>Portion of version number</td>
<td>Some defining characteristics¹</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>(17.1.3.2) — Minor</td>
<td>Minor version indicator. New core functionalities, communication libraries, bug fix roll-ups, and more.</td>
</tr>
<tr>
<td>(17.1.3.2) — Build</td>
<td>Build version indicator. Bug fixes and minor feature enhancements.</td>
</tr>
<tr>
<td>(17.1.3.2) — R&amp;D Use Only</td>
<td>Used for R&amp;D purposes only, should generally be 0.</td>
</tr>
</tbody>
</table>

¹. These are representative examples only. No development efforts are restricted to just the examples shown.
Chapter 2: Real-Time Statistics

Real-time statistics help you discover network load, utilization rates, and other connection statistics on your network. Real-time statistics tools can be used at any time; a packet capture is not needed.

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

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.

**Note:** 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.

- To discover conversations between local network devices and the Internet, use the Internet Observer tool.
- On the Home tab, in the Statistics group, click **Internet Observer**.
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

The Pair Statistics tool tracks established connection between local devices. Observer recognizes each of these conversations to be a station pair.

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.

To discover conversations between local network devices:

1. On the Home tab, in the Statistics group, click **Pair Statistics**.
2. Click the **Start** button to activate the tool.
3. (Optional) Click **Settings** for more configuration options.
4. (Optional) 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**.

Viewing real-time statistics per device

To view real-time statistics of individual stations, use the Web Observer tool, which focuses on HTTP traffic (port 80)—or all traffic if desired—to and from an individual station.
Prerequisite(s):
Classic mode (page 34) must be enabled.

1. On the Home tab, in the Analysis group, click Web Observer.
2. 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.
3. Click OK, and click Start to activate.

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 Window.

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

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.

Note: 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 list of protocols seen on the network:
2. Click the Start button to activate the tool,
3. To view a different layout, click the View button and select another or click Settings for more configuration options.
4. Right-click results to navigate to a list of stations using a particular protocol.

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

Viewing wireless access point statistics

The Wireless Access Point Statistics tool shows network traffic passing through any access points visible to the Observer wireless NIC.

Note: Wireless Access Point Statistics is only available using a supported VIAVI 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
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

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).

Prerequisite(s):

Classic mode (page 34) must be enabled.

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.

On the Classic tab, in the Statistics group, click **Router Observer**.

Figure 6: 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).

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.

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.

Note: Be sure to select the address of a port, on your router, that is visible to Observer. 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.

**Viewing bandwidth utilization**

To view real-time bandwidth utilization as seen by a probe instance, choose Utilization > 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.

Note: 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.

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.

To view real-time bandwidth utilization as seen by a probe instance and with one or more filters applied:

♦ On the Home tab, in the Statistics group, click **Utilization > Filtered Utilization**.

**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 (page 59) 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. The Size Distribution Statistics tool shows stations’ traffic patterns (subject to filter criteria) sortable by packet size.

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 incorrectly configured devices that could be wasting bandwidth on your network.

- On the Classic tab, in the Statistics group, click Size Distribution Statistics.

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

The 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.

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

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

**Note:** 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.

To discover current top talkers on the network:

2. Click Start to begin the tool.

Observer displays a tree of protocols and subprotocols seen on your network.
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. Doing so helps reveal problems in your network.

**Prerequisite(s):**

- Classic mode (page 34) must be enabled.

- To use the Traffic Generator tool, you must be using a local probe instance. The probe instance on which you want to generate traffic from cannot be on a remote system.

- 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.

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.

**Caution:** 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.

To use the Traffic Generator tool:

- On the Classic tab, in the Tools group, click **Traffic Generator**.

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

**Configuring your load test settings**

The Traffic Generator tool has several options that can be set.

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 5 (page 48).

**Note:** The VIAVI capture cards do not allow the generation of network traffic using this tool.

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.
### Table 5. Traffic generator settings

<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>

**Viewing utilization history**

**Note:** 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. 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 (page 45).

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

To view short-term utilization history of the network, follow the steps. For viewing utilization history over a longer period, we recommend using network trending features instead; see Understanding the Network Trending tool (page 155).

- On the Home tab, in the Statistics group, click **Utilization > Utilization History.**

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.

**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**

The Utilization Thermometer tool displays the current network bandwidth utilization as a percentage of the total theoretical network speed.

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. 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.

- On the Classic tab, in the Statistics group, click **Utilization Thermometer**.

**Viewing a summary of network activity**

To view a simple summary of current network activity:

- On the Home tab, in the Statistics group, click **Network 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**.

**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**

The Vital Signs tool gives you a complete snapshot of errors witnessed during current network activity.

The 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, like error occurrences:

- On the Classic tab, in the Statistics group, click **Vital Signs**.
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 delinated file using **File > Save > Save Data**.

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 network. 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.

**Prerequisite(s):**

**Classic mode (page 34) must be enabled.**

To discover network errors and their originating source:

1. On the Classic tab, in the Statistics group, click **Errors By Station**.
2. Click the **Start** button to activate the tool.
3. Click Settings for more configuration options.
4. Click **View** to select a different layout.

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

**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.

**Note:** Wireless Site Survey is only available using a supported VIAVI wireless driver.

To use the Wireless Site Survey tool and search for wireless interference:

- On the Classic tab, in the Statistics group, click **Wireless Site Survey**.

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.

See Table 6 (page 51) for a list of noteworthy settings.

**Table 6. Wireless interference**

<table>
<thead>
<tr>
<th>Tab Name</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>
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 7 (page 52)** shows how dB measurements are calculated into signal strength percentage.

**Table 7. 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>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>Sensed (dB)</td>
<td>Reported (%)</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</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”.

---

Checking the health of your network
Observer Expert (19 Feb 2020) — Archive/Non-authoritative version
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, use the Activity Display tool. The Activity Display tool tracks occurrences of broadcast/multicast packets.

Prerequisite(s):

Classic mode (page 34) must be enabled.

- On the Classic tab, in the Statistics group, click Activity Display.
- (Optional) Click the View button to choose a different layout.
- (Optional) Click Settings to further customize said layouts.

(Optional) 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.

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.

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

Tip! If you are connected to a Observer GigaStor, you can view statistics in the GigaStor Control Panel

2. 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.

**Figure 7: Statistics tools**

<table>
<thead>
<tr>
<th>VLAN Statistics</th>
<th>Shows the VLANs operating on your network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Talkers</td>
<td>Lets you see who is using the most network bandwidth.</td>
</tr>
<tr>
<td>Protocol Distribution Statistics</td>
<td>Displays all protocols running on the network.</td>
</tr>
<tr>
<td>Internet Observer</td>
<td>Show what websites users are visiting and how much time was spent on a website.</td>
</tr>
<tr>
<td>Internet Patrol</td>
<td>Allows you to view MAC to IP communication as a list, pairs circle, or charts.</td>
</tr>
<tr>
<td>Wireless environments</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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:

1. On the Home tab, in the Statistics group, click **VLAN**.
2. Click the **Start** button to activate the tool.

Results can be saved in a comma delimited file using **File > Save > Save Data**.
Observer uses application definitions to identify applications and services. Learn the best ways of identifying your network’s servers, clients, and the applications they use, by using discovery tools and the address book.

**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 Analyzer, 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.

Tip! 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:

2. Click Add Entry. The Add Alias dialog box appears.
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. Choose **Options > General Options**. Then, in the **General** tab, ensure **Disable IP Address DNS Resolution** is not selected.
- Remember that DNS names in the decode views are resolved by the Observer analyzer viewing the decode. Loading a saved packet capture might return different DNS names than originally seen, but this occurs because the IP addresses have changed since that time.
**Saving the address book**

To save the address book:

1. On the Home tab, in the Tools group, click **Discover Names**.
2. Run the tool, and click **Save Aliases**.

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, click the **File** tab, and select **Options > Address Table** to 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 (page 58).

To edit address book entries in Observer:

1. On the Home tab, in the Tools group, click **Discover Names**.
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:

1. On the Home tab, in the Tools group, click **Discover Names**.
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, router1 00:00:C0:13:4B:33, 223.188.11.3, Sue’s Accounting PC
-or-
0000C08B4194, 175.203.57.8, John C0134B33 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. Click the File tab, and click Options > Address Table.
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. If you use Observer Management Server (OMS), you can have OMS collect and publish your protocol definitions. The setting to enable is at Options > Observer General Options > Security > Synchronize user protocol definitions through OMS.

1. Click the File tab, and click Options > Protocol Definitions.
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 9 (page 63).

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

Note: Some SNMP devices on your network may not adhere to RFC1213, causing them to remain undiscoverable even when your other settings are configured correctly. 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 10 (page 64)). You may need to experiment with this setting if you are unsure of what to choose. Remember that RFC1213 is default.

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.

**Note:** This section only describes the process for automatic SNMP device discovery; to add SNMP devices manually (and perhaps with greater success than automatically) see .

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.

Set the IP address discovery ranges by completing the following:

1. On the Home tab, in the Tools group, click **SNMP > Device Discovery**.
2. Click the **Settings** button. The SNMP Device Discovery window appears. Figure 10: Configure SNMP IP discovery ranges

   ![Figure 10: Configure SNMP IP discovery ranges](image)

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 **step 4** 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.
Calculating subnet masks

The 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.

**Prerequisite(s):**

Classic mode (page 34) must be enabled.

To use the IP Subnet Mask Calculator tool:

- On the Classic tab, in the Tools group, click **IP 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

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.

**Prerequisite(s):**

Classic mode (page 34) must be enabled.

To use the Ping/Trace Route tool:

- On the Classic tab, in the Tools group, click **Ping/Trace Route**.

See Table 8 (page 65) for more information.

**Table 8. Ping/Trace Route options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Address</td>
<td>Allows you to specify the Internet address to ping, or the address to which the route will be traced.</td>
</tr>
<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><strong>Ping</strong></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><strong>Trace Route</strong></td>
<td>Allows you to select a route from the Observer personal computer to the specified Internet address to be traced.</td>
</tr>
<tr>
<td><strong>Timeout(sec)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Packets</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Packet size</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Display Window</strong></td>
<td>Displays the results of the ping or trace.</td>
</tr>
</tbody>
</table>

### 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 (page 69) for details about creating definitions for applications that are subsets of another application:

1. Click the File tab, and click **Options > Protocol Definitions**.
2. Click the applications definitions tab you want to add to (below the Start and Stop buttons).
3. Click **Add Application**. The **Add Application** window appears.

   **Figure 11:** Add an application from the list or define a custom application.
4. Select an application from the list, and click **Add**. If your application is not in the list, click **Custom** to create your own.

5. In the **Add Application Definition** dialog that appears, ensure these details are correct, (or type application details if you chose Custom), and click **OK**.

6. Click **Apply Changes**.

   Choices are displayed that allow you to set the scope of your changes.

7. Choose one of the following:
   
   - Apply changes to this Probe Instance only
   - Apply changes across all Probe Instances

   **Apply changes across all Probe Instances** only applies changes to currently connected probes instances. The changes cannot apply to disconnected probe instances.

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. Click the File tab, and click **Options > Protocol Definitions**.
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, or port range, to associate with the selected application.
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.

**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.

**How to import application definitions**

**Prerequisite(s):**

To import application definitions, you need access to an exported *.protodefs file. See [How to export application definitions](page 69) for details.

To import application definitions, follow the import process:

1. Click the File tab, and click **Options > Protocol Definitions**.
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**.

   Figure 12: The final importing dialog

   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. Click the File tab, and click **Options > Protocol Definitions**.
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. Click the File tab, and click **Options > Protocol Definitions**.
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 optional IP address 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. Click the File tab, and click **Options > Protocol Definitions**.
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](image)

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. Click the File tab, and click **Options > Protocol Definitions**.
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. Click the File tab, and click **Options > Protocol Definitions**.
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.

   **Apply changes across all Probe Instances** only applies changes to currently connected probes instances. The changes cannot apply to disconnected 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. Click the File tab, and click **Options > Protocol Definitions**.
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.
   
   **Apply changes across all Probe Instances** only applies changes to currently connected probes instances. The changes cannot apply to disconnected probe instances.

5. Click **OK** to apply and save your changes.

Your list is restored.
Capturing network traffic is the primary purpose of Observer. Network packets can be captured, merged, and saved to several file formats, plus the buffer settings can be tweaked for performance.

How to configure the capture buffer settings

Observer can perform packet captures without additional setup. However, to maximize Observer performance, you should consider configuring your capture settings manually.

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 before it is written to disk, and the statistical buffer stores statistical data entries (example buffer change shown in Figure 15 (page 74)).

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

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. 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.

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. On the Home tab, in the Probe group, click **Setup > Memory and Security Administration**.

2. Double-click the probe instance you want to configure.

3. Change the buffer sizes to better match the needs of your chosen probe instance.

4. **(Optional)** Select a statistics memory configuration from the list.

   (Optional) These choices affect the maximum number of entries per statistic tracked in real-time statistic modes. A larger choice allows more statistical entries to be held in non-reserved system memory (RAM available to Windows) than its preceding, smaller choice. The size shown is the maximum memory allowed to be used for this purpose—the memory footprint can grow up to this size but never greater. The memory used here follows FIFO rules (first-in, first-out), meaning if the limit is reached, the oldest data is discarded as the newest data arrives. Remember, this setting only affects real-time statistics modes only, and any statistics modes running will continue to fill up to your chosen limit for however long your real-time statistics tools are running. This is because the memory is not flushed until all statistical mode windows are closed.

5. **(Optional)** Select a trending memory configuration from the list.

   (Optional) These choices affect the maximum number of entries per statistic tracked in network trending during a 1-minute collection interval. One IP pair would be an example of one entry. The size shown is the maximum memory allowed to be used for this purpose—the memory footprint can grow up to

---

**Figure 15: Changing your buffer sizes**

![Image of changing buffer sizes](image.png)
this size but never greater. The memory used here follows FIFO rules (first-in, first-out), meaning if the limit is reached, the oldest data is discarded as the newest data arrives.

6. 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 re-evaluate 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.

How to adjust 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 memory configuration Medium - (default) is sufficient for most users and does not need to be changed. The memory settings are preconfigured based on network size. Each individual statistic is collected as a table entry in non-reserved system RAM, where the processed data is stored. Choose the relative size of the network you are monitoring with this probe instance.

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.

   **Note:** When allocating memory for a probe instance with a capture card 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.

2. Right click any instance and select **Configure Memory** to access the memory allocation dialog.
3. Choose the size of network you are monitoring with this probe instance.

4. Click **OK**.

### Configuring the packet capture options

There are many 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
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. On the Home tab, in the Capture group, click **Configuration > 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 three types of Expert Information Packets:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Load</td>
<td>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 <strong>Network Load</strong> tab within the Expert screen.</td>
</tr>
<tr>
<td>Start/Stop Packet Capture</td>
<td>These packets are inserted whenever you click <strong>Start</strong> or <strong>Stop</strong> from either the Packet Capture or Decode Screen. They are used to help expert know that there are gaps of time between packets.</td>
</tr>
<tr>
<td>Wireless Channel Change</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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...
Configuring the packet capture options

from GigaStor). Clear 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. On the Home tab, in the Capture group, click **Configuration > 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:

Note: 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 (page 148).

1. On the Home tab, in the Capture group, click Configuration > 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 (page 149).
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.
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.

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 9 (page 80).

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 (page 100) and the loadable file formats (page 101) of Observer.

After starting a packet capture—described in Capturing network traffic (page 82)—save the packet capture:

♦ Click the File tab, and click Save > Save Capture.

Tip! You can also press CTRL+S on the keyboard to save.

You can now choose which packets to save (all packets since the capture began are chosen by default) and in which file format.

Table 9. 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>Ethernet and Wireless</td>
<td>BFR can only be read in Observer and Wireshark. Retains both nanosecond resolution and expert information packets. Only BFR captures can be merged directly in Observer.</td>
</tr>
<tr>
<td>PCAPNG</td>
<td>Ethernet and Wireless</td>
<td>PCAPNG retains both nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>PCAP</td>
<td>Ethernet and Wireless</td>
<td>PCAP retains nanosecond resolution, but loses expert information packets.</td>
</tr>
<tr>
<td>CAP</td>
<td>Ethernet</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>XML¹</td>
<td>Ethernet</td>
<td>XML loses nanosecond resolution, but retains expert information packets. Limited in usefulness.</td>
</tr>
</tbody>
</table>

1. XML formatted packet captures cannot be re-opened by Observer.

♦ Saving to any format other than Observer’s native BFR format or PCAPNG 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 (page 77).

- Saving to any format other than Observer’s native BFR format, or the PCAPNG or PCAP formats, removes all nanosecond resolution from the resulting saved packet capture. If you need to retain nanosecond resolution, ensure you save a packet capture to BFR, PCAPNG, or PCAP format. See the table for a full list of limitations per format.

**Merging packet captures**

If you have packet capture files that captured the same data, but from different viewpoints, you can merge them to create a more comprehensive packet capture.

**Note:** Only *.BFR format captures can be merged in Observer.

To merge packet captures, complete the following steps:

1. Click the File tab, and click **Open > Local Packet Captures > Merge**.
2. Type a file name for the resulting capture.
3. Click **Add**, and navigate to and open a saved *.BFR capture.
   
   Repeat this step as necessary to add more captures. Also, when adding a capture you can also create a time adjustment for the other buffers (relative to the first buffer added).
4. (Optional) Select your criteria for how duplicate packets are handled.
   - **Skip duplicate packets only when packet time difference is less than**
   - **Data link layer**
   - **IP time to live (TTL)**
   - **IPv4 type of service or IPv6 traffic class**
   - **TCP sequence and acknowledgement numbers, and TCP options**

5. Click **Start Merge**.

   Depending on the size of the captures, this process may take a few minutes.

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

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

**Tip!** Are you seeing duplicate packets collected during your capture? Do you want to ignore them? See .

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. On the Home tab, in the Capture group, click **Configuration > Packet Capture**.
2. Click the **Start** button to begin your packet capture. If desired, filters can be defined before the capture from **Filters > Configure Software Filter**.
   
   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 **Save > Save Capture** to keep a shareable buffer file. For information about saving packet captures, see Saving packet captures (page 80).
- 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. On the Home tab, in the Capture group, click **Configuration > Capture Multiple**.
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.

**Note:** 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. 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 (page 78).

To schedule packet captures to begin at preset times, complete the following steps:

1. On the Home tab, in the Capture group, click **Configuration > 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** and **Open > Remote Packet Captures**.
   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 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. On the Home tab, in the Capture group, click **Configuration > 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.
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 (page 93).

Understanding duplicate packets

Duplicate packets lower the statistical accuracy of analysis, increase network link saturation, and can interfere with tools. Packet deduplication removes duplicate packets and helps you avoid those situations.

A duplicate packet is any packet that is identical to another packet. The packet header is inspected and all fields must be identical for it to be a duplicate. However, there are some situations where the header has been modified slightly during the packet’s journey. These situations require some fine-tuning of the deduplication settings to ignore those fields that were modified before the duplicate packet is received.

Understanding packet deduplication

Deduplication is useful when multiple copies of the same packet are received, but only a single copy should be seen.

Duplicate traffic is part of any network environment and is unavoidable. However, reducing duplicate packets as much as possible helps ensure your
Understanding duplicate packets

Network is more efficient. It also allows your tools to be more accurate. Duplicate packets reduce statistical accuracy, which leads to higher perceived levels of traffic or network connections. If you experience duplicate packets, consider your analytical needs and network topology when deciding whether deduplication should be used. You most often encounter them when packets are traversing multiple routers and those routers are copying their traffic to the SPAN/mirror port.

Removing duplicates from a saved packet capture can be more accurate than deduplication with the capture card. Observer has several more options than the capture card for ignoring packet header fields. These are header fields you choose to not examine (ignore) when determining if a packet is a duplicate. When all packet header fields are used as criteria (none are ignored) the capture card-based deduplication and Observer deduplication produce nearly the same results.

In some cases you may want to retain the duplicate packets. For example, when packets are being looped or when multiple VLANs are used with your hardware, you may want to keep the packets. Retaining a copy of duplicate packets and their traversal through both VLANs may be necessary when verifying whether the traffic was routed properly.

If you are attempting to find the source of duplicate packets in real time, do not deduplicate packets. Removing duplicate packets before they reach Observer or the GigaStor system lessens your ability to find the source of duplicates—if that is your goal. Instead, you can allow all duplicate packets and make changes to you monitored switches or SPANS and see if that resolves the duplicates coming in or helps locate the source.
Chapter 5: Filtering

Filtering narrows the scope and size of your packet captures so you get only what you want. This filtering can take place before (pre-filter) and after (post-filter) the packet capture is saved to disk.

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.

When you pre-filter your packet captures, you have two choices. You can choose to use a software pre-filter or a hardware pre-filter.

Some countries or locales have laws regarding data privacy and strictly regulate what information may be captured. Failure to abide by these laws could result in fines or jail time. This means that if you are troubleshooting an issue for a specific user you may not be able to create a generic filter. Instead, you must create a filter that captures only traffic for that individual. If you need to be very specific about what you capture, we recommend a hardware filter with a pattern filter (page 89). If it is necessary to filter multiple levels of VLAN tags, use an offset to find the necessary location in the packet payload.

Caution: Failing to click OK in step 8 causes Observer Analyzer to discard any and all changes made since the Active Filters window first appeared in step 1, 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 (page 94).

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

1. Choose one of the following to create your filter.
On the Home tab, in the Probe group, click Filters > Configure Software Filter.
On the Home tab, in the Probe group, click Filters > Configure Hardware Filter.

2. Click New Filter.
   The New Filter dialog 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.
   The maximum number of elements a filter expression may have is 256.
   See Tell me more about modifiers (page 92) 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.
   (Optional) 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.
   Your newly created filter is available to use when capturing packets.

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.

Figure 18: Protocol Filters

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.

Figure 19: Pattern Filter

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 10. Rules types

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address - IP Range/</td>
<td>Specify a hardware or IP address or range of addresses for source</td>
</tr>
<tr>
<td>IP</td>
<td>and destination. You can also limit the rule to apply only to</td>
</tr>
<tr>
<td></td>
<td>packets from particular source or destination ports. For IPv4</td>
</tr>
<tr>
<td></td>
<td>packets, you can specify a subnet mask for inclusion/exclusion.</td>
</tr>
<tr>
<td>Rule Type</td>
<td>Usage</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 to 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 (page 148)</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 strings allow you to filter for values embedded within a particular byte, word, or double word if you know the offset, either from the beginning of the packet, or from the beginning of a particular protocol header. If you want to filter for numeric value or range of values within a byte or word, consider using the numeric value filter. Regular Expression filters allow you to use Unix/Perl-style regular expressions, which let you wildcard for single characters, groups of characters, ranges of characters and numeric values, and more.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify a port or range of ports for inclusion or exclusion.</td>
</tr>
</tbody>
</table>
### Rule Type | Usage
---|---
**Protocol** | 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.

**VLAN 802.1Q** | 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.

**VLAN ISL** | VLAN ISL (Cisco proprietary VLAN). Beyond the VLAN ID, you can filter by user-defined bits.

- Source address (MAC):
- CDP and BPDU indicator:
- High bits of source address:
- Port index:
- Reserved field:

**VNTag** | Allows you to define the direction, loop, DVIF, and SVIF for tags created by the vNIC in your virtual network.

**WAN - DLCI Address** | Specify a WAN DLCI by number.

**WAN Port** | Specify a WAN Port by number.

**WAN Conditions** | Lets you filter for direction (DCE or DTE or both), and logically chain tests for forward congestion packets, backward congestion packets, and discard eligibility.

**Wireless Access Point** | Enter or select a hardware address that corresponds to the wireless access point you want to capture traffic from.

**Wireless Data Rate** | Select a wireless data rate, and whether you want to filter for packets traveling at, under, or over that rate.

**Wireless Channel** | Select a wireless channel, and whether you want to filter for packets received from channels less than, greater than, or equal to that channel.

**Wireless Channel Strength** | Select a wireless signal strength, and whether you want to filter for packets received at, under, or over that signal strength.

---

**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, 555B5155 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 11 (page 92) 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.

Table 11. 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>
</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.

**Tip!** 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.

**Note:** 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. On the Home tab, in the Probe group, click **Filters > Configure Software Filter**.
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 step 2. 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.

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>m</td>
<td>By default, the string is treated as one big line of characters. ^ and $ (two other meta-characters) match at the beginning and ending of the string. When \m is set, ^ and $ 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>
<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 ^)</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 (?). Greediness refers to how many characters it will consider when trying to match strings of variable length.</td>
</tr>
</tbody>
</table>

**Pre-filtering your packet captures**

Chapter 5: Filtering
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).

Figure 20: AND filter example

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:

Figure 21: OR filter example

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 (page 87).

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

1. Click the File tab, and click **Options > Fallback Instance**.
2. Choose 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 (page 101).

3. Click the File tab, and click **Open > Local Packet Captures > PreFilter and Analyze**.

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

5. Click Open. The Pre-Filtering window appears.

6. 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. The maximum number of elements a filter expression may have is 256.

7. 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 (page 110) 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. On the Home tab, in the Capture group, click **Configuration > 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.
After command-line filtering is enabled, you can post-filter via command line as described in Post-filtering via command line (page 96).

Post-filtering via command line

Post-filtering via command line can save you time if you are comfortable building a filter using text.

Prerequisite(s):
You have enabled command-line filtering (page 95).

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 (page 95).
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 Observer Management Server (OMS) 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. Click the File tab, and click **Open > Local Packet Captures > Load and Analyze**.
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.
   - If you do not see the **Type Script Filter** button, verify you have enabled command-line filtering (page 95).
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 12 (page 98).

