Trademark Notices

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

Open Source Copyright Notices

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

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

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

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

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

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

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

Limited Warranty—Hardware

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

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

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

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

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

CA (or its agent) will promptly repair or replace all defective Hardware (except for shipment-related damage and damage caused by Customer) for a period of ninety (90) days following delivery of the initially provided applicable Product (“Hardware Warranty Period”). CA (or its agent) will promptly repair or replace defective replacement Hardware only during the remaining Hardware Warranty Period of the original Hardware. Customer may obtain extended Hardware warranty coverage by purchasing ClientConnection Support Services. The foregoing limited warranty is expressly conditioned on Customer giving CA prompt notice of the defect during the applicable warranty period and returning all of the defective Hardware to CA.

Limited Warranty—Software

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

Should DEVELOPER release a newer version of the SOFTWARE within 60 days of shipment of the product, DEVELOPER will update the copy of the SOFTWARE upon request, provided request is made by the licensed END-USER within the 60 day period of shipment of the new version. This update may consist of a CD or a manual or both at the discretion of DEVELOPER. END-USER may be charged a shipping fee for updates.
The information in the SOFTWARE manuals is furnished for informational use only, is subject to change without notice, and should not be construed as a
commmitment by DEVELOPER. DEVELOPER assumes no responsibility or liability for any errors or inaccuracies that may appear in any SOFTWARE manual.

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

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

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

Liability

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

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

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

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

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

Ownership and Confidentiality

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

Technical Support

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

US & countries outside Europe at (952) 358-3800
UK and Europe at +44 (0) 1959 569880
By fax (depending on where you are located):
US & countries outside of Europe at (952) 358-3801
UK and Europe at +44 (0) 1959 569881

Or by e-mail at: US & countries outside of Europe: support@networkinstruments.com
UK and Europe: support@networkinstruments.co.uk

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

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

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

Chapter 1: Getting Started........................................................................................................1
  System requirements and installing or upgrading the software..................................................1
  FAQ: Licensing and updating......................................................................................................2
  Capture card driver requirements.................................................................................................3
  Overview of Observer..................................................................................................................5
  User interface.............................................................................................................................5
  The dashboard.............................................................................................................................6
  Customizing toolbars..................................................................................................................7
  Ports used by Network Instruments products............................................................................8

Chapter 2: Configuring Observer’s general settings.................................................................8
  General tab................................................................................................................................8
  Security tab................................................................................................................................9
  Folders tab.................................................................................................................................11
  SNMP tab..................................................................................................................................11
  IPv6 tab.....................................................................................................................................12
  Third Party Decoder tab............................................................................................................13
  GeoIP Settings...........................................................................................................................13

Chapter 3: Real-Time Statistics................................................................................................14
  Monitoring connection statistics.................................................................................................14
  Discovering conversations between local devices and the Internet.........................................14
  Configuring the IP application list..............................................................................................15
  Discovering conversations between local devices......................................................................16
  Viewing real-time statistics per device......................................................................................16
  Viewing a list of protocols seen on the network........................................................................17
  Viewing wireless access point statistics..................................................................................17

Chapter 4: Monitoring network load........................................................................................18
  Viewing router utilization statistics............................................................................................18
  Viewing bandwidth utilization.....................................................................................................19
  Viewing bandwidth utilization with a filter................................................................................19
  Wireless Access Point Load Monitor..........................................................................................20
  Viewing the distribution of packet sizes by station....................................................................21
  Discovering current top talkers on the network.........................................................................21
  Load testing the network............................................................................................................22

Chapter 5: Configuring your load test settings.........................................................................22

Chapter 6: Discovering conversations between local devices.................................................23
  Tell me more about the Utilization History tool......................................................................23
  Viewing real-time utilization......................................................................................................24
  Viewing a summary of network activity....................................................................................24

Chapter 7: Checking the health of your network....................................................................24
  Viewing network errors.............................................................................................................24
  About Vital Signs’ broadcasting LLC Exploratory packets.......................................................25
  Viewing network errors by device............................................................................................25
Chapter 6: Decodes

Decoding network traffic................................................. 67
I have a packet capture to analyze. What file formats can Observer load?........ 68
Removing duplicate packets.................................................. 68
Opening files from unknown locations.................................... 69
Private key locations per server.......................................... 70
Replaying a packet capture.................................................... 71

Chapter 7: Logs

Changing log file behavior................................................... 80
Disabling logging of certain event types................................. 81

Chapter 8: Alarms

Configuring and using alarms............................................. 83
Enabling probe instance alarms............................................ 83
Enabling individual alarms.................................................. 84
Creating filter-based alarms................................................ 85
Resetting statistical alarms.................................................. 86
Customizing triggers and actions........................................... 87
Customizing alarm triggers.................................................. 87
Customizing alarm actions.................................................. 87
Sharing alarms with others................................................... 88
How to export alarms.......................................................... 88
How to import alarms.......................................................... 89

Chapter 9: Security and Privacy

Security, privacy, and regulatory compliance.......................... 90
Securing communication between the analyzer and probes................ 91
Setting security options for the analyzer.................................. 91
Configuring user accounts for secure access............................ 93
Requiring a user account to open Observer............................... 93
Creating or editing a user account for the local probe.................... 93
Setting user permissions for the local probe.............................. 94
Important information about NIMS......................................... 94
Sharing packet captures with third-parties............................... 95
Password protecting the ability to change partial packet capture size............... 96
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Importing or exporting a server profile</td>
<td>142</td>
</tr>
<tr>
<td>Creating a Forensic Settings profile</td>
<td>142</td>
</tr>
<tr>
<td>Importing Snort rules</td>
<td>147</td>
</tr>
<tr>
<td>Chapter 13: Change Log</td>
<td>148</td>
</tr>
<tr>
<td>Recent documentation changes</td>
<td>148</td>
</tr>
<tr>
<td>Index</td>
<td>149</td>
</tr>
</tbody>
</table>
Chapter 1: Getting Started

System requirements and installing or upgrading the software

Prerequisite(s):

- The user running the probe software or Observer—as well as the user installing the software—must have local Administrator rights on the Windows system.

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

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

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

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

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Dual core Pentium</td>
<td>Quad core Pentium</td>
</tr>
<tr>
<td>RAM$^1$</td>
<td>2 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Operating system$^2$</td>
<td>Windows XP</td>
<td>Any Windows 64-bit</td>
</tr>
<tr>
<td>Network Card</td>
<td>Server-class</td>
<td>Intel server-class</td>
</tr>
<tr>
<td>Capture Card$^3$</td>
<td>Server-class</td>
<td>Intel server-class</td>
</tr>
</tbody>
</table>
What type of license do I have?

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

Why is my license number not working?

Each license number is case-sensitive, so be sure to type it in exactly the way it was given to you. Also, if you copy-pasted the license number into the activation prompt, be sure you did not introduce a leading or trailing space character—those are not part of your license number.

Also, ensure you are licensing the correct version of Observer. License numbers are version specific. Each license number works only within equal major version numbers of the product. For example, an Observer 16.0 license can be used to activate 16.0 and 16.1, but not 15.0, 15.1, etc.

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

Could I have my license re-sent to me?

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

Should I uninstall Observer before updating it?

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

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

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

Capture card driver requirements

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

Most NIC vendors provide solid, functional NDIS drivers for all cards available within the Ethernet, Token Ring, and FDDI marketplace.
Accessing a standard network with a “normal” network device is somewhat different from what a protocol analyzer requires. While both share a number of driver functions, a protocol analyzer requires a set of features and functions that the average network device will never need. Examples of these optional functions are promiscuous mode, error tracking, and network speed reporting. (Examples of mandatory functions would include functions to determine the maximum packet size, functions to verify the number of sent packets, and functions to specify or determine a packets’ protocol.)

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

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

- These optional counts only provide a numerical value to the total number of errors on the segment (i.e. the number of CRC errors found), they do not specify where (which station) the error originated from.
- After the error packet is identified and the proper error counter is incremented, the packet is discarded, and not sent to Windows (this is the reason it is impossible to determine the source of an Ethernet error packet with standard NDIS drivers).
- A number of vendor’s NDIS drivers return a positive acknowledgment when the NDIS error function is queried for existence, but the error statistic is not actually kept.
- A few vendors (3COM, for example) do not keep any error statistics whatsoever.

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

How collisions are counted

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

In an effort to provide a more realistic view of how many collisions are occurring on a LAN segment, Observer has an option (“on” by default when using the Vital Sign mode) to run the “Collision Test”. When turned on, this test sends packets onto the LAN at specific intervals, and records the number of collisions that the Observer station experiences. This test provides a good idea of what any station may see - with regards to collisions - during normal network usage. The collision statistic reported by Observer is an approximation of what any one station may be experiencing, as opposed to an aggregate statistic for the entire LAN segment (as is the case with CRC, Alignment, Jabbers and Runts).
Additionally, Observer includes the “Collision Expert” that both generates packets to approximate each station’s collision potential, and reports which stations are most likely to re-send directly after a collision and which stations were sending just prior to a collision. This information is then reported in an expert dialog and is key in helping to determine the station(s) that are causing the collisions on the segment.

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

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

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

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

**Overview of Observer**

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

All Observer versions use the same set of TCP ports to communicate with Network Instruments’ probes. For more details, seePorts used by Network Instruments products on page 8.

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.

The depth of features in Observer depends on which product license you purchased. For information about Observer licenses, seeFAQ: Licensing and updating on page 2.

**User interface**

...the software and its user interface, is described as the analyzer. The engine that makes traffic collection possible is the probe. The analyzer (i.e. the software) is the key to viewing, manipulating and controlling all of the data that a probe captures or sees flow through it. The analyzer
The leftmost portion of the 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 select the desired probe, then pick the desired tool from the main toolbar or from the main menu. You may have multiple tools running simultaneously for each probe. Each tool is in its own tab at the bottom of the tool window. Some tools have additional tabs along the top or bottom that provide even more functionality and display options.

Close any tool by right-clicking in the desired tab in tool tray and select Close. Close all active tools by choosing Window > Close All Statistics Windows.

Figure 1: Commonly seen user interface

The dashboard

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

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

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

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

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

**Customizing toolbars**

You can customize your Observer toolbars, which allows you to quickly move between tools without the need to navigate the menu system. To start a configuration session, select View > Toolbar Setup. The Customize dialog appears, allowing you to customize which items are shown.
Also, to move buttons from the main Observer display, hold the Shift key and drag and drop a button to a desired location. To delete a button, drag the button from the toolbar while holding the Shift key and drop it anywhere except on a toolbar.

**Ports used by Network Instruments products**

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

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

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

**Configuring Observer’s general settings**

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

**General tab**

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

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

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

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

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Sets the ports for the Gen2 capture card to be on or off from a command line using NiDecodeApi.exe -VIRTADAPTER. Parameters must be separated by a semi-colon (;).</th>
</tr>
</thead>
</table>
### Security tab

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

To view and change the security settings for an Observer analyzer, in the Observer analyzer choose Options > Observer General Options > Security tab. Use the information in Table 1 on page 9 to configure the analyzer’s security and NIMS options.

#### Table 1: Security options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Require Observer Login  | When enabled, this option forces a user to provide a user name and password to open the Observer analyzer. The user name can be stored locally if you are not using NIMS, or maintained by NIMS if the “Authenticate Observer login with NIMS” option is enabled. This option is not visible unless you have a special license enabling it.  
  **Caution:** Do not lose this password! There is no way to recover a lost administrative password.  
  Observer Login Credentials—Type a user name and password. This information is encrypted and stored locally. Only one user account is allowed per system. If you want numerous people to have access to the Observer analyzer with different user accounts, you must use NIMS.  
  Administrative Credentials—A local administrative user account that allows you to create a non-administrator account and to set security options for NIMS. |

---

**Parameters**

<table>
<thead>
<tr>
<th>C:</th>
<th>Specifies that the Gen2 capture card is a either a 1, 10, or 40 Gb capture card. The options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C:oneGig2010</td>
</tr>
<tr>
<td></td>
<td>C:tenGig2010</td>
</tr>
<tr>
<td></td>
<td>C:fortyGig2010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V:</th>
<th>Specifies the virtual port adapter number. The Gen2 card supports up to four virtual adapters. You may only specify one virtual adapter at a time.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V:1</td>
</tr>
<tr>
<td></td>
<td>V:2</td>
</tr>
<tr>
<td></td>
<td>V:3</td>
</tr>
<tr>
<td></td>
<td>V:4</td>
</tr>
</tbody>
</table>

| P: | Specifies whether a port is on or off for a given virtual adapter. The Gen2 card has up to 12 ports.  
  0=off  
  1=on  
  Ports can be partially filled. For instance:  
  P;; means all ports are off.  
  P:1; means port 1 is on and all others are off.  
  P:0001; means ports 1, 2, and 3 are off and port 4 is on. If the Gen2 card has more than four ports, any ports beyond 4 are also off. |
|----|---------------------------------------------------------------------------------------------------------------------------------------------|

**Use**

- NiDecodeApi.exe -VIRTADAPTER=C:oneGig2010;V:1;P:1111
- NiDecodeApi.exe -VIRTADAPTER=C:tenGig2010;V:3;P:01010101
- NiDecodeApi.exe -VIRTADAPTER=C:fortyGig2010;V:2;P:11110101
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Observer Encryption Key file for secure connections</strong></td>
<td>Strong encryption is available for Observer Expert and Suite users. Observer Encryption Key (.OEK) files let you use private encryption keys to ensure that unauthorized persons do not have access to the data flowing between Observer analyzers and probes. 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 NIMS.</td>
</tr>
<tr>
<td><strong>Authenticate users (for redirected Probe instances)</strong></td>
<td>Forces users to authenticate with NIMS before using remote probes. User accounts belong to user groups in NIMS and through the user group’s access to probe instances can be granted or restricted. Only probe instances to which the user has access will be visible in the analyzer. This option does not control whether users can open Observer. That is done through the “Authenticate Observer login with NIMS” option.</td>
</tr>
<tr>
<td><strong>Manage Observer / Probe license with NIMS</strong></td>
<td>An Observer or probe license can be stored and managed locally at each analyzer or probe, or it can be managed centrally by NIMS. If unchecked, it is managed locally and you must provide a license for each analyzer/probe. If selected, then you can provide a pool of licenses in NIMS and the analyzer or probe will take an available license when the analyzer or probe starts.</td>
</tr>
<tr>
<td><strong>Get list of Probe Instances available for redirection from NIMS</strong></td>
<td>When selected all probe instances to which you the user has access to through group permissions set in NIMS are available when connecting to a probe. When unchecked only the local probe instances are available and no probe instances are listed when connecting to a remote probe.</td>
</tr>
<tr>
<td><strong>Share filters with NIMS</strong></td>
<td>When selected you may create filters and share them with others. You may also get any filters created by others. Whenever a filter is updated, other users can be informed and update their local version. The list is maintained by NIMS.</td>
</tr>
<tr>
<td><strong>Synchronize user protocol definitions through NIMS</strong></td>
<td>When selected you synchronize protocol definitions, including any derived applications definitions, automatically through NIMS. If any protocol definitions are updated in another analyzer, you automatically receive those. If a protocol definition is updated in one analyzer, it is published to NIMS and NIMS pushes that new definition to all analyzers that choose to synchronize their protocol definitions. Extra caution should be used with this setting because definitions are automatically propagated to all analyzers (assuming the setting is selected in Observer). If two users are updating the same protocol definition, the last user to save and close the window is whose definition is used. Only one user (or a small select group of users) should be responsible for maintaining the list of protocol definitions. This ensures that no inadvertent changes are made.</td>
</tr>
<tr>
<td><strong>Primary/Secondary server</strong></td>
<td>Provide the IP address of the primary NIMS server. If you are also using a failover NIMS server, type its IP address in the Secondary server box.</td>
</tr>
<tr>
<td><strong>Allowed to modify shared filters</strong></td>
<td>When selected, you can get a shared filter from someone else, modify it locally, then upload your modified version to NIMS thereby making your new version available to everyone else. When disabled, you can only get filters from NIMS and upload your own. You cannot modify any filters you get from NIMS. This option requires that you have the ability to share filters with NIMS.</td>
</tr>
<tr>
<td><strong>Authenticate Observer login with NIMS</strong></td>
<td>This option works in conjunction with the “Require Observer Login” option. This forces Observer to use NIMS to authenticate users rather than Observer’s local user list. A user list is maintained in NIMS.</td>
</tr>
<tr>
<td><strong>Require a password to change partial packet capture size</strong></td>
<td>Select this option if you want to require someone to provide a password before they may change the partial packet capture size. This is a central password and all users must use the same password.</td>
</tr>
</tbody>
</table>
Launch Encryption Key Generator | Click this button to open the Network Instruments encryption key generator. If you want the GigaStor payload to be encrypted using 256 bit AES encryption before it is stored, select the “Encrypt GigaStor network traffic...” option. An encryption key is needed on the GigaStor (or a location accessible by the GigaStor) to encrypt and decrypt the data. The AES key is not needed on workstations, probes, or other collection points. A special license is required for this feature. Contact Network Instruments for this license.

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

### SNMP tab

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

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

**IPv6 tab**

IPv6 is fully and natively supported in Observer.

