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 Number</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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which version of Observer is right for you?</td>
<td>8</td>
</tr>
<tr>
<td>Observer Standard</td>
<td>11</td>
</tr>
<tr>
<td>How to install or upgrade the software</td>
<td>11</td>
</tr>
<tr>
<td>Minimum and recommended system specifications</td>
<td>12</td>
</tr>
<tr>
<td>How to upgrade to Windows 10</td>
<td>13</td>
</tr>
<tr>
<td>How to install all versions</td>
<td>14</td>
</tr>
<tr>
<td>How to upgrade version 17 and later</td>
<td>14</td>
</tr>
<tr>
<td>How to upgrade version 16 and earlier</td>
<td>15</td>
</tr>
<tr>
<td>FAQ: Licensing and updating</td>
<td>15</td>
</tr>
<tr>
<td>Capture card driver requirements</td>
<td>17</td>
</tr>
<tr>
<td>Installing Windows updates and updating virus protection</td>
<td>18</td>
</tr>
<tr>
<td>Virtual machine troubleshooting</td>
<td>18</td>
</tr>
<tr>
<td>Cannot capture traffic using VMware ESX VM</td>
<td>18</td>
</tr>
<tr>
<td>Experiencing BSOD when packet capture starts</td>
<td>19</td>
</tr>
<tr>
<td>Overview of Observer</td>
<td>20</td>
</tr>
<tr>
<td>User interface</td>
<td>21</td>
</tr>
<tr>
<td>Ports used by Observer Platform v17 and later</td>
<td>22</td>
</tr>
<tr>
<td>Configuring Observer’s general settings</td>
<td>22</td>
</tr>
<tr>
<td>General tab</td>
<td>23</td>
</tr>
<tr>
<td>Security tab</td>
<td>24</td>
</tr>
<tr>
<td>Folders tab</td>
<td>26</td>
</tr>
<tr>
<td>SNMP tab</td>
<td>26</td>
</tr>
<tr>
<td>IPv6 tab</td>
<td>27</td>
</tr>
<tr>
<td>Third Party Decoder tab</td>
<td>27</td>
</tr>
<tr>
<td>GeoIP Settings</td>
<td>28</td>
</tr>
<tr>
<td>How to have managed by OMS</td>
<td>28</td>
</tr>
</tbody>
</table>
Decoding network traffic................................................................. 93
I have a packet capture to analyze. What file formats can Observer load?.......... 94
Opening files from unknown locations.................................................. 94
Private key locations per server.......................................................... 95
Replaying a packet capture................................................................... 96
Working with packets...................................................................... 97
Using the Decode pane.................................................................... 99
Saving a packet capture.................................................................. 102
Searching for a specific packet.......................................................... 103
Filtering your saved packet capture.................................................. 104
Processing NetFlow or sFlow data..................................................... 104
Packet View Settings........................................................................ 104
Configure SNMP MIBs...................................................................... 105
General............................................................................................ 105
Protocol Colors.............................................................................. 107
Protocol Forcing............................................................................. 107
Summary......................................................................................... 107
TCP/UDP/SCTP Application Colors..................................................... 107

Chapter 7: Alarms.............................................................................. 108
Configuring and using alarms............................................................ 108
Enabling probe instance alarms......................................................... 108
Enabling individual alarms............................................................... 109
Creating filter-based alarms............................................................... 110
Resetting statistical alarms............................................................... 111
Customizing triggers and actions...................................................... 112
Customizing alarm triggers.............................................................. 112
Customizing alarm actions.............................................................. 112
Sharing alarms with others.............................................................. 113
How to export alarms..................................................................... 113
How to import alarms.................................................................... 114

Chapter 8: Security and Privacy...................................................... 115
Security, privacy, and regulatory compliance..................................... 115
Configuring user accounts for secure access..................................... 116
Sharing packet captures with third-parties........................................ 116
Password protecting the ability to change partial packet capture size.................................................. 117
Trimming data from your captures................................................... 117
How to encrypt captured data at rest................................................ 118
Understanding the certificate trust model........................................ 121
How to view certificates.................................................................. 122
How to change the trust of a certificate............................................. 122
Certificates and how they are used.................................................. 122

Chapter 9: Probes and Probe Instances........................................... 123
Introducing Probes........................................................................ 123
What is a probe instance?................................................................. 124
Which software probe is right for you?.......................................... 126
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How probes work with switches</td>
<td>128</td>
</tr>
<tr>
<td>How a probe uses RAM</td>
<td>129</td>
</tr>
<tr>
<td>Packet capture buffer and statistics buffer</td>
<td>130</td>
</tr>
<tr>
<td>Running Observer with reserved memory</td>
<td>131</td>
</tr>
<tr>
<td>How packet capture affects RAM</td>
<td>133</td>
</tr>
<tr>
<td>How to allocate the reserved RAM</td>
<td>134</td>
</tr>
<tr>
<td>Recommendations for the VIAVI capture cards</td>
<td>135</td>
</tr>
<tr>
<td>Troubleshooting common issues</td>
<td>135</td>
</tr>
<tr>
<td>Troubleshooting a slow probe system</td>
<td>136</td>
</tr>
<tr>
<td>A probe is not connecting to the analyzer or vice versa</td>
<td>137</td>
</tr>
<tr>
<td>No network adapter available</td>
<td>137</td>
</tr>
<tr>
<td>Integrated adapters report all sent packets with bad TCP checksum</td>
<td>138</td>
</tr>
<tr>
<td>“No VLAN” shown while using a Gigabit NIC</td>
<td>138</td>
</tr>
<tr>
<td>VLAN Statistics tool is not working</td>
<td>139</td>
</tr>
<tr>
<td>Using Discover Network Names on a Layer 3 switch that uses VLANS</td>
<td>140</td>
</tr>
<tr>
<td>Suspected NAT or VPN issues</td>
<td>141</td>
</tr>
<tr>
<td>Running Observer passively affects NetFlow</td>
<td>141</td>
</tr>
<tr>
<td>Daylight Savings Time</td>
<td>141</td>
</tr>
<tr>
<td>Configuring Cisco 6xxx switches using a SPAN port to a full-duplex Gigabit Probe</td>
<td>142</td>
</tr>
<tr>
<td>Chapter 10: Backups and Restoring</td>
<td>143</td>
</tr>
<tr>
<td>Configuring a FIX profile</td>
<td>143</td>
</tr>
<tr>
<td>Sharing alarms with others</td>
<td>144</td>
</tr>
<tr>
<td>How to import alarms</td>
<td>144</td>
</tr>
<tr>
<td>How to export alarms</td>
<td>144</td>
</tr>
<tr>
<td>Sharing application definitions with others</td>
<td>145</td>
</tr>
<tr>
<td>How to export application definitions</td>
<td>145</td>
</tr>
<tr>
<td>How to import application definitions</td>
<td>145</td>
</tr>
<tr>
<td>Private key locations per server</td>
<td>146</td>
</tr>
<tr>
<td>Microsoft Lync Server</td>
<td>146</td>
</tr>
<tr>
<td>Apache Web Server</td>
<td>146</td>
</tr>
<tr>
<td>Windows IIS Web Server</td>
<td>147</td>
</tr>
<tr>
<td>Non-encrypted private key file</td>
<td>147</td>
</tr>
<tr>
<td>Encrypted private key file</td>
<td>147</td>
</tr>
<tr>
<td>Restoring the default application list</td>
<td>148</td>
</tr>
<tr>
<td>How to restore TCP application definitions</td>
<td>148</td>
</tr>
<tr>
<td>How to restore UDP application definitions</td>
<td>148</td>
</tr>
<tr>
<td>Importing or exporting a server profile</td>
<td>148</td>
</tr>
<tr>
<td>Creating a Forensic Settings profile</td>
<td>149</td>
</tr>
<tr>
<td>Importing Snort rules</td>
<td>154</td>
</tr>
<tr>
<td>Index</td>
<td>155</td>
</tr>
</tbody>
</table>
Chapter 1: Getting started

Which version of Observer is right for you?