Figure 23: Use building blocks as your guide
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 12. Building blocks

<table>
<thead>
<tr>
<th>Building block</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-ip=</td>
<td>-ip=10.0.36.139</td>
<td>IPv4 Address—use this to filter for a single IP address (IPv4).</td>
</tr>
<tr>
<td></td>
<td>-ip=74.125.224.72</td>
<td></td>
</tr>
<tr>
<td>-ip_pair=</td>
<td>-ip_pair=10.0.36.139/10.0.36.154</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>-ip_pair=10.0.36.139/74.125.224.72/</td>
<td></td>
</tr>
<tr>
<td>-ip_range=</td>
<td>-ip_range=10.0.36.1/10.0.36.255</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>-ip_range=192.168.0.20/192.168.0.100</td>
<td></td>
</tr>
<tr>
<td>-ipv6=</td>
<td>-ipv6=FE80::F544:9E0:9C81:9FB1</td>
<td>IPv6 Address—use this to filter for a single IP address (IPv6).</td>
</tr>
<tr>
<td></td>
<td>-ipv6=ff00::7f00:1</td>
<td></td>
</tr>
<tr>
<td>-ipv6_pair=</td>
<td>-ipv6_pair=FE80::F544:9E0:9C81:9FB1/2002::4A7D:32DE:158B:9C81:9FB1</td>
<td>IPv6 Pair—use this to filter for two IP addresses (IPv6) that have conversed with each other.</td>
</tr>
<tr>
<td></td>
<td>-ipv6_pair=00:50:56:2E:AB:A0/00:0C:85:BD:08:80</td>
<td></td>
</tr>
<tr>
<td>-ipv6_range=</td>
<td>-ipv6_range=FE80::A00:2401/FE80::A00:24FF</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>-mac=</td>
<td>-mac=00:0C:85:BD:08:80</td>
<td>MAC Address—use this to filter for a single MAC (hardware) address.</td>
</tr>
<tr>
<td></td>
<td>-mac=00:50:56:2E:AB:A0</td>
<td></td>
</tr>
<tr>
<td>-mac_pair=</td>
<td>-mac_pair=00:50:56:2E:AB:A0/00:0C:85:BD:08:80</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:7F:FF:FF</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>-regex=</td>
<td>-tcp=22</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></td>
<td>-tcp=80</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-tcp=25901 -and -tcp=25903</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-tcp=63268</td>
<td></td>
</tr>
<tr>
<td>-tcp_pair=</td>
<td>-tcp_pair=63268/25901</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></td>
<td>-tcp_pair=25901/25903</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-tcp_pair=3389/3391</td>
<td></td>
</tr>
<tr>
<td>-tcp_range=</td>
<td>-tcp_range=0/5000</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</td>
</tr>
<tr>
<td>Building block</td>
<td>Examples</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-udp=</td>
<td>-udp=53</td>
<td>non-factor for this building block; the filter looks for a pair of ports regardless of source or destination.</td>
</tr>
<tr>
<td></td>
<td>-udp=88</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-udp=26000 -and -udp=61001</td>
<td></td>
</tr>
<tr>
<td>-udp_pair=</td>
<td>-udp_pair=63240/27015</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></td>
<td>-udp_pair=49501/42</td>
<td></td>
</tr>
<tr>
<td>-udp_range=</td>
<td>-udp_range=27901/27910</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></td>
<td>-udp_range=27030/27000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-udp_range=0/1023</td>
<td></td>
</tr>
<tr>
<td>-vlan=</td>
<td>-vlan=101</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>-vlan=101 -and -vlan=102</td>
<td></td>
</tr>
<tr>
<td>(space character)</td>
<td>-tcp=80 -tcp=8080</td>
<td>Use this to denote a logical OR statement. Use this to include more items and broaden the scope of your filter.</td>
</tr>
<tr>
<td></td>
<td>(TCP port 80 -OR- TCP port 8080)</td>
<td></td>
</tr>
<tr>
<td>/ (forward slash)</td>
<td>-ip_range=10.0.36.1/10.0.36.255</td>
<td>Use this to denote a value range or any pairs. Do not add a leading or trailing space character to the forward slash.</td>
</tr>
<tr>
<td></td>
<td>(Any IPv4 address between 10.0.36.1 and 10.0.36.255)</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6: Decodes

When you are working with packets or need to open a packet capture, the decoding tools are what you use. Customize your packet view settings and be able to search packet payload, process NetFlow data, or even replay a packet capture.

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 Analyzer 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 (page 82) before continuing. Also, that section describes how to decode a real-time packet capture, while this section does not.

Note: 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 (page 118).

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

1. Click the File tab, and click Open > Local Packet Captures > Load and Analyze.
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.

**Tip!** Are you seeing duplicate packets? See .

After completing this task:

See *Using the Decode pane (page 110)* 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
- CAP
- DMP
- ENC
- FDC
- PCAP
- PCAPNG
- TRC

For information about the formats Observer can save packet captures to, see *Saving packet captures (page 80)*.

---

**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)

**Note:** 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.

**Tip!** Create a probe instance just for analyzing packet captures that you load into Observer. 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 the following:

1. Click the File tab, and click **Options > Fallback Instance**.
2. Select a probe instance with settings you think are similar to the capture adapter used to capture the buffer.

### Private key locations per server

Private key locations differ from application to application.

#### 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 (page 102).

#### 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 Encrypted private key file (page 103).

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):

```plaintext
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 (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):

```bash
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.

### 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-----
MIICXgIBAAKBgQD7uhNymd6WCORqH0rp5zs4FEwCX2JrKtm0dmTf44SVaGvFLFl
vakeOYP/sFs4aa2uONPcbfa2s3IzZWum4aCvqnvb8211+13VcdyR+2SRx9Gmbu
SnoL/6FI8m+C0ghq6g0IolTAJnY+MOEC2bwbMykz1jPVUOXEc9EG0A0Q1DAQAB
AoGAFQOyWEVMQpW2NW6YXnJKxVbGcZrPiDrWfCo/ITXhYUt12I47QLd+ni
-----END RSA PRIVATE KEY-----
```

### 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...
JHQ80UpDeBFm9h2jZSmugxdq0a2q/MiX43Xa4Es6nKmzu90I/ZfpIdAHi8gwtsD
m5bQRIX9AXeIry+0tG2ibUaphQEv995FWUsbB9NdVumsqykmMXSwND7ktkB
i0/VVSAAD9bV3db15nbMwnPG+YC3S90GAk4ZRiqrHRQ94f/2ZAvP8kV91lwCmX6
swF1NBLGuKFllJ9qkyr+0QQqulrAy2AB2UThGCJJetELFtV4mLmIAhDgDICUpqJp==
-----END RSA PRIVATE KEY-----
```

### Decoding encrypted network traffic

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. (Supported Cipher Suites)

**Prerequisite:** Observer Expert or Observer Suite

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.

**Note:** 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 Observer Management Server (OMS) (if you own it), so each Observer installation wanting to decrypt a stream must have a local copy of the private key.

**Note:** If you are decrypting network traffic using a private key via a SafeNet HSM card and that card is located on a OMS server, you must provide the slot number under “Use SSL RSA Private Key From SafeNet HSM Card on OMS” seen in Figure 24 (page 105).

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 OMS.** This is the most secure option. OMS 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 OMS, OMS 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 OMS, 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. Click the File tab, and click **Options > Fallback Instance**.
2. Choose 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** (page 101).
3. Click the File tab, and click **Open > Local Packet Captures > Load and Analyze**.
4. Navigate to the capture file you want to load, and select it.
5. Click Open. The capture file loads into Observer and you arrive at the Decode and Analysis tool.
6. 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.

7. Right-click the encrypted conversation and select Decrypt SSL Conversation. The SSL/TLS Decryption Parameters dialog appears. Figure 24: Provide the location of your private key here

8. Provide the location of your private key file.

9. (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 (page 147)** for more information.

10. 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. Click the File tab, and click Options > Fallback Instance.
2. Choose 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 (page 101).
3. On the Home tab, in the Capture group, click Configuration > Packet Capture.
4. Click the Decode button. The Decode and Analysis window appears.
5. Click the Decode tab, then choose Tools > Process NetFlow or sFlow data. The Select Data Source window appears.
6. Choose the data source you want to process.
7. (Optional) Change your ToS/QoS settings if necessary.
8. 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., Observer 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.

Replaying a packet capture

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.

Prerequisite(s):
Classic mode (page 34) must be enabled.

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.

Note: Replaying a packet buffer is not the same as stream reconstruction.
For stream reconstruction, see Reconstructing TCP data streams (page
128).

To replay a packet capture:
♦ On the Classic tab, in the Tools group, click **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. On the Home tab, in the Capture group, click **Configuration > Packet 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 13 (page 108).

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

### Table 13. 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 (page 129).</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>
</tbody>
</table>
### Menu option | Description
--- | ---
Reconstruct Stream | Reconstructs the TCP stream and any files or other data objects exchanged. See [Reconstructing TCP data streams](page 128).
Decrypt SSL Conversation | Shows you the decrypted SSL conversation if you have the SSL key.
Decrypt TACACS+ Conversation | Shows you the decrypted TACACS+ conversation if you have the TACACS+ shared secret.
Previous/Next Packet in Conversation | Lets you follow a TCP conversation backward and forward in time.
Maximize Pane | Zoom in to the current pane (headers, decode, or hex window).
Packet List Color Setup | Displays the Color dialog.
Set Decode Relative Time Origin to Selected Packet | Resets timestamps.
Calculate Cumulative Bytes | Displays the byte count from the beginning of the capture (or the relative time origin) to the current packet.

5. For additional settings, choose **Settings > General tab**. These settings are described in Table 14 (page 109).

### Table 14. Expanded packet options

<table>
<thead>
<tr>
<th>Setting</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 checksum</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>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>
</tbody>
</table>
When loading a local buffer file, exclude expert packets from the display

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).

Bytes Per Row in Hexadecimal Display radio buttons

Choose 16 or 10 bytes per row.

Show decode list using radio buttons

Choose either fixed-point or variable space font.

Packet timing display resolution list

Allows you to select the packet timing display resolution.

### 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 (page 119).</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 (page 46).</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 (page 39).</td>
</tr>
</tbody>
</table>
Internet Observer

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 (page 39).

Application Transaction Analysis

Contains several tabs for the applications that Observer analyzes, including response time and statistics, URL statistics, FIX, and SQL.

For more details about Application Transaction Analysis, see Understanding Application Transaction Analysis (page 160).

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 (page 57).

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 Examining your network traffic with forensic analysis (page 298).

Access Point (AP) Statistics

Shows wireless access point statistics. This is similar to Viewing wireless access point statistics (page 42).

Fibre Events

Shows details related to your Fibre traffic.

Figure 25: Decode tab

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 sizable 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 (page 108).

### Saving a packet capture

1. **On the Home tab, in the Capture group, click** Configuration > Packet 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>First packet</th>
<th>Allows you to set the first packet in the capture buffer to be saved to the file. By default, this is packet 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last packet</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>Save as button</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>Append packets to existing file</td>
<td>When selected, allows you to add packets to the existing file.</td>
</tr>
<tr>
<td>Recombine ATM Packets</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>
</tbody>
</table>
Store alias names inside file | 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.

Save Partial Packets | 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.

Replace hardware address in all saved packets | 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 (*) 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.*
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.

Decrypt 802.11 WEP Encrypted Packets | If checked, you can select from several preconfigured WEP key profiles. The profiles themselves are configured as part of 802.11 setup.

Decompress FRF.9 compressed packets | If you have captured frames from a VIAVI 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.

Searching for a specific packet

1. On the Home tab, in the Capture group, click Configuration > Packet 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 15 (page 114) choose how you want to search the capture buffer.
Table 15. Searching a packet capture

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw Packet Data</td>
<td>Searches the entire raw (i.e., not decoded) packet for the given string.</td>
</tr>
<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. On the Home tab, in the Capture group, click **Configuration > Packet Capture**.
2. Click the **Decode** button.
   - The **Decode and Analysis** window appears.
3. Ensure you are on the **Decode tab**, then choose **Tools > Post Filter**.
4. Select your filter(s) and click **OK**.
   - The filtered decode appears.

For more details about the post-capture filters and for a faster filtering method, see **Post-filtering your packet captures (page 94)**.

Processing NetFlow or sFlow data

1. On the Home tab, in the Capture group, click **Configuration > Packet 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.
Packet View Settings

The Packet View Settings window is used for customizing the packet decode pane. Packet View Settings is located at Live > Packet Capture, and then click Decode > Settings and then.

Figure 26: Packet View Settings

Configure SNMP MIBs

The Configure SNMP MIBs tab displays all available compiled MIBs. Any selected are used for decoding SNMP traffic and displaying any relevant traps in packet captures.

General

The General tab controls how frames and packets are displayed in the decode pane.
<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto determine dynamic protocols by bit patterns</td>
<td>Designates a protocol as dynamic if that behavior can be determined.</td>
</tr>
<tr>
<td>Decode packets with bad checksums</td>
<td>Decodes packets that fail CRC checks.</td>
</tr>
<tr>
<td>Expand 2nd level trees</td>
<td>Auto-expands the tree view at the second folds.</td>
</tr>
<tr>
<td>Expand 3rd level trees</td>
<td>Auto-expands the tree view at the third folds.</td>
</tr>
<tr>
<td>Expand 4th level trees</td>
<td>Auto-expands the tree view at the fourth folds.</td>
</tr>
<tr>
<td>Mark packets in the same conversation (shown as (c) before a packet number)</td>
<td>When a packet is selected, all packets in the conversation are visually identifiable by a lowercase 'c'.</td>
</tr>
<tr>
<td>Set focus on the last packet during live packet capture</td>
<td>The latest packet to arrive is always in focus and auto-scrolls the window.</td>
</tr>
<tr>
<td>Show filter name window before automatic filter creation</td>
<td>Provides the opportunity to name your new filter before creating a filter using the right-click menu.</td>
</tr>
<tr>
<td>Show full duplex 'Port' (or 'Link' and 'DCE/DTE') parameters</td>
<td>Port information is displayed when using a Gen3 capture card.</td>
</tr>
<tr>
<td>Show preview of summary content text</td>
<td>Displays a preview of summary content.</td>
</tr>
<tr>
<td>Use EBCDIC for displaying SNA data</td>
<td>Use Extended Binary Coded Decimal Interchange Code (EBCDIC) for displaying legacy IBM Systems Network Architecture (SNA) data.</td>
</tr>
<tr>
<td>Use EBCDIC for all data</td>
<td>Instead of ASCII, use Extended Binary Coded Decimal Interchange Code (EBCDIC) for displaying data.</td>
</tr>
<tr>
<td>When loading a local buffer file, exclude expert packets from display</td>
<td>Hides any captured Expert Information Packets when viewing a local buffer file.</td>
</tr>
<tr>
<td>Enable type script filters</td>
<td>Allows filter creation by command-line.</td>
</tr>
<tr>
<td>Bytes per row in hexadecimal display</td>
<td>Sets how many bytes per row are shown. Depending on your preference, one may be easier for locating specific offsets.</td>
</tr>
<tr>
<td>Show decode list using</td>
<td>Sets the font display style.</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Packet timing display resolution</td>
<td>Sets the precision of time stamps displayed. These options do not affect any data.</td>
</tr>
<tr>
<td></td>
<td>1 millisecond</td>
</tr>
<tr>
<td></td>
<td>1 microsecond</td>
</tr>
<tr>
<td></td>
<td>1 nanosecond</td>
</tr>
<tr>
<td>OUCH version</td>
<td>Sets the version of the NASDAQ trading OUCH protocol.</td>
</tr>
<tr>
<td></td>
<td>Auto-determine</td>
</tr>
<tr>
<td></td>
<td>v 4.0</td>
</tr>
<tr>
<td></td>
<td>v 3.1 and prior</td>
</tr>
<tr>
<td>MPEG transport stream type</td>
<td>Sets which transport stream type is used when decoding.</td>
</tr>
<tr>
<td></td>
<td>MPEG-2 Part 1</td>
</tr>
<tr>
<td></td>
<td>DVB</td>
</tr>
<tr>
<td></td>
<td>ATSC</td>
</tr>
<tr>
<td></td>
<td>ISDB-T</td>
</tr>
</tbody>
</table>

**Protocol Colors**

The **Protocol Colors** tab configures the text and background colors used for specific protocols. If selected, the protocol is colored accordingly. If cleared, the protocol is not colored accordingly.

**Protocol Forcing**

The **Protocol Forcing** tab forces recognition of unknown protocols by assigning each a custom offset.

**Summary**

The **Summary** tab sets the information shown in the summary column of the decode window.

**TCP/UDP/SCTP Application Colors**

The **TCP/UDP/SCTP Application Colors** tab configures the text and background colors used for specific applications. If selected, the application is colored accordingly. If cleared, the application is not colored accordingly.
Chapter 7: Expert Analysis

Expert analysis events can tell you if something is wrong with the network, based on thresholds you configure. Expert analysis also allows you to use or view server analysis, time interval analysis, TCP stream reconstruction, response time and network delay calculations, and connection dynamics.

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 (page 121)
- Configuring expert thresholds (page 132)

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. On the Home tab, in the Capture group, click **Configuration > 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 16 (page 120) to see the variety of actions you can perform in Expert Analysis.

Table 16. 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 (page 123).</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.</td>
</tr>
</tbody>
</table>

The ICMP Expert shows ICMP events that have the status OK, marginal, and critical (green, yellow, red). 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...
### 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 (page 82) for more information.

To configure global settings for Real-Time Expert, complete the following steps:

1. On the Home tab, in the Capture group, click **Configuration > Packet Capture**.

<table>
<thead>
<tr>
<th>Tab group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection #2 is not critical, Observer discards connection #2 and keeps #1.</td>
<td>IPX Events 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>IPX Events</td>
<td>NetBIOS Events 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>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>
<td>VoIP and Videoconferencing Shows a summary of VoIP activity and call quality statistics. For more details, see Collecting VoIP or video conferencing trending data (page 175).</td>
</tr>
<tr>
<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>
<td>Wireless Events 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>Shows a selected conversation graphically, illustrating inter-packet delay as a spacing between packets. See Using Connection Dynamics (page 129).</td>
<td>Connection Dynamics Shows a selected conversation graphically, illustrating inter-packet delay as a spacing between packets. See Using Connection Dynamics (page 129).</td>
</tr>
<tr>
<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 (page 128).</td>
<td>Reconstruct Streams 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 (page 128).</td>
</tr>
<tr>
<td>Allows all of the captured TCP and UDP data to be dumped and viewed in a raw format.</td>
<td>TCP/UDP Dump Allows all of the captured TCP and UDP data to be dumped and viewed in a raw format.</td>
</tr>
<tr>
<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 (page 124).</td>
<td>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. See Using Time Interval Analysis (page 124).</td>
</tr>
<tr>
<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 (page 125).</td>
<td>Server Analysis 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 (page 125).</td>
</tr>
<tr>
<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 (page 126).</td>
<td>What-If Analysis 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 (page 126).</td>
</tr>
</tbody>
</table>
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 (page 132)**.

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 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.

### Network delay calculation

Network delay is calculated using the SYN - SYN/ACK - ACK packets. If you are not seeing any SYN, SYN-ACK and ACK packets, network delay cannot be calculated.

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 the server receives this ACK from the client indicates the **client network delay**. This is shown in [Figure 30 (page 123)](#).
Response time calculation

Response time is calculated using the time difference between data packet request to data packet response. Response time is not calculated with SYN, SYN/ACK, or ACK packets.

There is one circumstance where SYN-ACK is used for calculating client response time. The very first client response time is calculated by measuring the time difference between the server SYN-ACK and the client’s first data packet. In all other circumstances, the time between data request and data response is used for calculation, as shown in Figure 31 (page 123).

Figure 31: Response time calculations

Response Time is calculated from the time difference between data packets, and never SYN or SYN-ACKs.

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 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

With End-to-End Analysis 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.

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.

Note: End-to-End Analysis does not support MultiHop Analysis. For that you must use the MultiHop Analysis feature. See Using MultiHop Analysis (page 133).

To configure end-to-end analysis, complete the following steps:

1. Ensure you have two saved capture files to compare.
2. On the Home tab, in the Analysis group, click Server Analysis.
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.

---

**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.

**Note:** 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:

<table>
<thead>
<tr>
<th>DAAP (iTunes sharing)</th>
<th>FTP</th>
<th>HTML</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>IMAP4</td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>RTSP (streaming audio/video)</td>
<td>Shoutcast (streaming audio)</td>
</tr>
<tr>
<td>SMTP</td>
<td>Telnet</td>
<td>WMPNSS (Windows Media Player sharing)</td>
</tr>
</tbody>
</table>

**Note:** 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. 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 .
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 display and choose Format from the pop-up 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 Connection Dynamics

Connection Dynamics show a selected conversation graphically illustrating the inter-packet delays as 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 blue. At the bottom of the screen (above the lower tabs Expert Analysis, Decode, Summary, and others) more detailed information for that packet is shown. In general, the information has abbreviated titles:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( S^1 )</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>( A^1 )</td>
<td>Acknowledgment Number</td>
</tr>
<tr>
<td>( EA^1 )</td>
<td>Expected Acknowledgment Number. This value is calculated by Observer and is not part of any byte within the TCP header.</td>
</tr>
<tr>
<td>( W )</td>
<td>Window Size</td>
</tr>
<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>
</tbody>
</table>
ExpAck | Expected Acknowledgment Number
---|---
Ack | Acknowledgment Number
Wnd | Window Size
Port | Port Number
AbsoluteTime | Absolute Time
TSN | Transmission Sequence Number
DupTSN | Duplicate TSN detected. This value is reported by the SACK packet.
GapACK | Gap in TSN sequence detected. This value is reported by the SACK packet.

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.

♦ Blue – The selected packet.
♦ Green (Dark) – One of these:
  • Default – Expected packet data.
  • SCTP SACK Gap ACK – Indicates that gap ACK blocks were found.
♦ Magenta - Application.
♦ Magenta (Dark) – 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.
♦ Orange (Dark) – 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.

♦ Red – One of these:
  - Retransmitted packet (shortened to “Retrans”). This is based on Observer seeing two packets with data having the same sequence number.
  - Reset. The RST flag is set and the conversation abruptly ended. It may have ended for any number of reasons, including the port not being open or the intended service is not running. Reset packets may also be considered part of an RST attack.

♦ Red (Dark) – 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.

♦ Red (Medium) – 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).

♦ Yellow – One of these:
  - 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.
  - 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.
  - SCTP SACK Dup TSN. Observer sees a duplicate TSN in the SACK chunk.

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.

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.

Note: This section assumes you are familiar with creating packet captures and the packet capture window in general. See Capturing network traffic (page 82).

To configure expert thresholds, complete the following steps:

1. On the Home tab, in the Capture group, click Configuration > Packet Capture.
2. Click the Decode button. The Decode and Analysis window appears.
3. Ensure the Expert Analysis tab is selected.
4. Click the Expert Thresholds button. The Expert Thresholds (OSI Model) window appears.
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 (page 121).
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 (page 138) or call the support team if you encounter issues specific to your network environment.

**Tip!** VIAVI 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 (page 82) for details.
Note: 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. On the Home tab, in the Analysis group, click **MultiHop Analysis**.

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.

   Figure 35: The Edit Segment File dialog
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 (page 139).

8. Click **OK** to confirm this segment's inclusion.

9. Repeat step 4 through step 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 step 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.

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.

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 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 (page 133)—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 (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. On the Home tab, in the Capture group, click Configuration > Capture Multiple.

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.

| IP Address + IP ID (Port mapped) | This option is best for networks that implement Network Address Translation (NAT) firewalls between segments. |
### 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 were the captures? and 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.
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.

**Tip!** 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.

**Note:** The following steps assume you have already loaded two or more segments into MultiHop Analysis. See Using MultiHop Analysis (page 133) and Quickly using MultiHop Analysis (page 135).

To troubleshoot synchronization errors, navigate to the user offset values by completing the following steps:

1. On the Home tab, in the Analysis group, click **MultiHop Analysis**.
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.

**Tip!** 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.

**Note:** The following steps assume you have already loaded two or more segments into MultiHop Analysis. See Using MultiHop Analysis (page 133) and Quickly using MultiHop Analysis (page 135).

To use IP mapping in MultiHop Analysis, complete the following steps:

1. On the Home tab, in the Analysis group, click **MultiHop Analysis**.
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: Alarms

Alarm can be made in Observer with triggers and actions. A trigger is an event on your network, while an action is what should happen or who will be automatically notified if necessary.

Configuring and using alarms

Using alarms, you can trigger pre-defined actions to occur when network conditions are met, making network management simpler and more predictable.

Alarms are a powerful and often overlooked feature of Observer. 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.

Alarms can be triggered on ATA response times measured in milliseconds (for example, 0.001).

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 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 36: Click the Alarm Settings button](image)

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** (page 141).

### 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 VIAVI and includes alarms for packet size, checksum, BitTorrent, 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** (page 119).

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 (page 144)
- Creating filter-based alarms (page 142)

5. (Optional) Select “Enable Probe SNMP trap generation” and configure up to 10 Observer or other network management systems (for instance, HP OpenView or IBM Tivoli) to receive the SNMP traps. By enabling SNMP trap generation here, an SNMP trap is generated even when no Observer 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 (page 140)** 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 38: Creating a new filter-based alarm](image)

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](page 144).

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:

- On the Home tab, in the Probe group, click **Setup > Reset SNMP Device Alarm Counters**.