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

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

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

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

- Decimal separated represents the address as 16 decimal octets, for example: `254.128.0.0.0.0.0.0.37.78.243.93.125.180.0.17`
Third Party Decoder tab

Prerequisite: Observer Expert or Observer Suite

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

<table>
<thead>
<tr>
<th>Assign menu name</th>
<th>Defines the menu option that appears under the File menu. It defaults to “Decode Capture File using Wireshark,” but this menu item can be anything you want.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executable name</td>
<td>Provide the full path to the third party application you want to use to decode capture files. The decoder must be installed on the same system as the Observer analyzer, not the probe.</td>
</tr>
<tr>
<td>Command line</td>
<td>Provide any command line options you want to pass to the third party decoder when you are opening the application.</td>
</tr>
<tr>
<td>Capture buffer format</td>
<td>Choose which file format to export your capture to: Observer's native BFR format or PCAP. See Saving packet captures on page 53.</td>
</tr>
</tbody>
</table>

GeoIP Settings

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

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

You can look up the geolocation information for an IP address when you are on the Decode and Analysis tab in Observer or when you are on the IP Stations tab in the GigaStor Control Panel. For instance, click the Top Talkers tab, select an IP address, right-click and choose Connect to the Selected Station via > GeoIP Lookup.
Chapter 2: Real-Time Statistics

Monitoring connection statistics

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

Discovering conversations between local devices and the Internet

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

The Internet Observer tool has three distinct tabs:

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

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

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

**Internet Patrol tab**

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

**IP Subprotocols tab**

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

**Configuring the IP application list**

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

1. To edit or add a protocol, click the Edit or New button.
2. The Configure IP Application Ports dialog is displayed.
3. If you are editing a protocol, the protocol you selected on the List of IP SubProtocols will be displayed in the IP Application box. The information in this box is editable.
4. If you are adding a protocol, enter the desired name of the SubProtocol in the box. You can have a total of 24 subprotocols in your list of IP SubProtocols.
5. Choose either Add TCP or Add UDP, and another dialog is displayed that lets you define a port or range of ports for the IP application. The maximum is five ports. A range of ports counts as two ports. In other words, you can define one range and three ports, or two ranges and one port. You cannot assign three ranges.
6. Click OK to display the List of IP SubProtocols dialog.

Discovering conversations between local devices

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

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

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

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

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

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

Viewing real-time statistics per device

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

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

Results can be saved in a comma delimited file using File > Save > Save Data in Comma Delimited Format.
Web Observer can be configured to show additional individual stations—you are not limited to viewing one station at a time. To view the real-time statistics of individual stations in bulk, simply configure more stations in Web Observer.

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

Viewing a list of protocols seen on the network

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

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

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

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

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

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

Viewing wireless access point statistics

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

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

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

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

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

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

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

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

**After completing this task:**

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

### Monitoring network load

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

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

### Viewing router utilization statistics

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

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

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

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

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

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

After completing this task:

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

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

Viewing bandwidth utilization

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

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

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

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

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

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

**Viewing bandwidth utilization with a filter**

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

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

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

**Wireless Access Point Load Monitor**

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

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

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

1. **Statistics > Wireless Access Points Load Monitor**.
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 for more details.
4. In the Access Point speed (Bits/second), type the throughput speed for the wireless device. Typically, assuming theoretical maximums, this will be 300000000 for 802.11n (two-streams), 54000000 for 802.11a/g access points or 11000000 for 802.11b access points.

Dials provide a heads-up immediate display of packets/second, bits/second, and interface utilization.
**Viewing the distribution of packet sizes by station**

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

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

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

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

**Discovering current top talkers on the network**

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

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

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

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

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

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

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

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

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

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

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

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

Configuring your load test settings

The traffic generator tool is located at Tools > Traffic Generator. Several noteworthy settings can be configured directly in the tool, and they are described in Table 2 on page 22.

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

Table 2: 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.</td>
</tr>
</tbody>
</table>
Setting | Description
--- | ---
The start of the sequence is defined in the Edit Header dialog’s Destination MAC Address field.

You can also right-click anywhere in the Generated Packet Header area to reveal the following options:

- **Load Packet From File**—displays the Load Packet dialog, letting you load a particular packet number from a particular buffer file.
- **Save Packet to File**—lets you save the currently configured packet to a standard Observer capture file.
- **Open Packet in Decode**—shows currently formed packet in Observer’s packet capture decode window.

**Viewing utilization history**

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

**Note:** Bandwidth Utilization—a separate Observer tool—may serve as a substitute if you need to see utilization that adheres to your probe instance’s filters. For details, see Viewing bandwidth utilization with a filter on page 20.

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

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

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

**Tell me more about the Utilization History tool**

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

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

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

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

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

**Viewing a summary of network activity**

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

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

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

**Checking the health of your network**

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

**Viewing network errors**

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

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

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

Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.
If you are using an Ethernet network and are worried that errors may be traversing the network, yet this tool has not detected any, ensure that your NIC’s NDIS driver can indeed recognize errors. To check driver error support, choose Options > Selected Probe or SNMP Device Properties, and click the Parameters tab.

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

**Color codes**

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

**About Vital Signs’ broadcasting LLC Exploratory packets**

Vital Signs sends exploratory LLC packets when running the collision test. When the collision test option is on, Observer bursts 100 exploratory LLC packets per second, addressed to 00:00:FF:FF:FF, and listens for packet collisions. On a 1 Gb network this uses 0.004% of the network's bandwidth and significantly less on a 10 Gb 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.

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

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

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

To use the Wireless Site Survey tool—and search for wireless interference—choose Statistics > Wireless Site Survey. See Table 3 on page 26 for a list of noteworthy settings.

If you want to scan multiple channels:

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

Table 3: 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</td>
</tr>
<tr>
<td></td>
<td>stations are currently visible to wireless Observer. The status line at the</td>
</tr>
<tr>
<td></td>
<td>bottom of the display shows all channels currently being scanned, highlighting</td>
</tr>
<tr>
<td></td>
<td>each channel as it is looked at. Click Scan Setup to change the list of channels</td>
</tr>
<tr>
<td></td>
<td>to scan.</td>
</tr>
<tr>
<td>Frame Type Tab</td>
<td>This table summarizes frame type totals for wireless data, management, and</td>
</tr>
<tr>
<td></td>
<td>control packets.</td>
</tr>
<tr>
<td>Control Frames Tab</td>
<td>This table details control frames analyzed, including Power Save Polls,</td>
</tr>
<tr>
<td></td>
<td>Requests to Send (RTS), Clear to Send (CTS), acknowledge (ACK), and CF (</td>
</tr>
<tr>
<td></td>
<td>Contention Free) End packets.</td>
</tr>
<tr>
<td>Management Frames Tab</td>
<td>Displays detailed information about wireless management frames, including</td>
</tr>
<tr>
<td></td>
<td>association requests and responses, reassociation requests and responses,</td>
</tr>
<tr>
<td></td>
<td>ATIMs (Announcement Traffic Indication Message), and authentication/de-</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>the various supported rates. To switch between transmitting and receiving</td>
</tr>
<tr>
<td></td>
<td>speeds, click the down arrow next to the Tx (or Rx) and select the desired</td>
</tr>
<tr>
<td></td>
<td>setting.</td>
</tr>
<tr>
<td>Signal Tab</td>
<td>Displays detailed statistics on wireless signal strength, quality, and data</td>
</tr>
<tr>
<td></td>
<td>rates being used by stations and APs.</td>
</tr>
<tr>
<td>Channel Scan Tab</td>
<td>Shows the channel being tracked along with many statistics.</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 4 on page 27 shows how dB measurements are calculated into signal strength percentage.
Table 4: 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>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>
</tbody>
</table>
Ethernet errors tracked by Observer

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

Alignment Errors

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

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

MAC Frame CRC Errors

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

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

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

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

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

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

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

Collisions

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

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

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

Packets Too Small (Runts)

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

Packets Too Big (Jabbers)

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

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

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

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

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

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

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

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

Understanding Real-time Statistics

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

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

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

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

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

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

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

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

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

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

**Viewing optional VLAN statistics**

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

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

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

Results can be saved in a comma delimited file using **File > Save > Save Data in Comma Delimited Format**.
Chapter 3: Discovery

How to add application definitions

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

To add more application definitions for the Server Application Discovery tool to use, complete the following steps or see Adding derived application definitions on page 35 for details about creating definitions for applications that are subsets of another application:

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

![Add Application Window](image)

Figure 7: Add an application from the list or define a custom application

Your new application now appears in the list of application definitions.
How to associate non-standard ports with an application

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

The benefit of is that you do not need to wait for the Server Application Discovery tool to see something that you already know exists.

For example, the standard server port for MySQL is 3306. But you configured your MySQL server to use 63245 instead—a non-standard port. You must therefore associate port 63245 with the MySQL application definition so that it can be reported with greater ease in Server Application Discovery.

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

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

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

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

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

How to import application definitions

**Prerequisite(s):**

To import application definitions, you need access to an exported *.protodef file. See Exporting app definitions on page 35 for details.

To import application definitions, follow the import process:

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click any one of the applications definitions tabs (not the Server Application Discovery tab itself) to ensure one of these tabs has focus.

3. Click **Tools**, and click **Import Application Definitions**.

   The Open file dialog appears.

4. Locate and select the *.protodefs file that you want to import, and click **Open**. The Import Application Definitions dialog appears.

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

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

---

**How to export application definitions**

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

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

2. Click any one of the applications definitions tabs (not the Server Application Discovery tab itself) to ensure one of these tabs has focus.

3. Click **Tools**, and click **Export Current Application Definitions**. The Export Application Definitions dialog appears.

4. Select the groups of definitions you want to export, and click **Export**.

5. Type a name for your file, and click **Save**.

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

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

---

**Adding derived application definitions**

Creating a derived application definition allows Observer to take one large application that may have many sub-applications within it and identify each of the sub-applications.
For instance, Java traffic can be identified within HTTP. After Observer identifies the derived application, it appears on your reports and elsewhere within Observer as its own application. The Decode tab is unaffected though. The derived application decodes as part of its parent’s application type. In our Java example, all Java traffic is viewable on the Decode tab as part of HTTP.

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

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

Your new derived application now appears in the list of application definitions. Most importantly, the new application is discoverable using the Server Application Discovery tool and, if the application is seen, it is recognized correctly by Observer.

**Enabling or disabling applications that use dynamic ports**

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

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

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

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

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

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

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click an applications definitions tab that interests you.
   Application definition tabs are located below Start and Stop.
3. Scroll through the list of application definitions, and find one that you want to associate non-standard ports with per IP address.
4. Click an application definition to select it.
5. Click **Add Ports**.
6. Type the port number or port range to be associated with the selected application.
7. Select **Use Specific IP Address**, and type the IP address you want to treat differently.
8. Click OK.
9. Click Apply Changes.

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

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

How to restore TCP application definitions

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

1. Choose **Options > Protocol Definitions and Server Application Discovery**.
2. Click the TCP Application Definitions tab to ensure it has focus.
3. Click the Tools button, and click Restore Predefined TCP Applications. A confirmation prompt appears.
4. Click OK to confirm.
5. (Optional) Select Apply Changes Across All Probe Instances if you want to apply these changes to all probe instances.
6. Click OK to apply and save your changes.

Your TCP application definitions list is now restored.

How to restore UDP application definitions

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

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

Sharing application definitions with others

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

How to export application definitions

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

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

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

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

How to import application definitions

Prerequisite(s):

To import application definitions, you need access to an exported *.protodefs file. See Exporting app definitions on page 35 for details.

To import application definitions, follow the import process:

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

You successfully imported application definitions. The definitions you import are now part of your local collection.
Chapter 4: Captures

Configuring the capture buffer settings

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

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

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

During the creation of your probe instance(s), you set the size of your buffers. The capture buffer is used to store raw data captured from the network, and the statistical buffer stores statistical data entries (example buffer change shown in Figure 12 on page 41).

Figure 12: Changing your buffer sizes
If you are pushing the limits of the PC system on which the probe is installed by creating many instances, you may be able to avoid some performance problems by fine-tuning the memory allocation for each instance.

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

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

1. Choose Options > Selected Probe or Local Observer Instance, Memory and Security Configuration.
   The Observer Memory and Security Configuration window appears, listing all configured probe instances.

2. Double-click the probe instance you want to configure. The Edit Probe Instance window appears.

3. Change the buffer sizes to better match the needs of your chosen probe instance. Generally, more is better, but not always.

4. (Optional) Select a predefined statistics memory configuration from the drop-down list. Your configuration choices are small, medium, and large.
   The choices in 4 on page 42 affect the maximum number of entries per statistic. All of these allocated statistical entries combined determine the amount of memory used by statistics.

5. Click OK twice to confirm and save your changes.

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

**Fine-tuning the statistical buffer**

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

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

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

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

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

By tweaking the statistics allocation, you can fine tune how Observer processes its data.

You cannot modify the default statistics memory configuration. You must create a new profile based on one of the existing profiles (Small, Medium, Large, 4G LTE) and modify it.

1. To view and manage memory allocation for probe instances, click the Memory Management tab to display the list of instances and their buffer sizes.
2. Right click any instance and select Configure Memory to access the memory allocation dialog.

![Figure 13: Probe Instance Memory](image)

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

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

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

**Tell me more about the statistical memory allocations**

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

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

IP Top Talkers
This is linked to the IP tab within the Top Talkers mode. Since it is an IP based mode it is not part of the Global Statistics memory configuration. Each individual IP seen uses one entry.

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

IP Trending Patrol
This is specific to Network Trending. Data collected by this can be seen from within the Network Trending Viewer under the Internet Patrol tab within the IP area of the viewer and within the Web Based Reports under:
Drill Down (Classic Reports) - Internet Trending - on the Internet Patrol tab
Trending Pairs creates entries with both MAC and IP Addresses. For each packet seen 2 entries are used. Example:
1 packet is sent from IP 192.168.1.1 to 192.168.1.2
Source MAC Address: 00:00:E4:56:AB:08
<table>
<thead>
<tr>
<th>Source IP Address: 192.168.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination MAC Address: 00:08:F9:01:BC:12</td>
</tr>
<tr>
<td>Destination IP Address: 192.168.1.2</td>
</tr>
<tr>
<td>Inside of Trending you would see the following entries:</td>
</tr>
<tr>
<td>Station 1 MAC Station 2 IP Total Packets Packets 1-&gt;2 Packets 2&lt;-1</td>
</tr>
<tr>
<td>00:00:E4:56:AB:08 192.168.1.2 1 1 0</td>
</tr>
<tr>
<td>00:08:F9:01:BC:12 192.168.1.1 1 0 1</td>
</tr>
<tr>
<td>As you can see for a single packet two entries are used</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Trending Protocols by Station</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is specific to Network Trending. It collects a list of IP addresses seen. It is tied into the IP Trending Protocols by Station Buffer setting. It uses 1 entry per IP address seen.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Trending Protocols by Station Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is specific to Network Trending. It collects protocol information on a per IP address basis. The protocols are only collected for those IP Addresses in the IP Trending Protocols by Station list. By default we have ten times the number of Station Buffer entries for every by Station entry. So if there are 100 by Station entries, there would be 1000 by Station Buffer entries by default.</td>
</tr>
<tr>
<td>Let us say we have a machine that has sent an HTTP packet to a server, we would use six entries for that one packet.</td>
</tr>
<tr>
<td>Source IP</td>
</tr>
<tr>
<td>IP &gt; Entry 1</td>
</tr>
<tr>
<td>TCP &gt; Entry 2</td>
</tr>
<tr>
<td>TCP PORT # (OTHER) &gt; Entry 3</td>
</tr>
<tr>
<td>Destination IP</td>
</tr>
<tr>
<td>IP &gt; Entry 4</td>
</tr>
<tr>
<td>TCP &gt; Entry 5</td>
</tr>
<tr>
<td>HTTP &gt; Entry 6</td>
</tr>
<tr>
<td>This data can be viewed within the Network Trending Viewer under IP - TCP/UDP Application Tree</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internet Observer - IP Pairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is specific to the Internet Observer statistical mode and pertains to the IP to IP Matrix tab within that mode. It acts exactly like the IP Trending Pairs memory configuration in that it keeps track of IP to IP based conversations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internet Observer - IP Patrol</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is specific to the Internet Observer statistical mode and pertains to the Internet Patrol tab within that mode. It acts exactly like the IP Trending Patrol memory configuration in that it keeps track of MAC to IP based conversations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internet Observer - IP Protocols by Station</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is specific to Internet Observer statistical mode and pertains to the Protocols tab of that mode. It creates a list of IP Addresses and provides information about which protocols were used by that IP address. It uses 1 entry per IP address seen.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Trending Protocols by Station Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is specific to Network Trending. It collects data about which MAC address sent or received which protocol. As previously noted while describing IP Trending Protocols by Station Buffer, a list is created of stations seen, here based on MAC addresses, along with a list of protocols seen. Again we use multiple entries for each level of the packet. However unlike the IP Trending Protocols by Station Buffer, this keeps track of all protocols seen, not just IP based protocols.</td>
</tr>
<tr>
<td>Example:</td>
</tr>
<tr>
<td>Source MAC</td>
</tr>
<tr>
<td>IP &gt; Entry 1</td>
</tr>
<tr>
<td>TCP &gt; Entry 2</td>
</tr>
<tr>
<td>TCP PORT # (OTHER) &gt; Entry 3</td>
</tr>
<tr>
<td>UDP &gt; Entry 4</td>
</tr>
<tr>
<td>Telnet &gt; Entry 5</td>
</tr>
<tr>
<td>ARP &gt; Entry 6</td>
</tr>
</tbody>
</table>
As you can see an individual MAC address can have a large number of entries used. By default we allocate 25 entries for each entry allocated in Network Trending Stations. So if you have 100 allocated Network Trending Stations, by default there would be 2500 entries allocated for Network Trending Protocols by Station Buffer.

This data can be viewed within the Network Trending Viewer under the MAC header on the Protocols tab. This data can also be viewed in the Web Based Reports under:

- Network Summary - Protocol Distribution
- Network Summary - Protocol Summary
- Network Summary - IP Subprotocol Distribution
- Network Summary - IP Group Protocol Distribution
- Network Summary - IP Application Distribution
- Network Summary - IPX Subprotocol Distribution
- Network Stations - Protocols

**Network Trending Station Display**

This is specific to Network Trending. This memory configuration does NOT affect how data is collected within Network Trending. When looking at Network Trending, you will see a set of dials and a table which shows which statistics are being collected. This configuration adjusts how many stations are displayed within the Station/Pair column.