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

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

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

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

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

Table 1. Comparing Observer versions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Standard</th>
<th>Expert</th>
<th>Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Capture (page 75)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Packet Decode (page 93)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Feature</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Real-Time Packet Captures &amp; Decode (page 97)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated Packet Captures (page 76)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Nanosecond Resolution (page 74)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Financial Protocol Support</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Filters (page 80)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Find Virus and Hack Signatures</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Statistical Drill Down</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarms (page 108)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Custom Alarm Triggers (page 112)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Error Tracking (page 47)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Real-Time Statistics (page 33)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Top Talkers (page 40)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Bandwidth Utilization (page 38)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VLAN Analysis (page 51)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Internet Activity (page 33)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wireless Analysis (page 36)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IP Pair Statistics (page 35)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Protocol Distribution (page 36)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>64 &amp; 32-bit applications (page 11)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Network Trending/Reporting</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Comparison Reports</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ready-Made Reports</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Custom Reports</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Feature</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Report Scheduler</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Support (page 27)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trace File Aggregation</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SRTP Support</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated reporting with Apex</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Application Analysis Trending</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Stream Reconstruction</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web pages</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant messages</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP-transferred files</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expert Analysis</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over 600 Experts</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expert Summary</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Delay</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection Dynamics</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MultiHop Analysis</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;What-If&quot; Analysis</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Analysis</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citrix</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIX</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Exchange</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Networking (SMB)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</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.

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.

**Caution:** See the important information in How to upgrade to Windows 10 (page 13) if you want to upgrade the operating system!

1. Ensure your system meets the minimum requirements.
   See Minimum and recommended system specifications (page 12).
2. Choose one of the following:
   - How to install all versions (page 14)
   - How to upgrade version 17 and later (page 14)
   - How to upgrade version 16 and earlier (page 15)

After completing this task:

- License your software. See FAQ: Licensing and updating (page 15).
- If you use Observer on a virtual machine and network traffic cannot be captured or BSODs (bluescreens) are occurring, see Virtual machine troubleshooting (page 18).

**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>Dual core Pentium class processor</td>
<td>Quad core Pentium class processor</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB RAM</td>
<td>8 GB RAM</td>
</tr>
</tbody>
</table>
How to install or upgrade the software
Chapter 1: Getting started

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>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>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet capture - Hardware: Determined by your product</td>
</tr>
<tr>
<td>Packet capture - Observer</td>
</tr>
<tr>
<td>GigaStor Software Edition: Determined by your license.</td>
</tr>
<tr>
<td>Network trending: See .</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating system²</th>
<th>64-bit Operating System Windows 7 or newer</th>
<th>64-bit Operating System Windows 7 or newer</th>
</tr>
</thead>
<tbody>
<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 13) 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.

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.

How to upgrade to Windows 10

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

This information does not apply if you:

- Already uninstalled .

---

How to install or upgrade the software
Chapter 1: Getting started

---

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 13) for a full list of supported operating systems.
♦ 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 was not uninstalled prior to upgrading to Windows 10, the only path to recovery is to reinstall the operating system. Back up any files on the operating system, reinstall the operating system, then install and restore its files.

To upgrade a system with to Windows 10:
1. Back up your settings.
2. Uninstall using **Control Panel > Program and Features**.
3. Upgrade your operating system.
4. Install the software.
5. Restore your settings from step 1 using whatever method is best for you.

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](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:
How to install or upgrade the software

Chapter 1: Getting started

♦ 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 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 19).
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**

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 20).

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.

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 8).

The depth of features in Observer depends on which product license you purchased. For information about Observer licenses, see FAQ: Licensing and updating (page 15).

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 24) 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 &quot;Authenticate Observer login with OMS&quot; 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. Observers 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><strong>Option</strong> for redirection from OMS</td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td></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>
</tbody>
</table>

| **Share filters with OMS** | 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. |

| **Synchronize user protocol definitions through OMS** | 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. |

| **Primary/Secondary server** | 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. |

| **Allowed to modify shared filters** | 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. |

| **Authenticate Observer login with OMS** | This option works in conjunction with the "Require Observer Login" option. This forces Observer to use OMS to authenticate users rather than Observer's local user list. A user list is maintained in OMS. |

| **Require a password to change partial packet capture size** | 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. |

| **Launch Encryption Key Generator** | 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. |
Folders tab

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

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

SNMP tab

This tab will not be active unless you have purchased a licensed copy of Observer Suite. After installation, the SNMP Management Console will generally require little, if any, configuration before it can be used.

| 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. |
### IPv6 tab

IPv6 is fully and natively supported in Observer.

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

- Compressed hexadecimal represents the address as native IPv6 (i.e. each of the eight 16-bit portions of the address are specified), but with the 0000 portions of the address replaced by double colons (::). For example: `FE80::254E:F35D:7DB4:11`
- Not compressed hexadecimal represents the address as native IPv6 (i.e. each of the eight 16-bit portions of the address are specified), including the 0000 portions. For example: `FE80:0000:0000:0000:254E:F35D:7DB4:0011`
- The IPv4 compatible formats represent the address as `x:x:x:x:x:d.d.d.d`, where the x’s are the 16-bit left-most portions of the IPv6 address, and the d’s are four 8-bit (IPv4-style) decimal values derived from the last two portions of the 16-bit IPv6 address. An example of the compressed form is `FE80::254E:F35D:125.180.0.17`. In uncompressed format, it would be `FE80:0000:0000:0000:254E:F35D:125.180.0.17`
- Decimal. separated represents the address as 16 decimal octets, for example: `254.128.0.0.0.0.0.0.0.0.37.78.243.93.125.180.0.17`

### 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 74).</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 managed by OMS

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

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

To change 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, 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**

New and past versions of software are made available to you directly from VIAVI. Use the upgrade tool to check for, download, or install a version of.

**Prerequisite(s):**
- Internet access to [update.viavisolutions.com](http://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 31)** can be used if direct Internet access is unavailable.
The upgrade tool allows you to:

♦ Check the VIAVI upgrade repository for old and new versions of.
♦ Download any available version of for offline installation.
♦ Install any available version of without needing to leave the interface.

How to retrieve a list of available versions

A listing of software versions to upgrade or downgrade to is available directly in . 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 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**. 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

New or old versions of can be downloaded from the upgrade repository. 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

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, 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><strong>Type</strong></td>
<td>Sets which type of proxy server to connect to.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>The IP address or DNS name of the proxy server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port number accepting connections to the proxy server.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Sets the user name expected by the proxy server for authentication. Leave this box empty if authentication is not required.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Sets the password used to authenticate with the proxy server. Leave this box empty if authentication is not required.</td>
</tr>
<tr>
<td><strong>Edit Download Schedule</strong></td>
<td>Schedules the download of available upgrade versions.</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</th>
<th>Some defining characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>(17.1.3.2) — Major</td>
<td>Major version indicator. Full platform version. Moving past this number requires a new license for your product (or products).</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:

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 29) 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:

1. On the Home tab, in the Statistics group, click **Protocol Distribution**.
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
♦ Levels of signal strength, quality, data/non-data transfer rates for each station on the access point
♦ AP traffic totals

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

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

2. Click the **Settings** button.

After completing this task:

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

### Monitoring network load

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

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

### Viewing router utilization statistics

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 29) 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 53) 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:

1. On the Home tab, in the Statistics group, click **Top Talkers**.
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 29) 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 42).

**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 39)**.

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 .

- 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 delimited 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 29) 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 45)** for a list of noteworthy settings.

#### Table 6. Wireless interference

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information Tab</td>
<td>This table summarizes essential information about what access points and stations are currently visible to wireless Observer. The status line at the bottom of the display shows all channels currently being scanned, highlighting each channel as it is looked at. Click Scan Setup to change the list of channels to scan.</td>
</tr>
<tr>
<td>Frame Type Tab</td>
<td>This table summarizes frame type totals for wireless data, management, and control packets.</td>
</tr>
<tr>
<td>Control Frames Tab</td>
<td>This table details control frames analyzed, including Power Save Polls, Requests to Send (RTS), Clear to Send (CTS), acknowledge (ACK), and CF (Contention Free) End packets.</td>
</tr>
<tr>
<td>Management Frames Tab</td>
<td>Displays detailed information about wireless management frames, including association requests and responses, reassociation requests and responses, ATIMs (Announcement Traffic Indication Message), and authentication/de-authentications.</td>
</tr>
<tr>
<td>Data Frames Tab</td>
<td>Displays detailed information about data frames on the wireless network.</td>
</tr>
<tr>
<td>Speeds Tab</td>
<td>Shows what stations are either transmitting (or receiving) wireless data at the various supported rates. To switch between transmitting and receiving speeds, click the down arrow next to the Tx (or Rx) and select the desired setting.</td>
</tr>
<tr>
<td>Signal Tab</td>
<td>Displays detailed statistics on wireless signal strength, quality, and data rates being used by stations and APs.</td>
</tr>
</tbody>
</table>
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 46) 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”.
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 29) 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 an Observer GigaStor, you can view statistics in the GigaStor Control Panel

1. On the Home tab, in the Statistics group, click **Top Talkers**.
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 Statistics</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**.
Chapter 3: Network and Application Discovery

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:

1. On the Home tab, in the Tools group, click **Discover Names**.
2. Click **Start** to begin the discovery process.
3. Click **Stop** to end the discovery process.
4. Click **Save Aliases** to save your results.