To reset SNMP device alarm counters for all SNMP devices:

- On the Home tab, in the Probe group, click **Setup > Reset All SNMP Device 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:

**Note:** By default, Observer uses the same alarm actions for all enabled individual alarms. If, instead, you want to configure independent alarm
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 39: Independent alarm actions can now be customized.

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.

**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.
Learn about the web certificate trust model and how probe instance communication is encrypted by it. Also read about how to use Observer with regulation compliance and end-user and institutional privacy and security in mind.

Security, privacy, and regulatory compliance

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.

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)

**Tip!** Observer is compatible with hardware security modules that comply with the Federal Information Processing Standards (FIPS) number 140. See [Decoding encrypted network traffic](page 103) 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 Observer 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.

### Configuring user accounts for secure access

If you want to create and use user accounts, set probe permissions, or use third-party authentication like Active Directory, OMS is required.

If you are using OMS to control user accounts, you must control the accounts from the OMS interface. See [Understanding user accounts](the OMS User Guide) for more details.

### 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 locally either before or after the initial capture is made. Post-filtering is not possible from the GigaStor Control Panel, from local probe instance redirected to another system, or from remote probe instances. 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](page 79).
To create a filtered packet capture fit for sharing, ensure the full packet capture is loaded in Observer then:

1. On the Home tab, in the Probe group, click Filters > Configure Software Filter.
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

Packet headers may contain the most useful information because they contain routing information and protocol details. You can discard the packet payload for more efficient troubleshooting.

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

1. Choose Configuration > Packet Capture > Settings > Capture Options.
2. Enable Capture Partial Packets (Bytes).

![Packet Capture Settings](image)

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 at rest**

Captured data at rest can be encrypted using the 256-bit Advanced Encryption Standard (AES) algorithm. This significantly increases the security of your at-rest data.

**Prerequisite(s):**

- You must have a special Observer license to enable and use this feature. There is no extra charge for the license.
- You must have a GigaStor hardware appliance. This feature is not available to GigaStor Software Edition. See the differences in software and hardware (page 272) offerings for GigaStor.

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 Observer.

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. The RAID hardware is responsible for the encryption, and the data is encrypted before it is written to disk.

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 VIAVI 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 the Figure 42 (page 151) image.

Figure 42: Areca RAID application

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>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume RAID Level</td>
<td>Raid 5</td>
</tr>
<tr>
<td>Greater Two TB</td>
<td>64bit LBA</td>
</tr>
<tr>
<td>Volume Support</td>
<td>Foreground Initialization</td>
</tr>
<tr>
<td>Volume Initialization Mode</td>
<td>Foreground 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 Background Initialization, you may use your GigaStor, but it will take significantly longer to complete and performance will be negatively affected.</td>
</tr>
<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>


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.

10. Click Generate Key and save the key file in a secure location following your organization’s security policy.

- When rebooting, the system needs access to key in order to unlock the drive. This is the key necessary to write to and read from the RAID volume.
- Observer will not open unless it can find the key. Without the key present neither packet capture nor packet analysis can occur. 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.
11. Close Observer until the rest of this procedure is complete.
12. 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).
13. Repeat this process for each RAID volume for your GigaStor.
14. Open Observer.

Understanding the certificate trust model

The certificate trust model allows Observer Platform products to securely communicate using TLS encryption. It also provides resistance to man-in-the-middle attacks by requiring administrator intervention when a known certificate has changed.

All product-to-product communication is encrypted by default using SHA2. A web of trust between Observer Platform products is created by requiring certificates from each participating software application. The main benefit is that this ensures encryption of communication (page 154) between all parts of the Observer Platform.

Each software application owns a unique certificate. This certificate is automatically created during the first installation of an Observer Platform application, for example, Observer Apex. The unique application certificate is labeled Local when viewed from inside that software application. Upgrading to newer software versions does not create a new certificate, so no certificate maintenance is typically needed. However, uninstalling and reinstalling (fresh installs) creates a new certificate. The new certificate will be automatically rejected by other products that had a pre-existing association with the asset ID of the reinstalled software.

The first time two products communicate, each checks to see if they have the certificate for the asset ID of the other software application. If they do not, then certificates are exchanged, marked Trusted, and associated with the asset ID of the participating device. This enables the “easy configuration” model. After an association is made, each application will expect to see the same certificate (to remain trusted) when communicating.

Note: Prior to version 17 of the Observer Platform, encryption was available but not enabled by default. This has changed to become the default out-of-the-box behavior in Observer Platform version 17 and later, and it also uses a stronger cipher suite.

Certificates are automatically rejected when trust cannot be verified. If a certificate is associated to an asset ID, and an inbound connection from that asset (determined by the asset ID) occurs using a different certificate, the administrator must inspect and manually accept the certificate because the certificate is in a Rejected state. A rejected certificate breaks the trust model, so any offending device(s) and software are banned from product-to-product communication until an administrator investigates and accepts the certificate.
Certificates can be manually rejected by administrators. In the event that product-to-product communication must be immediately severed because of an imminent threat or other security risk, an administrator can manually reject certificates.

How to view certificates

You can view every certificate that Expert Probe has collected. This information shows certificate trust state, certificate ID, fingerprints, last time seen, last network location, signature algorithm, and more.

To view certificates:

1. (Optional) Select a certificate and click Details to view its full details.

You successfully viewed the certificates that this installation of Expert Probe has collected.

Certificate details

<table>
<thead>
<tr>
<th>Certificate ID</th>
<th>Asset type</th>
<th>Asset ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Issuing time</td>
<td>SHA1 Fingerprint</td>
</tr>
<tr>
<td>MDS Fingerprint</td>
<td>Asset name</td>
<td>Last seen IP</td>
</tr>
<tr>
<td>Last seen time</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How to change the trust of a certificate

The trust of a certificate can be changed between trusted and rejected states. The certificate must remain trusted for communication to occur.

To change the trust of a certificate:

1. Click a certificate to select it.

You successfully changed the trust state of a certificate.

View the certificate details (page 154), such as the signature algorithm, to ensure it matches your expectations.

Certificates and how they are used

Certificates ensure secure communication between Observer Platform products. The certificates encrypt this communication and help you the maintain the authenticity of device communication.

Certificates use public key infrastructure (PKI) to encrypt all product-to-product communication using the Transport Layer Security (TLS) cryptographic protocol. The communications that are encrypted include, but are not limited to:

- Probe instance redirections
- Capture data transfers
- Trending data transfers
- All other data transfers

Note: The initial handshake between Observer Platform products is not encrypted.
Chapter 10: Network Trending

Network trending records statistical data over long periods for other Observer Platform products to consume and display, such as Apex. Learn about, configure, and ultimately use network trending to see how your network is performing over time.

Understanding the Network Trending tool

The Network Trending tool allows you to collect, store, and analyze network traffic statistics over long periods of time.

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 analyze 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>Observer Analyzer feature set</td>
<td>Real-Time Statistics</td>
<td>Packet Captures</td>
<td>Network Trending(^1)</td>
<td>NetFlow/ sFlow(^2)</td>
</tr>
<tr>
<td>------------------------------</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

2. NetFlow and sFlow probe instances behave differently than most other types.
3. Long-term is considered any duration lasting one hour or longer.

Within Network Trending there are two similar tools that server 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 at HTTP or SMTP). APA is used for statistics about Layer 4 of the OSI Model and ATA is for Layers 5-7.

### 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.

**Tip!** Each network trending file can grow to a maximum of 4 TB.

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.

### Understanding Application Performance Analysis

Application Performance Analysis (APA) is a feature of the Network Trending tool. Using APA allows you to monitor performance trends for any application, server, and client by primarily analyzing Layer 4 of the OSI Model.

**Prerequisite:** Observer Expert or Observer Suite

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.

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 described in. Response times are calculated by actual data packets, not SYN or SYN-ACKs (see Response time calculation (page 123)), while network delay times are calculated exclusively with SYN and SYN-ACKs (see Network delay calculation (page 122)).

How to configure Application Performance Analysis

Application Performance Analysis is an always-on feature, meaning that Observer is always collecting metadata about the performance of numerous applications on your network. It cannot be disabled, only configured.

Prerequisite(s):

If you are unfamiliar with Application Performance Analysis, see Understanding Application Performance Analysis (page 156) before beginning.

The "always-on" nature of Application Performance Analysis is when both Observer and the probe are both at 17.2.0.0 or later. In certain circumstances your Observer may not match the version of your probe. This table describes what happens in those situations.

| Observer 17.2.0.0 and newer | Probe 17.2.0.0 and newer | Always on. Cannot be disabled. |
| Observer 17.1.1.4 and older | Probe 17.2.0.0 and newer | Probe collects and sends APA data to Observer even though the feature appears disabled in Observer. |
| Observer 17.2.0.0 and newer | Probe 17.1.1.4 and older | APA may be turned off. Since the probe collects the trending data and the probe does not have the new always-on functionality, therefore Observer can be configured to have the older probe honor the functionality it does have, which is the ability to turn APA on or off. |

1. On the Home tab, in the Capture group, click Network Trending > Network Trending.
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.
Figure 43: Configure your network trending settings here

**General tab**

The General tab allows you to set TCP retransmission settings and whether to track certain discovered servers.

### Table 17. General tab

<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</td>
<td>Enable this setting to track only defined servers. See Discovering server applications on the network (page 62).</td>
<td>Disabled</td>
</tr>
<tr>
<td>with associated ports defined in “Protocol Definitions and Server Application Discovery”</td>
<td></td>
<td></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>
Applications tab

The Applications tab allows you to configure TCP, UDP, and SCTP applications to monitor.

Table 18. 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 &quot;Track servers using the following protocols&quot; 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 a range or CTRL-click to select multiple items.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Subnet Ranges tab

The Subnet Ranges tab allows you define on what subnets your application servers are located.

Table 19. 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 to defined IP subnet ranges</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>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</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Understanding 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 times, errors, request and response trends for any supported server application protocol.

The server application protocols listed in Table 20 (page 160) can be configured for ATA. Most importantly, ATA can track and trend successes and failures of these client-server transactions, including response times at the application layer.

Table 20. 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>
</tbody>
</table>
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

**Tip!** If you are not sure why you would want to add any servers or applications to ATA, see Understanding the Network Trending tool (page 155). 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 44 (page 162) for an example.

Note: 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, the capture times are relative to the time in London, not New York. Be mindful of this during any analysis.

Figure 44: An example of Application Transaction 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. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.
3. Click the **Settings** button.
4. Select the **Application Transaction Analysis** group from the leftmost panel.
5. Ensure the Response Time Analysis grouping is selected, located at the leftmost portion of the window.
6. Click **Discover** or **Add**.
7. Ensure **Live Statistics** and **Network Trending Statistics** are selected.

Importing or exporting a server profile

You can import or export servers that you monitor from one Observer to another. This can save time and reduce typing errors if you have several Observer 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. On the Home tab, in the Analysis group, click **Application Transactions**.
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.

**Global Settings**

*Network Trending > Network Trending > Application Transaction Analysis*

On the **Global Settings** tab you can configure how response times are handled and whether URLs or SQL statement should be tracked.

**Figure 45: ATA Global Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track by URL</td>
<td>URLs can be tracked by specific URLs or by content types. You can also limit the level to which they are followed.</td>
</tr>
<tr>
<td>Track by SQL Statements</td>
<td>You can set the maximum statement length, track specific SQL statements, or track statements that include a specific command or token.</td>
</tr>
<tr>
<td>Ignore response time longer than</td>
<td>Transactions whose responses take longer than the specified value are ignored. The default is 10 seconds.</td>
</tr>
<tr>
<td>Collect distribution</td>
<td>A comma-separated list of values in milliseconds used as thresholds for statistics and graphs. A maximum of six values may be listed. A value may have up to three decimal places (for instance, <strong>1.500</strong>). The default values are: 5, 15, 50, 150, 500, 1500.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude specific URLs from Response Time Analysis</td>
<td>A list of URLs to ignore.</td>
</tr>
<tr>
<td>Server requests for DIAMETER</td>
<td>DIAMETER server requests will be monitored.</td>
</tr>
</tbody>
</table>

**ATA is reporting inaccurate values**

If ATA is showing data for **Response Time** or **Response Packets** and other columns that does not meet your expectations, check the **Ignore response times longer than setting**. It may be set too high or too low for your environment affecting the statistics reported.

ATA is based on statistical analysis. By default, Observer ignores any response time greater than 10 seconds. This is to present you with reasonable statistics while removing any outliers that take an exceedingly long time to respond. You can lower this value to exclude even more values (thereby showing reporting on a smaller, tighter data set) or increase the value to include a greater range of response times as necessary based on your environment.

1. **On the Home tab, in the Capture group, click Network Trending > Network Trending.**
2. **Select the server that is reporting data you believe to be inaccurate and choose Edit.**

Figure 46: Add/Edit Application Transaction Analysis Server
3. Change the **Ignore response times longer than** option to a value that meets your needs.

   This value is server specific, so you may need to change or adjust this value for each of your servers. It also means that servers can have different values that are appropriate to their environment and your expectations for it.

   The reported statistics should begin to match your expectations. If not, repeat this process until you find a value that works for you.

**Collecting network trending data**

To collect network trending data, complete the following steps:

1. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.
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 using it on-demand as described above, see [Configuring your network trending settings](page 166).

**Viewing network trending data**

Apex Lite, installed with your Observer application, allows you to view collected network trending data in a series of reports in your web browser.

To view collected network trending data:

- On the Home tab, in the Capture group, click **Network Trending > View Apex Reports**.

**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.

If you allow network trending data to accumulate without a deletion strategy, you could experience the following problems:

- The operating system drive runs out of free space (or free space becomes too low) and no new trending data is collected.
- System performance is severely degraded because not enough space is available to the Windows paging file to remain efficient, if it exists at all in your hardware configuration.
- If this Observer/GigaStor is feeding Observer Apex, Apex might not receive the latest trending data because Observer could no longer collect new network trending on the full disk drive.

**Tip!** Each network trending file can grow to a maximum of 4 TB.
By default, the trending files are kept for each trending instance in C:\Program Files\Observer\NetworkTrending. You can delete them using Windows Explorer.

Additionally, Observer can automatically delete old trending data for you when you set **Delete oldest trending data on the probe...** in **Network Trending > Network Trending** on the **Home** tab. Then choose **Settings > General** to find the option. When this option is set, you will virtually never need to worry about filling up the C: drive with too much network trending data. However, only the oldest two (2) files are deleted for each new trending file that is created. Because at least one new trending file is created each day, this means that each day when a new trending file is created, the two oldest network trending files are deleted. This is a net deletion of one (1) network trending file per day. The files are deleted at midnight UTC; this option is not configurable. (See the current UTC time and determine your offset.) You will want to set the amount of trending days retained to no more than you can store on the target disk drive. See How to determine disk space requirements for network trending (page 170).

The purpose of this design is to maintain disk write performance that might otherwise degrade if multiple, large deletions are made each day. Remember, you can delete trending files manually at any time from C:\Program Files \Observer\NetworkTrending, which is the default storage location. The automated tool operates with disk write performance as its highest priority—so it should be used—but if you are confident and wish to delete multiple network trending files manually through Windows, you can. Be aware that you risk negatively impacting the new, incoming network trending data being collected at the very same time as when multiple network trending files are being deleted through Windows Explorer.

If you are using Apex, you can safely delete the trending files after the data has been transferred to Apex. If you are not using Apex, 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.

**Note:** 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.

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 (page 167).**
2. Schedule the collection of data from those trending types—see Scheduling your network trending data collection (page 169).

3. Add specific servers to trend—Adding specific servers to network trending (page 171).

Choosing your network trending types

Trending types are categories of network traffic, and they loosely follow the OSI Layer model.

Trending data is saved to the operating system drive. Each mode requires a different amount of disk space based on data collected; however, all modes combined at running at maximum capacity could generate at most 1 TB of data per day.

To choose which network trending types you want to monitor, follow these steps:

**Note:** 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 (page 166).

1. On the Home tab, in the Capture group, click Network Trending > Network Trending.

2. Click the Settings button. The Network Trending Settings window appears. Change the Collection Settings.

Figure 47: Configure your network trending settings here

3. If you are using a NetFlow or sFlow single collector probe instance, you can use SNMP polling to automatically discover the NetFlow interfaces on your device, which will obtain one or more Interface Index, Interface Name, and Interface Speed values:
   
   a. Click SNMP Settings.
b. Configure your SNMP IP address and credentials so that you can poll the device, and click **OK**

c. Click **Edit Data Source Interfaces**.

d. Click **Retrieve Interface Names and Speed from Device**.

4. Click **OK** to save your changes.

<table>
<thead>
<tr>
<th>Trending type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Transaction Analysis Trending</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 Trending</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 Subnet Ranges Trending</td>
<td>The IP Subnet Ranges 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 Trending</td>
<td>The IPTV trending type allows you monitor multicast issues on your network specifically related to video. The streams can track UDP sequence numbers, packets, multiple protocol data units (PDUs) within a UDP packet, and stream type or ID.</td>
</tr>
<tr>
<td>Microburst Trending</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>
</tbody>
</table>
| Trading Multicast Trending      | The Trading Multicast trending type allows you 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
### Trending type | Description
---|---
VoIP and Videoconferencing Trending | 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.
Sampling divider | The sampling divider 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 .
Delete oldest trending data | 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 (page 165).
Use current filter | When selected, any filters that you applied to your probe instance are also applied to your network trending statistics.
1. NetFlow probe instances always use a sampling divider of 1.
2. Filtering is not available on NetFlow probe instances.

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 (page 169). You can import subnet ranges into network trending types using an ipsubnetrange file. See Structure of an .ipsubnetrange file (page 172).

### 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:

**Note:** 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 (page 166).

1. On the Home tab, in the Capture group, click **Network Trending** > **Network Trending**.
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 (page 171).

How to determine disk space requirements for network trending

Because network trending can consume a lot of disk space, you need to know how much disk space to reserve.

Network trending data consumes hard disk space. Depending on and your storage requirements for network trending data, the network trending data could fill that drive to full capacity—this is a problem. Therefore, determine your typical 24-hour data rate and how many days of trending data you want to retain. The result indicates how much storage space is required.

To determine the amount of space required to store your desired amount of trending data:

1. Determine your typical 24-hour data rate.
   
   **Example:** 15 MB or 20 GB.
   
   The *data rate* is amount of trending data collected in one 24-hour period.

2. Multiply your typical 24-hour data rate by the number of days you want to retain.
   
   **Example:** 15 MB x 365 days = 5.475 GB
   
   **Example:** 20 GB x 30 days = 600 GB

The result is the amount of hard drive space required to retain the trending data.

You can use the numbers you calculated to inform your decisions when deleting network trending data (page 165).

How to reduce the disk space consumed by network trending files

The size of your most recent network trending file increases whenever network traffic is seen. However, the file size is strongly affected by the volume of traffic (number of network connections), the network trending types you choose to track, and certain options within network trending settings. You can best reduce the disk space consumed by network trending files by limiting what you track.

Each network trending file is a summary of one day’s traffic as tracked by the Network Trending tool (page 155). In this way, the more network trending files you are able to retain in your storage directory (page 171)—without sacrificing all of your available disk space to do so—the more days of historical data can be transferred to Apex or viewed using Apex Lite.

Unless you want to rely on scheduled deletions of trending data (page 165) as your only disk space strategy, you can reduce the overall space consumed by network trending files by limiting what you track. This decreases the size of future network trending files, enabling you to retain more of them and for longer durations before deletions are necessary.
To reduce the disk space consumed by future network trending files, and your most recent in-progress file, perform any or all of the following steps:

- Decide if some network trending types are not useful to collect in your network environment, and turn them off.

  Choosing your network trending types (page 167)

- Set one or several options for Application Performance Analysis that limits tracking to protocols in the protocol list, server connections between defined subnets, or explicitly defined servers only.

  How to configure Application Performance Analysis (page 157)

By following any or all of these steps, you should see a reduction in the disk space consumed by future network trending files.

How to change where network trending is stored

Network trending data can be stored anywhere. By default, the trending files are kept for each trending instance in `C:\Program Files\Observer\NetworkTrending`.

The storage limits for the network trending data files are limited only by the hard drive space available. Your GigaStor license only limits how much packet capture data you may have; it has no effect on limits for storing network trending data. You may collect a limitless amount of network trending so long as your hard drive (or RAID) supports it.

1. Click the File tab, and click **Options > General Options**.
2. Click the **Folders** tab.
3. Change the **Network Trending Folder** to a new location of your choice.
   - We do not recommend pointing to networked directories or mapped drives.

Network trending data will be saved to its new location.

Given the potential volume of data stored by network trending, you may need to consider a management strategy to delete older files.

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 Understanding Application Transaction Analysis (page 160) 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 Understanding Application Transaction Analysis (page 160).

**Note:** 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 (page 166).

**Tip!** More information about Observer's address book can be found at Building and saving an address book (page 58).
Tip! If you have already created the server definition on a different Observer, you can import it here. See Importing or exporting a server profile (page 162).

1. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.
2. Click the **Settings** button. The **Network Trending Settings** window appears.
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.

**Structure of an .ipsubnetrange file**

An `.ipsubnetrange` file can be imported into, and exported from, various network trending settings. These files have a specific structure and allow subnet designations to be maintained outside of Observer. There is an expectation that such a file be “round tripped” back into Observer after changes are made.

Some limitations exist in how many subnets can be explicitly tracked for each network trending type. Explicitly tracked means that additional network trending statistics are measured for each defined subnet as a whole; however, these limitations do not influence how many subnets can be observed by Observer. These maximum tracked subnet ranges also means that your `ipsubnetrange` file(s) cannot have more entries than a network trending type supports. If you import an `ipsubnetrange` file having more entries than is supported by the target network trending type, only the first N-number will be successfully imported. These tracking limitations are as follows:

<table>
<thead>
<tr>
<th>Network trending type</th>
<th>Maximum tracked subnet ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Performance Analysis</td>
<td>4 subnet ranges</td>
</tr>
<tr>
<td>Application Transaction Analysis</td>
<td>4 subnet ranges</td>
</tr>
<tr>
<td>IP Trending</td>
<td>128 subnet ranges</td>
</tr>
<tr>
<td>Microburst</td>
<td>16 subnet ranges</td>
</tr>
<tr>
<td>VoIP and Videoconferencing</td>
<td>16 subnet ranges</td>
</tr>
</tbody>
</table>

Because IP Trending supports the largest number of maximum tracked subnet ranges, its `ipsubnetrange` file structure is the one you should mimic when maintaining your list of subnet ranges. The file structure of IP Trending’s `ipsubnetrange` file can be imported into the subnet tracking of any other network trending type. Be aware that if you have a list of 128 subnet ranges in an `ipsubnetrange` file and import it into a different trending type than IP Trending, only its first four entries will be imported into Application Performance Analysis or Application Transaction Analysis respectively; only its first 16 entries will be imported into Microburst; and only its first 16 entries will be imported into VoIP and Videoconferencing.
This is an example of an `ipsubnetrange` file exported from the IP trending network trending type. The file extension must always be `ipsubnetrange` and the spacing between commas is can be space characters or tabs. The use and positions of commas in these examples is important. This is how the file is structured, and multiple examples are shown of the same file to examine different pieces of the whole.

**The version number of the file format is highlighted. Always keep this at version 1.**

```
1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0, 10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0, 10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0, 10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0, 10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0
```

**The number of entries in this file is highlighted. Change it to match your list length.**

```
1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0, 10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0, 10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0, 10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0, 10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0
```

**The "original" type of ipsubnetrange structure is highlighted. Keep as is.**

```
1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0, 10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0, 10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0, 10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0, 10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0
```

**The configurable name of this subnet entry is highlighted. Keep these short.**

```
1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0, 10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0, 10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0, 10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0, 10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0
```

**The IP version type of ipsubnetrange entry is highlighted. 1=IPv4, 2=IPv6.**

```
1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0, 10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0, 10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0, 10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0, 10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0
```

**The scope of the subnet range is highlighted. 0=one subnet, 3=analyze traffic between two subnets.**

```
1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0, 10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0, 10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0, 10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0, 10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0
```

**Network speed in bits per second for this subnet is highlighted. Change accordingly, or set to '0' to use defaults.**

```
1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0, 10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0, 10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0, 10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0, 10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0
```
The first address of the first subnet range is highlighted.

1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0,10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0,10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0,10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0,10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0

The last address of the first subnet range is highlighted.

1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0,10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0,10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0,10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0,10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0

The first address of the second subnet range is highlighted.

1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0,10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0,10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0,10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0,10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0

The last address of the second subnet range is highlighted.

1,4,4 (IP Trending)
subnet 16 1,0,100000000,0,0,0,0,10.0.16.1, 10.0.16.254, 0.0.0.0, 0.0.0.0
s48 to 64 1,3,100000000,0,0,0,0,10.0.48.1, 10.0.48.254, 10.0.64.1, 10.0.64.254
subnet 64 1,0,100000000,0,0,0,0,10.0.64.1, 10.0.64.254, 0.0.0.0, 0.0.0.0
subnet 23 1,0,250000000,0,0,0,0,10.1.23.1, 10.1.23.254, 0.0.0.0, 0.0.0.0
Chapter 11: VoIP and Teleconferencing

Observer has dedicated tools for monitoring the quality of VoIP and teleconferencing traffic. These tools require some unique settings and configuration. You can also learn about VoIP best practices.

Collecting VoIP or video conferencing trending data

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.

Tip! You can learn more about Observer’s network trending tool by seeing Understanding the Network Trending tool (page 155)—a wealth of information is provided there should you need it.