If this entry is set to 100, then we will only show the statistics of the first 100 MAC addresses seen during the collection interval. If 1000 stations were seen, we will collect on all 1000 stations (if Network Trending Stations is set to 1000 or higher), but the number of stations along with packets and bytes will only reflect the first 100 stations seen during the collection interval.

**Network Trending Stations**

Specific to Network Trending. It collects information about individual MAC addresses seen. It uses 1 entry per MAC address seen, whether the MAC address is the Source or the Destination. This data can be viewed within any of the Web Based Reports under the headings Network Summary and Network Station. Also this data can be viewed within the Network Trending Viewer under the MAC section.

**Pair Statistics (Matrix)**

This is specific to the statistical mode Pairs Statistics (Matrix). This mode collects data based on MAC address pairs. For each MAC pair 1 entry is used.

**Server Discovery**

This is specific to the Application Analysis mode. It is used to limit the number of stations seen during discovery. The maximum number of servers that can actively be monitored is 32. For each server discovered 1 entry is used.

**VLAN Statistics**

This is specific to the VLAN Statistics mode. For each MAC address seen we monitor which VLAN it was seen from. 1 entry is used for each MAC address seen.

**VLAN Trending Stations**

This is specific to Network Trending and works in the same fashion as the VLAN Statistics memory configuration works, in that it uses 1 entry for each MAC address seen and keeps track of which VLAN it was seen on.

This data can be viewed only from the Web Based Reports under: Report Library - VLAN

**Web Server Statistics**

This is specific to the Web Observer statistical mode. This mode monitors connections to a server and keeps track of how much data is sent to and from the server being monitored. For each device which communicates to the server 1 entry is used.
Configuring the packet capture options

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

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

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

Excluding non-native packets from capture

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

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

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

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

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

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

What are Expert Information Packets?

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

Expert Load Packets – These packets are inserted every second into the capture. They include information about the number of packets and bytes seen during the previous second, along with the utilization seen.

These figures are used while drawing the graph seen on the Expert Events tab within the Expert screen.
Start/Stop Packet Capture – These packets are inserted whenever you click Start or Stop from either the Packet Capture or Decode Screen. They are used to help expert know that there are gaps of time between packets.

Wireless Channel Change – These packets are inserted when monitoring a wireless network adapter. They are inserted only if you are using the Channel Scan option. Each time Observer begins monitoring a new channel while in the Channel Scan mode, a new packet is inserted with the current channel being monitored.

Can I disable them?

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

Do I need them?

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

(Disabling Expert Load Packets) – Disabling these packets will cause Expert to draw the Summary graph based solely on those packets within the capture buffer. As an example assume 20,000 packets were seen during a one second period, also that there was 10,240,000 bytes and 10% utilization. With these packets enabled Expert would graph 20,000 packets and 10% utilization. Now assume during this one second you used a filter and captured only five packets during that second, with these packets Observer would graph 20,000 packets and 10% utilization. If you had disabled the Network Load Packets, Observer would graph five packets and 0% utilization.

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

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

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

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

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

   A circular buffer also allows you to save the packet capture buffer to multiple, sequentially labeled files instead of overwriting a circular capture file. Some of the next steps describe how to enable that functionality.

5. (Optional) Enable the Save Captured Packets to a File setting; type the maximum amount of disk space to be used for this purpose.

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

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

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

7. Click OK to confirm and save your changes.

Configuring Observer to capture partial packets

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

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

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

The partial packet capture setting affects all Observer consoles that connect to this probe instance. You cannot change this setting unless you have administrative privileges to do so. See Configuring user accounts for secure access on page 93.

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

Packet Captures

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

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

Capturing network traffic

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

Are you seeing duplicate packets collected during your capture? Do you want to ignore them? See Removing duplicate packets on page 68.

Using Observer, network traffic can be captured in real-time and examined immediately or later. This section describes several methods for capturing network traffic using Observer.

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

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

After completing this task:

After capturing is complete, you may want to:

- Save your capture—select **File > Save** to keep a shareable buffer file. For information about saving packet captures, see Saving packet captures on page 53.
- Analyze the capture—click Decode to examine the captured packets and how they interact over the network.
Capturing from multiple probe instances

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

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

Scheduling packet captures

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

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

**Note:** One way to prevent a premature end to scheduled captures is to use a circular capture buffer that writes to disk. See *Configuring a circular capture buffer on page 49.*

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

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

For by day of week at specified times, you must specify a capture begin and end time by clicking the Add button for each day you select. Multiple time intervals are configurable, per day, if the times do not conflict.

5. Click OK to confirm and save your changes

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

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

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

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

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

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

**Why am I missing packets?**

Assuming your Observer analyzer has the network visibility it needs— and packets are not being dropped due to hardware or driver issues—there are a few reasons Observer may not “see” packets that you, yourself, were expecting to see. Fortunately, this problem can typically be fixed by changing a simple setting in Observer, which is outlined in this section.
By default, Observer’s packet capture tool is configured to see (i.e. follow) only newly opened TCP connections. A newly opened TCP connection is any connection established after Expert Analysis was started. To change this behavior, complete the following steps:

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

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

This change should allow you to see connections that were established prior to opening the packet capture tool, along with the packets they contain. If you are still not seeing all packets, ensure you have all pre-filters deactivated. See **Activating and deactivating filters on page 61**.

### Saving packet captures

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

After starting a packet capture—described in **Capturing network traffic on page 50**—save the packet capture by choosing **File > Save > Save Capture Buffer**. Alternatively, you can press CTRL+S.
The available file formats you can save to depend on the network topology of the captured traffic—although Observer’s native BFR format can be saved to regardless of topology. Observer can save packet captures to any of the formats listed in Table 5 on page 54.

### Table 5: Save Capture Buffer options

<table>
<thead>
<tr>
<th>File format</th>
<th>Supported topologies</th>
<th>Limitations and other information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFR</td>
<td>Any topology[^1]</td>
<td>BFR can only be read in Observer and Wireshark. Retains both nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>CAP</td>
<td>Ethernet, FDDI, Token Ring</td>
<td>CAP loses nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>ENC</td>
<td>Ethernet</td>
<td>ENC loses nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>FDC</td>
<td>FDDI</td>
<td>FDC loses nanosecond resolution and expert information packets.</td>
</tr>
<tr>
<td>PCAP</td>
<td>Ethernet, FDDI, Token Ring</td>
<td>PCAP retains nanosecond resolution, but loses expert information packets.</td>
</tr>
<tr>
<td>TRC</td>
<td>Token Ring</td>
<td>TRC loses nanosecond resolution and expert information packets.</td>
</tr>
</tbody>
</table>

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

Saving to any format other than Observer’s native BFR format removes all expert information packets from the resulting saved packet capture. For more information about expert information packets, see Excluding non-native packets from capture on page 47. Saving to any format other than Observer’s native BFR format or the PCAP format removes all nanosecond resolution from the resulting saved packet capture. If you need to retain nanosecond resolution, ensure you save a packet capture to either the BFR or PCAP format. See the table for a full list of limitations per format.

Except for XML, Observer can load all of the files formats that it can save to, plus the DMP format. To load packet captures, see Decoding network traffic on page 67.

### Redirecting a probe instance

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

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

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

To redirect a probe instance, complete the following steps:
1. Choose **Actions > Redirect Probe Instance(s)**. The Remote Probe Administration and Redirection window appears.

   If you have several remote probe instances already configured in your Observer software, this window lists them. If you see none, you currently have no remote probe instances configured.

2. Do one of the following:
   - If you see a remote probe instance you want to redirect, skip directly to 6 on page 55.
   - If your list is empty or missing the remote probe instance you want to redirect, proceed to 3 on page 55.

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

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

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

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

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

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

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

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

10. Close the Probe Instance Redirection window.

If the operation succeeds, the remote probe instance is now redirected to the local Observer analyzer. Now you can use the remote probe instance just as you would if it was running on your local machine.
Chapter 5: Filtering

Pre-filtering your packet captures

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

Failing to click OK in 8 on page 56 causes Observer to discard any and all changes made since the Active Filters window first appeared in 1 on page 56, including all filters you may have created during that period of time.

This section describes pre-filters only; these filters affect what your future packet captures record. If you have an existing capture file and would like to post-filter it instead, see Post-filtering your packet captures on page 63.

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

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

Observer’s Protocol Data Field filter rule lets you search for specific values in selected protocol header fields. For example, you can filter for ICMP destination unreachable packets and wireless control, data, and management packets. You can also define your own custom protocol filter, either by port or search pattern.

Click Add and give the protocol filter a descriptive name and choose whether you want to define the protocol by a pattern filter or a port filter. After you click OK, the appropriate filter dialog is displayed allowing you to enter the pattern or port that defines the protocol.

Tell me how to filter by pattern

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

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

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

The pattern itself is the actual ASCII, Regular Expression, Hex or Binary string that you are filtering for.
For example, to define an offset-sequencing filter to look for telnet packets (i.e., looking for TCP port 23) in one direction, the offset would be 34 (14 bytes of Ethernet header + 20 more bytes of IP header) and the hex pattern would be 00 17 (23 in hex).

To create a Hex Pattern rule for telnet in both directions, you could first tell Observer you want to start the offset at the IP-TCP protocol portion of the header (specify IP-TCP in the Protocol dialog), then tell Observer that you want the first offset to start immediately (port number is the first field after the TCP header) by entering 0 in the first offset field and 00 17 in the first Offset Filter area. This will filter for telnet packets in the direction of source to destination. To see the telnet response packets, you should enter a second offset (in the same dialog) for offset 2 and with a value of 00 17. The second offset specifies the destination port (this is the reason for the offset of 2).

Table 6: Rules types

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address - IP Range/IP</td>
<td>Specify a hardware or IP address or range of addresses for source and destination. You can also limit the rule to apply only to packets from particular source or destination ports. For IPv4 packets, you can specify a subnet mask for inclusion/exclusion.</td>
</tr>
<tr>
<td>Packets with Comments</td>
<td>Filter for packets that have been commented by an Observer user and saved with a capture file. Comments are useful for annotating packets when two analysts are working on a problem together, perhaps sending each other captures from remote sites on a corporate network. There are no setup options. Available for post-filter only.</td>
</tr>
<tr>
<td>Error</td>
<td>Specify the categories of errors you want to filter for: CRC, Alignment, packet too small, and packet too large are available for all network types. You can also filter for Wireless WEP errors if you are analyzing a wireless network. If you are analyzing a WAN link, you can filter for WAN abort and RBIT errors. Observer also lets you filter for Token Ring error notifications when analyzing Token Ring networks.</td>
</tr>
<tr>
<td>Ethernet Physical Port</td>
<td>Allows you to filter on the physical port or link of the Ethernet capture card. When choosing to filter by link, you can also choose the direction (DCE or DTE).</td>
</tr>
<tr>
<td>Expert Packets</td>
<td>This rule lets you filter for Observer-generated Expert packets. These packets will only be generated if the Include Expert Load information packets box has been checked in Mode Commands Setup for Packet Capture. There are no setup options. Available for post-filter only.</td>
</tr>
<tr>
<td>Full Duplex Ethernet Port</td>
<td>Lets you filter for direction (DCE or DTE) on a selected full-duplex port.</td>
</tr>
<tr>
<td>Length (Bytes)</td>
<td>Specify a packet length, and whether you want to filter for packets that are less than, equal to, or greater than that length. You can also filter for packets that fall within a range of length values.</td>
</tr>
<tr>
<td>Rule Type</td>
<td>Usage</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MPLS</td>
<td>The MPLS filter allows you to filter on any level of the MultiProtocol Label Switching protocol.</td>
</tr>
<tr>
<td>Numeric Value</td>
<td>This rule is useful when you need to filter for a numeric value (or range of values) that is embedded within a byte, word or double word.</td>
</tr>
<tr>
<td>Packet Time</td>
<td>Allows you to create a capture file with packets only before, after, or during a specific time. This filter is only available for pre- and post-filtering.</td>
</tr>
<tr>
<td>Partial Packet Payload for TCP/UDP</td>
<td>Allows you to capture (or not capture) specific payload data based on how the rule is configured. This is especially useful if you need to share packet captures. See <a href="#">Sharing packet captures with third-parties on page 95</a>.</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>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 7 on page 61 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 7: Modifiers

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>Make the search case insensitive.</td>
</tr>
<tr>
<td>s</td>
<td>Interpret the period (.) meta-character to include newlines.</td>
</tr>
<tr>
<td>m</td>
<td>By default, the string is treated as one big line of characters. ^ 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.

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

By activating more than one filter (if desired), all activated filters are linked together with a logical OR statement.

Also, if you apply a rule that is not relevant to your pre-filter or post-filter scenario, that rule is ignored.

1. Choose Actions > Filter Setup for Selected Probe. The Active Filters window appears.
2. Browse the list of filters, and activate any filter by enabling it.
3. (Optional) Edit any filter by selecting it and clicking Edit Filter.
4. (Optional) If you want to deactivate all filters, activate the “Empty Filter” filter.
5. Click OK to save your changes.
All future packet captures now adhere to the rules of all active filters. When necessary, you
can deactivate filters by disabling them during 2 on page 61. 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 17: AND filter example

![AND filter example](image)

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 18: OR filter example

![OR filter example](image)

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

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

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

This section describes post-filters only; these filters affect what you see in a loaded capture file. If you have an existing capture file and would like to pre-filter it instead, see Pre-filtering your packet captures on page 56.

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

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

The Decode tab, of the Decode and Analysis window, displays each captured packet stored in the file matching the filter criteria. See Using the Decode pane on page 74 for more details.

Enabling command-line filtering

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

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

After command-line filtering is enabled, you can post-filter via command line as described in Post-filtering via command line on page 63.

Post-filtering via command line

As an alternative to traditional set-up of filters, it is possible to post-filter your packet captures via command line.
Note: Command-line filtering must be enabled before continuing. See Enabling command-line filtering on page 63.

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

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

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

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

To post-filter via command line:

1. Choose File > Load and Analyze Observer Capture Buffer.
2. Navigate to the capture file you want to load, and select it.
3. Click Open. The capture file loads into Observer and you arrive at the Decode and Analysis tool.
4. Click the Type Script Filter button.
5. Build your filter, using the building blocks list as your guide.
   
   Descriptions of each building block, including example usage, can be found in Table 8 on page 65.

   Figure 19: 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 8: Building blocks

<table>
<thead>
<tr>
<th>Building block</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
</table>
| -ip=           | -ip=10.0.36.139  
                | -ip=74.125.224.72 | IPv4 Address—use this to filter for a single IP address (IPv4). |
| -ip_pair=      | -ip_pair=10.0.36.139/10.0.36.154  
                | -ip_pair=10.0.36.139/74.125.224.72 | IPv4 Pair—use this to filter for two IP addresses (IPv4) that have conversed with each other. |
| -ip_range=     | -ip_range=10.0.36.1/10.0.36.255  
                | -ip_range=192.168.0.20/192.168.0.100 | 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. |
| -ipv6=         | -ipv6=FE80::F544:9E0:9C81:9FB1  
                | -ipv6=ff00::7f00:1 | IPv6 Address—use this to filter for a single IP address (IPv6). |
| -ipv6_pair=    | -ipv6_pair=FE80::F544:9E0:9C81:9FB1/2002::4A7D:E048 | IPv6 Pair—use this to filter for two IP addresses (IPv6) that have conversed with each other. |
| -ipv6_range=   | -ipv6_range=FE80::A00:2401/FE80::A00:24FF | 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. |
| -mac=          | -mac=00:0C:85:BD:08:80  
                | -mac=00:50:56:2E:AB:A0 | MAC Address—use this to filter for a single MAC (hardware) address. |
| -mac_pair=     | -mac_pair=00:50:56:2E:AB:A0/00:0C:85: | MAC Address Pair—use this to filter for two MAC addresses that have conversed with each other. |
| -mac_range=    | -mac_range=01:00:5E:00:00:00/01:00:5E: | 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. |
| -regex=        | -tcp=22  
                | -tcp=80  
                | -tcp=25901 - and -tcp=25903 | TCP Port—use this to filter for a single TCP port number. As with other building blocks, you can add more using an – and building block. |
| -tcp_pair=     | -tcp_pair=63268/25901  
                | -tcp_pair=25901/25903  
                | -tcp_pair=3389/3391 | 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. |
| -tcp_range=    | -tcp_range=0/5000  
<pre><code>            | -tcp_range=35/1023 | TCP Port Range—use this to filter for communication on any TCP port |
</code></pre>
<table>
<thead>
<tr>
<th>Building block</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-tcp_range=60000/63500</td>
<td></td>
<td>between the specified range. The port numbers that form the beginning and the end of the range are included in the filter. Direction is a non-factor for this building block; the filter looks for a pair of ports regardless of source or destination.</td>
</tr>
<tr>
<td>-udp=</td>
<td>-udp=53 -udp=88 -udp=26000 -and -udp=61001</td>
<td>UDP Port—use this to filter for a single UDP port number. As with other building blocks, you can add more using an -and building block.</td>
</tr>
<tr>
<td>-udp_pair=</td>
<td>-udp_pair=63240/27015 -udp_pair=49501/42</td>
<td>UDP Port Pair—use this to filter for any pair of UDP ports that have conversed with each other. Direction is a non-factor for this building block; the filter looks for a pair of ports regardless of source or destination.</td>
</tr>
<tr>
<td>-udp_range=</td>
<td>-udp_range=27901/27910 -udp_range=27030/27000 -udp_range=0/1023</td>
<td>UDP Port Range—use this to filter for communication on any UDP port between the specified range. The port numbers that form the beginning and the end of the range are included in the filter. Direction is a non-factor for this building block; the filter looks for a pair of ports regardless of source or destination.</td>
</tr>
<tr>
<td>-vlan=</td>
<td>-vlan=101 -vlan=101 -and -vlan=102</td>
<td>VLAN ID—use this to filter for a single VLAN ID. As with other building blocks, you can add more using an -and building block.</td>
</tr>
<tr>
<td>(space character)</td>
<td>-tcp=80 -tcp=8080 (TCP port 80 -OR- TCP port 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>/ (forward slash)</td>
<td>-ip_range=10.0.36.1/10.0.36.255 (Any IPv4 address between 10.0.36.1 and 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>
</tbody>
</table>
Decoding network traffic

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

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

The simplest method for decoding network traffic is to load a capture file—a saved file that is a complete, self-contained packet capture collected during an earlier time. If you do not have access to a capture file and need help creating one, see Capturing network traffic on page 50 before continuing. Also, that section describes how to decode a real-time packet capture, while this section does not.