You successfully built an address book, which will help you throughout numerous portions of Observer in the future because other modes and tools rely on it.

Adding entries to the address book manually

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

To build an address book to only contain specific network addresses:

- May help you stay organized (smaller list)
- Only solicits the stations you specify (good neighbor)

To add stations to an existing address book:

- Add network addresses without running another discovery

If the automatic discovery process is prohibited:

- Due to security policies, applicable laws, etc.
- Avoid introducing potential interference to devices within a mission critical environment

To manually add entries to the address book:

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

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 52).

To edit address book entries in Observer:

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

Importing a previously saved address book

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

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

After completing this task:

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

Tell me more about importing a previously saved address book

The format of address entries in an .ali file is:

```
MACaddress, IP, alias
```

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

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

00:00:C0:87:49:45, 168.0.0.1, router1 00:00:C0:13:4B:33, 223.188.11.3, Sue’s Accounting PC

-or-

00:00:C0:8B:41:94, 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

Tip! 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:
Tip! 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 57).

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 58)). 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](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 29) 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 29) 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 59) for more information.

Table 8. Ping/Trace Route options

<table>
<thead>
<tr>
<th>Internet Address</th>
<th>Allows you to specify the Internet address to ping, or the address to which the route will be traced.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save button</td>
<td>Allows you to save the present Internet address.</td>
</tr>
<tr>
<td>Delete button</td>
<td>Selecting an address in the saved addresses box and clicking this button allows you to delete the address from the saved addresses.</td>
</tr>
</tbody>
</table>
Ping
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.

Trace Route
Allows you to select a route from the Observer personal computer to the specified Internet address to be traced.

Timeout (sec)
Allows you to specify the number of seconds that Observer will wait for a response before assuming that the packet Observer sent was either not received or not responded to.

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

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

Display Window
Displays the results of the ping or trace.

How to add application definitions

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

To add more application definitions for the Server Application Discovery tool to use, complete the following steps or see Adding derived application definitions (page 63) 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 63) 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

   ![Import Application Definitions dialog](image)

   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 \texttt{(dynamic - enabled)} or \texttt{(dynamic - disabled)} in the ports column of the table.
4. Right-click a dynamic port application, and click Enable/Disable Dynamic Discovery.

Figure 13: Enabling or disabling a dynamic port application

Defining applications differently per IP address

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

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

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

1. 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.
Chapter 4: Packet Captures

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 68)).

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
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 Network Load tab within the Expert screen.</td>
</tr>
<tr>
<td>Start/Stop Packet Capture</td>
<td>These packets are inserted whenever you click Start or Stop from either the Packet Capture or Decode Screen. They are used to help expert know that there are gaps of time between packets.</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...
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 116).

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 117).
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 74).

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 93) and the loadable file formats (page 94) of Observer.

After starting a packet capture—described in Capturing network traffic (page 75)—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.
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 74).
♦ 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 72).

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 86).

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
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 82). 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 87).

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 85) 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/ IP</td>
<td>Specify a hardware or IP address or range of addresses for source and destination. You can also limit the rule to apply only to packets from particular source or destination ports. For IPv4 packets, you can specify a subnet mask for inclusion/exclusion.</td>
</tr>
<tr>
<td>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</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 116)</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>
<tr>
<td>Rule Type</td>
<td>Usage</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select a protocol and field to filter on. For example, you can filter for ICMP Destination unreachable messages, or the presence of a VLAN tag.</td>
</tr>
<tr>
<td>VLAN 802.1Q</td>
<td>Match specific tag values for a Virtual Local Area Network (VLAN). You can filter on VLAN ID, priority (or a range of priorities) and the canonical format indicator. You can also filter for packets that contain any VLAN tag regardless of values.</td>
</tr>
<tr>
<td>VLAN ISL</td>
<td>VLAN ISL (Cisco proprietary VLAN). Beyond the VLAN ID, you can filter by user-defined bits. Source address (MAC): CDP and BPDU indicator: High bits of source address: Port index: Reserved field:</td>
</tr>
<tr>
<td>VNTag</td>
<td>Allows you to define the direction, loop, DVIF, and SVIF for tags created by the vNIC in your virtual network.</td>
</tr>
<tr>
<td>WAN - DLCI Address</td>
<td>Specify a WAN DLCI by number.</td>
</tr>
<tr>
<td>WAN Port</td>
<td>Specify a WAN Port by number.</td>
</tr>
<tr>
<td>WAN Conditions</td>
<td>Lets you filter for direction (DCE or DTE or both), and logically chain tests for forward congestion packets, backward congestion packets, and discard eligibility.</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td>Enter or select a hardware address that corresponds to the wireless access point you want to capture traffic from.</td>
</tr>
<tr>
<td>Wireless Data Rate</td>
<td>Select a wireless data rate, and whether you want to filter for packets traveling at, under, or over that rate.</td>
</tr>
<tr>
<td>Wireless Channel</td>
<td>Select a wireless channel, and whether you want to filter for packets received from channels less than, greater than, or equal to that channel.</td>
</tr>
<tr>
<td>Wireless Channel Strength</td>
<td>Select a wireless signal strength, and whether you want to filter for packets received at, under, or over that signal strength.</td>
</tr>
</tbody>
</table>

Tell me more about regular expressions

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

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

/555.5155/

Which would match 555-5155, 555 5155, 555.5155, etc. But it would also match 555X5155, 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 85) 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>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>Make the search case insensitive.</td>
</tr>
<tr>
<td>s</td>
<td>Interpret the period (.) meta-character to include newlines.</td>
</tr>
<tr>
<td>Modifier</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<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>

### 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.
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 80).

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 94).

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 99) 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 89).

**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 88).

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 88).
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 88).
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 91).

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::FF00:1</td>
<td></td>
</tr>
<tr>
<td>-ipv6_pair=</td>
<td>-ipv6_pair=FE80::F544:9E0:9C81:9FB1/2002::4A7D:FF00:1</td>
<td>IPv6 Pair—use this to filter for two IP addresses (IPv6) that have conversed with each other.</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 <strong>-and</strong> 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></td>
<td>-tcp_range=35/1023</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-tcp_range=60000/63500</td>
<td></td>
</tr>
<tr>
<td>Building block</td>
<td>Examples</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-udp=</td>
<td>-udp=53</td>
<td>UDP Port—use this to filter for a single UDP port number. As with other building blocks, you can add more using an <code>–and</code> building block.</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 <code>–and</code> 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 75) 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 .

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 99) 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 74).

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 95).

#### 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 96).

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

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

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):

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

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

#### Windows IIS Web Server

Windows does not contain a searchable private key file. The key file must be extracted from the website server certificate, and the server certificate must contain the private key file.

Use the following Microsoft Support document to export your server certificate and private key to a single .pfx file: [http://support.microsoft.com/kb/232136](http://support.microsoft.com/kb/232136) (How to back up a server certificate in Internet Information Services).
After you successfully export the .pfx file (PKCS #12), you must obtain the OpenSSL utility. This utility can be obtained by following an appropriate link as follows:

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

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

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

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

### 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-----
MIICXgIBAAKBgQD7uhNymd6WCORqH0rpd5zs4FEwCX2JrKtm0dmTf44SVaGvFLFl
vaKeoYP/sPs4aa2UaNQVfcbFaS2w31ZWWum4aCtqtvb821l+13VcdyR+2SRx9Gm6bu
SnoL/6F186mC0gHq6g0ILo1TAJnY+MOEC2bwbMykz1jPVUOXEH9IEG0A0Q1DAQAB
AoGAFQOYogWEVMQrpW2NW6YxXkJxVGBGzRiDrWfgCO/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....
JHq8U0pDbeFMh9j2Smiugxdq0a2q/MiX43Xa4Es6nKmzu9oI/ZfpIdAHi8gwhsD
m5bQRI9X9AXeIRy+0tG2ibUaphQEsv1995FWUs8BN9dVumsqykMvXSwND7tkbHB
i0/VVSAAD9bV3db15nbMwMnPv+YC350gAK42RlqrHRQ94fd/ZAvP8kV91iWcmX6
swF1nBGLUkF11J9qkyr+OQQqu1rAy2AB2UThGCJJetELFtV4mLmIaHdgDiucUpqJp==
-----END RSA PRIVATE KEY-----
```

### 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 29) 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.

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 98).

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</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>Address</td>
<td></td>
</tr>
<tr>
<td>Fast Post-Filter on Hardware/IP</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>Address</td>
<td></td>
</tr>
<tr>
<td>Create Filter on Hardware/IP</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>Address</td>
<td></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>Address</td>
<td></td>
</tr>
<tr>
<td>Remove Offset Flags</td>
<td>Removes any offset flags that have been set.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Remove Hardware/IP Address Flags</td>
<td>Removes all address flags that have been set.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Connection Dynamics</td>
<td>Opens a Connection Dynamics chart of the selected TCP conversation.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Add Comment</td>
<td>Allows you to add comments to specific packets in the buffer file.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>TCP Dump</td>
<td>Sometimes may options after it such as (HTTP) or (NetBIOS session) when it can identify the type of packets. When selected the packets are processed and appear in the Expert Analysis tab.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Reconstruct Stream</td>
<td>Reconstructs the TCP stream and any files or other data objects exchanged.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Decrypt SSL Conversation</td>
<td>Shows you the decrypted SSL conversation if you have the SSL key.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Decrypt TACACS+ Conversation</td>
<td>Shows you the decrypted TACACS+ conversation if you have the TACACS+ shared secret.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Previous/Next Packet in Conversation</td>
<td>Lets you follow a TCP conversation backward and forward in time.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Maximize Pane</td>
<td>Zoom in to the current pane (headers, decode, or hex window).</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Packet List Color Setup</td>
<td>Displays the Color dialog.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Set Decode Relative Time Origin to</td>
<td>Resets timestamps.</td>
</tr>
<tr>
<td>Selected Packet</td>
<td>Address</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Calculate Cumulative Bytes</td>
<td>Displays the byte count from the beginning of the capture (or the relative time origin) to the current packet.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
</tbody>
</table>

5. For additional settings, choose **Settings > General tab**. These settings are described in **Table 14 (page 98)**.

### Table 14. Expanded packet options

<table>
<thead>
<tr>
<th>Menu option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set focus on the last packet</td>
<td>Causes the packet display to set focus on the last (rather than the first) packet in the capture, allowing you to see the most recently captured information. This is particularly useful when</td>
</tr>
</tbody>
</table>
viewing a capture live where the user wishes to examine data as it arrives.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>When loading a local buffer file, exclude expert packets from the display</td>
<td>Choose to enable/disable the display of Observer Expert packets (the packets are not actually stripped from the file, they are just filtered from display).</td>
</tr>
<tr>
<td>Bytes Per Row in Hexadecimal Display radio buttons</td>
<td>Choose 16 or 10 bytes per row.</td>
</tr>
<tr>
<td>Show decode list using radio buttons</td>
<td>Choose either fixed-point or variable space font.</td>
</tr>
<tr>
<td>Packet timing display resolution list</td>
<td>Allows you to select the packet timing display resolution.</td>
</tr>
</tbody>
</table>

**Using the Decode pane**

The Decode and Analysis tab is where the captured buffer is decoded and the packet conversations can be examined and analyzed in detail.

This pane has several tabs on it that show you specific information about your packet decode. These include:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expert Analysis</td>
<td>Displays all general, non-conversation specific problems that Observer finds when analyzing the packet capture.</td>
</tr>
<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.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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 40).</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 33).</td>
</tr>
<tr>
<td>Internet Observer</td>
<td>Has three tabs that show a graph of the packets total by device on the Internet Patrol tab, and lists of IP Pairs and IP Subprotocol. There are numerous settings that you can configure by clicking the Settings button. This feature is very similar to the Internet Patrol in Discovering conversations between local devices and the Internet (page 33).</td>
</tr>
<tr>
<td>Application</td>
<td>Contains several tabs for the applications that Observer analyzes, including response time and statistics, URL statistics, FIX, and SQL.</td>
</tr>
<tr>
<td>Transaction Analysis</td>
<td>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 51).</td>
</tr>
<tr>
<td>VLAN</td>
<td>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 .</td>
</tr>
<tr>
<td>Forensic Analysis</td>
<td>Shows wireless access point statistics. This is similar to Viewing wireless access point statistics (page 36).</td>
</tr>
<tr>
<td>Access Point (AP)</td>
<td>Shows details related to your Fibre traffic.</td>
</tr>
</tbody>
</table>
Figure 24: 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 97).
### 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>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First packet</td>
<td>Allows you to set the first packet in the capture buffer to be saved to the file. By default, this is packet 1.</td>
</tr>
<tr>
<td>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>
<tr>
<td>Store alias names inside file</td>
<td>When selected, the Discover Network Names-derived alias list is included with the packet capture. If you do not save the alias information along with the capture buffer, statistical displays will list hardware addresses rather than meaningful names.</td>
</tr>
<tr>
<td>Save Partial Packets</td>
<td>When selected, you can set how much of each packet to save (in bytes). This allows you to collect packet headers without payloads, which may be useful from a privacy or security standpoint.</td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>Decrypt 802.11 WEP Encrypted Packets</th>
<th>If checked, you can select from several preconfigured WEP key profiles. The profiles themselves are configured as part of 802.11 setup.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decompress FRF.9 compressed packets</td>
<td>If you have captured frames from a 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.</td>
</tr>
</tbody>
</table>

**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 103)** choose how you want to search the capture buffer.

**Table 15. Searching a packet capture**

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

1. 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 87).

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.
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>Option</th>
<th>Description</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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</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>Packet timing display resolution</td>
<td>Sets the precision of time stamps displayed. These options do not affect any data.</td>
</tr>
</tbody>
</table>

1 millisecond
### 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.
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 26: Click the **Alarm Settings** button

2. Enable any probe instance alarm by enabling your chosen probe instance.
3. Click **OK** to save your changes.

You successfully enabled the probe instance alarm for your chosen probe instance; this setting persists until disabled. Individual alarms can now be configured and used, and such information can be found in Enabling individual alarms (page 109).

### 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, Bit Torrent, duplicate IP addresses, microbursts, VoIP, and more.
- **Trading Multicast Dropped Sequence Alarms**—These alarms must be wholly created and configured by you because it requires specific details about your trading and network environment. There are several pre-defined trading multicast protocols that you can import for the alarm.
- **IPTV Alarms**—These alarms must be wholly created and configured by you because it requires specific details about your multicast stream and device environment.
- **Filter Based Alarms**—These alarms based on packet capture filters that exist in Observer.

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 112)
- Creating filter-based alarms (page 110)

5. (Optional) Select “Enable Probe SNMP trap generation” and configure up to 10 Observer or other network management systems (for instance, HPOpenView or IBM Tivoli) to receive the SNMP traps. By enabling SNMP trap generation here, an SNMP trap is generated even when no Observer 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 108)** 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.

![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 112).

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
actions per individual alarm, disable this setting: Apply the Same Action to All Enabled Alarms (end-result shown in Figure 29 (page 113)).

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 29: 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.
Chapter 8: Security and Privacy

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 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 in 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 73).
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. Figure 30: Creating a partial packet 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).

Figure 31: Configuring partial packet captures

It is possible to decrease or increase the default 64-byte partial packet capture size. Click the Change Size button to set a custom value. From then on, each packets' bytes following the target value are discarded from capture.

How to encrypt captured data 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 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 32 (page 119) image.

Figure 32: 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>Volume RAID Level</th>
<th>Raid 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater Two TB</td>
<td>64bit LBA</td>
</tr>
<tr>
<td>Volume Support</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 Initialization Mode</td>
<td></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.

**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 122) 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 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 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 122), 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 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 9: 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 33 (page 124) 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 33: 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 16 (page 124) compares the features of active and passive probe instances with an Observer probe instance found on all non-GigaStor probes.

Table 16. 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>X</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>X</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>X</td>
<td>X</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.

<table>
<thead>
<tr>
<th></th>
<th>GigaStor Active probe instance</th>
<th>GigaStor Passive probe instance</th>
<th>Observer Probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Able to set permissions</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Able to redirect to different analyzer, etc.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

1. An Observer probe is the Single Probe, Multi Probe, or Expert Probe software running on a non-GigaStor probe.

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 34 (page 126) 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>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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sends entire buffer(^1)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarms</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trending</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Triggers</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wireless</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encrypts buffer transfer (page 121)</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>
</tr>
<tr>
<td>Simultaneous users(^2)</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>
</tr>
<tr>
<td>Use reserved memory outside of Windows</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Integrated reporting with Apex</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Able to switch between probe and analyzer mode</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full-duplex(^3)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port bonding(^4)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote decode of GigaStor captures</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware &gt;</td>
<td>GigaStor, Portable probes, Probe Appliances, 3rd party hardware</td>
<td>Dual port Ethernet Probe, 3rd party hardware</td>
<td>Ethernet Single probe, 3rd party hardware</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Installed software &gt;</td>
<td>Sends expert summary &amp; decode packets ¹</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VolP expert, APA, ATA ⁵</td>
<td>X</td>
<td></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.
5. Application Performance Analysis and Application Transaction Analysis. Applications are generally OSI Layer7 applications like HTTP, FTP, RTSP, SMB, and so on.

**How probes work with switches**

The purpose of a switch is to isolate traffic to the local network, thereby reducing the amount of traffic each device on that network must see and process. Although a protocol analyzer puts a network interface card in “promiscuous” mode, the analyzer only sees packets addressed to or transmitted from the port that it is connected to on the switch.

To operate a probe in a switched environment, you must choose a method that provides network visibility to the port where the probe is connected. Most switches provide a function that “mirrors” all packets received or transmitted from either a single port of interest (for instance, a server or router), or multiple ports of interest. The mirrored traffic can then be captured or analyzed by connecting your analyzer (or in this case, the probe) to the “mirror port” (which is sometimes called a SPAN port).

**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 35 (page 129) describes the two different ways that Observer runs.

Figure 35: Windows protected memory, user memory, and reserved memory
Whether using protected memory or reserved memory, Observer uses the RAM to store data for things such as (and creates a section within the RAM dedicated to):

- Packet capture
- 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 36 (page 130) shows what options in Observer control the size of various portions of memory.

Figure 36: 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:

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

**Tip!** You want a buffer that will handle your largest, worst case unfiltered burst.

Use this formula to determine how much hard drive space a capture requires (in GB) and Observer’s write-to-disk capability. There is no limitation to the amount data Observer can write to disk other than the disk size itself.

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

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 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 17 (page 132) shows how much memory is required by the operating system. Anything beyond this amount may be reserved for Observer.

Table 17. Reserved memory requirements

<table>
<thead>
<tr>
<th>Operating System</th>
<th>RAM required for the operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit with less than 4 GB RAM</td>
<td>800 MB</td>
</tr>
<tr>
<td>64-bit with 4 GB RAM</td>
<td>4 GB 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 134) to help determine how to divide the memory.

4. After reserving memory for Observer you must restart the system for the changes to take affect. After you restart the system you can allocate the memory to the different probe instances.

How packet capture affects RAM

When you start a packet capture (Capture > Packet Capture and click Start), all packets that Observer sees are placed into the packet capture buffer (a specific portion of the protected memory). The packets stay in this protected memory until the buffer is cleared. If you are using a circular packet buffer, new packets overwrite old ones after the buffer is full.

Figure 37 (page 133) 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 37: 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 135).

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 136).

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
Troubleshooting common issues

Chapter 9: Probes and Probe Instances

137

• 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 15).

♦ 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 22) 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 141).

♦ 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.

♦ 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 139) 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 `PreserveVlanInfoInRxDXPacket` 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:
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:

```bash
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:

```bash
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:

```bash
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 10: 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 18. 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>
</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.

<table>
<thead>
<tr>
<th>This option...</th>
<th>Allow you to do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore duplicate requests</td>
<td>If selected, duplicate requests are ignored. This is the default setting. If unchecked, duplicate requests may be present in the analysis and reduces the number of unique requests in the tracked requests.</td>
</tr>
<tr>
<td>Maximum displayed results</td>
<td>Defines the maximum number of results to display in the GigaStor Control Panel for the fastest or slowest responses.</td>
</tr>
<tr>
<td>Track not responded requests within</td>
<td>Amount of time used as the threshold that the GigaStor should wait for a response to a request before discarding the request from its analysis data set. If you want only requests that have received a response, uncheck this option.</td>
</tr>
<tr>
<td>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>
5. Click the Export Checked Alarms button.
6. Give your file a name, and click Save.

You successfully exported your alarms to an *.ALM file. You can now share this file with other Observer installations or keep it as a backup copy.

### Sharing application definitions with others

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

### 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 63) 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 95).

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 96).

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](http://support.microsoft.com/kb/232136) (How to back up a server certificate in Internet Information Services).

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

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

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

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

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

**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.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD7uhNymd6WCOOrqHOrpd5zs4FEwCX2JrKtm0dmTf44SVaGvPLF1
vakeOYP/sFs4aa2UnaNOFCbFa62w3IZWum4aCtgtvb8zil+13VcdyR+2SRx9Gmbu
SnoL/6FI86m+C0gHq6g0ILOiTAJynY+M0EC2bwbMykzljPVUOXE91EGQoA0Q1DQAB
AoGAFQoYogWEVmQRpW2NW6YXnJKxVGBGczrPiDrWfgC0/ITXhYuIt12I47QLd+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....
JHQ80U0DbeFM9h2j2SmugxdqOa2q/MiX43Xa4Es6nKmzu90I/ZfpIdAHi8gwtsD
mZ5bQRIXD9XKe1Ry+0tG2ibUaphQEsV1995FWysh8N9dVumsqykMxSwN7tKbHB
i0/VVSAAD9bV3db15nbMwMnP+YC3S90GAK42RIqrHRQ94fd/ZAvP8kV911wCmX6
-----END RSA PRIVATE KEY-----
```
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.

Applying 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.

Applying 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 19. 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.</td>
</tr>
<tr>
<td></td>
<td>Defragmentation Policy is:</td>
</tr>
<tr>
<td></td>
<td>BSD=AIX, FreeBSD, HP-UX B.10.20, IRIX, IRIX64, NCD Thin Clients, OpenVMS, OS/2, OSF1, SunOS 4.1.4, Tru64 Unix, VAX/VMS</td>
</tr>
<tr>
<td></td>
<td>Last data in=Cisco IOS</td>
</tr>
<tr>
<td></td>
<td>BSD-right=HP JetDirect (printer)</td>
</tr>
<tr>
<td></td>
<td>First data in=HP-UX 11.00, MacOS, SunOS 5.5.1 through 5.8</td>
</tr>
<tr>
<td></td>
<td>Linux=Linux, OpenBSD</td>
</tr>
<tr>
<td></td>
<td>Solaris=Solaris</td>
</tr>
<tr>
<td></td>
<td>Windows=Windows (95/98/NT4/W2K/XP)</td>
</tr>
<tr>
<td>TCP Stream Reassembly</td>
<td>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</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
 | techniques to confuse the IDS so that it reconstructs an incorrect stream (in other words, the IDS processes the stream differently from that of the intended target). As with IP fragmentation, forensic analysis must be configured to mimic how the host processes ambiguous and overlapping TCP segments, and the topology between attacker and target to accurately reassemble the same stream that landed on the target. Re-assembly options are described below:

**TCP Stream Reassembly (Continued)**

| Log preprocessor events | Checking this box causes forensic analysis to display all activity generated by the TCP stream assembly preprocessor to the log. |
| Maximum active TCP streams tracked | If this value is set too high given the size of the buffer being analyzed, performance can suffer because of memory consumption. If this value is set too low, forensic analysis can be susceptible to denial of service attacks upon the IDS itself (i.e., the attack on the target is carried out after the IDS has used up its simultaneous sessions allocation). |
| Drop TCP streams inactive for this duration | A TCP session is dropped from analysis as soon as it has been closed by an RST message or FIN handshake, or after the time-out threshold for inactivity has been reached. Exercise caution when adjusting the time-out, because hackers can use TCP tear-down policies (and the differences between how analyzers handle inactivity vs. various operating systems) to evade detection. |
| TTL delta alert limit | Some attackers depend on knowledge of the target system’s location relative to the IDS to send different streams of packets to each by manipulating TTL (Time To Live) values. Any large swing in Time To Live (TTL) values within a stream segment can be evidence of this kind of evasion attempt. Set the value too high, and analysis will miss these attempts. Setting the value too low can result in excessive false positives. |
| Overlapping packet alert threshold | The reassembly preprocessor will generate an alert when more than this number of packets within a stream have overlapping sequence numbers. |
| Process only established streams | Check this box if you want analysis to recognize streams established during the given packet capture. |
| Reconstruct Client to Server streams | Check this box to have analysis actually reconstruct streams received by servers. |
| Reconstruct Server to Client streams | Check this box to have analysis actually reconstruct streams received by clients. |
| Overlap method | Different operating systems handle overlapping packets using one of these methods. Choose one to match the method of the systems being monitored. |

**TCP Stream Reassembly (Continued)**

| Reassembly error action | Discard and flush writes the reassembled stream for analysis, excluding the packet that caused the error. Insert and flush writes the reassembled stream, but includes the packet that caused the error. Insert no flush includes the error-causing packet and continues stream reassembly. |
| Reassembled packet size threshold range | Some evasion strategies attempt to evade detection by fragmenting the TCP
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>header across multiple packets. Reassembling the stream in packets of uniform size makes this easier for attackers to slip traffic past the rules, so forensic analysis reassembles the stream using random packet sizes. Here you can set the upper and lower limits on the size of these packets. Reassembled packet size seed value—Changing the seed value will cause forensic analysis to use a different pattern of packet sizes for stream reassembly. Running the analysis with a different seed value can catch signature matches that would otherwise escape detection. Port List—Enabling the Port List option limits analysis to (or excludes from analysis) the given port numbers.</td>