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:

1. On the Home tab, in the Capture group, click Network Trending > Network Trending.
2. Click the Settings button.
Collecting VoIP or video conferencing trending data

Figure 48: The Network Trending Settings window

The **Network Trending Settings** window appears.

3. Select the **VoIP and Videoconferencing Trending** data collection type.
4. Select the desired VoIP trending types from the two boxes directly below **VoIP and Videoconferencing Trending**.
5. 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 (page 180).

You can start the actual collection process by following the instructions at Collecting network trending data (page 165).

**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. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.
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

Observer constantly monitors network conditions to calculate the R-factor, and allows you to customize the non-network impairment factors such as room noise, loudness rating of the telephone, etc.

Prerequisite(s):
Either start a packet capture or import a capture file.

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.

Tip! 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 (page 100)—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 (page 82).

1. On the Home tab, in the Capture group, click Configuration > 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 (page 180).

6. (Optional) Click the **Expert Threshold** button to view or change settings that determine VoIP-specific decode settings.

By using MOS score and R-factor when looking at your VoIP environment, you can determine if your users are experiencing poor call quality. 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 21 (page 178) lists the abbreviations used in the VoIP Events tab for various packet types.

<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 Selecting a time frame to analyze (page 292).

**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. An 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 Setting the GigaStor general options.

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
--- | ---
A --> (ANY) | Extract call(s) where pattern A is in the SIP “From” field.
A <-- (ANY) | Extract call(s) where pattern A is in the SIP “To” field.
A <-> (ANY) | Extract call(s) where pattern A is in the SIP “From” or “To” field.
A <-> B | Extract call(s) where pattern A and pattern B is in either the SIP “From” or “To” field.
A --> B | Extract call(s) with pattern A in the SIP “From” field and pattern B is in a SIP “To” field.
Call-ID | Extract call(s) with the specified pattern in the SIP “Call-ID” field.

5. (Optional) Enable one or more search pattern modifiers:
   - Use regular expression(s)—Perl 5 regular expressions. For details and examples, see
   - 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 Mining data from your GigaStor (page 289).
   - 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.

**VoIP MOS**

The Mean Opinion Score (MOS), as estimated using the E-model. By using the E-model to estimate MOS, provides you with a highly accurate prediction of how a current user would rate the voice quality of your VoIP network. Examining the Burst Percentage and Burst Density metrics can often give you a clue as to what is driving MOS scores down.

Note that the traditional method of obtaining a Mean Opinion Score is to survey actual users listening to sample sentences, rating audio quality from 1 (poor) to 5 (excellent). The E-model was developed because this type of testing is simply not practical for most VoIP installations, and in any case cannot be updated in real time.

**VoIP R-Factor**

The E-model uses cumulative measurements of impairments to estimate what their effect would be on users’ perception of quality. In its simplest form, the E-
model subtracts the impairments from the R-factor to come up with a score of 0 to 100:

\[ R = Ro - Is - Id - Ie + A \]

Where \( Ro \) is the undistorted original signal (a constant of 100), \( Is \) measures the distortion of the speech signal from the telephone hardware, \( Id \) measures network delay and jitter, \( Ie \) measures the signal degradation due to speech encoding. \( A \) adds the users’ typical expectations for the type of connection being used, accounting for the fact that people are willing to accept lower voice quality in exchange for some other benefit, such as the cost savings of DSL, or the mobility of wireless.

Observer constantly monitors network conditions to calculate the R-factor, and allows you to customize the non-network impairment factors such as room noise, loudness rating of the telephone, etc.

### Configuring network trending settings for VoIP or video conferencing

This section describes how to access the VoIP settings menu and guides you through its most noteworthy settings.

**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. 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. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.
2. Click the **Settings** button. The **Network Trending Settings** window appears.
3. Click the **VoIP and Videoconferencing** group tab.

Figure 50: 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.

**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 22 (page 181) for a list of noteworthy settings.

**Table 22. 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 23 (page 182) 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 24 (page 182).

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.

**Tip!** 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 23. 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 recommend leaving these at their default values until you have reason to change them.</td>
</tr>
<tr>
<td></td>
<td>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 24 (page 182).</td>
</tr>
<tr>
<td>Defaults button</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 24. 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>
<tr>
<td>G.723-1 Annex C</td>
<td>17</td>
</tr>
</tbody>
</table>
If you use this codec | Use this value...
---|---
G.726-16 | 40
G.726-24 | 25
G.726-32 | 7
G.726-40 | 2
G.728 | 7
G.729 | 15
G.729 Annex A | 20
G.729 Annex B | 20
G.729 Annex A & B | 20
G.729 Extensions | 20
IS11172 | 11
IS13818 | 11
GSM Full Rate | 20
GSM Half Rate | 23
BV 16K | 17
BV 32K | 17
VBD | 17
ILBC | 17
Speex | 17
IMA ADPCM | 17
LPC10 | 17
Telephony Event | 17
Audio Tone | 17
G.711 (A-law) with PLP | 17
G.711 (U-law) with PLP | 17

### 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 25 (page 183) for a list of noteworthy settings.

#### Table 25. Device IP Address options

<table>
<thead>
<tr>
<th>Setting(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP device list</td>
<td>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.</td>
</tr>
<tr>
<td>Add button</td>
<td>Clicking the Add button allows you to add VoIP devices to the list. See the list of device types in Table 26 (page 184).</td>
</tr>
</tbody>
</table>

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 26 (page 184).
Table 26. 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 27 (page 184) for a list of noteworthy settings.

Table 27. 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 28 (page 184) for a list of noteworthy settings.

Table 28. 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.

Tip! You can learn more about Observer alarms by seeing Configuring and using alarms (page 140)—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 51: Enable VoIP alarms here

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 (page 144) and Creating filter-based alarms (page 142).

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.

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.

![Jitter buffering and packet loss concealment](image)

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.

**Differences between Jitter (RTP) and Jitter (ms)**

Jitter is calculated in two different ways: the first uses Real Time Protocol (RTP) time stamps, and the second uses packet time stamps. When jitter is represented in milliseconds (ms), the calculation is made using packet time stamps and *not* RTP time stamps.

Observer performs this calculation on every packet. Jitter max is the highest calculated jitter observed. Jitter itself is the **latest** calculated jitter value (most recent). Also note that jitter requires a minimum of 16 packets before a value will be displayed in Observer.

Observer displays jitter values for both jitter calculation methods. This is how the numbers are created in Observer:

1. **Translate the packet time to RTP time units.**
   \[
   \text{packet rtp-based time} = \left(\frac{\text{packet time stamp in ns}}{1000}\right) \times \frac{\text{sampling rate in s}}{\text{million}}
   \]
2. This time is used to calculate the difference between this packet and the previous packet.
   \[ \text{packet time difference} = (\text{packet rtp-based time}) - (\text{previous packet rtp-based time}) \]

3. The jitter is then calculated exactly as the RTP specification describes using the RTP time stamps.
   \[ \text{jitter} = \text{jitter} + ((\text{packet time difference}) - \text{jitter}) / 16.0 \]

4. Then for the jitter in milliseconds (ms), the time is converted using the sampling rate.
   \[ \text{jitter ms} = \text{jitter ms} + ((1000 \times \text{packet time difference}) / (\text{sampling rate}) - \text{jitter ms}) / 16.0 \]

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.
VoIP terminology

This section describes common VoIP terminology. If you are new to VoIP networking or just need more information about a certain term, this section may help.

Table 29. 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</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Significance</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 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>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. Gap densities climbing over time, coupled with low-density, short-duration &quot;burstiness&quot; can mean the VoIP network is attempting to service too many calls given the available bandwidth.</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.</td>
<td>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:</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Significance</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>G.711</td>
<td>64kbps (no compression)</td>
<td>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>
</tr>
<tr>
<td>G.729</td>
<td>8kbps</td>
<td></td>
</tr>
<tr>
<td>G.723</td>
<td>6.3kbps, 5.3kbps</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 12: Reports

Observer can notify you of network events using email alerts, text messages, and even pager services.

Setting up email notifications

For Observer Analyzer to send 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. Click the File tab, and click **Options > General Options**.
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 notifications to email addresses. If you want to receive notifications as text messages on your mobile device, see **Setting up text message notifications** (page 192).

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 VIAVI 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.

**Note:** VIAVI 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. 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@vmobil.com">mobilenumber@vmobil.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.

**Note:** When a VIAVI application (except Observer Apex) starts, it also starts a separate Windows process called VIAVI Paging Service, which you can find in the system tray. After configuring the pager, verify the settings for the paging service match your needs. Choose **Tools > Program Options > Notifications**.

1. Click the File tab, and click **Options > General Options**.
2. Click the **Notifications** tab.
3. 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.
4. To view the initial pager configuration dialog, click the **Properties** button. The Paging Service Properties dialog will be displayed.
5. 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.
6. 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.

7. 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.

8. Enter the maximum message length for the pager.

9. Click the **OK** button.

10. Check the Apply advanced pager settings and click the **Advanced** button to display the Phone Pager Schedule dialog.

11. 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 (page 194) and Viewing the Paging Server logs (page 194).

---

**Sending a page**

After you have configured the paging server using the instructions in Setting up pager notifications (page 193), you can choose to send a page.

![Windows Taskbar icon](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 (page 193), 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.
Chapter 13: Probes and Probe Instances

Introducing Probes

Discover the basics of probes, probe instances and what type is right for you, and how probes work with switches.

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 Observer 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. 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 VIAVI 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 VIAVI 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 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 55 (page 196) 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 Observer anywhere on your network so long as it has TCP connectivity to the probe.

Figure 55: Typical network

What is a probe instance?

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.

Observer 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.

Table 30 (page 196) compares the features of active and passive probe instances with an Observer probe instance found on all non-GigaStor probes.

Table 30. Active vs. passive GigaStor instances and Observer probe

<table>
<thead>
<tr>
<th>Better suited for troubleshooting</th>
<th>GigaStor Active probe instance</th>
<th>GigaStor Passive probe instance</th>
<th>Observer Probe</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Better suited for data capture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Start packet capture</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Stop packet capture</td>
<td>X</td>
<td>X</td>
<td>X</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>X</td>
</tr>
<tr>
<td>Change directories where data is stored</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
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 a virtual adapter or a network adapter that has data coming to it that you want to capture. You can change whichever adapter a passive probe instance is bound to without affecting any active probe instance. By default a passive probe instance uses 12 MB of RAM. You can reserve more memory for passive probe instances if you wish.

**Caution:** 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 capture card 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 capture card adapter, the capture card’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.

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 56 (page 198) 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?

Software probes are an economical choice for many situations.

For companies that cannot invest in dedicated hardware probes, Observer Platform 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. VIAVI 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.

- 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 VIAVI.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Installed software</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>Sends entire buffer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarms</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trending</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Triggers</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wireless</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encrypts buffer transfer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Simultaneous multi-topology support</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Simultaneous users</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Supports multiple NICs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Use reserved memory outside of Windows</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Integrated reporting with Apex</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Able to switch between probe and analyzer mode</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Full-duplex</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MPLS (page 232)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NetFlow (page 267)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Port bonding (page 264)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### 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).

**Note:** 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.
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 57 (page 201) describes the two different ways that Observer runs.

![Figure 57: Windows protected memory, user memory, and reserved memory](image)

---

How a probe uses RAM

Chapter 13: Probes and Probe Instances | 201
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
- Statistics queue buffer
- Collected statistical memory

Network packets seen by Observer are passed to both the packet capture memory and to the statistics queue buffer. After a packet is processed by the statistics queue buffer, the statistical information is passed to the statistical memory. All packets in both the packet capture memory and the statistical queue buffer stay in memory until the buffer is full and the oldest packets are replaced by newer packets (using FIFO).

Figure 58 (page 202) shows what options in Observer control the size of various portions of memory.

Figure 58: How to resize various memory options

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.

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:

\[
\text{Network Speed} \times \frac{\text{Average Throughput (MB/second)}}{\text{Seconds of data storable in RAM}}
\]

**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.

\[
\frac{(\text{Traffic Level} \div 8 \text{ bit}) \times 3600 \text{ Seconds}}{1024 \text{ bytes}} \text{ Gigabytes per hour}
\]

For instance a fully utilized 1 Gb port (1 Gbps is 125 MBps):

\[
\frac{(125 \text{ MBps} \div 8 \text{ bit}) \times 3600 \text{ Seconds}}{1024 \text{ bytes}} \approx 54.93 \text{ GB per hour}
\]

**Running Observer without reserved memory**

Single probes cannot use reserved memory. By default, no memory is reserved for Observer if you install it on your own system.

**Prerequisite(s):**

- All versions of Observer Expert, Observer Suite, Expert Probe software, and Multi Probe software installed on your own hardware, unless modified.
- Single Probe software at all times
- NetFlow probes
Observer without reserved memory 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.

**Note:** This section does not apply to the GigaStor or other hardware products from VIAVI. They are properly configured at the factory.

**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.

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). This is a limitation of the Windows memory pool and the Windows operating system.

Single Probes, unlike Multi-Probes and Expert Probes, cannot use reserved memory because of their design. By default, 16 megabytes is available for the Packet Capture and Statistics Queue buffer. Single Probes have a maximum of 52 megabytes that can be assigned from the Windows memory pool. Because of the Windows memory pool constraint, Single Probes are limited to a Packet capture buffer maximum of 72 megabytes, assuming you set the Statistics queue buffer to its minimum (12 megabytes). The Statistics queue buffer maximum is 76 megabytes if the Packet capture buffer is set to 0 megabytes.

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:

- 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 (page 208) to help determine how to divide the memory.

Running Observer with reserved memory

Reserved memory helps Observer run more efficiently by dedicating memory for its exclusive use.

**Prerequisite(s):**
- Observer Expert
- Observer Suite
- Expert Probe software
- Multi Probe software

Observer uses reserved memory for packet capture and the statistics queue buffer. It is highly-recommended that you use reserved memory. (GigaStor appliances running Observer are preconfigured this way.) You must determine how you want Observer to be configured for your system.

**Caution:** Never change the reserved memory settings of VIAVI hardware unless VIAVI instructs you do so. Reserved memory settings should only be modified on non-VIAVI hardware, such as a desktop computer running 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.

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.

When reserving RAM for Observer you are taking RAM away from the operating system. Table 31 (page 206) shows how much memory is required by the operating system. Anything beyond this amount may be reserved for Observer.

<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 ¹</td>
</tr>
<tr>
<td>64-bit with 6+ GB RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>32-bit²</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 (page 208) to help determine how to divide the memory.

4. After reserving memory for Observer you must restart the system for the changes to take effect. 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 60 (page 207) 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 60: 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

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 hardware appliance, read this section, but also be sure to consider the information in Recommendations for the VIAVI capture cards (page 209).

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.

**Note:** 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.

For each probe instance determine:

♦ If you want to mostly capture packets, then allocate 90% of the reserved 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 reserved 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 reserved 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 VIAVI capture cards

There are capture card requirements and considerations if you are using a GigaStor appliance, as the appliance may have a Gen3 capture card or Gen2 capture card installed.

Here are some special configuration issues to consider when dealing with these capture cards:

♦ For either the Gen3 capture card or Gen2 capture card, you need a minimum of 100 MB allocated to the capture buffer of any probe instance that is bound to the capture card. Allocating less than 100 MB to a probe instance monitoring a VIAVI capture card may cause instability.

♦ If you are using any hardware accelerated probe instance, you must have at least 80 MB for both packet capture and the statistics queue buffer. No packets are captured if either or both are below 80 MB. 80 MB is the minimum, but consider substantially raising this amount. The more RAM that you can allocate to packet capture and statistics, the better your GigaStor probe will perform.

♦ When using multiple probe instances on a GigaStor, ensure that only one probe instance is associated with the capture card. (If you are using virtual adapters to monitor disparate networks, then you may have more than one active instance bound to the capture card.) For performance reasons, all other probe instances should be associated with a different network card.

If you feel a capture 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 Gen3 capture card or Gen2 capture card. This does not apply if the other probe instances are connected to a regular network card.)

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 (page 210).

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 Observer, they are saved to the probe.

- A scheduled capture can be causing a system slow down. Determine if any scheduled capture is occurring. On the Home tab, in the Capture group, click Live > Packet Capture and then Settings > Schedule.
- 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 the File tab, and click Options > General Options. Scroll to Startup and runtime settings and clear these settings, 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, on the Home tab, in the Capture group, click Network Trending > Network Trending. Then click 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 Observer has useful information to give you an idea of why the connection is failing.

Verify the following:

- The probe is licensed. See Licensing and updating (page 20).
- Check that the Observer Platform ports are open on the firewall and if traffic is actually passing through it. Observer uses these ports to communicate with the probe. See Ports used by Observer Platform v17 and later (page 27) or depending on your version. Check any local system firewall as well as any network firewall. See also the information in Suspected NAT or VPN issues (page 215).
- Check that the security certificates are trusted between the Observer and the probe. If the settings do not match, you might get a message that says “Probe redirection Error <IPAddress> Authentication Negotiation Error” or “Probe authentication failed <IPAddress>.” Either a certificate is untrusted by one of the assets or a certificate is pending your approval. In Observer, click Options > General Options and click the Security tab. Verify that the specific certificates are in a trusted state.
- The probe and Observer are within the same minor build range. See Upgrading the probe software (page 226).
- You can access the VLAN if the probe or Observer 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 step 7.
   - 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 step 7.
7. From the Local Area Connection Properties (step 5), choose Install > Protocol > Add > VIAVI – 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 Observer 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 (page 213) 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
C6500 (config-if) #switchport nonnegotiate
C6500 (config-if) #exit
C6500 (config) # monitor session 1 source interface fastethernet 0/2
C6500 (config) # monitor session 1 destination interface fastethernet 0/6

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 , 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 Observer 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
Chapter 14: Expert Probe Software

Observer needs a probe to capture network traffic. The probe can be local to Observer Analyzer or remote.

How to install or upgrade the software

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

Prerequisite(s):

♦ An administrator account is required to install and run any version of Observer or probe software except Observer Expert Console Only (ECO). Observer ECO requires an administrator account just for installation; a standard user account can be used for running Observer ECO.

♦ 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. VIAVI sells hardware probes that are guaranteed to keep up with heavy loads. See the Observer Platform 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 (page 256).
1. Ensure your system meets the minimum requirements.
   See Minimum and recommended system specifications (page 17).

2. Choose one of the following:
   • How to install all versions (page 19)
   • How to upgrade version 17 and later (page 19)
   • How to upgrade version 16 and earlier (page 20)

After completing this task:
   ♦ License your software. See FAQ: Licensing and updating (page 20).
   ♦ If you are using a wireless network adapter to capture traffic, see Installing the wireless NIC driver on Windows 7/Vista (page 223).
   ♦ If you are using a USB wireless network adapter to capture traffic, see Installing a third-party USB wireless adapter (page 224).
   ♦ If you use Observer on a virtual machine and network traffic cannot be captured or BSODs (bluescreens) are occurring, see Virtual machine troubleshooting (page 23).

Comparing software probe features

Single Probes are appropriate for sites with smaller administrative staffs. This type of probe communicates with only one Observer 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 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. An Expert 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 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>Sends entire buffer(^1)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Alarms</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Trending</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Triggers</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Wireless</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Encrypts buffer transfer (page 153)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Simultaneous multi-topology support</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Simultaneous users(^2)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Supports multiple NICs (page 239)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Use reserved memory outside of Windows (page 240)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Able to switch between probe and analyzer mode (page 254)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full-duplex(^3)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>MPLS (page 232)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>NetFlow (page 267)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Port bonding (page 264) (^4)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Remote decode of GigaStor captures</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Sends expert summary &amp; decode packets(^5)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>sFlow</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>VoIP expert, APA, ATA (page 254) (^5)</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

1. Buffers are sent to Observer 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 VIAVI.
4. Decoding and expert analysis are performed by the probe and a summary is sent to Observer reducing network bandwidth use.
Minimum and recommended system specifications

If you are installing the software on your own hardware or a virtual machine, these are the minimum and recommended specifications for a production environment.

Table 32. Observer Expert Console Only (ECO)

<table>
<thead>
<tr>
<th>Processor / CPU</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM¹</td>
<td>2 GB RAM</td>
<td>8 GB RAM</td>
</tr>
<tr>
<td>Operating system²</td>
<td>64-bit Operating System Windows 7 or newer</td>
<td>Windows 7 or newer</td>
</tr>
</tbody>
</table>

| Network Card | Server-class | Intel server-class |

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. See Supported Operating Systems (page 18) for a full list of supported operating systems.

Table 33. Observer or GigaStor Software Edition in a virtual server

<table>
<thead>
<tr>
<th>Processor / CPU</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM¹</td>
<td>Minimum 16 GB (8 GB for Observer and 8 GB for the operating system)</td>
<td>64 GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Card</td>
<td>Virtualized network adapter</td>
</tr>
<tr>
<td>Capture Card²</td>
<td>Virtualized network adapter</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. See Supported Operating Systems (page 18) for a full list of supported operating systems.
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 (page 22).

Current compatibility and incompatibility of virtual machines with the GigaStor Software Edition (GSE) is described in this list:

- VMWare ESXi Server
  - ESXi 5.0 and higher is compatible with GSE.
♦ VMWare Workstation Pro is not supported with GSE
♦ Microsoft Hyper-V may function but is not supported with GSE

Supported Operating Systems

Your product must be installed on one of these operating systems to receive assistance from Technical Support.

<table>
<thead>
<tr>
<th>Product name</th>
<th>64-bit Windows</th>
<th>32-bit Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows 7 (SP1 or higher)</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>or newer</td>
<td></td>
</tr>
<tr>
<td>Windows Server</td>
<td>Windows Server 2008 R2 Enterprise, Standard, Web</td>
<td></td>
</tr>
<tr>
<td>2008 R2</td>
<td>(SP1 or higher) or newer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 7 (SP1 or higher)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or newer</td>
<td></td>
</tr>
</tbody>
</table>

How to upgrade to Windows 10

Due to the way Microsoft has designed its Windows® 10 operating system upgrade feature, Expert Probe will not function if you upgrade your operating system from Windows 7, Vista or Windows 8 to Windows 10 without first uninstalling Expert Probe.

This information does not apply if you:
♦ Already uninstalled Expert Probe.
♦ Are installing Windows 10 rather than upgrading to it.
♦ Are already using Windows 10.
♦ Are upgrading using the Observer Platform OS Upgrade product because it replaces the operating system rather than upgrading it. Additionally, it uses Windows Server 2012 R2.

**Note:** Unfortunately, if you have already upgraded the operating system and Expert Probe was not uninstalled prior to upgrading to Windows 10, the only path to recovery is to reinstall the operating system. Back up (page 228) any Expert Probe files on the operating system, reinstall the operating system, then install Expert Probe and restore its files.

To upgrade a system with Expert Probe to Windows 10:
1. Back up your settings.
3. Upgrade your operating system.
4. Install the Expert Probe software.
5. Restore your settings from step 1 using whatever method is best for you.

Expert Probe is now available to use on Windows 10.

How to install all versions

Use this procedure to install all versions of the software.
Prerequisite(s):
An administrator account is required to install and run any version of Observer or probe software except Observer ECO. Observer ECO requires an administrator account just for installation; a standard user account can be used for running Observer ECO.

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

   http://update.viavisolutions.com/latest/ObserverSetupx64.exe

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.

How to upgrade version 17 and later
Version 17 allows you to upgrade directly from within Observer or from OMS (if used).

   If OMS is not controlling Observer, then do the following in Observer:
   - Click the File tab, and click Info > Update Observer.

   If OMS is controlling Observer:
   - See How to manage software versions using OMS.

The software is updated to the latest version.

How to upgrade version 16 and earlier
Upgrading version 16 uses the same procedure as installing the software. The process is different for version 17 and later.

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

   http://update.viavisolutions.com/latest/ObserverSetupx64.exe

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.
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 VIAVI 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.

Installing the wireless NIC driver on Windows 7/Vista

See the information in Monitoring a wireless access point (page 255), 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:
   
   **Example:** 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 61: 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 (page 20).
- 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 (page 240).

### Installing a third-party USB wireless adapter

You can capture wireless 802.11 traffic on systems lacking built-in wireless by installing a third-party USB wireless adapter. Wireless access point statistics and other features become usable as well. Installing a special driver on your USB wireless adapter is necessary.

**Prerequisite(s):**

The USB wireless adapter is only supported on systems running Windows Vista or 7 (32- or 64-bit).

**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 wireless adapter before installing the software, unplug the USB adapter, uninstall the software, restart your system, and then proceed with step 1.

**Note:** If using a Belkin N600DB USB wireless adapter, only revision number “F9L1101v1” is compatible. These adapters have a Broadcom chipset. The second revision, “F9L1101v2” does not have a Broadcom chipset and is incompatible.

1. Install the software that came with your USB wireless adapter.
2. Insert the USB wireless adapter into 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. From 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 a Windows service.
6. Restart your system.
   
   Restarting allows the software and 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.
8. On the Home tab, in the Probe group, click **Setup > Select NIC**.
9. 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 anti-virus software, follow these guidelines:

- Ensure TCP ports 25901 and 25903 are open. All Observer Platform products communicate on these ports.
- Ensure UDP ports 25901 and 25903 are open if you use OMS.
- 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 anti-virus software.

**Upgrading the probe software**

Observer and probe software must be within the same major release. This may require you to upgrade your probe software.

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.

Version 17 requires a 64-bit operating system. 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.