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

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

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

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

After completing this task:

See Using the Decode pane on page 74 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
- TRC

For information about the formats Observer can save packet captures to, see Saving packet captures on page 53.

Removing duplicate packets

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

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

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

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

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

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

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

Opening files from unknown locations

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

You may want to use this option if you are:

- Unsure of the header, MPLS analysis, or ToS/QoS settings
- Decrypting wireless data
- Decoding protocols on non-standard ports (although user-defined protocols are not decoded for a NetFlow instance)

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

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

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

Microsoft Lync Server

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

By default, the Lync Server key is not exportable. You must create an exportable key for Observer to use. Getting the Lync Server key is similar to that for the IIS Web Server. See Windows IIS Web Server on page 70.

Apache Web Server

Perform a search for the file with the name “server.key”. Check the format of the server.key file to ensure it is not an encrypted private key file. See Example of an encrypted private key file on page 71.

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):

```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 (How to back up a server certificate in Internet Information Services).

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

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

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

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

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

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

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

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD7uhNymd6WCORqH0rpd5zs4FEmx2JrKtm0dmTf44SVaGvFLF1
vakeOYP/sFs4a2aUaNOFCbFaS2w3IZWUm4sCtqtvb8zil+13V6dyR+2Srx9GMbu
SnoL/6F186m+C0qHq6g0ILoiTaJnY+MOEC2wbwMykz1jPVUOXEnEGOA0IQDAQAB
AoGAFQOyqWEVmqRPwZw6XnXkJxVGVGcZrPiDrWfgc0/ITXhYUt12I47QLd+ni
-----END RSA PRIVATE KEY-----
```

### Example of an encrypted private key file

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

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,7BC....
JHQBUpdoBneFM9h2j2Smiugxd0a2q/MiX43xa4Es6nKmzu90I/ZfpIdAHii9wtsD
mZ5bQRiXD9AxeIRy+0cG2ibUaphQEv995PWUsh8N9RumsgykM6SwNd7tkbHB
i0/VVSAda9bV3db15n6MwMnPG+YC3S90GAK42RlqHRQ94fd/ZAaPV9i1wCmX6
swF1NBLGuKFl1J9qkyr+O0QqulrAayZAB2UTbGCJJetELFtV4mLm1aHdgDiUCpJp==
-----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.

To replay a packet capture, you must be using a local probe instance. The probe instance on which you want to replay a packet capture cannot be on a remote system. Choose **Tools > Replay Packet Buffer**.
Dial displays—the left dial displays the speed (packets per second) of the buffer as it is being replayed. The right dial displays the speed (bytes per second) of the buffer as it is being replayed.

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

Settings pane:
- Select buffer and button—allows you to enter the name of the buffer (.BFR) file to be transmitted. Enter the name and address of the file to be transmitted or click the Select buffer button to browse to it.
- First packet—allows you to set the number of the first packet in the buffer to be transmitted.
- Last packet—allows you to select the number of the last packet in the buffer to be transmitted.
- Speed (pkt/sec)—allows you to set the speed, in packets per second, which you would like to attempt to transmit the buffer.

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

Generation Mode:
- Time period to generate (1-65500 sec)—packets will be generated at the configured speed for the number of seconds specified in the edit box. If the specified contents of the buffer are completely transmitted before the end of that period, the transmission will loop back to the first packet as chosen above.
- Number of times to replay this buffer—the buffer file, or the selected portion of it, will be replayed the number of times specified in the edit box.

**Working with packets**

1. Choose **Capture > Packet Capture** or load a saved capture.
2. Click the Decode button. The Decode and Analysis window appears.
3. Click the Decode tab, then select a packet.
4. Right-click and a menu appears with many options. Those options are described in Table 9.

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

**Table 9: Packet options**

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

5. For additional settings, choose **Settings > General tab**. These settings are described in **Table 10**.

**Table 10: Expanded packet options**

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

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

<table>
<thead>
<tr>
<th>Expert Analysis</th>
<th>Displays all general, non-conversation specific problems that Observer finds when analyzing the packet capture.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decode</td>
<td>Shows the raw packets for you to examine yourself. The tab has three sections. The top section shows the list of packets. Right-click any of the packets to see a list of actions you can take on it. The middle section is detailed information about the selected packet. The bottom section is the contents of the packet in hexadecimal and EBCDIC. Press F4 to maximize this bottom section to see more of the packet contents. There are numerous settings, such as colors and protocol forcing, that you can configure by clicking the Settings button. You can save buffers, search for packets and other actions using options under the Tools menu.</td>
</tr>
<tr>
<td>Summary</td>
<td>Summarizes network details, errors, data rates, packets, and utilization for the traffic Observer saw. The information on the Summary tab is only for the packets seen on the Packet Capture window or in the buffer file you loaded.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Lists the protocols seen and shows how many packets and bytes of that protocol were seen, what percentage of the total packets or bytes that is, and utilization.</td>
</tr>
<tr>
<td>Top Talkers</td>
<td>Shows what devices are the most active on your network. The MAC address, DNS name, IP address are listed. There are several tabs to see the data in different ways. There are numerous settings that you can configure by clicking the Settings button. This feature is very similar to the Top Talkers covered in Discovering current top talkers on the network on page 21.</td>
</tr>
<tr>
<td>Pairs (Matrix)</td>
<td>Graphs the top 10 most active device pairs by packets per second. This feature is very similar to the Pairs Matrix in Discovering conversations between local devices and the Internet on page 14.</td>
</tr>
<tr>
<td>Internet Observer</td>
<td>Has three tabs that show a graph of the packets total by device on the Internet Patrol tab, and lists of IP Pairs and IP Subprotocol. There are numerous settings that you can configure by clicking the Settings button. This feature is very similar to the Internet Patrol in Discovering conversations between local devices and the Internet on page 14.</td>
</tr>
<tr>
<td>Application Transaction Analysis</td>
<td>Contains several tabs for the applications that Observer analyzes, including response time and statistics, URL statistics, FIX, and SQL.</td>
</tr>
</tbody>
</table>
Using the Decode pane | 75

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Lists a summary and stations of VLAN activity. Shows packets, bytes, broadcasts, multi-casts, and utilization. You can configure how the list appears by using the Settings button. This feature is very similar to VLAN Statistics described in Viewing optional VLAN statistics on page 32.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensic Analysis</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 ../observer/using_network_forensics_to_track_acceptable_use_or_compliance.html.</td>
</tr>
<tr>
<td>Access Point (AP) Statistics</td>
<td>Shows wireless access point statistics. This is similar to Viewing wireless access point statistics on page 17.</td>
</tr>
<tr>
<td>Fibre Events</td>
<td>Shows details related to your Fibre traffic.</td>
</tr>
<tr>
<td>4G LTE Analysis</td>
<td>Contains several tabs specific to 4G LTE devices, applications, and connections.</td>
</tr>
</tbody>
</table>

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.

![Figure 20: Decode tab](image-url)
Last—the last packet number in the buffer.

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

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

For details about the packet header menu, see Working with packets on page 72.

Using keyboard shortcuts

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

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

When focus is on the packet header pane:
> or > Move to the next or previous packet.
F7 or F8 Move to the next or previous packet.
Ctrl+Shift+> or Ctrl+Shift + > Move to the next or previous packet in the conversation. A conversation is a set of packets exchanged between IP/Port pairs.

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

When focus is on the hexadecimal pane:
> or > Move to the next or previous line of the hex (or character) display.
> or > Move forward or backward one character at a time.
F7 or F8 Move to the next or previous packet in the buffer (same as arrow keys when focus is on the packet header pane).
Ctrl+> or Ctrl+ > Move to the next or previous packet in the buffer (same as arrow keys when focus is on the packet header pane).
Ctrl+Shift+> or Ctrl+Shift + > Move to the next or previous packet in the conversation. A conversation is a set of packets exchanged between IP/Port pairs.
Saving a packet capture

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

<table>
<thead>
<tr>
<th>Feature</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>
<tr>
<td>Replace hardware address in all saved packets</td>
<td>when selected, enables hardware address substitution in the saved buffer. You can have Observersubstitute either MAC addresses, IP addresses, or both. In either case, the controls are the same: Original address—allows you to specify which addresses will be searched for during the replacement. Wildcard substitution with the asterisk character allows you to select multiple addresses. The last 10 specifications entered are conveniently available in a drop-down menu. New address—allows you to specify which hardware address will be substituted in place of the original. An asterisk (<em>) or x used in the same position as the Original address specification causes that portion of the address to be retained in the saved file. For example, specifying Original address: 123.123.100.</em> 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.</td>
</tr>
</tbody>
</table>
Decrypt 802.11 WEP Encrypted Packets

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

Decompress FRF.9 compressed packets

If you have captured frames from a Network Instruments WAN probe, Observer can decompress the frames before saving them. Decompression will not work unless the probe captured all the packets from the beginning of a connection initialization between the router and the CSU/DSU. You can force an initialization during data collection by resetting either the CSU/DSU or the router.

**Searching for a specific packet**

1. Choose Capture > Packet Capture or load a saved capture.
2. Click the Decode button. The Decode and Analysis window appears.
3. Click the Decode tab, then Choose Tools > Find Packet. The Find Packet window appears.
4. Using the information in Table 11 choose how you want to search the capture buffer.

<table>
<thead>
<tr>
<th>Table 11: Searching a packet capture</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Raw Packet Data</strong></td>
</tr>
<tr>
<td><strong>Decoded Data</strong></td>
</tr>
<tr>
<td><strong>ASCII</strong></td>
</tr>
<tr>
<td><strong>EBCDIC</strong></td>
</tr>
<tr>
<td><strong>Hexadecimal</strong></td>
</tr>
<tr>
<td><strong>Decimal</strong></td>
</tr>
<tr>
<td><strong>Find Sequence</strong></td>
</tr>
<tr>
<td><strong>Find All Conversations Containing Search Sequence</strong></td>
</tr>
</tbody>
</table>

**Filtering your saved packet capture**

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

**After completing this task:**
For more details about the post-capture filters and for a faster filtering method, see Post-filtering your packet captures on page 63.

**Processing NetFlow or sFlow data**

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

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

Changing log file behavior

To set where log file data is saved, what types of events are logged, and how long to retain information, click the Log Settings button located above the log window. By default, Observer logs the following event types to a daily log file:

- Alarm
- SNMP
- Probe
- Information
- VoIP

The daily log file is stored in the LogWindow folder in your Observer installation directory. The log file is written (or appended to) each time you close Observer, or automatically at midnight if Observer is running when the date changes.

To change the behavior of the log file, complete the following steps:

1. In the bottom portion of Observer’s main window, click Log Settings. The Log Settings window appears.
Disabling logging of certain event types

Logs are a simple and effective way for you to track Observer related events. This section describes which events Observer can log and how to control the behavior of Observer log files in general.

By default, Observer logs the following event types to a daily log file:

- Alarm
- SNMP
- Probe
- Information
- VoIP

This section describes how to disable logging of any event type. If you have no reason to disable logging of certain event types, this section has little to offer you. As an alternative, see Changing log file behavior on page 80 instead.

To disable logging any or all event types, complete the following steps:

1. In the bottom portion of Observer’s main window, click Log Settings. The Log Settings window appears.
2. Disable any or all event types from being logged.
3. (Optional) Disable logging for specific devices and/or probe instances from this menu.
4. Click OK to confirm and save your changes.
Disabled event types do not appear in the log window of Observer’s main window and are not recorded in the log file.
Chapter 8: Alarms

Configuring and using alarms

Alarms are a powerful and often overlooked feature of Observer. Using alarms, you can trigger pre-defined actions to occur when network conditions are met, making network management simpler and more predictable. Best of all, alarms allow you to proactively manage your network no matter where you are physically located.

There are two locations in Observer where alarms can be enabled, disabled, and configured. You may enable or disable all alarms associated with a specific probe instance or you may choose to disable individual alarms.

Enabling probe instance alarms

Probe instance alarms are tied directly to your probe instances. Each probe instance alarm is the alarm gatekeeper for one probe instance. This means individual alarms only function if its respective probe instance alarm is enabled. The benefit of this design allows you to enable or disable all alarms without affecting the enabled/disabled status of the underlying individual alarms.

Note: If you are using Observer in analyzer mode and switch to its Expert Probe interface, any alarms you had directed to the analyzer are automatically disabled. You should direct the probe instance to a different Observer analyzer before switching to the Expert Probe to receive those alarms.

To enable a probe instance alarm, complete the following:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window (circled in the image).
2. Enable any probe instance alarm by enabling your chosen probe instance.
3. Click OK to save your changes.

You successfully enabled the probe instance alarm for your chosen probe instance; this setting persists until disabled. Individual alarms can now be configured and used, and such information can be found in Enabling individual alarms on page 84.

**Enabling individual alarms**

Individual alarms are individual, trigger-based network alarms. Before these alarms can prove useful, they must be enabled. There are four basic types of alarms in Observer:

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

Enable individual alarms by completing the following steps:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Enable each alarm you want to enable.
   Until you customize the alarms, Observer uses the built-in, default triggers and actions for each. If necessary, see these pages:
   - Customizing triggers and actions on page 87
   - Creating filter-based alarms on page 85

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

6. Click OK to save your changes.

You successfully enabled individual alarms. Remember, individual alarms remain disabled if the probe instance alarm they are associated with is disabled—even if the individual alarms are enabled.

**Creating filter-based alarms**

A filter-based alarm is an individual alarm created from an Observer filter. This means any filters you create in Observer can be used as alarms.
The first step in creating a filter-based alarm is to become familiar with Observer alarms in general; see Configuring and using alarms on page 83 if you have not already.

To create a filter-based alarm, complete the following steps:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. In the Filter Based Alarms area, click New. The Alarm Filter window appears.

![Figure 25: 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 on page 87.

Remember, you can enable any number of filter-based alarms, but each filter-based alarm can only be created from one filter.

**Resetting statistical alarms**

Statistical alarms (as opposed to filter-based alarms) maintain cumulative counts of various network statistics, triggering only once upon exceeding the threshold. Therefore, triggered (tripped) statistical alarms must be reset before they can trigger once again.

SNMP devices have a different method for resetting alarms. To reset SNMP device alarm counters, of a currently selected SNMP device, choose Actions > Reset SNMP Device Alarm Counters.

**Tip!** To reset SNMP device alarm counters for all SNMP devices, choose Actions > Reset All SNMP Devices Alarm Counters.

To reset the counters and enable the alarms to once again trigger, click Alarm Settings at the bottom of the log window. Select the probe with the alarms you want to reset by clicking on the probe list, then click Reset Probe Alarms.
Customizing triggers and actions

An alarm has two components: a trigger and an action. Explore how a simple car alarm works: a thief breaks a car window (the trigger) and the car responds by sounding a loud siren (the action). Observer alarms behave in the same manner, except you can customize your own triggers and actions—and any amount of them.

Before continuing, we recommend becoming familiar with enabling individual alarms.

Customizing alarm triggers

Alarms triggers are highly flexible; you can customize the sensitivity of each trigger based on your needs. There are almost 200 predefined alarm triggers. Different background colors are used to distinguish one type of alarm from another type.

Some notes about the triggers.

- Analysis interval—The analysis interval can be unique for each trigger. It can be as low as 1 second. For VoIP the minimum analysis interval is 60 seconds (1 minute for the “Repeat alarm for chronic condition” setting). For triggers that do not have a configurable analysis interval, it is 15 seconds.
- Minimum active calls—For VoIP triggers, the minimum active calls is the number of active calls during that analysis interval. It does not mean the number of active calls above or below your defined threshold.

Try customizing some triggers yourself:

1. Click the Alarms Settings button, near the bottommost portion of Observer’s window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Enable any alarms by selecting them. At least one alarm must be enabled before step 5 operates correctly.
5. Click the Triggers tab. Triggers for all enabled alarms now appear.
6. Customize any or all alarm triggers to your liking.
7. Click OK to save your changes.

You successfully customized the triggers of your enabled individual alarms. You can repeat this process at any time in the future and for any reason.

Customizing alarm actions

Prerequisite: Observer Suite
Alarm actions are extremely powerful as they allow Observer to automatically react to triggered alarms any way you feel necessary. Customize the actions of any of your enabled alarms by completing the following steps:

By default, Observer uses the same alarm actions for all enabled individual alarms.

**Note:** If, instead, you want to configure independent alarm actions per individual alarm, disable this setting: Apply the Same Action to All Enabled Alarms (end-result shown in Figure 26 on page 88).

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 26: Independent alarm actions can now be customized](image)

4. Select each alarm you want to enable. At least one alarm must be enabled before step 5 operates properly.
5. Click the Actions tab. Actions for all enabled alarms now appear.
6. Customize any or all alarm actions to your liking.
7. Click OK to save your changes.

You successfully customized the actions of your enabled individual alarms. You can repeat this process at any time in the future and for any reason.

### Sharing alarms with others

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

### How to export alarms

To share alarms, the alarms must first be saved to a file. Create your file by following this export process:

1. Click the Alarms Settings button, near the bottommost portion of the Observer window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Select each alarm you want to export.
5. Click the Export Checked Alarms button.
6. Give your file a name, and click Save.