</tr>
</tbody>
</table>

<p>| 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 URIs, doing so can result in a lot of noise because this type of encoding is common. Lookup Unicode in code page—Enables Unicode codepoint mapping during pre-processing to handle non-ASCII codepoints that the IIS server accepts. |</p>
<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>
<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</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
can edit variable definitions by double-clicking on the variable you want to edit.
The VRT Rule Set variable settings (and those of most publicly-distributed rule sets) will work on any network without modification, but you can dramatically improve performance by customizing these variables to match the network being monitored. For example, the VRT rules define HTTP servers as any, which results in much unnecessary processing at runtime.
Address variables can reference another variable, or specify an IP address or class, or a series of either. Note that unlike native Snort, Observer can process IPv6 addresses.
Port variables can reference another variable, or specify a port or a range of ports. To change a variable, simply double-click the entry. The Edit Forensic Variable dialog shows a number of examples of each type of variable which you can use as a template when changing values of address and port variables.

**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 15
25901 (port) 137
25903 (port) 137
32-bit 131
3-D Pie/Chart Display Properties 70
64-bit 131
64-bit, RAM 131
802.11 123, 123, 126
802.1Q 139

A
access point statistics 36, 36, 39, 39
activate and deactivate 86, 86
active instance vs. passive instance 124
Activity Display 49
Activity Display tool 49
adapter
    see network adapter 38, 38
see network adapter 38, 38
Add Rename Filter Profile 80
Add/Edit Protocol Filter 80
adding 63
adding derived definitions 63
address book 55
    addresses, resolving 54
    building 52, 52, 53, 53, 53
    discovery method 52, 52
    editing 55
    entries, adding 53, 53, 55
    importing 55, 55, 55
    saving 52, 55, 55
    using 56
Address Filter 80
addresses, resolving 54
AES 118
Alarm Settings 108
alarms 113, 113, 113, 113, 113, 113, 114, 114, 126,
    136, 144, 144, 144, 144, 144, 144, 144, 144, 144
    configuring 108, 108, 112
    customizing 112, 112, 112, 112, 112
    enabling 108, 108, 109, 109
    exporting 113, 113, 144, 144
    filter-based, creating 110, 110
    high latency 109
    importing 114, 114, 144, 144
    resetting 111, 111, 111
    retransmissions, excessive 109
allocating 134
analyzer connection 137
Anyone account 137, 137
Apache Web Server 95, 146
Application Definitions and Server Application
Discovery Settings 56
Application Discovery, Server 60
applications, see server applications 60
applying 87, 87, 104
ArcaBook Multicast 60
ARP inspection 149
ARP Inspection, network forensics preprocessor 149
Asset ID 122
Asset name 122
Asset type 122
ATM Address Filter 80
B
backup
    installation 15
bad TCP checksums 138
    troubleshooting 138
Bandwidth Utilization 38
Bandwidth Utilization - Full Duplex Display 38
Bandwidth Utilization tool 38, 38, 39
Bandwidth Utilization with Filter 39
best practices 124
BFR 27, 74, 94
BIOS memory hole 131
broadcast and multicast storms 49
buffer 130
buffer size 124
buffer statistics 130
buffer, see capture buffer and statistics buffer 130
buffers 124, 126, 126, 126, 131, 133
    circular 72, 72
    configuring 67, 71
    replaying 96
building 52, 52, 53, 53, 53
C
Calculate Cumulative Bytes 97
CAP 74, 94
capture buffer
    64-bit Windows 130
    IP defragmentation 149
Max Buffer Size 130
RAM limitations 130
size 130
TCP stream 149
capture card 41, 69
driver requirements 17
passive probe instance 124
performance 124
probe instance warning 124
recommendations 135
capture card driver 17
Capture Decode 99
Capture Graph 70
Capture Internet Observer 33
Capture Pairs (Matrix) 35
Capture Protocols 36
Capture Summary 43
Capture Top Talkers 40
Capture VLAN 51
captures
see packet captures 76
see packet captures 76
capturing 75
CAPWAP Control 60
CAPWAP Data 60
Certificate ID 122
CIR 108
circular 72, 72
Cisco 6xxx switches 142
troubleshooting 142
Classic Mode 29
CME RLC 60
collision test 141, 141
command line 89, 89
command line, enabling 88, 88
Committed Information Rate 108
common issues 135
common problems with 136, 137
Configure IP Application List for Internet Observer Statistics Dialog 33
Configure IP Application Ports Dialog 35
configuring 38, 67, 70, 71, 72, 73, 75, 108, 112
   Expert Information 71
   partial packets 73, 73, 73
Connection Dynamics 93
connections 33, 33, 33, 33, 35, 35, 35, 40
creating 75, 86

D
daylight savings time 141
Daylight Savings Time 141, 141
Decode and Analysis 99
decoding 93, 93, 97, 103, 104, 104, 126, 126, 126
   expert analysis 93
gеolocation 28
NetFlow 104
packet captures 93, 93, 93, 93, 103
   encrypted 95, 95, 146, 146
sFlow 104
user interface 97, 97, 99, 99
using third party decoder 27, 27
defining its purpose 134
definition 123
definitions, restoring 65, 148
denial of service 149
derived application definitions 63
derived applications 24
devices 57
discovering 57, 57, 57
Discover Network Names 140, 140, 140
   VLANS 140
Discover Network Names (Address Book) 56
Discover Network Names Mode 56
Discover Network Names tool 52, 53
Discover SNMP Devices 57
discovering 56, 56, 56, 57, 57, 57
discovery method 52, 52
Display Protocols for Selected Station 36
Display Stations sending Selected IP 93
DLCI Address Filter 80
DLCI CIR Setup 108
DMP 74, 94
DNS 53, 54
DNS names
   resolving 54
driver error support 43
driver requirements 17, 17, 17
duplicate, removing 75
dynamic 64

E
Edit IP Application Port Dialog 33
Edit Pager Entry Dialog 93
Edit Probe User Account Dialog 93
Edit Statistics Memory Configuration 93
   editing 55
      ports 64
effects of packet capture 133
efficiency 117
   enabling 108, 108, 109, 109
   ENC 74, 94
   encrypted 95, 95, 146, 146
   encryption 24, 24, 24, 24, 24
      AES 118
      see also security 118
   encryption key 137
   entries, adding 53, 53, 55
   Error Filter 80
   errors 43, 44, 44, 44, 47
   Ethernet 47
   Errors by Station 44
   Errors by Station tool 44
   ErrorTrak 11
   ESX/ESXi
      troubleshooting 18, 19, 20
   Ethernet 47, 123, 123, 126
      ARP inspection 149
      errors 47
      full-duplex 126
   Ethernet Physical Port Filter 80
   Ethernet Vital Plot Properties 43
   Ethernet Vital Signs 43
   Ethernet Vital Signs and Collision Expert 43
   expert analysis 93
   Expert Connection Dynamics 93
   Expert Fibre Events 93
   Expert Global Settings 93
   Expert Global Settings - Connection Dynamics 93
   Expert Global Settings - General 93
   Expert Global Settings - IP Range 93
   Expert Global Settings - TCP IP 93
   Expert Global Settings - Time Interval Analysis 93
   Expert Global Settings - What-if Analysis 93
   Expert ICMP Events 93
   Expert Information 71, 71
   Expert Information, excluding 71
   Expert IPX Events 93
Expert NetBIOS Events 93
Expert Probe 126, 126, 126
Expert Reconstruct Streams 93
Expert Server Analysis 93
expert summary 126
Expert Summary 93
Expert TCP Dump 93
Expert TCP Events 93
Expert Time Interval Analysis 93
Expert UDP Events 93
Expert VoIP 93
Expert VoIP Analysis 93
Expert VoIP Events 93
Expert VoIP Settings - General 93
Expert VoIP Settings - MOS 93
Expert What-If Analysis 93
Expert Wireless Events 93
exporting 56, 56, 113, 113, 144, 144