**Note:** 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. Start the Observer installation program.
2. Follow the on-screen instructions and choose your probe type.
3. After the installer completes, restart the system.
   - New major builds may have new drivers or other files that require a restart.
4. Connect the probe to an Observer.

**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.

**How to license Observer and GigaStor**

To license and activate a compatible GigaStor, Observer, or Probe:

1. Install and launch the application.
2. After launching the application in DEMO mode, click the **Help** menu and select **License Observer**.
3. Click the **Enter Name** button in the lower left corner.
4. Type into the **Contact/Department** and **Company** boxes exactly what is listed in your license document.
5. Click **OK**, and then click **Accept** on the confirmation dialog.
6. Ensure the **Identification Number** matches the number on your license document. If they do not match, click **Re-Type Name?** to correct any mistakes.

7. Type the license number, from your license document, into the **License Number** box.

8. Click **OK**.

You successfully licensed and activated your product.

If licensing and activating your product remains unsuccessful, please contact Technical Support.

### How to update your license

If Observer or GigaStor is already licensed and you need to modify, update, or change that license, you can do so.

**Prerequisite(s):**

- This task requires you have already licensed (page 20) your Observer or GigaStor.
- This task cannot be completed if the license to your Observer or GigaStor is managed by OMS. Instead, refer to How to edit an asset license.

Updating your license refers to changing, editing, or updating the license that is already applied to your product. Some reasons for needing to do this can include:

- Activating a new license. The new license might provide different or increased functionality over your existing license, like increased data storage for a GigaStor Software Edition (GSE).
- Changing a license. Perhaps you accidentally applied the wrong license to your product and need to change it.

To update a license:

1. Click the File tab, and click **Info > License Observer**.
2. Click **OK** to confirm you want to re-license.
3. Type the license number, from your license document, into the **License Number** box.
4. Click the **Re-Type Name?** button in the lower left corner.
5. Type into the **Contact/Department** and **Company** boxes exactly what is listed in your license document.
6. Click **OK**, and then click **OK** on the confirmation dialog.

You successfully updated your license. Observer begins using the license the next time Observer is launched.

Close and restart Observer for the new license to take effect. You may need to coordinate a suitable time to do so if restarting would affect many users or significantly interrupt your data collection.

### 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.
Ensure you are licensing the correct version of Observer. License numbers are version-specific. License numbers work within equal major version numbers of the product only. For example, an 17.0 license can be used to activate 17.x versions but not 16.1, 16.0, 15.1, 15.0, etc.

**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).

**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 software version the license number applies to. If it does not, or you notice any other error, please call our support team for assistance.

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

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.

**Backing up your GigaStor settings**

You can back up most Observer settings and configuration data. Backups are useful when migrating to new hardware, upgrading the operating system, or recovering from data loss.

*Caution:* If you are using data encryption on your GigaStor system, you must save the encryption keys before upgrading the operating system. Because the keys are typically stored on the operating system drive, they will be lost during the upgrade process. If you do not have a copy of the keys elsewhere, you will not be able to access stored data (packets) after the upgrade is complete.

Your Observer may not have each directory referenced in this topic, but you can back up those that are present. Use whatever backup method is best for you.

To back up many Observer settings and files, do the following:

- Copy the files and directories in Table 34 (page 228) to a backup location. This must be a location other than the operating system drive of the system you are planning to upgrade.

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>
<thead>
<tr>
<th>Directory or file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Trending</td>
<td><code>C:\Program Files\Observer\NetworkTrending</code> 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. Use the Folders tab in Options.</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 the <strong>Folders</strong> tab in <strong>Options &gt; General Options</strong> 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. &lt;br&gt; C:\Program Files\Observer\ProbeAddressTable &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>
</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 branch: &lt;br&gt; 32-bit Windows operating system running any version, or 64-bit Windows operating system running version 16 or higher: &lt;br&gt; HKEY_LOCAL_MACHINE\SOFTWARE\Network Instruments</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>Make note of the license information in <strong>Info &gt; License Observer</strong>. You need the contact/department, company, identification number, and license number.</td>
</tr>
</tbody>
</table>
Creating a probe instance

You can create a probe instance to monitor network traffic seen on a network adapter, explore saved packet captures, and have multiple people be able to see the captured data from their copy of Observer. Create a passive or active probe instance depending on what your goals are.

**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 (page 239) 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 (page 267). For MPLS, see Creating and configuring an MPLS probe instance (page 232). For sFlow, see .

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: 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 (page 240) 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 (page 238).

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. Click Finish.

Creating GigaStor active and passive probe instances

Prerequisite: Expert Probe

GigaStor probe instance creation is only available when you are using the Expert Probe locally on a GigaStor probe and with the program in application mode, not as a Windows service. 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 How to use additional storage volumes on the GigaStor active instance (page 232) 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? (page 196).
- 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 (page 230). 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: 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 (page 230) for details about creating an MPLS probe instance. In Creating a probe instance (page 230) 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.

2. On the General tab, use the options in the MPLS Analysis Settings to 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.
3. Click OK.

How to use additional storage volumes on the GigaStor active instance

When expanding your RAID array beyond 256 TB of usable disk space, you must add the additional volumes to 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.

1. On the GigaStor probe, click the GigaStor Instances tab.
2. Select the Use additional storage volumes option and click Configure.
3. In the message box that appears, click Yes.
4. Select the additional storage volumes you want to assign to your active probe instance, and click OK.
5. In the message box that appears, click Yes.
The additional storage is allocated. This may take a few moments.

**Connecting to a Probe**

You can connect to a probe from multiple directions: *from* or *to* a different Observer analyzer, to its own probe instance (connect to itself), and change the network adapter that is monitored on each probe instance.

**How to change the monitored network adapter**

If your probe has multiple network cards in it, you can choose which card you want to monitor.

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on VIAVI or third party hardware.

<table>
<thead>
<tr>
<th>Note: 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 (page 211).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tip! 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.</td>
</tr>
</tbody>
</table>

♦ When choosing the monitored adapter from within Observer for all probe versions:

1. In the probes list, select the probe instance.
2. Choose **Setup > Select NIC**.
   
   The **Select Network Adapter** window appears.
3. Select the network adapter you want to monitor, and click **Select**.
   
   ♦ When choosing the monitored adapter on the probe for Multi Probe and Expert Probe:

   1. Click **Adapters and Redirection**.
   2. Select your probe instance and click **Configure Adapter/Redirection**.
      
      The **Edit Probe Instance** window appears.
   3. In the **Selected Network Adapter** area, 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 Observer**

1. Click the File tab, and click **Setup > Redirect Probe Instance(s)**.
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 Observer 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 (page 234) for details. If the probe is not connecting, see **A probe is not connecting to the analyzer or vice versa** (page 211). After the probe is connected, see **Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling** (page 240).

7. Close the Probe Instance Redirection window.

### Connecting the Multi Probe or Expert Probe to an Observer

**Prerequisite:** Multi or Expert Probe.

There are two ways to connect the probe to an Observer. 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 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 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 Observer system. If the probe is not connecting, see **A probe is not connecting to the analyzer or vice versa** (page 211).
4. After the probe is connected, see **Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling** (page 240).

### Connecting to a probe instance from an Observer analyzer

**Prerequisite:** Multi or Expert Probe.

Probe instances can be redirected from one Observer to another or disconnected from any analyzer. This is done from Observer.

1. Click the File tab, and click **Setup > Redirect Probe Instance(s)**.
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 Observer, you must add the probe to your list. See **Connecting to a probe for the first time from Observer** (page 233).
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 (page 234) for details. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa (page 211).

5. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling (page 240).

Connecting the probe to an Observer

There are two ways to connect the probe to an Observer. 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 (page 234). All actions are done on the probe itself.

1. Choose **Options > Probe Redirection Settings**. The Probe Redirection Settings dialog opens.

2. Use Table to complete the settings. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa (page 211).

<table>
<thead>
<tr>
<th>Observer IP address</th>
<th>Type the address of Observer 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. If you want the probe to be able to connect to only one Observer, 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 (page 240).

Redirecting a probe instance

Your local Observer 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.

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.

**Note:** Probe redirection can either be password protected or disabled, depending on the target probe.

To redirect a probe instance, complete the following steps:

1. Click the File tab, and click **Setup > Redirect Probe Instance(s)**.

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

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.
5. If necessary for probe access, type a user name and password, and click **OK**. Figure 62: Credentials may be needed

![](image)

6. Select the remote probe instance from the list, and click **Redirect Selected Probe Instance(s)**.

   Allow time for the remote probe to redirect. How long this operation can take is limited by a timeout countdown.

   The probe instances of the remote probe are shown.

7. Select a probe instance from the list, and click **Redirect Selected Instance**.
8. Select the **Redirect to this Observer**, and click the **Redirect** button.
9. Close the **Probe Instance Redirection** window.

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

### Configuring a probe's name and other probe options

Set the probe network adapter speed, reserve system memory for probes, configure connections to multiple network adapters, set “always on” traffic capture, customize statistic and capture buffers, and more.

**Prerequisite(s):**

These steps assume you are viewing the probe interface, which is the only choice when using Expert Probe software. But if you are using a GigaStor, ensure that you are viewing the probe interface (page 254).

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 Observer 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</td>
</tr>
</tbody>
</table>
**Setting** | **Description**
--- | ---
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 (page 230).

Network Trending folder | 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.

Folder for GigaStor | Allows you to specify where the GigaStor and network packet data will be saved. The default is C:\Program Files\Observer\Data if a software install or non-GigaStor probe or D:\Data if a GigaStor hardware appliance. Unless you have a specific reason to use another directory, we suggest using the default.

Maximum IP DNS resolution entries | 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 of storage space, whichever is less. The probe keeps the first 10,000 entries (or whatever amount you define) it sees; it does not keep a rolling list of the last 10,000. After the limit is reached, no more entries are kept. They are discarded.

Run Probe as Windows Service | 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.

View certificates from other Observer assets | Click the Certificates button to view trusted, untrusted, and pending trust, certificates that allow secure asset-to-asset communication. See Understanding the certificate trust model (page 153) for details.

---

**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 (page 201).

- To change memory allocation for probe instances, see Running (page 205)Observer (page 205) with reserved memory (page 205).
- To fine-tune the Statistics Memory Configuration, see How to adjust the statistical buffer (page 75).
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.

To configure when packet capture should run, complete these steps:

1. In Observer, select a probe instance in the Probes list.
2. On the Home tab, in the Capture group, click **Configuration > Packet Capture**.
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.

1. Do one of the following:
   - On the probe: Click the **Synchronization tab**.
   - In Observer: 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

**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 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 (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

After connecting the probe instance to Observer Analyzer, there still may be some additional configuration that you must do. This is completely dependent on your network environment and your needs.

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on VIAVI or third party hardware.

In Observer:

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 Configuring a probe’s name and other probe options (page 237).

<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 <strong>Probe Properties field-level descriptions (page 241)</strong>.</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 <strong>Probe Properties field-level descriptions (page 241)</strong>.</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 <strong>Probe Properties field-level descriptions (page 241)</strong>.</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...</td>
</tr>
</tbody>
</table>
### Tab Description

- **Wireless 802.11**
  - 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 (page 255). For field descriptions, see Probe Properties field-level descriptions (page 241).

- **D3/E3/HSSI**
  - 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 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 Probe Properties field-level descriptions (page 241).

- **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 Probe Properties field-level descriptions (page 241).

- **Virtual adapters**
  - See Configuring virtual adapters on the capture card.

- **Packet Broker Integration**
  - See How to configure packet broker integration (page 247).

---

**Your probe instance is now configured. You can begin collecting network traffic and statistics using it. Typically, this is done in Observer by choosing Capture > Packet Capture and clicking the Start button. See Configuring probes to collect data even when not connected to an analyzer (page 239) 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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication timeout</strong></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><strong>Probe report period or local Observer information refresh time</strong></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><strong>Statistics report (refresh) period</strong></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><strong>Vital signs report (refresh) period</strong></td>
<td>Allows you to set the Network Vital Signs refresh period. Values are from 10 to 600 seconds.</td>
</tr>
<tr>
<td><strong>Sampling Divider</strong></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...</td>
</tr>
</tbody>
</table>
### Configuring a probe’s name and other probe options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table 36. Parameters tab</strong></td>
<td><strong>Option</strong></td>
</tr>
<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>

Encapsulated Traffic Analysis

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.

Nortel OEL2 Metro Ethernet Analysis Settings

Choose if frame headers should be analyzed as OEL2 headers.

MPLS Analysis Settings

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.
### Table 37. 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 38. 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>
</tbody>
</table>
| Autoupgrade probe for major version release          | 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 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. |
| Force Probe Autoupgrade to the current Observer version | This provides a manual mechanism for updating a probe.                     |

### Table 39. 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</td>
</tr>
</tbody>
</table>

---

**Configuring a probe's name and other probe options**

Chapter 14: Expert Probe Software | 243
### Table 40. Wireless 802.11 tab

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></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>
</tbody>
</table>
| Monitor Wireless Traffic by | Choose one of the following:  
Scan Channels—Click the **Channel Map** button and choose which channels you want to scan, then choose how often you want to scan them.  
Scan Interval—Define the scan interval.  
Fixed Channel—Pick a channel to monitor.  
BSSID—Specify the Basic Service Set ID of the Access Point you want to monitor.  
ESSID—Specify the Extended Service Set ID of the network you want to monitor. |
| Use encryption keys | 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. |
| Antenna to use      | The type of antenna connected to your system. Specify one of the following:  
Antenna Diversity—Use the stronger signal from the two antenna ports. This is the recommended setting for the standard snap-on antenna.  
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).  
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). |

### Table 41. DS3/E3/HSSI tab

<table>
<thead>
<tr>
<th><strong>Setting</strong></th>
<th><strong>Explanation</strong></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 42. 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>

**Understanding the Packet Broker Integration tab**

When using network packet broker integration, you can dynamically reduce traffic flow to your GigaStor when it is at risk of oversubscription giving you the content you need. Additionally, metadata tags identify the network segment where the packets came from, providing you context when troubleshooting.

As a network administrator, you need really good content to be able to quickly troubleshoot your network environment. If you do not have the appropriate metadata or packets, determining where a problem is occurring and, more importantly, why the problem is occurring is very difficult. Content is king, and context is important. Dynamic traffic management gives you the content, and port tags give you the context.

**Dynamic traffic management**

Dropped packets are never desirable and they occur when a link is oversubscribed. If your analytics device does not have all of the packets of a conversation, troubleshooting is very difficult.

If your GigaStor is at risk of oversubscription, you should reduce the flow of traffic to the GigaStor. You have two options for reducing the traffic. First, you can choose to pre-filter traffic (page 87) using fixed, preset filters that you create. This is the minimalist approach. Second, you can allow all traffic and dynamically exclude traffic only when oversubscription occurs. We’ll explore each choice in a bit more detail.

With the minimalist approach to packet capture, you only capture the traffic that you think is relevant. In other words, you exclude everything from packet capture except the specific traffic you allow. For instance, you may decide that YouTube is not critical to your business and do not need to troubleshoot problems with that traffic. Therefore, you would never capture and save YouTube traffic. It is excluded with a pre-filter. This gives you longer retention capabilities for the content you do capture because your capture devices are not filling as quickly. Also, by not seeing YouTube and other non-critical traffic you are not overwhelmed with unnecessary information when troubleshooting. When you
do identify a problem in your network, you can allow in more traffic by changing your pre-filters to troubleshoot the problem.

The opposite approach is to capture everything and use post-filters (page 94) to find what you are looking for. If GigaStor is at risk of oversubscription, then using traffic filters that GigaStor dynamically and automatically apply to a Gigamon can reduce the flow. This eliminates the oversubscription risk while continuing to capture the most amount of traffic relevant to you. You can set the types of traffic that interest you up front and GigaStor automatically captures it. After the initial configuration (page 247), it is no longer a manual process you need to remember to implement to capture the content you need. The dynamic filters allow you to focus on the business critical applications.

Figure 64: When filters are applied and removed

Unlike pre-filters, which can be used anytime, dynamic filtering is only available when using a Gigamon network packet broker.

**Contextual visibility**

Using Gigamon-applied port tags, you know which network segments are experiencing performance issues.

For context, you can have numerous streams of information coming into GigaStor, but, when you are troubleshooting, it is very helpful to know where in your network the packets came from. This is where port tags help. With port tags you have the context of knowing where in your network the problem occurred.
Using the port tags helps you solve correlative analysis issues. For example, if you are troubleshooting a VoIP call that shows excessive jitter or a low MOS score, it is important to know what portion of the network you are seeing in the packet captures. One network segment may not be experiencing any problems at all, while the other network segment does. By filtering on conversation and port tags, you will be able to see the conversation from different perspectives and begin to draw conclusions.

**How to configure packet broker integration**

Using a network packet broker ensures that the Observer Platform has the right content at the right times so that you can troubleshoot your network.

Configuring packet broker integration allows GigaStor to work with systems such as GigaVUE.

Using filters created in GigaStor, you can filter traffic as it leaves your packet broker reducing the load the GigaStor. Using Gigamon-applied port tags allows you to identify packets that come from your network packet brokers.

**Prerequisite(s):**

Exactly these versions are required:

- Gigamon Fabric Manager 3.3
- Gigamon GigaVUE H series nodes 4.6

With this feature, you can choose to use port tags without enabling dynamic filters, or you can decide to use dynamic filters and not use port tags, or you can enable both. You decide what is best for your environment.

You might choose to filter traffic because you only want certain traffic to be kept on this GigaStor or because the traffic load temporarily exceeds the GigaStor FIFO abilities. If there are multiple filters, they are applied one at a time in descending order until the FIFO level drops below 50%.

1. Select a probe instance in the Probes list.
2. Right-click and choose **Probe or Device Properties**.
3. Choose the **Packet Broker Integration** tab.

4. Use the information in **Packet Broker Integration (page 248)** to configure GigaStor to work with your packet broker.

**Figure 66: Packet Broker Integration tab**

GigaStor sends commands to your packet broker whenever FIFO levels are too high (above 50%). This temporarily reduces the traffic load coming into the GigaStor until FIFO levels drop below 20%.

**What to do next:** Turn on the **NPB Port Tagging** tab in GigaStor Control Panel in **Setting the GigaStor general options**.

### Packet Broker Integration

Use the packet broker integration settings to configure the connection between GigaStor and your packet broker (for instance, GigaVUE).

<table>
<thead>
<tr>
<th>Fabric Manager address</th>
<th>The DNS name or IP address of the GigaVUE-FM system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster ID</td>
<td>The cluster name or IP address of the GigaVUE-FM visibility fabric node.</td>
</tr>
<tr>
<td>Username</td>
<td>Your GigaVUE-FM user name.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for your GigaVUE-FM user name.</td>
</tr>
</tbody>
</table>

**Test Configuration**

Use this button to validate your packet broker settings, including addresses, user name, and password. If you enter any invalid ports, a message box returns with a list of valid ports for the cluster.
| Enable Gigamon port tagging | Provides contextual visibility by using the GigaVUE-FM-applied VLAN 802.1Q port tags that are added to every packet. This allows for filtering in GigaStor. Be sure to turn on NPB Port Tagging in Setting the GigaStor general options to show the NPB Port Tagging tab in GigaStor Control Panel where you can see the GigaVUE-FM port from which the packet came, the port tag, the number of packets from the port, the amount of bytes, and utilization. |
| Enable Dynamic Filtering | Allows the GigaStor to send filters to GigaVUE-FM whenever the FIFO load on the GigaStor reaches 50% and there is a risk of dropping packets. When this option is enabled, GigaStor clears any existing filters on Gigamon and replaces them with the new filters. When disabled, GigaStor removes all filters. |
| Tool ports attached to this instance | A list of Fabric Manager ports that are associated with the GigaStor active instance. They are listed in the format required by Fabric Manager: Chassis/Slot/Port. For example, 1/1/x1. |
| Port (Chassis/Slot/Port) | The first value is the GigaVUE chassis in which the port is found, the second value is the slot within the GigaVUE chassis where the port is found, and finally is the port itself. All three values are required and must be separated by the / character. |
| Enable rollback of filters | If selected, any filters in the Applications to be filtered list that have been applied to the packet broker are removed after the specified number of minutes. The minimum is one minute. The time frame you choose allows for a smooth rollback of filters so that a momentary drop in network traffic does not cause filters to be repeatedly applied and removed in a short timespan. |
| Applications to be filtered | This section defines the filters to push to GigaVUE to exclude certain content before the traffic is sent to GigaStor. Each time you add, remove, change, or reorder these filters, all filters on the GigaVUE system are deleted and replaced with these filters. This ensures that only the filters you specify in this list and no others are used. The risk of dropping packets occurs when the FIFO reaches 50%. When that level is reached, a message is logged and the first filter in the list is applied. If applying the filter does not lower the FIFO level below 50% within one second, the next filter is applied. This process continues until the FIFO level remains below 50%. This ensures that a minimum number of filters is applied while allowing the most amount of traffic to be written to GigaStor. The order of the filters is important. Filters are applied in descending order. In other words, the filter listed at the top is applied first, then the next if necessary, and so on. If the FIFO does not drop below 50% even after all filters have been applied, you should identify other application traffic to exclude. Filters are removed in reverse order starting with lowest priority (last) filter, then the next lowest, and so on until all filters are removed only after the GigaStor FIFO (page 292) falls below 20% with that filter applied and the allotted time from the Enable rollback of filters field has passed. If the FIFO level goes back above 50% the filter that was just removed will be reapplied. The 50% and 20% threshold values are fixed and cannot be modified. Use the arrows buttons to change the order of your filters to find the arrangement that works best for you. |
The buffer size (page 288) of the active instance affects FIFO abilities. Changing the buffer size is described in Setting the GigaStor general options and may help in some instances; otherwise application filtering is needed.

You can choose to filter TCP-, UDP-, and SCTP-based applications, including any derived applications (page 69) you created in How to add application definitions (page 66).

In GigaStor, an application can be defined (page 66) using a port, port range, or port/IP address combination (or any combination of these). GigaVUE does not have a way to identify applications based on port/IP address. Therefore, the port/IP address combination will be removed from any filter before it is sent to GigaVUE. For example, if an application definition is 9000, 2343:10.74.33.101, only 9000 will be passed to GigaVUE; 2343:10.74.33.101 will be dropped from the filter. Again, this is a limitation of GigaVUE.

A maximum of 100 tool port filter rules can be created. An application that uses a port range (9001-9005) counts as one rule not as five rules.

GigaStor uses a REST API to communicate with GigaVUE. If there are communication interruptions between the two systems for whatever reason, GigaStor will attempt several times to reissue the command until it is successful. If it is still not successful after several attempts, a message will be written to the log.

**How Gigamon-applied port tags are identified**

GigaStor identifies packets with headers applied by Gigamon because a Gigamon system tags packets using an 802.1Q tag.

The Gigamon administrator may apply port tags to each ingress port on the GigaVUE. For each ingress port a unique VLAN 802.1Q tag is used. This tag is applied using the outermost VLAN tag. When there is a VLAN 802.1Q tag on the inner frame, only the information in the outermost 802.1Q tag is used.

GigaStor queries the list of port tags used by Gigamon and maintains a copy of that list. When traffic is received by GigaStor it is compared against the list. If there is a match, the GigaStor knows exactly which ingress port on the Gigamon was used and displays the information accordingly.

**How to encrypt captured data at rest**

Captured data at rest can be encrypted using the 256-bit Advanced Encryption Standard (AES) algorithm. This significantly increases the security of your at-rest data.

**Prerequisite(s):**

- You must have a special Observer license to enable and use this feature. There is no extra charge for the license.
- You must have a GigaStor hardware appliance. This feature is not available to GigaStor Software Edition. See the differences in software and hardware (page 272) offerings for GigaStor.
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 Observer.

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. The RAID hardware is responsible for the encryption, and the data is encrypted before it is written to disk.

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 VIAVI 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 the Figure 67 (page 251) image.

![Figure 67: Areca RAID application](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>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume RAID Level</td>
<td>Raid 5</td>
</tr>
<tr>
<td>Greater Two TB</td>
<td>64bit LBA</td>
</tr>
<tr>
<td>Volume Support</td>
<td></td>
</tr>
<tr>
<td>Volume Initialization Mode</td>
<td>Foreground 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 Background Initialization, you may use your GigaStor, but it will take significantly longer to complete and performance will be negatively affected.</td>
</tr>
<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>


   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.

10. Click **Generate Key** and save the key file in a secure location following your organization’s security policy.

   - When rebooting, the system needs access to key in order to unlock the drive. This is the key necessary to write to and read from the RAID volume.
   - Observer will not open unless it can find the key. Without the key present neither packet capture nor packet analysis can occur. 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.

- Securely storing the key is a critical part of your responsibility.

11. Close Observer until the rest of this procedure is complete.

12. 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).

13. Repeat this process for each RAID volume for your GigaStor.

14. Open Observer.

**Using the Probe**

The probe has two interfaces: the probe service and the analyzer user interfaces. You can switch between the two depending on what you want to accomplish. Also learn about monitoring a wireless access point (AP) and where to enable network trending.

**Using the Expert Probe software**

Learn how to create, configure, redirect, and delete both local and remote probe instances.

**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 68: Expert Probe on a GigaStor

An Expert Probe transfers decode data to an Observer 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. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.
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

Most probes can be run as either a Windows service or in application mode. Some settings can only be made when the probe is in application mode.

**Prerequisite:** Multi or Expert Probe.

Depending on how you want or need to use your Expert Probe, it can be either an Observer to help you view your network data or it can be a probe to capture data and to which other Observer 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, click **File** and **Options > Switch Interface**. You must restart the application to see the change.