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

**How to import alarms**

To import alarms, you need access to an exported *.ALM file. You must bring this file back into Observer using the import process described here:

1. Click the Alarms Settings button, near the bottommost portion of the Observer window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Click the Import Alarms button.
5. Navigate to, and select, your file; click Open.

You successfully imported an alarm file. The alarms contained within are now part of your local collection, including the triggers and actions associated with each alarm.
Security, privacy, and regulatory compliance

Security and privacy concerns are a reality for most businesses—perhaps even greater for worldwide enterprises. Fortunately, Observer accommodates virtually any privacy or security need that arises within or outside of your company, including any governmental regulations.

Observer is a software application that collects network traffic, and as sensitive or personal information flows over the network (as it does), it too is collected. The following are some examples of sensitive information that Observer may collect:

- IP and MAC addresses
- Web form submissions, including passwords
- Email and visited web sites
- Instant messages and chats
- Application usage statistics
- Downloaded and uploaded content
- Sensitive files on network storage
- Employee or client records
- Payment transactions
- Phone calls (VoIP only)

Regardless of how any sensitive information is gathered, being a processor of it subjects your institution to all regulations, laws, statutes, and policies that may apply, and Observer can help you achieve and maintain compliance with many of them.

Observer is compatible with hardware security modules that comply with the Federal Information Processing Standards (FIPS) number 140. See for more information.

To become better aware of how you might follow regulations, here are some (non-exhaustive) examples of decisions to consider while configuring Observer and/or GigaStor:
- Data retention length—how long should you keep data?
- User accounts—who gets access to privileged data?
- Encryption—does our data need to be impenetrable?
- Exclusions—should some data never be collected, ever?
- Sharing—how can we share our data safely and securely?
- Physical security—do we need to isolate our equipment?
- Notification—who else should know we collect data?

Ultimately, your institution alone is responsible for regulation compliance, but Observer can help you meet those requirements.

**Securing communication between the analyzer and probes**

User authentication plays a key role in securing Observer. One best practice is to add the extra layer of security that authentication provides. Doing so ensures that authorized persons are genuine, not spoofed, and probe redirection can only be performed by the right people.

To enable user authentication, you must first tell Observer to encrypt all connections by securing communication between probes and analyzers.

To require user authentication, enable the Authenticate Users option.

User authentication is conceptually different than creating user accounts in Observer and setting user permissions.

**Setting security options for the analyzer**

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

To view and change the security settings for an Observer analyzer, in the Observer analyzer choose **Options > Observer General Options > Security**. Use the information in **Table 12 on page 91** to configure the analyzer’s security and NIMS options.

**Table 12: Security tab options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Observer Login</td>
<td>When enabled, this option forces a user to provide a user name and password to open the Observer analyzer. The user name can be stored locally if you are not using NIMS, or maintained by NIMS if the “Authenticate Observer login with NIMS” option is enabled. This option is not visible unless you have a special license enabling it.</td>
</tr>
<tr>
<td>Observer Login Credentials—Type a user name and password. This information is encrypted and stored locally. Only one user account is allowed per system. If you want numerous people to have access to the Observer analyzer with different user accounts, you must use NIMS.</td>
<td>Administrative Credentials—An local administrative user account that allows you to create a non-administrator account and to set security options for NIMS.</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Do not lose this password! There is no way to recover a lost administrative password.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Use Observer Encryption Key file for secure connections</strong></td>
<td>Strong encryption is available for Observer Expert and Suite users. Observer Encryption Key (.OEK) files let you use private encryption keys to ensure that unauthorized persons do not have access to the data flowing between Observer analyzers and probes. 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 NIMS.</td>
</tr>
<tr>
<td><strong>Authenticate users (for redirected Probe instances)</strong></td>
<td>Forces users to authenticate with NIMS before using remote probes. User accounts belong to user groups in NIMS and through the user groups access to probe instances can be granted or restricted. Only probe instances to which the user has access will be visible in the analyzer. This option does not control whether users can openObserver. That is done through the “Authenticate Observer login with NIMS” option.</td>
</tr>
<tr>
<td><strong>Manage Observer / Probe license with NIMS</strong></td>
<td>An Observer or probe license can be stored and managed locally at each analyzer or probe, or it can be managed centrally by NIMS. If unchecked, it is managed locally and you must provide a license for each analyzer/probe. If selected, then you can provide a pool of licenses in NIMS and the analyzer or probe will take an available license when the analyzer or probe starts.</td>
</tr>
<tr>
<td><strong>Get list of Probe Instances available for redirection from NIMS</strong></td>
<td>When selected all probe instances to which you the user has access to through group permissions set in NIMS are available when connecting to a probe. When unchecked only the local probe instances are available and no probe instances are listed when connecting to a remote probe.</td>
</tr>
<tr>
<td><strong>Share filters with NIMS</strong></td>
<td>When selected you may create filters and share them with others. You can also get any filters created by others. Whenever a filter is updated, you can be informed and update your local version. The list is maintained by NIMS.</td>
</tr>
<tr>
<td><strong>Synchronize user protocol definitions through NIMS</strong></td>
<td>When selected you can have NIMS manage your protocol definitions and share them with other Observer analyzers in your network. Protocol definitions created or modified on one Observer analyzer are shared and synchronized with all other Observer analyzers. The list is maintained by NIMS.</td>
</tr>
<tr>
<td><strong>Primary/Secondary server</strong></td>
<td>Provide the IP address of the primary NIMS server. If you are also using a failover NIMS server, type its IP address in the Secondary server box.</td>
</tr>
<tr>
<td><strong>Allowed to modify shared filters</strong></td>
<td>When selected, you can get a shared filter from someone else, modify it locally, then upload your modified version to NIMS thereby making your new version available to everyone else. When disabled, you can only get filters from NIMS and upload your own. You cannot modify any filters you get from NIMS. This option requires that you have the ability to share filters with NIMS.</td>
</tr>
<tr>
<td><strong>Authenticate Observer login with NIMS</strong></td>
<td>This option works in conjunction with the “Require Observer Login” option. This forces Observer to use NIMS to authenticate users rather than Observer’s local user list. A user list is maintained in NIMS.</td>
</tr>
<tr>
<td><strong>Require a password to change partial packet capture size</strong></td>
<td>Select this option if you want to require someone to provide a password before they may change the partial packet capture size. This is a central password and all users must use the same password.</td>
</tr>
</tbody>
</table>
| **Launch Encryption Key Generator** | Click this button to open the Network Instruments encryption key generator. If you want the GigaStor payload to be encrypted using 256 bit AES encryption before it is stored, select the “Encrypt GigaStor network traffic…” option. An encryption key is needed on the GigaStor (or a location accessible by the GigaStor) to encrypt and decrypt the data. The AES key is not needed on
### Configuring user accounts for secure access

If you want to restrict access to packet captures and reporting provided by a probe instance, you can create user accounts, permissions, and define security attributes of the local probe.

If you are using Network Instruments Management Server (NIMS) to control user accounts (if Authenticate Users is enabled; ), you must control accounts from the NIMS interface.

Again, configuring user accounts for secure probe access is conceptually different than requiring a user account to open the analyzer.

### Requiring a user account to open Observer

With a special Observer license, you can require users to log in to the Observer analyzer. To enable this option, choose Options > Observer General Options > Security tab, then select Require Observer Login. For more details, see Setting security options for the analyzer on page 91.

Requiring a user account to open Observer does not restrict access to probes or probe instances. That is done by user accounts on the probes or by NIMS. See Configuring user accounts for secure access on page 93.

### Creating or editing a user account for the local probe

A user account used to open Observer does not restrict access to probes or probe instances. That is done by user accounts on the probes or by NIMS. See Configuring user accounts for secure access on page 93.

To create or edit an Observer user account, choose Options > Selected Probe or Local Observer Instance, Memory and Security Administration, and click the Security tab.

Alternatively, right-click any probe instance and select Administer Selected Probe; then click the Security tab.

From the security tab, click User Accounts to view all configured probe instances. Then, use the drop-down to select any existing user account.
To create a new user account, click New User. The New User Account dialog appears, allowing you to create a new user name and password, plus tell Observer if the user should have administrator rights and access to some or all probe instances.

The setup options for editing a user account are identical to creating a new one; just select a user and click Edit User.

**Setting user permissions for the local probe**

Observer is a powerful application that can store a wealth of data—some of which may be personally identifiable. Therefore, you may want to deactivate some features of the software on a per user basis; this ensures that not everyone has access to sensitive data and features.

For example, deactivate the ability of some users to replay VoIP calls if you are concerned about the potential for abuse. Again, this is accomplished by setting user permissions. A special Observer license also exists to disable VoIP audio playback entirely.

To set user permissions, select a user account.

**Important information about NIMS**

The Network Instruments Management Server (NIMS) simplifies probe administration, management, security, and maintenance for IT professionals responsible for maintaining multiple Network Instruments probes across enterprise networks.

For network managers, NIMS offers added security, centralized licensing, a centralized update service, and failover redundancy. For network administrators, NIMS provides shared access to analysis tools, including Observer and probe filter libraries.

**Note:** The Network Instruments Management Server (NIMS) is only used for centralized user and probe management; it does not eliminate the need for running the Observer application on a local machine.

Documentation for the Network Instruments Management Server (NIMS) is not included in this user guide; see the NIMS User Guide.
Sharing packet captures with third-parties

Unless necessary, it is generally unwise to share “full” packet captures with outside sources because you could end up sharing too much information—information that should not be shared.

To prevent this from happening, Observer allows you to create a filtered packet capture from a larger capture. Filtered captures behave exactly like full captures—as they are indeed a complete capture file—except they only contain packets of your choice.

Creating a filtered capture can be done either before or after the initial capture is made. We recommend you become familiar with both processes before continuing.

**Note:** You can also configure Observer to create partial packet captures regardless of protocol. See Configuring Observer to capture partial packets on page 49.

To create a filtered packet capture fit for sharing, ensure the full packet capture is loaded in Observer then:

1. Choose **Actions > Filter Setup for Selected Probe**. The Active Filters window appears.
2. From the Active Filters window, click **New Filter**. Give your filter a name, and click OK.
3. Right-click the new filter, and select **Edit Rule As > Packet Partial Capture**.

![Figure 28: Creating a partial packet capture](image)

4. Within the Partial Packet Payload for TCP/UDP Filter window, set up rules for how the filter is applied.
   
   Specifically, the uppermost portion of the window is for filtering by IP address, range or subnet, and MAC or IPv6 address. The lowermost portion is for filtering application or protocol.
5. Click OK to confirm your changes.
6. Click OK to save your filter.
7. Enable your new filter to activate it, and click OK to save your changes.
Password protecting the ability to change partial packet capture size

To password protect the ability to change partial packet capture size, choose Options > Security tab, and enable Require a Password to Change Partial Packet Capture Size.

Password protecting this option helps ensure your partial captures remain partial, saving you disk space and enhancing data subject privacy because payload is not recorded in full.

Trimming data from your captures

Typically, packet headers contain the most useful information because they contain routing information and protocol information; The packet payload counterpart, however, is sometimes wasteful to collect because most troubleshooting is done just with the header.

Under these circumstances, you may want to truncate most payload data from the packet header(s). In Observer, the result is a partial packet capture.

Some benefits of partial packet captures include:

- Smaller capture sizes
  - More overall storage space for packet captures
  - Greatly increases the effective storage size of a GigaStor (or other capture buffer)
- Performance metrics remain intact
- Increased overall privacy
- Least resource intensive capturing

Some disadvantages of partial packet captures include:

- Not all network traffic is stored to disk
  - Forensics may be hindered without full payload data
  - Data stream reconstruction may not work
- Most resource intensive capturing
  - Increases CPU utilization

To configure Observer to trim all packet data beyond the first 64-bytes, choose Capture > Packet Capture > Settings > Capture Options tab, and enable Capture Partial Packets (Bytes).

Figure 29: Configuring partial packet captures
It is possible to decrease or increase the default 64-byte partial packet capture size. Click the Change Size button to set a custom value. From then on, each packets’ bytes following the target value are discarded from capture.

**How to encrypt captured data**

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

**You must have a special Observer license to enable and use this feature. There is no extra charge for the license.**

Data at rest encryption prevents visibility into any packets or even the metadata about the packets stored on the GigaStor. Any packets that are captured by the GigaStor are considered "data" and while they are stored on the GigaStor they are considered "at rest." Should any of the drives in the GigaStor be removed or misplaced, the data on the drives is protected. There is no remote access to this data apart from Observer’s own analyzer, and the data tagging methods for organizing and retrieving data can only be used in conjunction with the Observer analyzer.

The GigaStor can capture 10 Gb line rate while simultaneously encrypting the traffic with AES-256 encryption without any significant performance impact on write or read speeds of the GigaStor.

These instructions describe how to apply data at rest encryption to a GigaStor already in your possession. If your GigaStor shipped from the warehouse with the data at rest security already enabled, you do not need to complete this process unless two or more drives in your RAID have failed.

**CAUTION!** This procedure deletes all of the data on your GigaStor! Ensure you have a backup of any data you wish to keep.

1. Download the latest firmware for the Areca 1882 Series RAID card or contact Network Instruments Support for the file.
2. Choose Start > All Programs > Areca Technology Corp > ArcHttpSrvGui > Areca HTTP Proxy Server GUI. The program starts. You should see something similar to this image.
3. Select Controller#01 and click Launch Browser. If the controller is not running, click the Start button then launch the browser. The Areca RAID application attempts to connect to its web server.

4. Type the user name and password. The default user name is admin. There is no default password. Click OK to open the browser.

In the browser you can see the RAID set, IDE channels, Volume, and capacity.

5. In the web browser, choose System Controls > Upgrade Firmware. In the Browse field, choose each of the four files from the firmware package you downloaded or received from Technical Support in step 1 and click Submit. Choose the files in the order they are listed below. After adding the arch1882firm.bin file you are prompted to restart the system. Ignore that restart request and add the fourth file.

ARC1882BIOS.BIN
ARC1882BOOT.BIN
arc1882firm.bin
ARC1882MBR0.BIN

6. Restart the GigaStor.

7. Choose Volume Set Functions > Delete Volume Set. Select the volume, then select Confirm The Operation and click Submit. This deletes all of the existing data on the RAID.

8. Choose Volume Set Functions > Create Volume Set. Set the following options to these values, select Confirm The Operation, and click Submit.

<table>
<thead>
<tr>
<th>Volume RAID Level</th>
<th>Raid 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater Two TB Volume Support</td>
<td>64bit LBA</td>
</tr>
<tr>
<td>Volume Initialization Mode</td>
<td>Background Initialization. It may take several hours (six hours for 48 TB) to initialization the volume. While the volume is being initialized, the</td>
</tr>
</tbody>
</table>
9. Open Observer and apply your new license. Restart Observer. Because this is the first time that Observer is opened with the new license, it does not yet have a key for the encrypted volume. A window appears indicating that the volume is locked. Click **Generate Key** and save the key file. This is the key necessary to write to and read from the RAID volume. You can choose to remember the key file location so that Observer opens automatically, or, if left cleared, each time Observer is opened you must provide the path to the key file.

Every time Observer opens it looks for the encryption key that allows access to encrypted volume. Without the key present neither packet capture nor packet analyzation can occur.

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

11. In **Control Panel** > **Administrative Tools** > **Computer Management** > **Storage** > **Disk Management** select the RAID volume, right-click and choose **Initialize**. In the Initialize Disk window, select Disk 1 and GPT (GUID Partition Table). Convert the volume to a Simple Layout, assign a drive letter (typically, D:), and provide a name (typically, DATA).

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

13. Open Observer.
Chapter 10: Probes and Probe Instances

Introducing Probes

As a network administrator, when something goes wrong on your network, seeing what is happening on the wire can quickly lead you to a solution. Use this guide to assist you with choosing, deploying, configuring, and using your probes. The probes, along with the Observer analyzer software, let you see all traffic on the network to which it is connected. To monitor multiple networks from a single analyzer, probes must be installed at every point where network visibility is required.

Probes collect and report network traffic and statistics (usually from a switch) to an Observer analyzer. This enables you to detect and anticipate problems on both local and remote portions of the network. Probes gain insight and visibility into every part of the network, access remote networks as easily as local networks, eliminate the time and expense of traveling to remote sites, and speed troubleshooting.

A probe is a hardware device on your network running Network Instruments probe instance software. Each hardware probe has at least one probe instance that captures packets from your network to analyze. The probe hardware device could be an appliance purchased from Network Instruments or you could install the probe software on your own hardware.

The probe can be located on the same system as the analyzer (every Observer analyzer includes a “local probe”), or the probe can communicate with remote analyzers over TCP/IP.

Probes monitor the following topologies:

- 10/100 Mb, 1/10/40 Gb Ethernet (half- and full-duplex)
- Wireless (802.11 a/b/g/n)

Figure 31 on page 101 shows how probes provide visibility into your network. It may be obvious, but it also shows that you cannot see traffic on portions of your network where you do not have a probe. Finally, you can put the Observer analyzer anywhere on your network so long as it has TCP connectivity to the probe.
What is a probe instance?

The Observer analyzer uses probes to capture network data. In some cases you may want or need more than one probe in a specific location. You can achieve that through probe instances. A probe instance provides you the ability to look at multiple network interfaces, have multiple views of the same interface, or to publish to multiple Observer analyzers.

Observer has only one kind of probe instance: the probe instance. If you have a GigaStor then you have two special probe instance types available to you: the active probe instance and the passive probe instance.

Table 13 on page 101 compares the features of active and passive probe instances with an Observer probe instance found on all non-GigaStor probes.