alarms 113, 113, 113, 113, 113, 144, 144, 144, 144, 144
protocol definitions 56
server applications 62, 63, 145, 145

F

FDDI 93
FDDI Errors by Station 43
FDDI Vital Signs 43
feature suitability 73
Federal Information Processing Standards 115
Fibre Channel Vital Signs 43
Filter Names 80
filter-based, creating 110, 110
filtering 80
post-filters
applying 87, 87, 104
command line 89
command line, enabling 88
pre-filters
"exclude" rules 80
creating 80, 80, 86
exporting 80
importing 80
scope 86
pre-filters, scope 86
filters
activate and deactivate 86, 86
command line 89
command line, enabling 88
see also filtering 80
partial packets 75
Filters 80, 81
Find Packet 103
FIPS 115, 115
firewall, ports 137
FIX 99
Folders tab 26
forensic analysis 149
format
PCAPNG 74, 94
XML 74, 94
formats 74, 94
BFR 74, 94
CAP 74, 94
dump 74, 94
ENC 74, 94
PCAP 74, 94
from multiple sources 75
from unknown sources 94, 94
full-duplex 126
full-duplex Ethernet 126
G

GeoIP Settings 28
gеolocation 28, 28
Gigabit 126
Gigabit Probe 15
gigabytes 130, 130
GigaStor 134
collision test 141
RAM 134
recommendations 135
reserved memory 134
traffic generation 141
GigaStor capture 124, 126
GigaStor Control Panel
t forensic analysis 149
Snort 149
Snort rules 154
GigaStor Portable 141
Graph Display Properties 93
Graph Display Properties - Graph Time 93

H

H.323 93
hardware 12
hardware acceleration 135
hardware requirements 11
hidden features
See Classic Mode
high latency 109

I

ICMP Expert 93
IIS Web Server, Windows 95, 146
importing 55, 55, 55, 56, 56, 62, 114, 114, 144, 144, 145
address book 55
alarms 113, 113, 114, 114, 144, 144, 144, 144, 144, 144
protocol definitions 56
server applications 62, 145
in a switched environment 128
individual stations 35, 35, 35, 40
install 14
installation 14, 14, 15, 15
installer 14
installing 14, 14, 15
Interface Properties 93
interface switching 126
Internet Observer 33
Internet Observer Internet Patrol 33
Internet Observer IP Subprotocols View 33
Internet Observer Settings 33
Internet Observer tool 33, 33, 33
Internet Patrol 33
Internet Patrol - Pair Circle 33
IP address
IPv6 149
NAT 141
IP Calculator 56
IP defragmentation 149
IP Discovery 56

Index | 157
IP flow 149
IP Fragment Bits Filter 80
IP Fragment Offset Filter 80
IP masquerading, see NAT 141
IP Pairs - Pair Circle 93
IP Properties 93
IP Subnet Mask Calculator 56
IP Subprotocols 93
IPv4 Options Filter 80
IPv4 TOS Precedence 73
IPv6 27, 149, 149
IPv6 Address representation 93
IPv6 Flow Label 73
IPv6 Options Filter 80
IPv6 Traffic Class 73
Issuing time 122

J
Jitter 93

L
Last seen IP 122
Last seen time 122
Layer 3 Switch 140
LDAP 86, 86
license update 16
licenses
  redeeming 15
  troubleshooting 15
licensing 16
List Bar Display Properties 93
List Display Properties 93
load 37
  preprocess settings 149
load, preprocessor 124
load, testing 41, 41
loading 74, 94
local probe 21
Locator, Switch Station 56

M
MAC addresses 140
MAC Properties 93
matching between probe and analyzer 137
Max Buffer Size 130
MDS Fingerprint 122
Mean Opinion Score (VoIP Expert) 93
megabytes 124
memory management 130
memory tuning 130
memory, see RAM 133
Microsoft 18
Microsoft Lync Server 95, 146
Microsoft Network Discovery 56
minimum specifications 12
minimum specs 12
mirror port 128
mirror port, see also SPAN ports 128
missing 77, 137
missing features
  See Classic Mode
Modify Observer Reserved Memory dialog 93
MOS Settings 93
moving through RAM 133

N
NAT 141, 141, 141
NetFlow 104, 126, 141
decoding 104
TAPs and 141
network 43, 43, 44, 45, 49
errors 44
load 37
load, testing 41, 41
summary 43, 43
troubleshooting 43, 43, 43, 43
utilization 37, 38, 39, 39, 42, 42, 43, 43
Network Activity Display Properties 49
network adapter
capture card 41, 69
configuring 38
Network Errors Settings 44
network load 37, 41, 41
network masquerading, see NAT 141
Network Summary 43
Network Summary tool 43
network trending 126, 136
server profiles 148
Network Trending Settings - MOS 93
Network Vital Signs tool 43
NIC 126
missing 137
NIProbe.exe 15
not connecting 137
Notify Probe User 73
Numeric Value Filter 80

O
Observer
  encryption 24
  feature suitability 73
  regulation compliance 115
  switching to probe 126
  system requirements 11
  user interface 21
Observer Analyzer 15
Observer General Options - folders 93
Observer General Options - IPv6 93
Observer General Options - Security 93
Observer General Options Tab 93
Observer GigaStor 15
observer.exe 15
OMS 24, 24, 24, 24, 24, 24, 24, 126
synchronizing protocol definitions 56
OpenView 109
operating system 13
OR filter example 86

P
packet 149
packet alert threshold 149
packet capture 133
active instance vs. passive instance 124
buffer 130
daylight savings time 141
decoding 126
GigaStor Portable 141
RAM 133
reassembling 149
Packet Capture on Multiple Instances Settings 75
Packet Capture Options 70
Packet Capture Schedule 76
packet captures 70, 76, 76, 76, 93, 93, 93, 93, 103, 116, 117
configuring 67, 70, 71, 72, 73, 75
  Expert Information 71
  partial packets 73, 73, 73
creating 75
decoding 93, 93, 97, 103
efficiency 117
encrypted 95, 95, 146, 146
filtering 80
from multiple sources 75
from unknown sources 94, 94
loading 74, 94
replaying 96
saving 74, 74, 94, 94, 102
scheduling 76, 76
security 117
sharing 116
timestamps 70
transferring 76
wireless 11
packet fragmentation 149
Packet Length Filter 80
packet storms 49
Packet Time Filter 80
Packet View Settings - Column Order 93
Packet View Settings - Configure SNMP MIBs 93
Packet View Settings - General 93
Packet View Settings - Protocol Forcing 93
Packet View Settings - Summary 93
packets 40, 75
capturing 75
duplicate, removing 75
Expert Information 71
Expert Information, excluding 71
missing 77
moving through RAM 133
RAM 133
saving 102
searching for 103
sizes 40
Pair Statistics (Matrix) 93
Pair Statistics Settings 93
Pair Statistics Settings - List 93
Pair Statistics Settings - Pair Circle 93
Pair Statistics Settings - Statistics Settings 93
Pair Statistics tool 35
Partial Packet Capture for TCP/UDP Payload Filter 116
partial packets 73, 73, 73, 75
passive probe instance 124
Pattern Filter 80, 82
PCAP 27, 74, 94
PCAPNG 74, 94
performance 124
Phone Pager Schedule 93
Ping Trace Route 59
Ping/Trace Route 59, 59
port bonding 126
Port Filter 80
ports 22, 61, 64, 64
Post Capture Filtering 87
post-filters
  applying 87, 87, 104
  command line 89
  command line, enabling 88
pre-filters
  creating 80, 86
  scope 86, 86
preprocess settings 149
Probe Alarms Settings - Actions 112
Probe Alarms Settings - Alarm List 109
Probe Alarms Settings - Triggers 112
probe connection 137
probe instance
  active 124, 130
  active vs. passive 124
  best practices 124
  defining its purpose 134
  definition of 124
  memory tuning 130
  passive 124
  reserving memory 130
probe instance warning 124
Probe redirection error 137
probe, local 21
probes 75
  common problems with 136, 137
  definition 123
  hardware acceleration 135
  in a switched environment 128
  not connecting 137
  protecting 18
  software, versions 126
  SPAN ports 126
  switching to analyzer 126
  updating 18
  VLAN access 137
promiscuous mode 11, 128
protected memory 129, 131, 133
protecting 18
Protocol
  Filters 81
  protocol definitions 56, 56
  exporting 56
  importing 56
Protocol Definitions and Server Application Discovery 93
Protocol Distribution 36
Protocol Distribution Settings 36
Protocol Distribution Statistics 36
Protocol Distribution Statistics Switched 36
Protocol Distribution tool 36
Protocol Filter 80
protocols 35, 35, 36, 36, 36
  statistics 36
Q
Quality of Service (QoS) 93
RAID 124, 124
RAM 12, 133, 133, 133, 134
allocating 134
buffer size 124