**Note:** 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**.
Figure 69: Probe Service Configuration Applet

The **Probe Administration** window opens.

2. Choose **Options > Probe Options**.
3. Clear the option **Run Probe as a Windows Service** option, and click **OK**. This removes the VIAVI Expert Probe service from Windows.
4. Start Observer.
5. Click the File tab, and click **Options > Switch Interface**.
6. Choose **Observer**, click **OK**, and click **OK** again when prompted. This closes Observer.
7. Start Observer.

Observer is now set to use the analyzer interface.

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 Observer choose Statistics > and then select the statistic you want to have the probe collect and report.
2. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.

### 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 VIAVI 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 VIAVI 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.

Note: 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. 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

Learn when to use a virtual TAP, its purpose an benefits, and how to configure them for use in a VMware ESX server.

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.

**Tip!** 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: 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

A virtual machine is a convenient way to add monitoring capabilities to your network. Use this information to create a virtual switch.

**Prerequisite(s):**
- Your virtual machine meets the [minimum specifications](page 17)
- Multi or Expert Probe is installed
- A free physical NIC

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.

In the virtual switch to be monitored, add a virtual port group and set it to run in Promiscuous Mode.

**Caution:** 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.

1. Open VI Client and highlight the VMware ESX Server Entry.
2. Click 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.
10. Setup a second virtual switch and bind a second physical NIC to that virtual switch.

See Figure 71 (page 263) Virtual Infrastructure Client > Configuration tab. Then see Figure 73 (page 264) 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 72 (page 264). See your VMware ESX Server documentation if you need more detailed information on adding a virtual switch.
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 second 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.

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 capture card.

How to assign physical ports to probe instances

By default, the active instance monitors network traffic from every physical port of your capture card—all the traffic is aggregated. If you want to instead “divide” your monitored network traffic by physical ports, to help you monitor certain SFPs separately from others, then you can use virtual adapters to assign specific physical ports to probe instances.
**Prerequisite(s):**

Your hardware appliance must have one of the following:

- Gen2 capture card
- Gen3 capture card

For example, suppose you are deploying an 8-port Gen3 capture card as follows:

- Ports 1-4 are monitoring a collection of trunked links
- The remaining ports are each connected to the SPAN (or mirror) port on a switch

In this scenario, it makes sense for Observer to view ports 1-4, for example, as a single stream of network traffic and to separate each of the four remaining ports into separate data streams. Virtual adapters are a convenient way to accomplish this separation or aggregation in real time, rather than depending on filters to sort through the traffic post-capture.

These are the general steps for assigning physical ports to a probe instance:

- Create a virtual adapter (or have one already).
- Assign physical ports to this virtual adapter.
- Set a probe instance to use this virtual adapter as its NIC.

**Tip!** As a general reminder, you risk severe performance loss when using more than one active instance. These instructions do not create multiple active instances.

To assign physical ports to a specific probe instance:

1. In Observer, right-click the Gen3 capture card-equipped probe instance from the probe list, and click **Probe or Device Properties**.

   A Gen3 capture card-equipped probe instance shows (Gigabit) or similar after the name.

2. Click the **Virtual Adapters** tab.
3. Select a virtual adapter, and click **Edit Adapter**.
4. Select physical ports from the **Available Ports** list, and click **Add**.
   You can select more than one physical port by holding **CTRL** as you click.
5. Click **OK** to return to the **Virtual Adapters** window.
6. Click **OK** to save the virtual adapter and close the **Virtual Adapters** window.
   Changes to virtual adapters are not be saved until **OK** is clicked in the **Virtual Adapters** window.
   The virtual adapter appears in the list of available network adapters when creating a probe instance. This allows you to assign the virtual adapter to a specific probe instance, among other benefits.
Next, you should change the monitored network adapter of a probe instance to use the virtual adapter.

**Using the NetFlow features in Observer**

Watch a video about NetFlow in Observer, and see a list of some important NetFlow considerations to know.

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.
- 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**

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.

**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 (IPFIX)
- 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 50 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.
Creating a NetFlow collector or NetFlow Trending collector

<table>
<thead>
<tr>
<th>One flow per collector</th>
<th>NetFlow Trending collector</th>
<th>NetFlow collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 50 flows per trending collector</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Collects live statistics(^1)</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 (page 230) for details about creating a NetFlow collector or a NetFlow Trending collector. In Creating a probe instance (page 230) 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. On the Home tab, in the Probe group, click **Setup > Probe Properties**.
2. On the General tab, configure the Timing and Statistics Packet Sampling sections for your needs and Click **OK**.
3. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.
4. Click the **Settings** button.
5. Configure any settings for Network Trending here.
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
Chapter 15: GigaStor Control Panel

The GigaStor Control Panel is the interface in Observer Analyzer that works specifically with 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.

Prerequisite(s):

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 Observer to connect to the GigaStor probe.

Before getting started with your GigaStor probe, these tasks should already be complete:

1. It has been decided where to install the GigaStor probe as discussed in Deciding where to place probes in your network.

2. The GigaStor probe has been installed into a server 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.

All GigaStor probes use the Expert Probe software. Learn more about the Expert Probe in Using the Expert Probe software (page 253).

To get the most out of your GigaStor, you need:

♦ A good working knowledge of your network. You can use Observer 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.
♦ An understanding of probe instances and why you want to use them. In particular, a GigaStor is heavily reliant on a unique probe instance called an active instance.

To get started with your GigaStor probe:

1. 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).

In a typical installation, the GigaStor probe runs the Expert Probe software as a Windows service and a remote Observer connects to the GigaStor probe to complete the configuration.

From the Observer system, complete the following steps. These steps requires that you have an Observer installed and licensed separate from the GigaStor probe.

2. Connect to the GigaStor probe from your Observer.

3. 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 step 1, renaming the probe instance is different. For details, see Creating a probe instance (page 231). Pay attention to the special instructions if your GigaStor array is larger than 256 TB.

4. Set the adapter speed for the active instance. See Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling (page 240).

5. To capture network traffic, you must have the GigaStor capture running. See Configuring probes to collect data even when not connected to an analyzer (page 282).

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.

6. Using a passive probe instance, begin analyzing the traffic you are capturing. See Using the GigaStor Control Panel (page 274).

After you have collected data, you will want to see what is happening on your network.

- Mining data from your GigaStor (page 289).
- Reconstructing streams of HTTP, VoIP, and more (page 311).
- Examining your network traffic with forensic analysis (page 298).
- Analyzing FIX transactions (page 315).

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 (page 274) to fine-tune your GigaStor.

7. (Optional) If you want to track physical ports individually, ensure you enable Track statistics information per physical port. See Setting the GigaStor general options.
Tip! All GigaStor probes come with a capture card. Details about this unique capture card, including physical port indexing or virtual adapters, is covered in .

8. (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 (page 287).

9. (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.

10. (Optional) The default settings for Observer is to be unaware of TCP connections that were opened after the GigaStor or packet capture started. You can change this default setting by doing the following:

   a. Mine some data from the GigaStor by following Analyzing data without any filters (page 294).

      This opens the Decode and Analysis tab.

   b. Ensure the Expert Analysis tab is selected, and click the Settings button at the top.

      The Expert Global Settings window appears.

   c. Click the TCP/IP tab and clear the Follow only newly opened TCP connections.

      (Optional) 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.

By following the steps, you successfully configured the GigaStor probe to collect network traffic. You also made some configuration changes that help the GigaStor probe work well in your network. Also, you mined data from the GigaStor probe.

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 RAID coupled with the capture card in a rack unit. The capture card allows you to capture a number of different full-duplex media by swapping standard SFP or SFP+ modules in and out. When Observer 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 the GigaStor in the cores of data centers. Locate near servers to capture their server-to-server traffic. The distribution layer is another optimal position for GigaStor.

By utilizing 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.
Differences between GigaStor Software Edition and GigaStor

The GigaStor Software Edition (GSE) is identical in most ways to a hardware GigaStor purchased from VIAVI. However, there are differences that exist due to GSE naturally lacking GigaStor hardware components like the capture card and high-performance RAID card(s).

<table>
<thead>
<tr>
<th>Capability</th>
<th>GigaStor Software Edition</th>
<th>GigaStor as Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mining &amp; Analysis Interface</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Packet Capture</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Real-Time Statistics</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trending</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Triggers and Alarms</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data-at-Rest Security</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Capture card</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hardware Acceleration</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hardware Filtering</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Packet Deduplication</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Physical Port Indexing</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Precision Time Stamping</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Virtual Adapters</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>High-performance RAID card</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Minimum and recommended system specifications

If you are installing the software on your own hardware or a virtual machine, these are the minimum and recommended specifications for a production environment.

Table 43. Observer Expert Console Only (ECO)

<table>
<thead>
<tr>
<th>Processor / CPU</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dual core Pentium class processor</td>
<td>Quad core Pentium class processor</td>
</tr>
<tr>
<td>RAM¹</td>
<td>2 GB RAM</td>
<td>8 GB RAM</td>
</tr>
<tr>
<td>Operating system²</td>
<td>64-bit Operating System Windows 7 or newer</td>
<td>64-bit Operating System Windows 7 or newer</td>
</tr>
<tr>
<td>Network Card</td>
<td>Server-class</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. See Supported Operating Systems (page 18) for a full list of supported operating systems.
Table 44. Observer or GigaStor Software Edition in a virtual server

<table>
<thead>
<tr>
<th>Processors / CPU</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Four core</td>
<td>Six core</td>
</tr>
<tr>
<td>RAM¹</td>
<td>Minimum 16 GB (8 GB for Observer and 8 GB for the operating system)</td>
<td>64 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>Packet capture - Hardware: Determined by your product</td>
<td>Same</td>
</tr>
<tr>
<td></td>
<td>Packet capture - GigaStor Software Edition: Determined by your license.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network trending: See How to determine disk space requirements for network trending (page 170).</td>
<td></td>
</tr>
<tr>
<td>Operating system²</td>
<td>64-bit Operating System Windows 7 or newer</td>
<td>64-bit Operating System Windows 7 or newer</td>
</tr>
<tr>
<td>Network Card</td>
<td>Virtualized network adapter</td>
<td>Intel server-class</td>
</tr>
<tr>
<td>Capture Card³</td>
<td>Virtualized network adapter</td>
<td>Server-class onboard network adapter</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. See Supported Operating Systems (page 18) for a full list of supported operating systems.
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 (page 22).

Current compatibility and incompatibility of virtual machines with the GigaStor Software Edition (GSE) is described in this list:

- VMWare ESXi Server
  - ESXi 5.0 and higher is compatible with GSE.
- VMWare Workstation Pro is not supported with GSE
- Microsoft Hyper-V may function but is not supported with GSE

Storage limits of packet capture for GigaStor Software Edition (GSE)

The disk storage capacity usable for packet capture and of GigaStor Software Edition (GSE) is governed by your GSE license. This allows flexible cost options when considering the storage available to the computer, or virtual machine, that you are installing GSE on.

GSE licenses are available at these maximum storage sizes:

- 256 GB
- 1 TB
- 4 TB
- 16 TB
- 32 TB
- 48 TB
- 64 TB
Maximum storage size is a measure of how much network data (in the form of packets) can be retained by the GigaStor Software Edition before the oldest GigaStor data is removed in a first-in first-out (FIFO) storage scheme. The maximum storage size is not an indication of how much disk space the GigaStor Software Edition will consume on your hard disk. For example, the program files and libraries, storage of network trending data (not packets), and other executables are not governed by your GSE license and do not count towards the maximum storage capacity.

Network trending storage is a separate issue from packet capture storage and they are not connected in any way except both require writing data to the hard drive. When estimating file size, retention, and system maintenance, you may want to look at the system holistically and consider both simultaneously. Read more about network trending in Configuring your network trending settings (page 166).

How to determine disk space requirements for network trending

Because network trending can consume a lot of disk space, you need to know how much disk space to reserve.

Network trending data consumes hard disk space. Depending on and your storage requirements for network trending data, the network trending data could fill that drive to full capacity—this is a problem. Therefore, determine your typical 24-hour data rate and how many days of trending data you want to retain. The result indicates how much storage space is required.

To determine the amount of space required to store your desired amount of trending data:

1. Determine your typical 24-hour data rate.

   **Example:** 15 MB or 20 GB.

   The *data rate* is amount of trending data collected in one 24-hour period.

2. Multiply your typical 24-hour data rate by the number of days you want to retain.

   **Example:** 15 MB x 365 days = 5.475 GB

   **Example:** 20 GB x 30 days = 600 GB

   The result is the amount of hard drive space required to retain the trending data.

You can use the numbers you calculated to inform your decisions when deleting network trending data (page 165).

Using the GigaStor Control Panel

This section covers the GigaStor Control Panel, its settings, and its use when you choose GigaStor from the Capture group in the Home tab.

**Note:** Packet decoding, Connection Dynamics, and analysis types like TCP, UDP, or VoIP Events are covered elsewhere.

After the GigaStor probe is up and running on the network, you can use an Observer 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 75 (page 275).
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**, clear **Enable Analysis types** for whichever analysis types you do not need. 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 Maximize button if needed. Clicking this button maximizes or minimizes the 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 Observer. Some settings in Observer 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 Observer 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 (page 294). 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 the GigaStor general options

The **General Options** tab configures packet capture and buffer size; whether partial packets are captured; indexing of MAC, IP, VLANs; capture and analysis options; sampling; analysis types; and more.

This tab lets you configure many options for the GigaStor.

1. On the Home tab, in the Capture group, click **GigaStor**.
2. Click the **Settings** button.
3. Click **General Options**. See Table 45 (page 277) 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.

Table 45. GigaStor configuration options

| Capture Buffer size | 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. 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 |
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 the inability of Windows to multi-task the receiving and analysis of the data going and coming from the Observer PC.

Capture Partial Packets

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, email 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 **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.

Collect and Show GigaStor Indexing Information by

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, Physical Ports, and Network Packet Broker (NPB) Port Tagging. 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 Addresses is 200,000 (the default is 1000). See Discovering current top talkers on the network (page 46) for tips on how to narrow your time slice.

Capture and Analysis Options

**Enable intelligent TCP protocol determination**: Displays only known applications while hiding dynamic ports by using the TCP three-way handshake (SYN SYN+ACK ACK). Clearing this option shows all ports.

**Limit to ports defined in “Protocol Definitions”**: 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.

**Track statistics information per physical port**: When selected, causes the GigaStor to index the data it collects by 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.

**Collect counts for all IP protocols in addition to TCP and UDP**: 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.
### Enable Analysis Types:

Choose whether to enable the GigaStor Control Panel to process and display these types of data. By clearing these options, the corresponding tab is hidden in the GigaStor Control Panel and you cannot analyze packets for these data types:

- **Forensic Analysis (uses Snort rules)**
- **FIX Analysis**: used to process FIX financial transactions.
- **Microburst Analysis**: used to process data to identify microbursts on your network, typically a concern for network administrators in trading firms, but also other companies.
- **Trading Multicast Analysis**
- **IPTV Analysis**

### GigaStor Packet Sampling

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 (page 283).

### Use physical port selections...

You can choose this option to display statistics sorted by 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.

### Auto-update GigaStor chart...

When selected, causes the listed actions to have the same effect as clicking the **Update Chart/Statistics** buttons.

### Keep focus on GigaStor...

Keeps the focus in the GigaStor Control Panel instead of switching to the decode pane.

### Update display...in 30 second intervals

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.

### Display only defined subnets

When selected only defined subnets are displayed. The subnets must be defined on the **Subnet** tab. See Defining your subnets in GigaStor (page 287) for details about defining a subnet.

### Enable IP DNS resolution

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.

### Enable packet time charting...

Because the charts can be configured to show sub-second intervals that means that some packets will cross the boundaries of your chosen intervals. This makes it hard to tell in the chart how long your scenario occurred. When enabled, this setting...
makes the charts display every interval in which the bits were present from your packet, not just the first interval. This setting works even if it was not enabled when the packet was captured. It can be enabled later and you will see every interval where a bit was present.

You set the general options for your GigaStor system. These options have a large effect on the operation of the GigaStor system, so if anything seems wrong or you are not seeing all the packets you anticipated, return to these settings and see if they should be changed.

**Shorten your time slice to find a top talker**

The Top Talker list may appear to be missing entries. This occurs because of a combination of two settings in your GigaStor Control Panel. Temporarily adjust these settings to get the data you want.

If you are trying to find what system or systems are responsible for certain traffic on your network, you'd typically use Top Talkers to identify them. There is, however, a limit to the number of systems that Top Talkers identifies. By default, that limit is 1000. As soon as the 1000\(^{th}\) system is identified in a time slice—chronologically—all remaining systems are ignored even if they were "chattier" (that is, causing more traffic on the network) than any of the first 1000 systems. In other words, the GigaStor Control Panel does not show the 1000 most talkative systems, but the first 1000 systems it encounters.

The solution is to shorten your time slice, perhaps down to milliseconds if necessary so that the Top Talker list does not reach the 1000 stations. Additionally, you can increase the number of IP Addresses allowed in the list up to a maximum of 200,000.

Also keep in mind that in the GigaStor Control Panel you are looking at statistics, not actual packet data. Therefore, you could set the GigaStor Control Panel sampling ratio to 1 and set the maximum number of entries allowed to a very high number (100,000 or even higher). This won't give you 100% accurate data, but you will get a very good idea of the situation based on statistics.

**Caution:** If you change the maximum IP address or sampling ratio, consider changing its value back after you have identified your top talker. The reason is that both settings affect memory and can adversely affect performance if there is a high number of IP address and extremely low sampling ratio. Returning these values to their defaults (10,000 IP Addresses and a sampling ratio of 10) will restore GigaStor performance.

The GigaStor Control Panel indexing maximums and sampling ratio are configured in Setting the GigaStor general options.

**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 the 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 clearing this setting, 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 (page 283) and Understanding GigaStor indexing (page 284).

**Capturing packets with the GigaStor**

The GigaStor allows packet captures to be scheduled, trimmed (partial packet captures), and all its data can be exported for archiving. Also learn about GigaStor indexing and the difference between statistics and packets.

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 Observer 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.

To schedule packet captures to begin at preset times, complete the following steps:

1. On the Home tab, in the Capture group, click **GigaStor**.
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 and the payload may contain sensitive information.

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 the GigaStor probe to trim all packet data beyond the first 64-bytes, choose Live > Packet Capture and then Settings > Capture Options. In that tab, enable Capture Partial Packets (Bytes).

1. On the Home tab, in the Capture group, click GigaStor.
2. Click the Settings button.
3. Click the General Options tab. See Setting the GigaStor general options for a description of each field.
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.

In Observer, to password protect the ability to change partial packet capture size:

- Click the File tab, and click Options > General Options.
- Click the 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 capture 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 is 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 writes 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 on 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. This can be done for archival or backup purposes.

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 mode rather than Expert Probe. See Switching between the probe and analyzer user interfaces (page 254). 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.
2. On the Home tab, in the Capture group, click **GigaStor**.
3. Click the **Settings** button to open **GigaStor Settings**.
4. Click the **Export** tab.
5. Choose how you want to export the data and in which format (BFR, PCAP, or CAP).
6. (Optional) Choose to schedule the export so that it can happen automatically.
7. If you want to export data from specific time ranges only, or just export the data on an “as needed” basis, click **Manual Export**.
8. (Optional) Choose if you want to have Observer write a progress status every 30 seconds to the **Log** window.
9. Click **OK**.

---

**Configuring your GigaStor**

Learn how to configure packet capture and buffer sizes, define subnets, and change the storage directory where packets and other data is stored.

---

**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.

1. On the Home tab, in the Capture group, click **GigaStor**.
2. Click the **Settings** button.
3. Click the **Subnet tab**.
4. Use the Add, Delete, Modify, Import, and Delete All buttons to configure the subnet settings for the GigaStor. When you define subnets in the GigaStor Control Panel, Observer 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.

**Tip!** You can import subnet ranges using an *ipsubnetrange* file. See Structure of an .ipsubnetrange file (page 172).

---

**Tracking individual analysis ports**

When using the capture card in your GigaStor, you can track statistical information per physical port.

Data captured by the 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.

1. On the Home tab, in the Capture group, click **GigaStor**.
2. Click the **Settings** button.
3. Click the **General Options** tab.
   See [Setting the GigaStor general options](#) 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.

### How to change the GigaStor storage directory or drive

You can change the directory where packets collected by your GigaStor are stored. However, if you are using a GigaStor hardware appliance, this should always remain set to **D:\DATA**.

This can also be performed on any Observer and is not limited to the GigaStor.

Some reasons for changing the GigaStor storage directory include:

- You are using the GigaStor Software Edition and need to store packets somewhere else than the C:\ drive.
- You regularly schedule packet captures, so you want those captures to be saved in a specific location.
- You need to store packet captures on a higher capacity hard disk.

To change the directory where collected packets are stored:

1. Click the File tab, and click **Options > General Options**.
2. Click the **Folders** tab.
3. Change the directory used for packet captures.
Configuring options for the GigaStor charts, graphs, and reports

When updating charts and reports, keep in mind that the GigaStor Control Panel uses statistics, not packets. The indexing maximums and sampling ratio for statistics are configured in Setting the GigaStor general options and affect what appears on the charts and reports.

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. On the Home tab, in the Capture group, click GigaStor.
2. Click the Settings button.
3. Click the Statistics Lists tab.
4. Choose how you want the statistics to be displayed.

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.

Note: 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 46 (page 290) describes the different options available on the GigaStor Analysis Options screen that appears when you click the Analyze button on the GigaStor Control Panel.
### Table 46. 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 (page 294).</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 (page 294).</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 (page 296)</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 (page 178)</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. How to reorder packets based on a trailer timestamp (page 292)</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>
<tr>
<td><strong>Analysis Type</strong></td>
<td></td>
</tr>
<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><strong>This option:</strong></td>
<td><strong>Allow you to do this:</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 (page 315). 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 &quot;Expert analysis and decode&quot; 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 &quot;acceptable use&quot; 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. See Examining your network traffic with forensic analysis (page 298).</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 (page 306).</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>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</td>
</tr>
</tbody>
</table>
This option: | Allow you to do this: |
---|---
| 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. |

Third Party Decoder | Observer allows you to use other software to view packet decodes if you wish. 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 > General Options and click the Third Party Decoder tab. By default the menu text is “Decode Capture File using Wireshark,” but is completely configurable. See Third Party Decoder tab (page 32) for details on how to change the menu text and what application is used. |

Remember Analysis Options and Type | The selected the last analysis options are used for any subsequent analysis. This is useful if you typically use the same analysis options repeatedly. |

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.

Tip! 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.

How to reorder packets based on a trailer timestamp

You can change how Observer filters and sorts packets in the Decode pane based on a timestamp from your switch aggregator rather when GigaStor saw the packets.

Reordering packets is limited to post capture analysis only; it 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.

1. In the GigaStor Control Panel, select the time range of traffic you want to decode and click **Analyze**.

   **GigaStor Analysis Options** opens with the start and end time selected.

2. Select a filter type.

3. Select **Reorder and filter based on trailer timestamp** and click Settings.

   **Trailer Timestamp Settings** opens.

   Figure 78: Trailer Timestamp Settings

4. In **Timestamp type**, choose your switch aggregator.

   **Timestamp types (page 293)**

5. Choose what filters to apply.

   **Trailer filters (page 294)**

   The Decode pane displays packets in the sorted (and filtered) order based on your chosen switch aggregator.

**Timestamp types**

The Timestamp types provides a list of the supported switch aggregators that can be used to reorder packets before they are shown in the Decode pane.

<table>
<thead>
<tr>
<th>Switch Aggregator</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arista</td>
<td>Keyframes are used to correlate packets to a physical port group. For instance, any keyframe seen on port 1 associates packets with that keyframe only with port 1. Likewise, a keyframe seen on port 2 associates the packets only to port 2, and so on. A keyframe is unique to a physical port group.</td>
</tr>
<tr>
<td>cPacket</td>
<td></td>
</tr>
<tr>
<td>Gigamon</td>
<td></td>
</tr>
<tr>
<td>GigaSMART</td>
<td></td>
</tr>
<tr>
<td>Gigamon H-Series</td>
<td></td>
</tr>
<tr>
<td>Switch Aggregator</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>IXIA Anue</td>
<td></td>
</tr>
<tr>
<td>NetScaler</td>
<td></td>
</tr>
<tr>
<td>Network Instruments</td>
<td>Choose if you use Observer Matrix.</td>
</tr>
<tr>
<td>PacketPortal PDG</td>
<td></td>
</tr>
<tr>
<td>VSS Monitoring</td>
<td></td>
</tr>
<tr>
<td>VSS Monitoring w/ Port</td>
<td>VSS Monitoring with Port Stamping.</td>
</tr>
<tr>
<td></td>
<td>VSS Monitoring’s Port and Time Stamping Feature</td>
</tr>
</tbody>
</table>

### Trailer filters

Trailer filters allow you to exclude or include packets from your switch aggregator based on where the trailer occurs and other location-specific information.

<table>
<thead>
<tr>
<th>Trailer level</th>
<th>Use when multiple timestamps are found in a packet to identify which timestamp to use. The levels are identified starting at the end of the packet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>The port group ID from Matrix. You can find this ID on the Matrix in <strong>System &gt; General &gt; Trailer Configuration</strong>.</td>
</tr>
<tr>
<td>Box ID</td>
<td>The port box ID from Matrix. You can find this ID on the Matrix in <strong>System &gt; General &gt; Trailer Configuration</strong>.</td>
</tr>
<tr>
<td>Port</td>
<td>The ingress port on the switch aggregator where the packet was seen.</td>
</tr>
<tr>
<td>Probe ID(s)</td>
<td>A comma separated list of hexadecimal characters from a PacketPortal IV SFProbe or JMEP. Use PacketPortal System Manager (IV SFProbe) or the SFP Programmer GUI (JMEP) to view a list of probe IDs. A sample probe ID: 5e65eb52f633.</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 (page 292).
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 the GigaStor general 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 (page 292).
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.
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.