Table 13: Active vs. passive GigaStor instances and Observer probe

<table>
<thead>
<tr>
<th></th>
<th>GigaStor Active probe instance</th>
<th>GigaStor Passive probe instance</th>
<th>Observer Probe(^1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better suited for troubleshooting</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Better suited for data capture</td>
<td>X</td>
<td>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>
<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.
A passive probe instance may capture packets to RAM and allows you to do reactive analysis or look at real-time statistics for troubleshooting.

The passive probe instance binds to whichever network adapter you want. You can change whichever adapter a passive probe instance is bound to without affecting any active probe instance.

With a GigaStor you have the option of which NIC to bind the passive probe instance. Do not bind any passive probe instances to the Gen2 adapter if at all possible. A copy of all packets is sent from the adapter to every passive probe instance attached to it. If you have several passive probe instances attached to the Gen2 adapter, the Gen2’s performance is significantly affected. Instead attach the passive probe instances to either a 10/100/1000 adapter or to a non-existent one.

If you have a passive probe instance connected to a GigaStor, you can mine data that has already been written to the RAID disk by using an active probe instance. There should be one passive probe instance for each simultaneous Observer user on a GigaStor. By using a passive probe instance, instead of an active probe instance, only one copy of data is being captured and written to disk, which reduces the processor load and the required storage space. For troubleshooting and most uses in Observer passive probe instances are appropriate.

By default a passive probe instance uses 12 MB of RAM. You can reserve more memory for passive probe instances if you wish.

An active probe instance on a GigaStor captures network traffic and writes it to the RAID array. An active probe instance should have as large of a RAM buffer as possible to cushion between the network throughput rate and the array write rate.

Like a passive probe instance, it can also be used to mine data from the hard disk, however a passive instance is better suited for the task. An active probe instance cannot start a packet capture while the GigaStor Control Panel is open.

By default there is one active probe instance for GigaStor. It binds to the network adapter and its ports. If you have a specific need to separate the adapter’s ports and monitor them separately, you can do so through passive probe instances or you can create separate virtual adapters.

Only one active probe instance per GigaStor.

Set scheduling to Always for the active probe instance so that it is constantly capturing and writing data. Use a passive probe instance to mine the data.

Do not pre-filter, unless you know exactly what you want to capture. Of course, if something occurs outside the bounds of the filter, you will not have the data in the GigaStor.

Do not allow remote users access to the active probe instance.

- 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 32 on page 103 shows how one active probe instance captures and writes to the GigaStorRAID. Passive probe instances 1 and 2 mine data from the RAID array. As a best practice, the passive probe instances are bound to the slowest network adapter in the GigaStor.

Additionally, passive probe instance 3 and 4 are each capturing packets separate from each other and separate from the active probe instance. However, since they are also bound to the same adapter as the active probe instance, they are capturing the same data as the active probe instance.

**Which software probe is right for you?**

For companies that cannot invest in dedicated hardware probes, Network Instruments’ software probes provide a low-cost monitoring option and are easy to install and configure. Software probes support Ethernet, Gigabit and wireless and are appropriate for analyzing speeds of up to 1000 Mbps or for low-utilization gigabit networks via a SPAN/mirror port on a switch. The Observer software can handle fast network speeds (including 40 Gigabit), but it is the network adapter that is the bottleneck on home-grown systems. Network Instruments uses a custom-designed network adapter removing the bottleneck in our probes. These levels of software probes are available:

- **Single probe**—Single probes have only one probe instance and it is not user-configurable. Single probes are appropriate for sites with small administrative staffs where only one user needs to look at a probe at a time. (Not sure what a probe instance is, watch [this video](#).)
- **Multi Probe**—Multi probes may have one or more probe instances. Multi probes allow multiple users to each connect to the probe and use their own probe instance. Each probe instance can be looking at the same packet capture or different capture.

- **Expert probe**—Expert probes are the same as a Multi probe except that they have local expert analysis and decode capabilities in the probe that allows for remote decoding and expert analysis in real time. The Expert probe software comes pre-installed on most hardware probes from Network Instruments.

<table>
<thead>
<tr>
<th>Hardware &gt;</th>
<th>GigaStor, Portable probes, Probe Appliances, 3rd party hardware</th>
<th>Dual port Ethernet Probe, 3rd party hardware</th>
<th>Ethernet Single probe, 3rd party hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed software &gt;</td>
<td>Expert Probe</td>
<td>Multi Probe</td>
<td>Single Probe</td>
</tr>
<tr>
<td>Sends entire buffer¹</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</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NIMS support</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Simultaneous multi-topology support</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Simultaneous users²</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Supports multiple NICs</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Use reserved memory outside of Windows</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>User security</td>
<td>X</td>
<td>X</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-duplex³</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 bonding⁴</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote decode of GigaStor captures</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sends expert summary &amp; decode packets⁴</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sFlow</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP expert, APA, ATA⁵</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How probes work with switches

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

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

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 33 on page 106 describes the two different ways that Observer runs.

---

**Figure 33: Windows protected memory, user memory, and reserved memory**

<table>
<thead>
<tr>
<th>With Reserved Memory</th>
<th>No Reserved Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Protected Memory</td>
<td>User Memory for Windows and other programs</td>
</tr>
<tr>
<td>User Memory</td>
<td>User Memory</td>
</tr>
<tr>
<td>Reserved Memory for Observer</td>
<td>User Memory</td>
</tr>
<tr>
<td>Statistics queue buffer</td>
<td>User Memory</td>
</tr>
</tbody>
</table>

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 34 on page 107** shows what options in Observer control the size of various portions of memory.
There are two kinds of buffers that a probe uses to store data in real-time: capture buffers and statistical buffers. The capture buffer stores the raw data captured from the network while the statistical buffer stores data entries that are snapshots of a given statistical data point.

Selecting an appropriate capture buffer size given system resources is all most users need to worry about; the default settings for the statistical buffers work perfectly fine in the vast majority of circumstances.

However, if you are pushing the limits of your probe system by creating many probe instances, you may be able to avoid some performance problems by fine-tuning the memory allocation for each probe instance.

For example, suppose you want to give a number of remote administrators access to Top Talkers data from a given probe. You will be able to add more probe instances within a given system’s memory constraints if you set up the statistics buffers to only allocate memory for tracking Top Talkers and to not allocate memory for statistics that no one will be looking at.

Observer has no limitations on the amount of RAM that can be used for a buffer.

You can allocate up to 4 gigabytes, limited only by the physical memory installed on your Windows system. Note that when run on a 64-bit Windows, there is no 4 GB limitation for the capture buffer; you are limited only by the amount of physical memory installed on the probe.

In all cases, the actual buffer size (Max Buffer Size) is also reduced by 7% for memory management purposes. Should you try and exceed the Max Buffer Size an error dialog will be displayed indicating the minimum and maximum buffer size for your Observer (or probe) buffer.

For passive probe instances, which are most often used for troubleshooting, the default settings should be sufficient. If you are creating an active probe instance (one that writes to disk and not just reads from it), then you may want to use the following formula as a rough guideline to determine...
how much RAM to reserve for the probe instance when doing a packet capture. (This formula does not apply when doing a GigaStor capture to disk. It is only for probe instances doing packet captures.)

Use this formula to determine your RAM buffer size:

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

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

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

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

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

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

### Running Observer with reserved memory

This section discusses how Observer uses the reserved memory for packet capture and the statistics queue buffer. It applies to Observer Expert, Observer Suite, and Expert and Multi-instance probes. This is not the default configuration, but it is the one we recommend you use.

**CAUTION!** Never change the reserved memory settings of Network Instruments hardware unless Network Instruments instructs you do so. Reserved memory settings should only be modified on non-Network Instruments hardware, such as a desktop computer running an Observer analyzer.

Although your requirements are unique, there are some general recommendations where the system is dedicated to Observer: For 64-bit, reserve all memory above 4 GB for Observer and for 32-bit, reserve all memory above 400 MB for Observer.

**Tip!** If you need more RAM for the statistics queue buffer, you may need to lower the amount of RAM dedicated to packet capture so that it is freed and available to add to the statistics queue.

Reserving memory allows Observer to allocate RAM for its exclusive use. This ensures that Observer has the necessary memory to store packets for statistical analysis, or for capturing large amounts of data for decoding. The more memory you reserve for Observer, the larger the packet capture and statistical queue buffers can be. This allows you to store more packets and analyze a longer time period.
If the memory buffer for the statistics queue buffer is too small, you may end up with inaccurate statistical data because some data may get pushed out before it can be processed. Observer processes packets on a first-in, first-out (FIFO) basis, so it is important that the buffer be large enough to allow for processing.

If you want to do a packet capture over an extended period of time it is vital that you have a buffer large enough to hold the packets in memory. The only way to ensure you have a large enough buffer is to reserve memory for use by Observer.

When reserving RAM for Observer you are taking RAM away from the operating system. Table 14 on page 109 shows how much memory is required by the operating system. Anything beyond this amount may be reserved for Observer.

Table 14: 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-bit $^2$</td>
<td>256 MB (although 400+ MB is recommended)</td>
</tr>
</tbody>
</table>

---

$^1$ Because of how 64-bit Windows loads its drivers when 4 GB of RAM is installed all 4 GB is used by Windows. This is sometimes referred to as the BIOS memory hole and means you cannot reserve any memory for Observer. To capture packets on 64-bit Windows install either more than or less than 4 GB of RAM.

$^2$ 32-bit operating systems do not support more than 4 GB of RAM. Observer cannot use any RAM above 4 GB.

1. To see how much protected memory the probe has, click the Memory Management tab.
2. Click the Configure Memory button at the top of the window to view and modify how Observer uses the protected memory for this probe instance. The Edit Probe Instance window opens.

On the Edit Probe Instance window, you can see how memory is allocated for:

- Packet capture
- Statistics queue buffer

You can also see how much protected memory is still available in the Windows memory pool.

3. Use the arrows to the right of the Packet capture and Statistics queue buffer to increase or decrease the amount of RAM you want dedicated to each. See How to allocate the reserved RAM to help determine how to divide the memory.

4. Click View to see the different types of networks and how the memory is allocated to the numerous statistics collected by Observer. See Tweaking the statistics memory configuration for details about the window and why you may want to change some allocations.

5. After reserving memory for Observer you must restart the system for the changes to take affect. After you restart the system you can allocate the memory to the different probe instances.
How packet capture affects RAM

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

Figure 35 on page 110 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 35: How packets move through Observer’s memory

- The capture card receives data off the network.
- The capture card passes data into RAM. In the RAM it goes into the packet capture buffer and the statistics queue buffer.
- The statistics queue buffer passes the information to the statistics memory configuration.
- The statistics memory configuration passes the data to the real-time graphs.
- The Network Trending Files receive data from the statistics queue buffer through the NI trending service, where they are written to disk.

The following steps occur only if you are writing the data to disk through a packet capture to disk or a GigaStor capture.

If you are using packet capture to disk, the packet capture buffer passes the data to the operating system’s disk.
If you are using GigaStor capture, the statistics queue buffer and the packet capture buffer passes the information to the RAID.

A few notes about how some buffers are used:

- Packets received by the statistics queue buffer are processed and put in the collected statistics buffer.
- Data for network trending comes from the statistics queue buffer, then it is written to disk, and finally flushed from the buffer every collection period.
- The collected statistical buffer does not use first-in, first-out to determine statistics. Therefore, after the statistic limit is reached the remaining data is no longer counted; however, data for known stations continue to be updated indefinitely.
- Regardless of whether Observer is using reserved memory, the statistics memory, statistics queue buffer, and packet capture buffer function the same. The storage space available for storing packets in memory increases though when you reserve memory.

How to allocate the reserved RAM

If you have a lot of network traffic, then you may need to allocate at least one gigabyte of RAM to the packet capture buffer, the statistics queue buffer, or both.

After you have the RAM reserved for Observer, you must allocate it for the probe instances. Here are our basic recommendations for allocating the memory. These are just recommendations and may be changed or modified for your circumstances. If you are using a GigaStor, read this section, but also be sure to consider the information in Recommendations for the Gen2 capture cards on page 112.

How many probe instances will you have on this system? How are you using the probe instance(s)? Are you using it to capture packets or to analyze statistics? After you know how you want to use the probe instance, you can decide how to properly divide the memory amongst the probe instances, and further how you will allocate the memory between the packet capture and statistics queue buffers.

You want to create and use as few probe instances as absolutely necessary. Each probe instance you create divides the memory pool into smaller chunks. The more probe instances you have, the more processing the system must do.

For each probe instance determine:

- If you want to mostly capture packets, then allocate 90% of the RAM to packet capture and 10% to the statistics queue buffer. At a minimum, you should allocate 12 MB to collect statistics. If you are using a GigaStor, you should allocate the vast majority of the RAM for the active probe instance to packet capture.
- If you want to collect statistics or trending data, or use analysis, then allocate 90% (or even 100%) of the RAM to the statistics queue buffer.
- If you want to do both, determine which you want to do more of and allocate the memory accordingly.
**Recommendations for the Gen2 capture cards**

Unless specifically stated, all information in this section applies to both the 1 Gb Gen2 card, 10 Gb Gen2 card, and 40 Gb Gen2 card. The Gen2 card is only available in hardware products from Network Instruments.

There are additional requirements and considerations if you are using a GigaStor. A GigaStor may have one of several different capture cards installed. Here are some special configuration issues to consider when dealing with a Gen2 capture card:

- When using multiple probe instances on a GigaStor, ensure that only one probe instance is associated with the Gen2 card. (If you are using virtual adapters to monitor disparate networks, then you may have more than one active instance bound to the Gen2 card.) For performance reasons, all other probe instances should be associated with a different network card.

If you feel a Gen2 card is not performing as expected, ensure that there is only one probe instance bound to it. If there is more than one, verify that the other probe instances are not collecting any statistics. It is possible that the probe instance you are looking at is not collecting any statistics, but one of the other probe instances may be. (This is only an issue if there are multiple probe instances connected to the Gen2 card. This does not apply if the other probe instances are connected to a regular network card.)

**Tweaking the statistics memory configuration**

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

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

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

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

For instance, if you are using Discover Network Names it will run until it fills the 800 stations. After it reaches 800 entries it cannot add any more because there is no memory space available. Any stations beyond 800 are not included in the list. You must increase the number of stations that may be allocated. This increases the memory requirements though. If you have 8,500 stations on your network, you will need at least 8,500 entries, which requires 1.2 MB of RAM.
Conversely, if you are not using statistics, such as VoIP, the RAM is still allocated to it. The default VoIP Trending is for 1,500 entries, which requires 12.6 MB of RAM. By reducing the allocated entries to 10 (the minimum) you need only 86.3 KB of RAM — saving nearly 12 MB to be used elsewhere.

By tweaking the statistics allocation, you can fine tune how Observer processes its data.

You cannot modify the default statistics memory configuration. You must create a new profile based on one of the existing profiles (Small, Medium, Large, 4G LTE) and modify it.

1. Click the Memory Management tab to display the list of probe instances and their buffer sizes.
2. Select a probe instance and click Configure Memory to change the packet capture or statistics queue buffer sizes. The Edit Probe Instance window opens.
3. Click the New button to open the New Statistics Memory Configuration window.
4. Type a name and choose which memory configuration on which you want to model yours. Click Finish. You have now created a new statistics configuration, but it is identical to the one you modeled yours on. You must now edit it.
5. Click Edit. Click Yes to the message that appears about needing to restart the probe software after making memory changes. The Edit Statistics Memory Configuration appears.
6. At the top, choose your network type from the list.
7. The statistic's memory that you can modify are highlighted in yellow. To change the amount of memory for it, click in the Allocated Entries column and provide a new value. Repeat until you have tweaked the statistics memory for your needs.

Troubleshooting common issues

Use the information in this section to assist you if you have a problem with your probe not connecting to your analyzer, your probe does not have a network adapter available, or if you are using an nTAP and want to capture NetFlow traffic or several other common issues. If you feel your probe is slow, see Troubleshooting a slow probe system on page 114.

Although most installations of Observer proceed without any trouble, due to the vast number of network configurations and hardware/software options that Observer supports, sometimes difficulty arises.

If you experience trouble in setting up Observer, keep a number of things in mind.

First and foremost, try to simplify your configuration in any way possible. This means if you have a screen saver loaded, disable it. If you are running some network add-on peer-to-peer jet engine turbo stimulator, remove it. This does not mean that you will not be able to use Observer with your other products but, if you can determine where the problem is, you can focus on that piece of the puzzle and you may be well on your way to solving the problem.

Second, do not trust anyone or anything. The only way to really know what your hardware settings are is to have the card or device in one hand and the documentation in the other. Programs which discover interrupts and other settings only function properly when everything is working correctly — exactly when you do not need them. Do not blindly trust other network drivers — they may or may not be reporting the correct information.
Third, do not, under any circumstances, share interrupts, I/O ports, or memory addresses between adapters. No matter what has worked before or what might work in the future, sharing interrupts or memory settings is not a valid configuration.

Troubleshooting checklist:

Does your network work without any Observer programs or drivers loaded? If not, check your network installation instructions. After your network appears to be running correctly, install Observer again. Try installing Observer on a different system and see if you experience the same problem. This does not mean that you will not be able to use Observer on the desired system. It may give you some insight into the problem that you are having.

Troubleshooting a slow probe system

If a probe is overloaded, consider whether any of the following affect the system. You can clear these one at a time to see if that resolves the system’s issue.

Although all of the settings discussed in this section are configured in the Observer analyzer, they are saved to the probe.