effects of packet capture 133
formula 130
GigaStor 134
limitations 130
packet capture 124, 130
see also buffer 130
see also protected memory, user memory, and
reserved memory 129
recommendations 131
resizing 129
statistics 130
TCP stream reassembly 149
tuning 130
used in Observer 129
Windows 130
RAM limitations 130
RAM needed for busy networks 134
Random Access Memory, see also RAM 129
Real-time Transport Control Protocol 93
Real-time Transport Protocol 93
reassembling 149
recommendations 131
recommended specifications 12
recommended specs 12
reconstruction, stream 93
regulation compliance 115, 115
see security 115
see security 115
Remote Probe Expert Analysis and Decode 93
Replay Packet Buffer 93
replaying 96
requirements, hardware/software 11
Reserve Observer Memory 93
reserved memory 126, 131, 133, 134
see also RAM 129
reserved memory from 126
reserving memory 130
resetting 111, 111, 111
resizing 129
Resolve IP 56
resolving DNS names 54
restoring 65, 65, 66, 148, 148, 148
retransmissions, excessive 109
RFC1213
see SNMP 57, 57
see SNMP 57, 57
RMON 128
RMON Extension Configuration 73
RMON Tables 93
Router Observer 37
Router Observer Settings 37
Router Observer tool 37
routers 37, 37, 37, 37
statistics 37
RTCP 93
RTF Report Options 93
RTP 93
RTP RTCP Graph 93
rules profiles 149
sampling divider 136
Save Packet Capture 102
saving 52, 55, 55, 74, 74, 94, 94, 102, 102
saving packet captures 74, 94
saving, formats 74, 94
scheduling 76, 76
packet captures 76, 76, 76
scope 86, 86
searching for 103
security 117, 126
encryption 118
encryption key 137
matching between probe and analyzer 137
packet captures 116, 117
personal information 15
Probe redirection error 137
probes 75
regulation compliance 115
user accounts 116
Select WEP Profile 102
Server Analysis
using 93, 93
Server Application Discovery 56, 56, 60
adding derived definitions 63
definitions, restoring 65, 148
server applications
adding 60, 63
discovering 56, 56, 56
editing 64
exporting 56, 62, 63, 145, 145
importing 56, 62, 62, 145, 145
ports 61, 64, 64, 64, 64
restoring 65, 65, 66, 148, 148, 148
see also applications 60
derived server profiles 148
Server, Apache Web 95, 146
Server, Windows IIS Web 95, 146
Set Local Probe Name 93
settings 128
settings profiles 149
sFlow 104, 126
decoding 104
SHA1 Fingerprint 122
sharing 116
Shoutcast 60
signal strength 46
signal strength conversion 46
simultaneous 126
Single Probe 126, 126
Anyone account 137
site survey 45
Size Distribution Settings 40
Size Distribution Statistics 40
Size Distribution Statistics tool 40
sizes 40
slow probe system 136
Sniffer 74, 94
SNMP 128
devices 57
discovering 57, 57, 57
SNMP General Options Tab 93
SNMP traps 109
Snort 149, 149
IP flow 149
IPv6 149
variable name 149
Snort rules 154
software probes 126
software requirements 11
software, versions 126
SPAN
VLANs 139
SPAN port 139
see also mirror port 128
SPAN ports 126
settings 128
software probes 126
see also mirror port 128
specifications 12
specs 12
SSL 97, 97, 97
SSL/TLS Decryption Parameters 93
State 122
Stations - Pair Circle 93
statistics 36, 36, 36, 37, 39, 39, 45, 130
connections 33, 33, 33, 33, 35, 35, 35, 40
errors 43, 44, 44
individual stations 35, 35, 35, 40
network load 37
packets 40
protocols 35, 36, 36, 36
RAM needed for busy networks 134
routers 37, 37, 37, 37
sampling divider 136
top talkers 40, 40, 40, 40
utilization 38, 39, 42, 43
VLAN 51, 51, 51
wireless 36, 45, 45
statistics buffer 130, 130
Statistics Memory Allotment Page 93
statistics queue buffer 129, 131, 133, 133, 134, 135
storage 12
stream reconstruction 93
Stream Reconstruction 93
Subnet mask 73
Subnet Mask Calculator 59, 59
summary 43, 43
Switch Station Locator tool 56
switching to analyzer 126
switching to probe 126
synchronization 141
synchronizing protocol definitions 56
system requirements 11
system specification 12
T
TAP
NetFlow 141
TAPs and 141
TCP 141, 149, 149, 149, 149, 149, 149, 149, 149, 149, 149
TCP Expert 93
TCP stream 149
TCP stream reassembly 149
TCP/IP 141
testing
network load 41, 41
third-party decoder 27
third-party capture card
driver requirements 17
third-party hardware 12
Time Interval Analysis
using 93
time synchronization 141
timestamps 70
packet captures 70
Tivoli 109
Token Ring Errors by Station 44
Token Ring Vital Signs 43
top talkers 40, 40, 40, 40
Top Talkers 49, 130
Top Talkers Statistics 40
Top Talkers tool 40, 40
top talkers, defined 40
topologies 123, 126
802.11 123
Ethernet 123
traffic generation 141, 141
Traffic Generator 41
Traffic Generator Settings 41
transferring 76
transferring packet captures 76
triggers 126, 136
troubleshooting 43, 43, 43, 43, 138, 142
analyzer connection 137
bad TCP checksums 138
broadcast and multicast storms 49
Cisco 6xxx switches 142
common issues 135
network 41, 43, 43, 43, 44, 45, 49
packet storms 49
probe connection 137
slow probe system 136
virtual machines 18
VLAN Statistics tool 138, 139
VLAN visibility 140
TTL Hop Limit 73
U
UDP Expert 93
updating 18
Observer 15
updating virus protection 18
upgrade 14, 15
upgrading 14, 15
upgrading version 16 15
upgrading version 17 14
user accounts
security 116
user interface 21, 97, 97, 99
see Observer 21
user memory 129
users 126, 137
simultaneous 126
using 56, 93, 93, 93
using third party decoder 27, 27
utilization 37, 38, 38, 39, 39, 39, 39, 42, 42, 42, 42, 43, 43, 43
Utilization History 42
Utilization History tool 42
Utilization Thermometer Mode 42
Utilization Thermometer tool 43
V
v16 15
v17 14
variable name 149
version 16 15
version 17 14
version numbering 32
virtual adapter 124
virtual machine 11, 12
vSphere 18, 19, 19, 20
Virtual Tap 93
Virtual Tap Settings Dialog 93
virus protection 18
VLAN 51, 51, 51, 139, 139
"No VLAN" 138, 139
VLAN access 137
VLAN Filter 80
VLAN ISL Filter 80
VLAN Properties 51
VLAN Statistics 51, 139
VLAN Statistics tool 51, 138, 139
VLAN visibility 140
VLANs 139, 139, 140
Discover Network Names 140
SPAN port 139
VM specs 12
VMONI 137
VMONI Protocol Analyzer 137
VMware 12
VoIP 93, 126
VoIP RTP RTCP Graph 93
VPN 141
vSphere 12
troubleshooting 18, 19, 19, 20

W
WAN alarms 108
WAN Conditions Filter 80
WAN Load 49
WAN Port Filter 80
WAN switch 56
WAN vital plot properties 43
WAN Vital Signs 49
WAN Vital Signs by DLCI 43
Web Observer 35
WEB Observer Settings 35
Web Observer tool 35
Web Server, Apache 95, 146
Web Server, Windows IIS 95, 146
Windows
32-bit 131
64-bit 130, 131
reserved memory from 126
Windows 10 13
Windows 2003 13
Windows 2008 13
Windows 2012 13
Windows 2016 13
Windows 7 13
Windows 8 13
Windows IIS Web Server 95, 146
Windows protected memory 129
Windows updates 18
Windows Vista 13
wireless 11, 36, 36, 36, 39, 39, 45, 45, 45, 123, 126, 126
access point statistics 36, 36, 39, 39

signal strength conversion 46
site survey 45
Wireless Access Point Filter 80
Wireless Access Point Load Monitor 36
Wireless Access Point Settings 36
Wireless Access Point Settings - List 36
Wireless Access Point Statistics 36
Wireless Access Point Statistics tool 36
Wireless Channel Filter 80
Wireless Data Rate Filter 80
wireless interference 45
Wireless Network Errors by Station 44
wireless packets, raw 11
Wireless QoS 73
Wireless Signal Strength Filter 80
Wireless Site Survey 45
Wireless Site Survey - Channel Scan 45
Wireless Site Survey - Ctrl. Frames 45
Wireless Site Survey - Data Frames 45
Wireless Site Survey - Frame Types 45
Wireless Site Survey - General Info 45
Wireless Site Survey - Mgmt. Frames 45
Wireless Site Survey - Signal 45
Wireless Site Survey - Speeds 45
Wireless Site Survey tool 45
Wireless Vital Signs 43
Wireshark 27, 74, 94
Word Report Options 93

X
XML 74, 74, 94, 94

Symbols
"No VLAN" 138, 139