**Note:** 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 (page 292).
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 the GigaStor general 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.

Figure 79: 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 (page 296).

### Analyzing data by combining GigaStor Control Panel and Observer filters

**Tip!** 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.


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. On the Home tab, in the Capture group, click **GigaStor**.

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 (page 274) for details.

---

**Understanding GigaStor accelerated analysis**

GigaStor accelerated analysis significantly increases the speed that analysis results are made available in the GigaStor Control Panel. Accelerated analysis first became available in 17.1.0.0, and starting in 17.2.0.0 it is now always enabled.

**Accelerated analysis improves speed by bypassing the data mining process for packets pre-determined to not match your criteria.** In non-accelerated analysis, every packet in the GigaStor during your selected time slice requires examination against your analysis query before processing can complete. With accelerated analysis this is no longer the case. If your analysis query can be accelerated, your query will be accelerated in-part or in-full without any extra steps to follow. Your returned results are always as accurate as the "normal" speed data mine.

**Note:** GigaStor accelerated analysis requires version 17.1.0.0 or later. Starting in 17.2.0.0, it remains enabled at all times.

**No special or extra hardware is required for accelerated analysis to operate.** This means both the GigaStor hardware appliances from VIAVI and GigaStor Software Edition on your own hardware can all use accelerated analysis. Likewise, the speed increase from accelerated analysis works on active instances and their passive instances. For example, redirected probe instances to a local Observer will benefit from accelerated analysis.

**Accelerated analysis cannot increase the data mining speed of traffic that was collected previous to 17.1.0.0.** To determine which incoming packets can be accelerated in future data mines and why, accelerated analysis must see the packets as they arrive. For example, if you are upgrading to 17.1.0.0 from a previous version, none of your existing GigaStor data can benefit from accelerated analysis because old versions did not have the feature. Anything new you collect is a candidate for accelerated analysis.

**If any portion of your analysis query cannot be accelerated, log entries are shown in the Observer log.** This means that if no log entries are recorded when you perform GigaStor analysis, the entire query was sped up with accelerated analysis. If you see log entries that state accelerated analysis could not be used for part or all of your data mine, it may lead to clues as to why that happened. Accelerated analysis attempts to speed up as much of your data extraction as possible.

**Accelerated analysis cannot accelerate any analysis that is specifically asked to include Expert Information Packets in the results.** Asking that...
Expert Information Packets be in your GigaStor analysis results causes a condition where Expert Information Packets are meeting the criteria of your analysis query every 1-second (the frequency that expert packets are stored) and therefore negates any performance gains from accelerated analysis because no packets are bypassed. A warning message of longer extraction times is displayed in the GigaStor Control Panel if you attempt to include expert packets. Overall, you do not need to disable the collection of Expert Information Packets for accelerated analysis to operate correctly—simply do not ask for expert packets in your analysis results.

Filter elements that support accelerated analysis

GigaStor accelerated analysis supports single and multiple-element data extraction filters. If at least one of these listed element configurations is in your analysis filter, then accelerated analysis is possible.

Accelerated analysis occurs when your GigaStor extraction filter has at least one of these filter elements. You can join these with any other filter element using an **AND** statement and get the benefits of accelerated analysis. Conversely, your extraction cannot be accelerated if you use an **OR** statement in your extraction filter; in these cases, the GigaStor extracts data at normal speeds.

**Note:** IP addresses refer to either IPv4 and IPv6 unless otherwise noted.

| IP Address |
| IP Pair |
| IP Range |

Examining your network traffic with forensic analysis

Forensic Analysis 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.

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.

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. You can obtain the rules from [http://www.snort.org](http://www.snort.org).

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, follow these steps to import them into Observer.

1. On the Home tab, in the Capture group, click GigaStor.
2. Click the Forensic Analysis tab.
3. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.
4. Choose your profile and click Edit. The Forensic Settings window opens.
5. At the bottom of the window, click the Import Snort Files button.
6. 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.

7. 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 (page 299).

1. On the Home tab, in the Capture group, click GigaStor.
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.

Note: 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. On the Home tab, in the Capture group, click GigaStor.
2. Click the Forensic Analysis tab.
3. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.
4. Choose your profile and click Edit. The Forensic Settings window opens.
5. From the Forensic Settings window, complete the following:
   - Import Snort rules
   - Define Forensic Settings.
   - Define Rule Settings—Select the rules you want to enable.
6. 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 47. Forensic Settings options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings Profile</strong></td>
<td>Settings Profiles provide a mechanism to save and load different preprocessor settings, and share them with other Observer.</td>
</tr>
<tr>
<td><strong>IP Flow</strong></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>
</tbody>
</table>
| **IP Defragmentation** | 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)
  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 |
Examining your network traffic with forensic analysis

Field | Description
--- | ---
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Stream Reassembly (Continued)</td>
<td>Log preprocessor events—Checking this box causes forensic analysis to display all activity generated by the TCP stream assembly preprocessor to the log.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Process only established streams—Check this box if you want analysis to recognize streams established during the given packet capture.</td>
</tr>
<tr>
<td></td>
<td>Reconstruct Client to Server streams—Check this box to have analysis actually reconstruct streams received by servers.</td>
</tr>
<tr>
<td></td>
<td>Reconstruct Server to Client streams—Check this box to have analysis actually reconstruct streams received by clients.</td>
</tr>
<tr>
<td></td>
<td>Overlap method—Different operating systems handle overlapping packets using one of these methods. Choose one to match the method of the systems being monitored.</td>
</tr>
<tr>
<td>TCP Stream Reassembly (Continued)</td>
<td>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.</td>
</tr>
</tbody>
</table>
|  | Reassembled packet size threshold range—Some evasion strategies attempt to evade detection by fragmenting the TCP header across multiple packets. Reassembling the stream in
Examining your network traffic with forensic analysis
Chapter 15: GigaStor Control Panel

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 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 URLs, 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 pre-processing 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.</td>
</tr>
<tr>
<td>Normalize directory traversal—</td>
<td>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.</td>
</tr>
<tr>
<td>Normalize multiple slashes to one—</td>
<td>Another directory traversal strategy is to attempt to confuse the web server with excessive multiple slashes.</td>
</tr>
<tr>
<td>Normalize Backslash—</td>
<td>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.</td>
</tr>
<tr>
<td>Log preprocessor events—</td>
<td>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.</td>
</tr>
<tr>
<td>Report non-broadcast requests—</td>
<td>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.</td>
</tr>
<tr>
<td>Log preprocessor events—</td>
<td>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>
<tr>
<td>Port List—</td>
<td>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>
</tbody>
</table>
| 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
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 (page 292).


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 VIAVI to 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 (page 292).
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 (page 289). This opens your data in the Decode tab in Observer.
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 may be dropped, which causes them to be retransmitted 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.\(^1\)

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.\(^2\) 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.

- Using triggers and alarms to inform you when microbursts occur. Customize your triggers and actions and choose Microbursts from the Alarms list.

---

1. Information Week, April 21, 2007.
2. Microsoft Research, June 1, 2009.
Using the Microburst Analysis tab is the easiest way to analyze large chunks of time for microbursts and view the decoded packets.

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.

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 a probe instance.
2. On the Home tab, in the Capture group, click GigaStor.
3. Click the Microburst Analysis tab.
4. Highlight the data in the Detail Chart you want to analyze for microbursts and click Analyze. The GigaStor Analysis Options screen opens.
5. Choose whether you want any filters and select Microburst analysis in the Analysis Type section.
6. 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 (page 308).

Tip! 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.
To enable microburst analysis and define what on your network qualifies as a microburst:

1. On the Home tab, in the Capture group, click **GigaStor**.
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 48 (page 310) 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 48 (page 310) 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 lowest threshold allowed is 10%. The highest threshold is 100%, although it is extremely rare that 100% is ever achieved. Ninety-nine percent utilization is not uncommon though. See Table 48 (page 310) 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 capture card. We do not recommend attaching passive probe instances to the 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 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.

**Note:** 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:

1. \[ \text{Screen resolution interval} \times \frac{\text{Duration}}{\text{Time}} = \frac{\text{Maximum number of intervals}}{\text{Maximum number of intervals}} \]
2. \[ \frac{\text{Number of duration intervals with microbursts}}{\text{Maximum number of intervals}} \times 100 = \text{Percent of interval durations with microbursts} \]

**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 48 (page 310)** shows how changing one variable changes the calculations and can affect what you see in your charts.

<table>
<thead>
<tr>
<th>Table 48. Changing interval, duration, or MB Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interval</strong></td>
</tr>
<tr>
<td>Bits/sec in Interval</td>
</tr>
<tr>
<td>Bytes/sec in Interval</td>
</tr>
</tbody>
</table>
Reconstructing streams of HTTP, VoIP, and more

The process of capturing and reconstructing traffic is pretty much the same regardless of traffic type. Use these steps to reconstruct the stream.

**Note:** Stream reconstruction (including VoIP) is illegal in some jurisdictions and may be disabled by VIAVI to comply with those laws.

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 (page 292).
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 (page 289). This opens your data in the Decode tab in Observer.
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 VIAVI 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.

1. On the Home tab, in the Capture group, click **GigaStor**.
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 Selecting a time frame to analyze (page 292).

**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. An *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 Setting the GigaStor general options.
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
   - 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 Mining data from your GigaStor (page 289).
   - 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.

**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.

- **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, either 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 49. 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</td>
</tr>
</tbody>
</table>
Troubleshooting the GigaStor Control Panel

Use the information in this section to assist you if you have a problem with the GigaStor Control Panel.

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.

<table>
<thead>
<tr>
<th>This option...</th>
<th>Allow you to do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>same FIX analysis options, modify or create the profiles on one system, export them, and import them into the other GigaStor probes.</td>
<td>Import Use this button to import FIX profiles that was created and exported from another Observer.</td>
</tr>
<tr>
<td>Export Use this button to export a FIX profile.</td>
<td></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. |
| Maximum displayed results | Defines the maximum number of results to display in the GigaStor Control Panel for the fastest or slowest responses. |
| Track not responded requests within | 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. |
| Track/Type/Message | 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. |
GigaStor is full or does not have the history you expect

Your GigaStor has storage space to capture your network’s traffic. The GigaStor probe will save data until its hard drives are full (or you fill the storage capacity of a GigaStor Software Edition), 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 hardware probe or software license.

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 Observer is slow

If your Observer 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.
Chapter 16: Backups and Restoring

Many of the tools in Observer have the ability to import and export settings. You can use this functionality to back up or restore certain parts of your software configuration.

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 50. 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 Observer 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.</td>
</tr>
<tr>
<td>Export</td>
<td>Use this button to export a FIX profile.</td>
</tr>
<tr>
<td>General Settings</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,</td>
</tr>
<tr>
<td>This option...</td>
<td>Allow you to do this...</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ignore duplicate</td>
<td>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>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>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.

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.
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.

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. Click the File tab, and click Options > Protocol Definitions.
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 How to export application definitions (page 69) for details.

To import application definitions, follow the import process:

1. Click the File tab, and click Options > Protocol Definitions.
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.
Private key locations per server

Private key locations differ from application to application.

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 (page 102).

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 Encrypted private key file (page 103).

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
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 (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
♦ 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.

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-----
MIICXgIBAAKBgQD7uhNymd6WCorQh0rpd5zs4FEwCX2JrKtm0dmTf44SVaGvPLFl
vake0YP/sPs4a2uANpCbfbai2w3I2WWum4aCtqtvb82i11+13VcdyR+2SRx9Gmbu
SnoL/6FI86m+C0gHq6g0ILoiTAJnY+M0EC2bwbykz1jPVUOXE9IEGOA0QIDAQAB
AoGAFQ0YogWEVmqQp2W2NW6YXnJKxVGBGcZrPdWf9qCO/ITXhYUlt12I47QLd+ni
-----END RSA PRIVATE KEY-----

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....
JHq8U0pDbeFM9h2jZSmugxdq0a2q/MiX43Xa4Es6nKmzu9oI/ZfpIdAHi8gwtsD
mZ5bQR1X9Ae1ry+0tG2ibUhphQEsv1995FWush8N9dVumsykmMXSwND7tkwHB
i0/VVSAAD9bV3db15nbMwMnP+YC3S90GAK4ZRIqrHRQ94fd/ZAvP8kV9i1wCmX6
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. On the Home tab, in the Capture group, click **Network Trending > Network Trending**.
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. Click the File tab, and click **Options > Protocol Definitions**.
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.

   **Apply changes across all Probe Instances** only applies changes to currently connected probes instances. The changes cannot apply to disconnected 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. Click the File tab, and click **Options > Protocol Definitions**.
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.

   **Apply changes across all Probe Instances** only applies changes to currently connected probes instances. The changes cannot apply to disconnected probe instances.

5. Click **OK** to apply and save your changes.

   Your list is restored.

---

**Importing or exporting a server profile**

You can import or export servers that you monitor from one Observer to another. This can save time and reduce typing errors if you have several Observer 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. On the Home tab, in the Analysis group, click **Application Transactions**.

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.

   **Note:** 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. On the Home tab, in the Capture group, click **GigaStor**.

2. Click the **Forensic Analysis** tab.

3. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.

4. Choose your profile and click **Edit**. The Forensic Settings window opens.
5. From the Forensic Settings window, complete the following:
   - Import Snort rules
   - Define Forensic Settings.
   - Define Rule Settings—Select the rules you want to enable.

6. 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 51. 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.</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</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
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)  
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:

**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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Process only established streams—Check this box if you want analysis to recognize streams established during the given packet capture.</td>
</tr>
<tr>
<td></td>
<td>Reconstruct Client to Server streams—Check this box to have analysis actually reconstruct streams received by servers.</td>
</tr>
<tr>
<td></td>
<td>Reconstruct Server to Client streams—Check this box to have analysis actually reconstruct streams received by clients.</td>
</tr>
<tr>
<td></td>
<td>Overlap method—Different operating systems handle overlapping packets using one of these methods. Choose one to match the method of the systems being monitored.</td>
</tr>
</tbody>
</table>

TCP Stream Reassembly (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>Port List—Enabling the Port List option limits analysis to (or excludes from analysis) the given port numbers.</td>
</tr>
</tbody>
</table>

HTTP URI Normalization

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Unicode Code Page—Specify the appropriate country code page for the traffic being monitored.</td>
</tr>
</tbody>
</table>
|        | 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
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| HTTP URI Normalization (Continued) | 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.  
Look up Unicode in code page—Enables Unicode codepoint mapping during pre-processing 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 // 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). |
| 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) |
### Field | Description
--- | ---
 | 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td></td>
<td>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>
<tr>
<td></td>
<td>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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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>
</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. On the Home tab, in the Capture group, click **GigaStor**.
2. Click the **Forensic Analysis** tab.
3. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.
4. Choose your profile and click Edit. The Forensic Settings window opens.
5. At the bottom of the window, click the **Import Snort Files** button.
6. 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.

7. To use the Snort rules you just imported, right-click anywhere on the Forensic Analysis tab and choose Analyze from the menu.
Numerics
10 Gb Probe 20, 226
25901 (port) 211
25903 (port) 211
32-bit 205
3-D Pie/Chart Display Properties 76
64-bit 205, 256
64-bit, RAM 205
802.11 195, 195, 198, 218, 240
802.1Q 213, 250

A
about 271
accelerated analysis 276, 297
access point statistics 42, 42, 45, 45
activate and deactivate 93, 93
active instance vs. passive instance 196
Activity Display 55
Activity Display tool 55
adapter
see network adapter 44, 44
see network adapter 44, 44
adapter speed 240
Adapter Speed tab 240
Add Rename Filter Profile 87
Add Server to Application Transaction Analysis - Add
Server to Application Transaction Analysis 161
Add/Edit Application Transaction Analysis Server 161
Add/Edit Protocol Filter 87
Add/Edit VoIP IP 183
adding 69
adding derived definitions 69
additional volumes, using 232
address book 61
addresses, resolving 60
building 58, 58, 58, 59, 59, 59
discovery method 58, 58
editing 61
entries, adding 59, 59, 61
importing 61, 61, 61
saving 58, 61, 61
using 62
Address Filter 87
address tables 228
addresses, resolving 60
AES 150, 237, 237, 250
aggregator 293
Alarm Settings 140
alarms 145, 145, 145, 145, 145, 145, 145, 145, 146, 146, 146,
185, 185, 198, 210, 218, 319, 319, 319, 319, 319, 319, 319,
319, 319, 319
configuring 140, 140, 144
customizing 144, 144, 144, 144, 144, 144, 144
enabling 140, 140, 141, 141
exporting 145, 145, 319, 319
filter-based, creating 142, 142
high latency 141
importing 146, 146, 319, 319
resetting 143, 143, 143
retransmissions, excessive 141
VoIP 185, 185, 185
allocating 208
analyzer connection 211
analyzing 298
analyzing data 178, 178, 294, 295, 312, 312
Anue 293
Anyone account 211, 211
Apache Web Server 102, 321
Application Definitions and Server Application
Discovery Settings 62
Application Discovery, Server 66
Application Performance Analysis 254
about 156
collection intervals 156
configuring 157
response time calculation 156
Application Transaction Analysis 161, 254
about 160, 161
response time calculation 160
Application Transaction Analysis - Graph Properties
161
Application Transaction Analysis Trending Specific -
Servers 161
applications, analyzing 161, 171
applications, see server applications 66
applying 94, 94, 114
ArcaBook Multicast 66
archiving data 286
Arista 293
ARP inspection 300, 324
ARP Inspection, network forensics preprocessor 300,
324
as probe or analyzer 254
Asset ID 154
Asset name 154
Asset type 154
ATA 164
ATM 232, 232, 240, 241
ATM Address Filter 87
autoupgrade 237
Autoupgrade tab 240
autoupgrading 237, 240

Index
B
backup 20, 226
backups 228
bad TCP checksums 212
troubleshooting 212
Bandwidth Utilization 44
Bandwidth Utilization - Full Duplex Display 44
Bandwidth Utilization tool 44, 44, 45
Bandwidth Utilization with Filter 45
best practices 196
BFR 32, 80, 101
BIOS memory hole 205
Box ID 294
broadcast and multicast storms 55
broadcast traffic 233
buffer 202
buffer size 196, 288
buffer statistics 202
buffer, see capture buffer and statistics buffer 202
buffers 196, 198, 198, 198, 205, 207, 218, 218, 218
circular 78, 78
configuring 73, 77
replaying 107
bugtraq 299, 299
building 58, 58, 58, 59, 59
C
Calculate Cumulative Bytes 108
calculating
network delay 122
response time 123
caller ID 184
CAP 80, 101
capacity 273
Capture Application Transaction Analysis 161
capture buffer
64-bit Windows 202
FIFO 276
IP defragmentation 300, 324
Max Buffer Size 202
overwriting 276
physical ports 276
RAM limitations 202
size 202
TCP stream 300, 324
capture card 47, 75, 239
driver requirements 22, 223
filter ports 276
passive probe instance 196
performance 196
ports 276
probe instance warning 196
recommendations 209
statistics 276
time synchronization 239
capture card driver 22, 223
Capture Decode 110
capture decodes 240
Capture Graph 76
Capture Internet Observer 39
Capture Pairs (Matrix) 41
Capture Protocols 42
Capture Summary 49
Capture Top Talkers 46
Capture VLAN 57
captures
see packet captures 83
see packet captures 83
capturing 82
capturing packets 281
CAPWAP Control 66
CAPWAP Data 66
CDU 240
Certificate ID 154
CIFS 160
CIR 140
circular 78, 78
Cisco 6xxx switches 216
troubleshooting 216
Cisco EAP/LEAP 255
Classic Mode 34
clock synchronization 239
CME RLC 66
collecting data 239
collection interval 267
collection intervals 156
collision test 215, 215
color codes 130
command line 96, 96
command line, enabling 95, 95
Committed Information Rate 140
common issues 209
common problems with 210, 211
Configure IP Application List for Internet Observer Statistics Dialog 39
Configure IP Application Ports Dialog 41
Expert Information 77
network trending folder 237
partial packets 79, 79, 79
probe name 237
configuring statistics memory 238
connecting 234
connecting to analyzer 234, 234, 234, 235, 239
Connection Dynamics 100
about 129
color codes 130
packet types 130
using 129
connections 39, 39, 39, 39, 41, 41, 41, 46
content 245, 245
context 245, 246
contextual visibility 245, 246, 248
cPacket 293
CRC-16 241
CRC-32 241
creating 82, 93
CSU 240
encapsulation 241, 241
customizing 144, 144, 144, 144, 144, 144
D
D3 240
D3/E3/HSSI 240
DAAP 128
data rate 170, 274
data storage 288
data transfer 253, 253, 253, 253
data, collecting 165, 169
data, deleting 165
data, viewing 165
daylight savings time 215
Daylight Savings Time 215, 215
Decode and Analysis 110
Decode pane 293
decodes
troubleshooting 317
decoding 100, 100, 103, 108, 113, 114, 114, 132, 177, 177, 177, 198, 198, 198, 218, 218, 218, 281, 299
expert analysis 100, 119, 129
configuring 118, 121, 121
summary view 123
using 124
expert thresholds
configuring 132, 132
geolocation 33
NetFlow 106, 114
packet captures 100, 100, 100, 100, 103, 113
encrypted 102, 102, 103, 103, 321, 321
reconstruction 128
sFlow 106, 114
user interface 108, 108, 110, 110
using third party decoder 32, 32
VoIP 177, 177
defining its purpose 208
definition 195
definitions, restoring 71, 323
deleting
network trending data 165
denial of service 300, 324
derived application definitions 69
derived applications 29
Device Configuration 106
devices 63, 183
discouring 63, 63, 63
DHCP 160
DHCPv6 160
Diameter 160
difference from packets 283
difference from statistics 283
directory 288
Discover Network Names 214, 214, 214
VLANs 214
Discover Network Names (Address Book) 62
Discover Network Names Mode 62
Discover Network Names tool 58, 59
Discover SNMP Devices 63
discovering 62, 62, 62, 63, 63, 63
discovery method 58, 58
Display Protocols for Selected Station 42
Display Stations sending Selected IP 100
DLCI Address Filter 87
DLCI CIR Setup 140
DMP 80, 101
DNS 59, 60, 160
DNS names
resolving 60
DNS resolution 237
driver error support 49
driver requirements 22, 22, 22, 223, 223, 223
drivers, wireless 223
DS3
fractionalized 241
DSU
encapsulation 241, 241
duplicate, removing 82, 123
dynamic 70
dynamic traffic management 245, 245, 248

E

e1 240
   WAN relay type 241
e3 240
   fractionalized 241
EAP/LEAP 255
Edit IP Application Port Dialog 39
Edit Pager Entry Dialog 100
Edit Probe Instance 203
Edit Probe User Account Dialog 100
Edit Statistics Memory Configuration 100
editing 61
ports 70
effects of packet capture 207
efficiency 149
e-mail, via 192
E-Model 181
enabling 140, 140, 141, 141
ENC 80, 101
encrypted 102, 102, 103, 103, 321, 321
encrypted traffic 103
encryption 29, 29, 29, 29, 29, 237, 237
   AES 150, 250
see also security 150, 250
encryption key 211, 226, 237, 255
encryption keys 226
End to End Server Analysis - MultiHop Analysis 125
End to End Server Analysis - Server Analysis 125
End to End Server Analysis Settings - Display - End to End Analysis 125
End to End Server Analysis Settings - Display - Response Time 125
End to End Server Analysis Settings - Display - Server Load 125
End to End Server Analysis Settings - Display - Utilization 125
End to End Server Analysis Settings - Files 125
End to End Server Analysis Settings - General 125
End to End Server Analysis Settings - Synchronization 125
End-to-End Analysis
using 125
End-to-End Analysis
using 125, 125, 125, 125, 125
entries, adding 59, 59, 61
Error Filter 87
erors 49, 50, 50, 50, 53
Ethernet 53
Errors by Station 50
Errors by Station tool 50
ErrorTrak 16, 217
ESX/ESXi
troubleshooting 23, 24, 24
Ethernet 53, 195, 195, 198, 240
ARP inspection 300, 324
errors 53
full-duplex 198, 218
Index

geolocation 33, 33
getting started 269
Gigabit 198, 240
  jumbo frames 240
Gigabit Probe 20, 226
Gigabit tab 240
gigabytes 202, 202
Gigamon 245, 245, 246, 250, 293
Gigamon GigaSMART 293
Gigamon H-Series 293
GigaStor 208, 233, 247, 248, 253
  about 271
  AES 237
  collision test 215
  encryption 237
  Expert Probe 253
  getting started 269
  indexing 284
  RAM 208
  recommendations 209
  reserved memory 208
  traffic generation 215
  virtual machine with 256
GigaStor capture 196, 198, 218
GigaStor Control Panel 280
  analyzing data 178, 178, 294, 295, 312, 312
  archiving data 286
  buffer size 288
  capturing packets 281
  configuring 276, 287
  filters 294, 295, 296
  finding a specific time 292
  FIX 315
  forensic analysis 298, 300, 305, 306, 324
  getting started 269
  mining data 289, 292
  Observer settings 276
  packet capture 282, 282, 282, 288
  ports 287
  privacy 282
  scheduled capture 282
  security breach 305
  Snort 300, 324
  Snort rules 299, 299, 329
  stream reconstruction 311, 312
  subnets 287
  trimming data 282
  troubleshooting 296
  using 274
GigaStor Portable 215
GigaStor Software Edition 272
GigaVUE 245, 245, 246, 247, 248
GigaVUE H series node 247
Graph Display Properties 100
Graph Display Properties - Graph Time 100
  group ID 294
  GSAA 276, 297, 298
  GSE 272, 273

H

H.245 160
H.248 160, 160
H.323 100, 160
hardware 17, 203, 220, 272
hardware acceleration 209

hardware requirements 16, 217
hidden features
  See Classic Mode
high latency 141
high-volume 298
HSSI 240, 241
HSSI, fractionalized 240
HTTP 128, 160

ICA 160
ICMP Expert 100
Ignore response times longer than 164
IIS Web Server, Windows 102, 321
IMAP 160
IMAP4 128
importing 61, 61, 61, 62, 62, 68, 146, 146, 146, 176, 319, 319, 320, 323
  address book 61
  alarms 145, 145, 146, 146, 146, 319, 319, 319, 319, 319
  protocol definitions 62
  server applications 68, 320
  VoIP 176, 323
in a switched environment 200
indexing 280, 284, 284
individual stations 41, 41, 41, 46
install 19, 221
installation 19, 19, 20, 20, 221, 222, 222, 226
installer 19, 221
installing 19, 19, 20, 221, 222, 222
Interface Properties 100
interface switching 198, 218
Internet Observer 39
Internet Observer Internet Patrol 39
Internet Observer IP Subprotocols View 39
Internet Observer Settings 39
Internet Observer tool 39, 39, 39
Internet Patrol 39
Internet Patrol - Pair Circle 39
IP address
  GigaStor 233
  IPv6 300, 324
  NAT 215
  statistics 289
IP Calculator 62
IP defragmentation 300, 324
IP Discovery 62
IP flow 300, 324
IP Fragment Bits Filter 87
IP Fragment Offset Filter 87
IP mapping 138, 139, 139, 139
IP masquerading, see NAT 215
IP Pairs - Pair Circle 100
IP precedence 240, 240
IP Properties 100
IP range 184
IP Subnet Mask Calculator 62
IP Subprotocols 100
ipsubnetrange 172
IPTV 167, 289
IPv4 232, 232
IPv4 Options Filter 87
IPv4 TOS Precedence 79
IPv6 32, 232, 232, 300, 300, 324, 324
IPv6 Address representation 100
IPv6 Flow Label 79
IPv6 Options Filter 87
IPv6 Traffic Class 79
Issuing time 154
IXIA 293
IXIA Anue 293

J
jitter
calculating 187
Jitter 100
jumbo frames 240, 240, 240

L
LAPB 240
laptop
NICs 255
using as probe 255
wireless 255
Last seen IP 154
Last seen time 154
Layer 3 Switch 214
LDAP 93, 93, 160
license 228, 273
license update 20, 227
licenses
redeeming 20, 226
troubleshooting 20, 226
licensing 20, 227
limitations 156, 156, 161
limitations of 254
line frame 240
List Bar Display Properties 100
List Display Properties 100
load 43
preprocess settings 300, 324
load, preprocessor 196
load, testing 47, 47, 126
loading 80, 101
local probe 26
Locator, Switch Station 62

M
MAC address
statistics 289
MAC addresses 214
Mac Header 232, 232
MAC Properties 100
macro graph, see Outline Chart 292
matching between probe and analyzer 211
Matrix 293, 294
Max Buffer Size 202
MDS Fingerprint 154
Mean Opinion Score (VoIP Expert) 100
megabytes 196
MEGACO 160
memory 203, 203
memory allocation 238
memory management 202
memory tuning 202
memory, see RAM 207
merging 81
micro graph, see Detail Chart 292
microburst analysis 292
microbursts, about 306, 306
microbursts, searching for 306
Microsoft 23, 225
Microsoft Lync Server 102, 321
Microsoft Network Discovery 62
minimum specifications 17, 220, 272
minimum specs 17, 220, 272
mining data 289, 292
mirror port 200
mirror port, see also SPAN ports 200
missing 84, 211
missing features
See Classic Mode
missing from Observer 233
Modify Observer Reserved Memory dialog 100
MOS 181
MOS Settings 100
moving through RAM 207
MPLS 198, 218, 230, 232, 240, 240
ATM 232
IPv4 232
IPv6 232
Mac Header 232
pseudowire word 232
MPLS Filter 87
Msft (Microsoft) Configuration 62
MSRPC 160
Multi Probe 198, 198, 218
changing NIC 233
configuring 240, 240
connecting to analyzer 234
data transfer 253
limitations of 254
redirection 234
multicast 228
Multicast Pitch 66
MultiHop Analysis 133
configuring 136, 136
IP mapping 138, 139, 139, 139
synchronization method 136, 136
user offset 136, 138
using, quickly 135
Multiple Address Tables 62
Multiple Filters 87
multiple in a system 239
name, changing 237
naming 231
NAT 215, 215, 215
NetFlow 106, 106, 114, 198, 216, 218, 240, 267
decoding 114
TAPs and 215
versions supported 267
NetFlow collector 267
NetFlow Device Configuration 106
NetFlow Trending collector 267
NetScaler 293
network 49, 49, 49, 50, 51, 55
errors 50
load 43
load, testing 47, 47, 126
summary 49, 49
troubleshooting 49, 49, 49, 49
utilization 43, 44, 44, 45, 45, 48, 48, 49, 49
Network 1 probe instance 231
Network Activity Display Properties 55
network adapter
capture card 47, 75
configuring 44
network adapter, see also NIC 233
Network Errors Settings 50
Network Intrusion Detection 298, 298
network load 43, 47, 47
viewing 292
network masquerading, see NAT 215
network packet broker 245, 245, 246
Network Summary 49
Network Summary tool 49
network trending 171, 180, 181, 198, 210, 218, 255
about 161
Application Performance Analysis
about 156
collection intervals 156
configuring 157
Application Transaction Analysis 160
applications, analyzing 161, 171
configuring 166, 167, 171
data, collecting 165, 169
data, deleting 165
data, viewing 161, 165
devices 183
disk space requirements 170
enabling 175
filters 267
hard drive space 170
IP range 184
limitations 156, 156, 161
MOS 181
sampling divider 267
scheduling 169
server profiles 162, 324
settings 180, 181
VoIP 175, 180, 181, 181, 181, 183, 184
Network Trending 155, 228
network trending default location 171
network trending disk space requirements 170, 274
network trending folder 237
Network Trending Folder 171
network trending hard drive space 170, 274
network trending limit 171
network trending max 171
network trending maximum 171
Network Trending Schedule 169
Network Trending Settings - MOS 100
network trending space required 170, 274
network trending storage limits 171
Network Trending Viewer 165
Network Vital Signs tool 49
NFS 160
NIC 198, 218, 223
broadcast traffic 233
changing 233
missing 211, 233
missing from Observer 233
multiple in a system 239
NICs 255
NIDS 298
NIProbe.exe 20, 226
NNTP 128
no network card 233
not connecting 211
notifications 192, 192, 192, 193, 193, 193, 194, 194
Notify Probe User 79
NPB 245, 245, 246
Numeric Value Filter 87
Observer
encryption 29
feature suitability 79
no network card 233
notifications 192, 192, 192, 193, 193, 193, 194, 194
regulation compliance 147
switching to probe 198, 218
system requirements 16, 217
user interface 26
Observer Analyzer 20, 226
Observer General Options - folders 100
Observer General Options - IPv6 100
Observer General Options - Security 100
Observer General Options Tab 100
Observer GigaStor 20, 226
Observer Management Server 237
Observer settings 276
observer.exe 20, 226
OMS 29, 29, 29, 29, 29, 29, 29, 198, 218, 237
SafeNet HSM 103
synchronizing protocol definitions 62
OpenView 141
operating system 18, 221
options 237
OR filter example 93
OSI Layer 7 254
other codecs 128
overwriting 276
Packet
analyzing 298
decoding 299
sampling 276
packet alert threshold 300, 324
packet broker 247, 248
packet broker integration 247
Packet Broker Integration tab 245
packet capture 207, 240, 240, 282, 282, 282, 288
active instance vs. passive instance 196
buffer 202
daylight savings time 215
decoding 198, 218, 281
GigaStor Portable 215
high-volume 298
memory 203
partial 292
RAM 207
reassembling 300, 324
packet capture directory 288
Packet Capture on Multiple Instances Settings 82
Packet Capture Options 76
Packet Capture Schedule 83
packet captures 76, 83, 83, 83, 100, 100, 100, 100, 100, 103, 113, 148, 149
configuring 73, 76, 77, 78, 79, 82
Expert Information 77
Index | 337
partial packets 79, 79, 79
creating 82
decoding 100, 100, 103, 108, 113, 132
efficiency 149
encrypted 102, 102, 103, 103, 321, 321
filtering 87
from multiple sources 82
from unknown sources 101, 101
loading 80, 101
merging 81
replaying 107
saving 80, 80, 101, 101, 112
scheduling 83, 83
security 149
sharing 148
synchronizing 136, 136, 138, 138
timestamps 76
transferring 83
wireless 16, 217, 255
packet filters 298
packet fragmentation 300, 324
packet headers, limiting captures to 276
Packet Length Filter 87
Packet Portal 293
packet storms 55
Packet Time Filter 87
packet types 130
Packet View Settings - Column Order 100
Packet View Settings - Configure SNMP MIBs 100
Packet View Settings - General 100
Packet View Settings - Protocol Forcing 100
Packet View Settings - Summary 100
PacketPortalPDG 293
packets 46, 82
capturing 82
difference from statistics 283
duplicate, removing 82, 123
Expert Information 77
Expert Information, excluding 77
missing 84
moving through RAM 207
RAM 207
saving 112
searching for 113
sizes 46
skipped 131
Paging Server Properties Dialog 193
paging service 193, 193
Pair Statistics (Matrix) 100
Pair Statistics Settings 100
Pair Statistics Settings - List 100
Pair Statistics Settings - Pair Circle 100
Pair Statistics Settings - Statistics Settings 100
Pair Statistics tool 41
partial 292
Partial Packet Capture for TCP/UDP Payload Filter 148
partial packets 79, 79, 79, 82
partial packets, saving 276
passive probe instance 196
Pattern Filter 87, 89
PCAP 32, 80, 101
PCAPNG 80, 101
performance 196
Phone Pager Schedule 100
physical port indexing, see virtual adapters 269
physical ports 276
Ping Trace Route 65
Ping/Trace Route 65, 65
POP3 128, 160
port 294
port bonding 198, 218, 264
Port Filter 87
port tag 250
ports 27, 67, 70, 70, 276, 280, 287
filtering, physical 295
Post Capture Filtering 94
post-filters
applying 94, 94, 114
command line 96
command line, enabling 95
pre-filters
creating 87, 93
scope 93, 93
preprocess settings 300, 324
privacy 282
Probe Alarms Settings - Actions 144
Probe Alarms Settings - Alarm List 141
Probe Alarms Settings - Triggers 144
probe connection 211
probe ID 294
probe instance 292
active 196, 202
active vs. passive 196
best practices 196
configuring 240
configuring statistics memory 238
connecting 234
connecting to analyzer 239
defining its purpose 208
definition of 196
memory allocation 238
memory tuning 202
naming 231
passive 196
redirecting 233
reserving memory 202
specifying NIC 239
probe instance warning 196
probe instances
redirecting 235
probe name 237
probe redirection 234
Probe redirection error 211
Probe Service Configuration Applet 254
probe, local 26
probes 82, 235
Adapter Speed tab 240
Autoupgrade tab 240
autoupgrading 237, 240
backing up 228
clock synchronization 239
collecting data 239
common problems with 210, 211
configuring 237
connecting to analyzer 234, 235
D3/E3/HSSI 240
definition 195
encryption keys 226
General tab 240
Gigabit tab 240
hardware 203
hardware acceleration 209
physical port indexing, see virtual adapters 269
physical ports 276
in a switched environment 200
IP precedence 240
MPLS 232, 240
name, changing 237
not connecting 211
options 237
port bonding 264
see probe instances 235
protecting 23, 225
running as Windows service 237
security 235
software, versions 198
SPAN ports 198
statistics sampling divider 240
switching to analyzer 198, 218
T1/E1 tab 240
upgrading 226, 226
Virtual Adapters tab 240
virtual TAPs 256
VLAN access 211
WAN 240
wireless 240
Wireless 802.11 tab 240
see probe instances 235
promiscuous mode 16, 200, 217, 255, 256
protected memory 201, 203, 203, 203, 205, 207
protecting 23, 225
protocol 160
Protocol Filters 88
protocol definitions 62, 62
exporting 62
importing 62
Protocol Definitions and Server Application Discovery 100
Protocol Distribution 42
Protocol Distribution Settings 42
Protocol Distribution Statistics 42
Protocol Distribution Statistics Switched 42
Protocol Distribution tool 42
Protocol Filter 87
protocols 41, 41, 42, 42, 42, 280
statistics 42
pseudowire word 232, 232

Q
QoS 240
Quality of Service (QoS) 100

R
RADIUS 160
RAID 196, 196, 232
RAM 17, 207, 207, 207, 208, 220, 272
allocating 208
buffer size 196
effects of packet capture 207
formula 202
GigaStor 208
limitations 202
packet capture 196, 202
probe instance 292
see also buffer 202
see also protected memory, user memory, and
reserved memory 201
recommendations 205
reserving for Observer 240
resizing 201
statistics 202
TCP stream reassembly 300, 324
tuning 202
used in Observer 201
Windows 202
RAM limitations 202
RAM needed for busy networks 208
Random Access Memory, see also RAM 201
Real Time Protocol 187
Real-time Transport Control Protocol 100
Real-time Transport Protocol 100
reassembling 300, 324
recommendations 205
recommended specifications 17, 220, 272
recommended specs 17, 220, 272
reconstruction 128
see stream reconstruction 128
see stream reconstruction 128
reconstruction, stream 100, 128, 128
redirecting 233, 235
redirecting, see probes 235
redirection 234, 234, 234, 234
registry 228
regulation compliance 147, 147
see security 147
see security 147
Remote Probe Expert Analysis and Decode 100
Reorder and filter based on trailer timestamp 292
reorder packets 293
Replay Packet Buffer 100
replaying 107
reports
email, via 192
requirements, hardware/software 16, 217
Reserve Observer Memory 100
reserved memory 198, 203, 203, 205, 207, 208, 218
see also RAM 201
reserved memory from 198, 218
reserved memory in Observer 240
reserving for Observer 240
reserving memory 202
resetting 143, 143, 143
resizing 201
Resolve IP 62
resolving DNS names 60
response time 123, 164
response time calculation 160
restoring 71, 71, 72, 323, 323, 323
retransmissions, excessive 141
RFC1213
see SNMP 63, 63
see SNMP 63, 63
RMON 200
RMON Extension Configuration 79
RMON Tables 100
Router Observer 43
Router Observer Settings 43
Router Observer tool 43
routers 43, 43, 43, 43
statistics 43
RTP 100

Index | 339
SafeNet HSM 103, 103
sampling 276
sampling divider 210, 267, 267
sampling ratio 280
Save Packet Capture 112
saving 58, 61, 64, 80, 80, 101, 101, 112, 112
saving packet captures 80, 101
saving, formats 80, 101
SCCP 160
scheduled capture 282
scheduling 83, 83, 169
scope 93, 93
scripts 228
searching for 113
security 149, 198, 218, 235
  encryption 150, 250
  encryption key 211
  matching between probe and analyzer 211
  packet captures 148, 149
  personal information 20, 226
  Probe redirection error 211
  probes 82, 235
  regulation compliance 147
  user accounts 148
security breach 305
Select WEP Profile 112
self-optimizing management 245, 245
Server Analysis
  using 100, 100, 125, 125
Server Application Discovery
  adding derived definitions 69
  definitions, restoring 71, 323
server applications
  adding 66, 69
  discovering 62, 62, 62
  editing 70
  exporting 62, 68, 69, 320, 320
  importing 62, 68, 69, 320, 320
  ports 67, 70, 70, 70
  restoring 71, 71, 72, 323, 323, 323
  see also applications 66
server profiles 162, 324
Server, Apache Web 102, 321
Server, Windows IIS Web 102, 321
service 237
services 254
Set Local Probe Name 100
settings 181, 200
settings profiles 300, 324
sFlow 106, 106, 114, 198, 218, 240
  decoding 114
  Device Configuration 106
sFlow, versions supported 267
SHA1 Fingerprint 154
sharing 148
Shoutcast 66, 128
signal strength 52
signal strength conversion 52
simultaneous 198, 218
Single Probe 198, 198, 218
  Anyone account 211
  changing NIC 233
  configuring 240, 240
  data transfer 253
  redirection 234
  VoIP 254
Single Probe memory limit 203
SIP 160, 183, 183
site survey 51
Size Distribution Settings 46
Size Distribution Statistics 46
Size Distribution Statistics tool 46
sizes 46
skipped 131
skipped packets 131
slow 230
slow probe system 210
SMB 160
SMTP 128, 160, 192, 192
Sniffer 80, 101
SNMP 200, 228
  devices 63
  discovering 63, 63, 63
  SNMP General Options Tab 100
  SNMP traps 141
Snort 298, 299, 300, 300, 324, 324
  IP flow 300, 324
  IPv6 300, 324
  variable name 300, 324
SNORT 228
Snort rules 299, 299, 299, 329
software probes 198, 226
software requirements 16, 217
software, versions 198
SPAN
  VLANs 213
  SPAN port 213
see also mirror port 200
SPAN ports 198
  broadcast traffic 233
  settings 200
  software probes 198
  see also mirror port 200
  virtual machine 256
specifications 17, 220, 272
specifying NIC 239
specs 17, 220, 272
SSL 103, 103, 103, 103, 103, 103, 108, 108, 108
SSL, decrypting 103
SSL/TLS Decryption Parameters 100
State 154
Stations - Pair Circle 100
statistics 42, 42, 42, 43, 45, 45, 51, 202, 240, 255, 276, 289, 289
  collection interval 267
  connections 39, 39, 39, 39, 41, 41, 41, 46
  difference from packets 283
  errors 49, 50, 50
  individual stations 41, 41, 41, 46
  memory 203
  network load 43
packet capture 240
packets 46
protocols 41, 42, 42, 42
RAM needed for busy networks 208
routers 43, 43, 43, 43
sampling divider 210, 267
top talkers 46, 46, 46, 46
utilization 44, 45, 48, 49
VLAN 57, 57, 57
wireless 42, 51, 51

statistics buffer 202, 202
Statistics Memory Allotment Page 100
statistics queue buffer 201, 203, 205, 207, 207, 208, 209
statistics sampling divider 240
storage 17, 220, 272
storage size 273
stream reconstruction 100, 128, 128, 311, 312
other codecs 128
Stream Reconstruction 100
Subnet mask 79
Subnet Mask Calculator 65, 65
subnets 287
summary 49, 49
summary view 123
supported 298
switch 293
switch aggregator 292, 293, 294
Switch Station Locator tool 62
switching to analyzer 198, 218
switching to probe 198, 218
synchronization 138, 215, 239
synchronization method 136, 136
synchronizing 136, 136, 138, 138
synchronizing protocol definitions 62
system load 276
system requirements 16, 217
system specification 17, 220, 272

timestamp 292
timestamps 76, 294
packet captures 76
Tivoli 141
TNS 160
Token Ring Errors by Station 50
Token Ring Vital Signs 49
top talker 280
top talkers 46, 46, 46, 46
Top Talkers 55, 202
Top Talkers Statistics 46
Top Talkers tool 46, 46
top talkers, defined 46
topologies 195, 198, 218
802.11 195
Ethernet 195
ToS 240
traffic generation 215, 215
Traffic Generator 47
Traffic Generator Settings 47
trailler 294
trailler filters 294
trailler level 294
trailler timestamp 292, 294
Trailler Timestamp Settings 292
trailler 294
transferring 83
transferring packet captures 83	
trending
see network trending 161
triggers 198, 210, 218
trimming data 282
troubleshooting 49, 49, 49, 49, 212, 216, 296, 316
analyzier connection 211
bad TCP checksums 212
broadcast and multicast storms 55
Cisco 6xxx switches 216
common issues 209
network 47, 49, 49, 49, 50, 51, 55
packet storms 55
probe connection 211
slow decode 317
slow probe system 210
SSL, decrypting 103
synchronization 138
virtual machines 23
VLAN Statistics tool 212, 213
VLAN visibility 214
TTL Hop Limit 79

UDP Expert 100
Update Chart button 276
updating 23, 225
Observer 20, 226
upgrading 19, 20, 222, 222
upgrading 19, 20, 222, 222, 226, 226, 226
upgrading version 16 20, 222
upgrading version 17 19, 222
upgrading, encryption keys 226
user accounts
security 148
user interface 26, 108, 108, 110
see Observer 26
user memory 201
user offset 136, 138
users 198, 211, 218
simultaneous 198, 218
using 62, 100, 100, 100, 124, 124, 125, 125, 125, 125, 125, 125, 126, 126, 274
using as probe 255
using third party decoder 32, 32
using, quickly 135
utilization 43, 44, 44, 44, 45, 45, 45, 48, 48, 48, 49, 49
Utilization History 48
Utilization History tool 48
Utilization Thermometer Mode 48
Utilization Thermometer tool 49

V
v16 20, 222
v17 19, 222
variable name 300, 324
version 16 20, 222
version 17 19, 222
version numbering 37
versions supported 267
viewing 292
virtual adapter 196, 240, 256, 264
virtual adapters 269
Virtual Adapters tab 240
virtual machine 16, 17, 217, 220, 256, 256, 256, 272
vSphere 23, 23, 24, 24
virtual machine with 256
virtual NIC 256
virtual Tap 100
Virtual Tap Settings Dialog 100
virtual TAPs 256
virus protection 23, 225
VLAN 57, 57, 57, 213, 213, 250
"No VLAN" 212, 213
VLAN access 211
VLAN Filter 87
VLAN ISL Filter 87
VLAN Properties 57
VLAN Statistics 57, 213
VLAN Statistics tool 57, 212, 213
VLAN visibility 214
VLANs 213, 213, 214
Discover Network Names 214
SPAN port 213
VM specs 17, 220, 272
VMONI 211
VMONI Protocol Analyzer 211
VMware 17, 220, 272
VoIP 100, 176, 176, 177, 177, 177, 181, 181, 181, 183, 184, 185, 185, 185, 198, 218, 240, 254, 254, 323, 323
alarms 185, 185
caller ID 184
decoding 177, 177
exporting 176, 323
filtering telephone numbers 177
importing 176, 323
network trending 175, 180, 181
devices 183
IP range 184
MOS 181
settings 181
terminology 189
VoIP RTP RTCP Graph 100
VoIP Settings - Caller ID 184
VoIP Settings - Device IP Address 183
VoIP Settings - General 181
VoIP Settings - IP Range Filters 184
VoIP Settings - MOS Score 181
VPN 215
vSphere 17, 220, 272
troubleshooting 23, 23, 24, 24
VSS 293
VSS Monitoring 293
VSS Monitoring w/Port 293

W
WAN 136, 240, 246, 240, 240
fractionalized 240
WAN alarms 140
WAN Conditions Filter 87
WAN Load 55
WAN Port Filter 87
WAN relay type 241, 241
WAN switch 62
WAN Type 241, 241
WAN vital plot properties 49
WAN Vital Signs 55
WAN Vital Signs by DLCI 49
Web Observer 41
WEB Observer Settings 41
Web Observer tool 41
Web Server, Apache 102, 321
Web Server, Windows IIS 102, 321
WebSphere 160
What-if modeling
using 126, 126
Windows 223
32-bit 205, 228
64-bit 202, 205, 228, 256
registry 228
reserved memory from 198, 218
reserved memory in Observer 240
service 237
services 254
Windows 10 18, 221
Windows 2003 18, 221
Windows 2008 18, 221
Windows 2012 18, 221
Windows 2016 18, 221
Windows 7 18, 221
Windows 8 18, 221
Windows IIS Web Server 102, 321
Windows memory pool 203, 203
Windows protected memory 201
Windows updates 23, 225
Windows Vista 18, 221
access point statistics 42, 42, 45, 45
signal strength conversion 52
site survey 51
Wireless 802.11 tab 240
wireless access point 255
Wireless Access Point Filter 87
Wireless Access Point Load Monitor 42
Wireless Access Point Settings 42
Wireless Access Point Settings - List 42
Wireless Access Point Statistics 42
Wireless Access Point Statistics tool 42
Wireless Channel Filter 87
Wireless Data Rate Filter 87
wireless driver 223
wireless interference 51
Wireless Network Errors by Station 50
wireless network, encryption key 255
wireless packets, raw 16, 217, 255
Wireless QoS 79
Wireless Signal Strength Filter 87
Wireless Site Survey 51
Wireless Site Survey - Channel Scan 51
Wireless Site Survey – Ctrl. Frames 51
Wireless Site Survey – Data Frames 51
Wireless Site Survey – Frame Types 51
Wireless Site Survey – General Info 51
Wireless Site Survey – Mgmt. Frames 51
Wireless Site Survey – Signal 51
Wireless Site Survey – Speeds 51
Wireless Site Survey tool 51
Wireless Vital Signs 49
Wireshark 32, 80, 101
WMPNSS 128
Word Report Options 100

X
XML 80, 80, 101, 101

Y
YouTube 245, 245

Symbols
“No VLAN” 212, 213