- A scheduled capture can be causing a system slow down. Determine if any scheduled capture is occurring. Capture > Packet Capture > Settings > Schedule tab.
- Some extra processing happens when you have triggers and alarms configured. Determine what alarms are enabled by clicking the Alarm Settings button in the lower left.
- Are you running real-time Expert Analysis? Observer requires some processing resources to get through the data, which could be a lot of data. Real-time expert processes data as it is received. This requires continuous processing of incoming data while the real-time expert is running.
- Are you collecting combined station statistics or protocol distribution summary for your network? If so, these could be causing the system to slow down. To determine if you are, click Options > Observer General Options > General tab. Scroll to the “Startup and runtime settings” and uncheck these, if necessary:
  - Collect combined station statistics at all times
  - Collect protocol distribution for the whole network
- Are you collecting network trending statistics? If so, is the sampling divider less than 10? If so, increase the sampling divider to 10 or greater. To determine your sampling divider, click Trending/Analysis > Network Trending > Settings > General tab. In the Collection Settings section, change the sampling divider.

A probe is not connecting to the analyzer or vice versa

If the probe is not connecting, it could be one of several reasons. The log window in the Observer analyzer has useful information to give you an idea of why the connection is failing. If the log window is hidden, choose View > Log Window to show it.

Verify the following:
The probe is licensed. See Licensing and updating on page 2.

Ports firewall and the traffic is actually passing through it. Observer uses these ports to communicate with the probe. See Ports used by Network Instruments products on page 8. Check any local system firewall as well as any network firewall. See also the information in Suspected NAT or VPN issues on page 119.

Security and encryption settings match between the Observer analyzer and the probe. If the settings do not match, you will get a message that says “Probe redirection Error <IPAddress> Authentication Negotiation Error” or “Probe authentication failed <IPAddress>.” Either the security feature has been turned off for one side of the connection (but not the other), or their encryption keys do not match. In Observer, click Options > Observer General Options from the menu, then click the Security tab. On the probe, click the Security tab. Verify that the security properties match. If necessary, generate a new key and use that on both the probe and analyzer.

The user name you are using from the analyzer exists on the probe. Although very uncommon, the default “Anyone” account can disappear. If it does and you use that account to connect, your connections are prohibited. If the Anyone account has been deleted, you can recreate it on the probe by clicking the Security tab, then the New User button. Click the “Create Anyone Account” button.

If a Single Probe does not have a user name defined in the Options > Probe Redirection Settings, you must create a new account called “Anyone” (without quotes) and use that account to access the Single Probe.

The probe and Observer analyzer are within the same minor build range. You can have the Observer analyzer automatically force an upgrade of an older probe version.

You can access the VLAN if the probe or Observer analyzer are on different VLANs. There is nothing you need to configure in Observer or the probe to enable a connection when they are on different VLANs. However, if you do not have network permissions to access a probe on a different VLAN, it is a network configuration issue (usually for security reasons) and you should contact the network administrator.

No network adapter available

After starting Observer, if you do not see any available adapters listed in the “Select Network Adapter” list, it means your NIC does not have the necessary driver or VMONI Protocol settings installed. Use this information to enable your adapter and to install the proper drivers.

1. If Observer is running, close it.
2. Ensure you are logged in to the system with an account with administrator rights.
3. From the Windows Start menu, choose Control Panel > Network and Sharing Center.
4. Click Change Adapter Settings.
5. Right-click any of the Local Area Connections and choose Properties.
6. Look at the list of installed components to verify that the VMONI Protocol Analyzer is listed. Then do one of the following:
   • If it is not installed, skip to 7 on page 116.
If the VMONI driver is listed, remove it. Select VMONI Protocol Analyzer and click the Uninstall button. After the VMONI driver is removed, restart the system and continue with 7 on page 116.

7. From the Local Area Connection Properties (5), choose Install > Protocol > Add > Network Instruments – VMONI Protocol Analyzer and click OK. If the VMONI driver is not listed, click Have Disk, then browse to the VMONI.SYS file located in the Observer directory on your hard drive, select it, and click OK.

The VMONI Protocol Analyzer will now be available to install.

8. Restart the computer after you have completed installing the driver.

You should now be able to select an adapter when starting Observer.

Integrated adapters report all sent packets with bad TCP checksum

Symptoms: All TCP packets sent from the Observer analyzer or probe station across an integrated network adapter contain bad TCP checksums.

Causes: Default driver settings for the card are incorrect. You must update the driver and then disable the “Offload Transmit TCP Checksum” option.

Solutions: Upgrade the driver for the integrated network adapter to the Network Instruments/Intel Pro 1000 adapter driver. This driver is located in the: \<Observer installation directory>\Drivers\IntelPro1000 directory.

1. After upgrading the driver, right-click the adapter and go to Control Panel > Network Connections > Properties.
2. On the General tab, click the Configure button.
3. Click the Advanced tab and find the Offload Transmit TCP Checksum option and disable it.
4. Restart your system.

“No VLAN” shown while using a Gigabit NIC

Symptoms: “No VLAN” is displayed in VLAN Statistics and/or no 802.1Q tag information is shown in your decode. The network adapter you use to capture traffic is a Gigabit NIC.

Causes: Observer is not seeing the 802.1Q tag on packets being captured. This is sometimes caused by your switch not sending tagged packets to Observer. See VLAN Statistics tool is not working on page 117 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.
The Gigabit NIC no longer strips VLAN tags, so the symptom in Observer is resolved.

**VLAN Statistics tool is not working**

**Symptoms:** “No VLAN” is the only VLAN ID that shows up in the VLANs column in VLAN Statistics. You are not seeing all VLANs you have on the network.

**Causes:** To display VLAN Statistics, Observer checks each packet for a VLAN tag; if no tag is present, the packet is logged as “No VLAN.” Both 802.1Q or ISL VLAN tags are stripped unless the SPAN destination port to which the analyzer is attached has been configured to include VLAN tags.

**Solutions:** Configure the switch to retain the VLAN tags through the monitor port. This may be an option in the Mirror or SPAN command on the switch, or you may have to configure the port as a trunk prior to defining it as a SPAN port. Even if the switch is monitoring a trunk or uplink port it may strip VLAN tags unless you configure that port to retain the tags. Refer to the documentation from your switch for details on configuring VLANs, trunks, and analyzer ports.


If you use a Cisco Catalyst 4500/4000, 5500/5000, or 6500/6000 Series Switch running CatOS you must configure the destination port as a trunk port prior to configuring the SPAN port using the set trunk and set span commands:

```
set trunk
module/port
    [on | off | desirable | auto | nonegotiate]
    [vlan_range] [isl | dot1q | negotiate]

set span
source_port
destination_port [rx | tx | both]
```

For example, to configure module 6, port 2 for monitoring an 802.1Q VLAN setup, you would enter the following commands:

```
switch (enable) set trunk 6/2 nonegotiate dot1Q
switch (enable) set span 6/1 6/2
```

For Cisco Catalyst 2900/3500, 4500/4000 and 5500/5000 Series Switches Running IOS 12.1 or later, encapsulation forwarding is set as a part of the SPAN command, which has the following syntax:

```
monitor session session_number (source | destination)
    interface type/num  [encapsulation (dot1q | isl)]
```

To monitor 802.1Q VLAN traffic passing through Fast Ethernet 02 via a SPAN port set up on Fast Ethernet 0/6, you would enter the following commands:

```
C4000 (config) # monitor session 1 source interface fastethernet 0/2
C4000 (config) # monitor session 1 destination interface
    fastethernet 0/6 encapsulation dot1Q
```

For a 6500/6000 Series Switch running Native IOS 12.1 or later you must configure the destination port as a trunk port prior to configuring the SPAN, which have the following syntax:

```
set trunk
module/port
    [on | off | desirable | auto | nonegotiate]
    [vlan_range] [isl | dot1q | negotiate]
```
C6500(config) # Interface Type slot/port
C6500(config-if) # Switchport
C6500(config-if) # Switchport trunk encapsulation { ISL | dot1q }
C6500(config-if) # Switchport mode trunk
C6500(config-if) # Switchport nonnegotiate

To monitor 802.1Q VLAN traffic passing through Fast Ethernet 02 via a SPAN port set up on Fast Ethernet 0/6, you would enter the following commands:

C6500(config) # interface fastethernet 0/6
C6500(config-if) # switchport
C6500(config-if) # switchport trunk encapsulation dot1q
C6500(config-if) # switchport mode trunk
C6500(config-if) # switchport nonnegotiate
C6500(config-if) # exit
C6500(config) # monitor session 1 source interface fastethernet 0/2
C6500(config) # monitor session 1 destination interface fastethernet 0/6

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

**Symptoms:** While running Discover Network Names against a Layer 3 Switch that uses VLANs, you see only a limited number of MAC addresses, which typically have multiple IP Addresses associated with them.

**Causes:** Layer 3 Switches that have been configured to perform routing replace the originating station's MAC Address with the MAC Address of the switch port. For example, suppose CADStation1 has a MAC Address of 00:00:03:AB:CD:00 and an IP Address of 10.0.0.1. It is connected to switch port 1 through a hub. Port 1 of this switch has a MAC Address of 00:11:22:33:44:55.

When a probe is connected to a SPAN or mirror port of that switch, it shows CADStation1 with an IP of 10.0.0.1 and MAC address of 00:11:22:33:44:55 rather than 00:00:03:AB:CD:00 because of this substitution.

Now, suppose there is another station (CADStation2) with MAC address of 00:00:03:AB:EF:01 and has an IP address of 10.0.0.2 that is also connected to port 1 of the switch through a hub. Because Discover Network Names stores station information by MAC address (i.e., the MAC address is the unique station identifier), it changes the IP address of switch port 1's MAC address.

Because a switch configured as such hides originating station MAC addresses from Observer, MAC-based station statistics (such as Top Talkers-MAC, Pair Statistics matrix, etc.) can only be calculated by port. To make the Observer displays more useful, follow this solution.

**Solutions:** By examining the switch configuration you can obtain a list of MAC addresses that are associated with each port of your switch. Then, use Discover Network Names to edit the alias entry for 00:11:22:33:44:55, labeling it “SwitchPort1.”

The IP based statistical modes (Internet Observer, Top Talkers – IP (by IP Address) still show you statistics calculated from individual stations by their IP address. But MAC-based statistical modes (Pairs Statistics Matrix, Protocol Distribution, Size Distribution Statistics, Top Talkers –MAC (by hardware Address) will now show data by Port.
Suspected NAT or VPN issues

If you use network address translation (NAT) in your environment, you must make some configuration changes in Observer. Using the TCP/IP port information in Ports used by Network Instruments products on page 8, you should be able to set up the NAT properly.

If the probe is outside the network where Observer is running, you must forward port 25901 from the probe’s address to the system running Observer.

When redirecting the probe, you must specify the NAT outside IP address instead of the address that Observer puts in automatically. By default, Observer tries to use its local IP address, which the probe will not be able to find. Select “Redirect to a specified IP address” in the Redirecting Probe or Probe Instance dialog and type the VPN client’s IP address.

Running Observer passively affects NetFlow

When analyzing a link using a TAP, which is common, Observer runs “passively.” Passive operation guarantees that analysis will not affect the link; however, it does have some implications when running NetFlow. Because there is no link over which the system can transmit packets or frames, the following features are unavailable:

- Traffic Generation
- Collision Test
- Replay Packet Capture

Daylight Savings Time

Observer is not coded with a specific date in mind. Daylight Savings Time is controlled by the operating system. When the clock rolls backwards or forwards Observer rolls with it, with one exception: packet capture/decode.

Packet capture provides nanosecond time resolution, which none of the rest of the product does. Because of this, packet capture does not rely on the system clock to provide time stamps. It relies on the processor time ticks. When Observer opens it requests the system time and the number of processor time ticks and uses those. This allows Observer to know what date and time it is when a packet is seen.

Because the Observer only asks the operating system for the system time when Observer is started, packet capture does not know that the time has jumped forward or backward. To get this to happen you need restart Observer after the time change. It is that simple.
Configuring Cisco 6xxx switches using a SPAN port to a full-duplex Gigabit Probe

When using a full-duplex Gigabit Probe to capture directly from a SPAN/mirror port, use a straight-through cable from the Gigabit port on the switch to either port A or B on the Gigabit card in the probe. Do not use the Y-cable or TAP (the TAP and Y-cable should only be used inline).

To use the Observer analyzer with the Cisco 6xxx switch, you must disable auto negotiation. With auto negotiation enabled, the switch and probe may create a link when first starting the probe, but if the cable is unplugged or if a configuration change to the SPAN/mirror port is applied, you will lose connectivity to the switch. To turn auto negotiation off on the switch, follow the directions based on the OS you are using on your switch.

Tip! Disabling Auto Negotiation is recommended on all models/brands of switches when using a SPAN/mirror port to a full-duplex Gigabit Probe.

Cisco CatOS switches

1. To disable port negotiation:
   Console> enable
   Console>(enable) set port negotiation mod_num/port_num disable

2. To verify port negotiation:
   Console.(enable) show port negotiation [mod_num/port_num]

3. To enable port negotiation (should you remove the gigabit Observer product from the switch):
   Console>(enable) set port negotiation mod_num/port_num enable

Cisco IOS switches

1. To disable port negotiation:
   Console> enable
   Console# configure terminal
   Console(config)# interface gigabitethernet mod_mun/port_num
   Console(config-if)# speed nonegotiate

2. To verify port negotiation:
   Console# show interfaces gigabitethernet mod_mun/port_num

3. To enable port negotiation (should you remove the gigabit Observer product from the switch):
   Console(config)# interface gigabitethernet mod_mun/port_num
   Console(config-if)# no speed nonegotiate
Ports used by Network Instruments products

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

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

<table>
<thead>
<tr>
<th>Ports</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 25901</td>
<td>Observer expert and trending data</td>
</tr>
<tr>
<td></td>
<td>Observer Reporting Server to Observer/GigaStor/Probe</td>
</tr>
<tr>
<td>TCP 25903</td>
<td>Observer/GigaStor/Probe redirection/connection request</td>
</tr>
<tr>
<td></td>
<td>GigaStor/Probe administration</td>
</tr>
</tbody>
</table>
Chapter 11: Supported Protocols

Protocols supported by Observer

The following list is current at the time of publication.

For the most complete and up-to-date protocol list, always visit:

http://www.networkinstruments.com/protocols

- 29West - LBT-TCP
- 29West - LBT-RM
- 29West - LBT-RU
- 29West - LBMC
- 29West - LBMR
- 3COM - MIP - Extensions to Mobile IP
- 3COM - NBP - Name Binding Protocol
- 3COM - NetBIOS - NetBIOS
- 802.11b, 802.11g and 802.11n wireless protocols.
- 802.11 - Management
- 802.11 - Control
- 802.11 - Data
- 802.11 - WEP - Wireless Encryption Protocol
- 802.11 - LWAPP (ports 12222, 12223)
- 802.11e - QoS for Wireless LANs
- 802.11i - TKIP - Temporal Key Integrity Protocol
- 802.11i - RSN - Robust Security Network
- 802.11a - Outdoor Channel Support - channels 149, 153, 157, 161, 165 (at 5.470-5.745Ghz)
- 802.1Qad - Service VLAN Tag
- 802.1Qag - CFM - Connectivity Fault Management
- 802.1Qah - PBB - Provider Backbone Bridge
- 802.1x - PEAP - Protected EAP (draft-josefsson-pppext-eap-tls-eap-07)
- 802.1x - TLS - Transport Layer Security - RFC2246 and RFC3546
- 802.1x Port-Based Network Access Control - EAP over LANs (EAPOL)
- AFS - Replication Server
- AppleTalk
- AppleTalk - AARP - Address Resolution Protocol
- AppleTalk - ADSP - Data Stream Protocol
- AppleTalk - AEP - Echo Protocol
AppleTalk - AFP - Filing Protocol
AppleTalk - ALAP - Link Access Protocol over WAN
AppleTalk - ASP - Session Protocol
AppleTalk - ATP - Transaction Protocol
AppleTalk - DDP - Datagram Delivery Protocol Phase 1 & 2
AppleTalk - ELAP - Ethernet Link Access Protocol
AppleTalk - NBP - Name Binding Protocol
AppleTalk - PAP - Printer Access Protocol
AppleTalk - RTMP - Routing Table Maintenance Protocol
AppleTalk - SoftTalk - Session Layer Protocol
AppleTalk - ZIP - Zone Information Protocol
ATM
ATM - SONET/SDH
Banyan VINES - ARP - Address Resolution Protocol
Banyan VINES - AS - Application Services
Banyan VINES - Echo - Echo
Banyan VINES - ICP - Internet Control Protocol
Banyan VINES - IP - Network Layer
Banyan VINES - IPC - Interprocess Communication Protocol
Banyan VINES - LLP - Link Layer Protocol
Banyan VINES - Matchmaker - Program to Program Communication
Banyan VINES - RTP - Routing Update Protocol
Banyan VINES - SMB - Server Message Block
Banyan VINES - SPP - Sequenced Packet Protocol
Cellular - 3GPP2
Cellular - A11
Cellular - A10
Cellular - SMPP - Short Message Peer-to-peer
Cellular - LTE - GTPv2-c - GPRS Tunneling Protocol version 2
Cellular - LTE - NAS - Non-Access-Stratum
Cellular - LTE - SIAP - SI Application Protocol
Cellular - LTE - X2AP - X2 Application Protocol
Cisco - CDI - Cisco Device Identification
Cisco - CDP - Cisco Discovery Protocol
Cisco - CGMP - Cisco Group Membership Protocol
Cisco - DISL - Dynamic ISL
Cisco - DLSw - Data Link Switching
Cisco - DTP - Dynamic Trunking Protocol
Cisco - EIGRP - Enhanced Interior Gateway Routing Protocol
Cisco - ERSPAN - Enhanced Remote Switch Port Analyzer
Cisco - HSRP - Hot Standby Router Protocol (RFC2281)
Cisco - IGRP - Internet Gateway Routing Protocol
Cisco - ISL - Inter-Switch Link Protocol
Cisco - Netflow (v1-9)
Cisco - LEAP
Cisco - PVSTP+
Cisco - RUDP - Reliable UDP
Cisco - SLARP - Serial Line Address Resolution Protocol
Cisco - SLE - Cisco - Serial Link Encapsulation
Cisco - SSP - Skinny Station Protocol
Cisco - STUN - Serial Tunneling of SDLC header
Cisco - TDP - Tag Distribution Protocol over TCP
Cisco - VNTag
Cisco - VTP - Virtual Trunking Protocol
Cisco -VoIP - SGM - Skinny Gateway Message
Cisco -VoIP - SCCP - Skinny Client Control Protocol
Cisco - WIDS - Wireless IDS Protocol
Citrix - CGP - Common Gateway Protocol
Citrix - Decrypt "Light Encryption"
Citrix - Decompress "Reducer Version 2"
Citrix - Independent Computing ARchitecture (ICA) 3.0
Citrix - Name Enumerator
Citrix - Name Resolver
Citrix - Protocol Driver
Citrix - Scripting
Citrix - Seemless Windows Interface (VC)
Citrix - Speedbrowse
Citrix - SubDriver
Citrix - Thinwire1 (VC)
Citrix - Thinwire2 (VC)
Citrix - Transport Driver
Citrix - User Interface
Citrix - User Interface Extension
Citrix - Virtual Driver
Citrix - Winstation Driver
Citrix - Winstation Driver - Client Drive Mapping
Citrix - Winstation Driver - Speedbrowse
Citrix - Winstation Driver - Remote Windows Data (Thinwire)
DCE - Distributed Time Service Local Server
DCE - Distributed Time Service Provider
DCE - Name Service
DCE - RPC
DCE - Security ID Mapper
DCE/RPC - BOS Server
DCE/RPC - BUDB
DCE/RPC - BUTC
DCE/RPC - CDS Solicitation
DCE/RPC - Conversation Manager
DCE/RPC - Directory AC1 Interface
DCE/RPC - Endpoint Mapper
DCE/RPC - Endpoint Mapper4
DCE/RPC - FLDB
DCE/RPC - FLDB UBIK TRANSFER
DCE/RPC - ICL RPC
DCE/RPC - Kerberos V (under TCP or UDP)
DCE/RPC - NCS 1.5.1 Local Location Broker
DCE/RPC - Operations between registry server replicas
DCE/RPC - Prop Attr
DCE/RPC - RS_ACCT
DCE/RPC - RS_BIND
DCE/RPC - RS_MISC
DCE/RPC - RS_PROP_ACCT
DCE/RPC - RS_UNIX
DCE/RPC - Registry Password Management
DCE/RPC - Registry Server Attributes Schema
DCE/RPC - Registry server propagation interface - ACLs.
DCE/RPC - Registry server propagation interface - PGO items
DCE/RPC - Registry server propagation interface - properties and policies
DCE/RPC - Remote Management
DCE/RPC - Repserver Calls
DCE/RPC - TokenServer Calls
DCE/RPC - UpServer
DECNet IV - CTERM - Command Terminal
DECNet IV - DAP - Data Access Protocol
DECNet IV - DECnet-DNS - Distributed Name Services
DECNet IV - DNAv4 - Digital Network Architecture v4
DECNet IV - DRP - DECnet Routing Protocol
DECNet IV - FOUND - Found
DECNet IV - LAT - Local Area Transport Protocol
DECNet IV - LANBridge (DEC Spanning Tree Protocol)
DECNet IV - MOP - Maintenance Operations Protocol
DECNet IV - NICE - Network Information & Control Exchange
DECNet IV - NSP - Network Services Protocol
DECNet IV - SCP - Session Control Protocol
DECNet IV - SMB - Server Message Block
DICOM - AC-PDU - DICOM Upper Layer Protocol
DICOM - P-DATA-PF - DICOM Upper Layer Protocol
DICOM - P-DATA-TF - DICOM Upper Layer Protocol
DICOM - PDV-Header - DICOM Upper Layer Protocol
DICOM - Message Control - DICOM Upper Layer Protocol
DICOM - A-RELEASE-RQ - DICOM Upper Layer Protocol
DICOM - A-ASSOCIATE-AC - DICOM Upper Layer Protocol
DICOM - DICOM Message Control Protocol
DICOM - DICOM Group Length
DICOM - DICOM Affected SOP Class
DICOM - C-SEND-RQ - DICOM Command Set
DICOM - C-SEND-RSP - DICOM Command Set (Command Field)
DICOM - DICOM Message ID
DICOM - DICOM Application Control Protocol
DICOM - DICOM Data Set Type Fields
DICOM - DICOM Status Fields
DICOM - DICOM Affected SOP Instance UIDs
DICOM - DICOM Associate RQ/AC
DICOM - DICOM Data Control
DICOM - JPEG - DICOM Presentation Protocol
DICOM - RQ/AC - DICOM Associate RQ/AC
FDDI - MAC - Media Access Control
FDDI - SMT - Station Management
FIBRE Channel - ISO/IEC 8802-2 LLC
FIBRE Channel - ISO/IEC 8802-2 LLC/SNAP
FIBRE Channel - iSCSI
FIBRE Channel - IPI-3
FIBRE Channel - SBCCS
FIBRE Channel - Fibre Channel Services
FIBRE Channel - FC-FG
FIBRE Channel - FC-XS
FIBRE Channel - FC-AL
FIBRE Channel - SNMP
FIBRE Channel - HIPPI - FP
FIBRE Channel - FCIP Fibre Channel Over IP
LAN - Ethernet - Non-802.3 Ethernet
LAN - FDDI - Fiber Distributed Data Interface
LAN - IEEE 802.3 - IEEE 802.3
LAN - IEEE 802.3x - IEEE 802.3 extensions
LAN - IEEE 802.5 - Token Ring
LAN - IEEE 802.5/MAC - Token Ring Media Access Control
LAN - IEEE 802.3 Slow Protocol OAM - Operations Administration and Maintenance
LAN - IEEE 802.3.ad - Link Aggregation Control Protocol
LAN - Ethernet Loopback
LAN - IEEE 802.11b - Management
LAN - IEEE 802.11b - Control
LAN - IEEE 802.11a - Management
LAN - IEEE 802.11a - Control
LAN - IEEE 802.11g - Management
LAN - IEEE 802.11g - Control
LLC - 802.1Q - Load-balanced switch-to-switch trunking on VLAN
LLC - ARM - Component of VIVID
LLC - ARM TLV - Component of VIVID
LLC - BME - Component of VIVID
LLC - CCP - Component of VIVID
LLC - CCP TLV - Component of VIVID
LLC - Ethernet - Ethernet Data Link Control
LLC - FNA - Fujitsu Network Architecture
LLC - IEEE 802.1 - Spanning Tree
LLC - IEEE 802.1p - VLAN - GARP GVRP GMRP
LLC - IEEE 802.1Q - Flow control
LLC - LLC - Logical Link Control
LLC - MPLS - Multi-Protocol Label Switching - Internet Draft
LLC - PPoE - Point-to-Point over Ethernet
LLC - SNAP - Subnet Access Protocol
LLC - Token Ring MAC - Token Ring Medium Access Control
LLC - VIVID - System LAN Emulation
LLC - XTP - Xpress Transfer over Ethernet, Token-Ring, FDDI
Microsoft - DCOM - Distributed COM
Microsoft - DS - Datagram Service
Microsoft - NetBIOS - LAN Manager
Microsoft - NS - Name Service
Microsoft - NTLMSSP - NT Lan Manager Secure Socket Protocol
Microsoft - SMB - LAN Manager SMB
Microsoft - SS - Session Service
Microsoft - SMB Mailslot - SMB Mailslot
Microsoft - SMB Pipe - SMB Pipe
Microsoft - RPC SvcCtl - Microsoft RPC Service Control
Microsoft - RPC NETLOGON - Directory Service Functions
Microsoft - Directory Replication Service
Microsoft - Distributed File System
Microsoft - Distributed Link Tracking Server Service
Microsoft - Encrypted File System Service
Microsoft - LLMNR - Link Local Multicast Name Resolution
Microsoft - Local Security Architecture
Microsoft - Local Security Architecture (Directory Services)
Microsoft - MAPI (Exchange)
Microsoft - RPC Endpoint Mapper
Microsoft - RPC MGMT
Microsoft - Messenger Service
Microsoft - NetLogon
Microsoft - RPC NSPI
Microsoft - Registry
Microsoft - Security Account Manager
Microsoft - Server Service
Microsoft - Service Control
Microsoft - MS RPC SAMR
Microsoft - MS RPC SRVSVC
Microsoft - MS RPC SVCCTL
Microsoft - MS RPC WKSSVC
Microsoft - Spool Subsystem
Microsoft - Task Scheduler Service
Microsoft - Telephony API Service
Microsoft - Web Service Discovery
Microsoft - Windows Browser Protocol
Microsoft - Windows Lanman Remote API Protocol
Microsoft - Windows Logon Protocol
Microsoft - Workstation Service
MPLS - BGP-4 - Carrying Label Information in BGP-4
MPLS - CP - Label Encapsulation Protocol
MPLS - CR-LDP - Label Distribution Protocol
MPLS - DiffServ - Support of Differentiated Services
MPLS - ICMP - Internet Control Message for MPLS
MPLS - ICMPv6 - Internet Control Message Protocol for MPLS
MPLS - LDP - Label Distribution Protocol
MPLS - LSE - Label Stack Encoding
MPLS - RSVP ext - RSVP-TE - Internet Draft
NASDAQ - MoldUDP
NASDAQ - MoldUDP64
NASDAQ - OUCH
NASDAQ - SoupBin TCP
NASDAQ - UQDF - UTP Plan Quotation Data Feed
Nortel - IWF - Inter-Working Function
Nortel - SLPP - Simple Loop Prevention Protocol
Nortel - UNIStim
Novell - Diagnostic - Diagnostic
Novell - Diagnostic - Serialization
Novell - Diagnostic - Watchdog
Novell - Diagnostic - Broadcast Notification
Novell - Echo - Echo
Novell - Error - Error
Novell - IPX - Internet Packet Exchange
Novell - IPX - IPX under IP
Novell - NCP 2.x 3.x - Netware Core Protocols 2.x,3.x
Novell - NCP 4.x - Netware Core Protocols 4.x
Novell - NCP 5.x - Netware Core Protocols 5.x
Novell - NetBIOS - NetBIOS
Novell - NLSP - Novell Link State Protocol
Novell - Novell-5 - Netware Core Protocols
Novell - Packet Burst - Packet Burst
Novell - PEP - Packet Exchange Protocol
Novell - RIP - Routing Information Protocol
Novell - SAP - Service Advertising Protocol
Novell - SPX - Sequenced Packet Exchange
Novell - IPX NDS - Netware Directory Protocol
Oracle - NET8
Oracle - TNS - Transparent Network Substrate
Oracle - TDS - Oracle Tabular Data Stream
OSI - ACSE - Application Control Service Element
OSI - ASN.1 - Abstract Syntax Notation
OSI - CLNP - WAN/Connectionless Mode Network Sevice Protocol - ISO 8473
OSI - CLNS OSI - CMIP/CMISE - Common Management Information Protocol
OSI - COIT OSI - EISIS - Connectionless-Mode Network Service End System to Intermediate System
OSI - FTAM - File Transfer Access and Management, MAP decode
OSI - IN - Inactive Network
OSI - ISIS - WAN/Intermediate-System to Intermediate-System - RFC 1195
OSI - ISIS ext - ISIS extensions for Traffic Engineering and Update
OSI - MMS - Manufacturing Messaging Service
OSI - MNLP - Mobile Network Location Protocol
OSI - NLCP PPP - OSI Network Layer Control Protocol
OSI - NSAP - WAN/Connectionless-Mode Network Service Access Point - ISO 8348
OSI - Presentation - Presentation
OSI - ROSE - Remote Operation Service Element
OSI - RTSE - Reliable Transfer Service Element
OSI - Session - Session
OSI - TP0 - Transport Protocol class 0
OSI - TP1 - Transport Protocol class 1
OSI - TP2 - Transport Protocol class 2
OSI - TP3 - Transport Protocol class 3
OSI - TP4 - Transport Protocol class 4
OSI - X.400 - Electronic Mail
OSI - X.500 - Directory Services
PPP - BAC/BACP - Bandwidth Allocation Control Protocol
PPP - CCP - Compression Control Protocol
PPP - CHAP - Challenge Handshake Authentication Protocol
PPP - EAP - Extensible Authentication Protocol
PPP - IPXCP - IPX Control Protocol
PPP - L2TP - Layer 2 Tunneling Protocol
PPP - LCP - Link Control Protocol
PPP - MP - Multilink Protocol
PPP - NETBCP - NetBIOS Frames Control Protocol
PPP - PAP - Password Authentication Protocol
PPP - PPP - Point to Point Protocol
PPP - PPP w/HDLC - PPP with HDLC-like framing over SONET/SDH
PPP - BAC/BACP - Bandwidth Allocation Control Protocol
PPP - CCP - Compression Control Protocol
PPP - CHAP - Challenge Handshake Authentication Protocol
PPP - EAP - Extensible Authentication Protocol
PPP - IPXCP - IPX Control Protocol
PPP - L2TP - Layer 2 Tunneling Protocol
PPP - LCP - Link Control Protocol
PPP - MP - Multilink Protocol
PPP - NETBCP - NetBIOS Frames Control Protocol
PPP - PAP - Password Authentication Protocol
PPP - PPP - Point to Point Protocol
PPP - PPP w/HDLC - PPP with HDLC-like framing over SONET/SDH
SCTP
SCTP - DUA - ISDN Q.921 DPNSS 1/DASS 2 User Adaptation
SCTP - IUA - ISDN Q.921 User Adaptation Layer
SCTP - S1AP - S1 Application Protocol
SCTP - x2AP - X2 Application Protocol
SCTP - M3UA - MTP3 User Adaptation Layer
SIGTRAN - M3UA - MTP3 User Adaptation Layer
SNA - DFC - SNA Session Layer Data Flow Control
SNA - DCAP - Document Content Architecture Protocol
SNA - DIAP - Document Interchange Architecture Protocol
SNA - DSP - Distributed Services Protocol
SNA - FSP - File Services Protocol
SNA - FMD - SNA Function Management
SNA - General Data Stream - SNA General Data Stream
SNA - Management Services - SNA Management Services
SNA - NCP - Network Control Protocol
SNA - NetBIOS - NetBIOS
SNA - Path Control - SNA Network Layer
SNA - PU 2.0 (Token Ring)
SNA - SCP - Session Control Protocol
SNA - SMB - Server Message Block
SNA - Transmission Control - SNA Transport Layer
SNA - FID1
SNA - FID2
SNA - FID3
SNA - FID4
SNA - FID5
SNA - FIDF
SNA - RH
SQL - SQL - SQL Database Functions
SQL - SQL/TDS - SQL Tabular Data Stream
Sun - BOOTPARAM - Boot Parameters
Protocols supported by Observer

Sun - MOUNT - Mount
Sun - NFS - v2 Network File System - RFC1094
Sun - NFS - v3 Network File System - RFC1813
Sun - NFS - Mount v3 - RFC1813
Sun - NFS - Lock Manager v4 - RFC1813
Sun - NIS - Network Information Services
Sun - PCNFS - PC Network File System
Sun - PMAP - Port Map - RFC1833
Sun - RLOCK - RLOCK
Sun - RPC v2 - Remote Procedure Call - RFC1831
Sun - RSTAT - RSTAT
TCP/IP - AH - Authentication Header
TCP/IP - ArcaBook Multicast
TCP/IP - ARP - Address Resolution Protocol
TCP/IP - BFD Control - Bidirectional Forwarding Detection Control
TCP/IP - BFD Echo - Bidirectional Forwarding Detection Echo
TCP/IP - BGMP - Border Gateway Multicast Protocol
TCP/IP - BGP - Border Gateway Protocol
TCP/IP - BGP-4 - BGP version 4
TCP/IP - BGP-4 ext - BGP ASC
TCP/IP - BitTorrent
TCP/IP - BOOTP - BOOT Protocol
TCP/IP - BSD Syslog - Berkeley Software Distribution Syslog
TCP/IP - CAPWAP - Control And Provisioning of Wireless Access Points
TCP/IP - CIFS - Common Internet File System
TCP/IP - CME RLC - CME Market Data Platform RLC
TCP/IP - CPHA - Checkpoint High-Availability
TCP/IP - CQS - SIAC Consolidated Quotation System
TCP/IP - CTS - SIAC Consolidated Tape System
TCP/IP - DAAP
TCP/IP - DCE RCP - DCE Endpoint
TCP/IP - DHCP - Dynamic Host Configuration Protocol
TCP/IP - DHCPv6 - Dynamic Host Configuration Protocol v6
TCP/IP - DIAMETER (RFC 3588)
TCP/IP - DIFFSERV - Differentiated Services
TCP/IP - DirectEdge Multicast
TCP/IP - DISL - Dynamic ISL
TCP/IP - DISP - Dispatching for SNMP
TCP/IP - DLSw - Data Link Switching
TCP/IP - DNP3 - Distributed Network Protocol 3.0
TCP/IP - DNS - Domain Name Service
TCP/IP - DVMRPv3 - Distance Vector Multicast Routing Protocol
TCP/IP - EGP - Exterior Gateway Protocol
TCP/IP - EIGRP - Enhanced Interior Gateway Routing Protocol
TCP/IP - EtherIP - Ethernet over IP Tunneling
TCP/IP - Finger - User Information - RFC 1288
TCP/IP - FLAP/SNAC - AOL Instant Messenger
TCP/IP - FIX - Financial Information Exchange
TCP/IP - FTP - File Transfer Protocol
TCP/IP - GGP - Gateway to Gateway Protocol
TCP/IP - GIDP - General Inter-ORB Protocol
TCP/IP - GMRP - 802.1 GARP Multicast Registration Protocol
TCP/IP - GOPHER - File Retrieval
TCP/IP - GRE - Generic Routing Encapsulation
TCP/IP - GTP - GPRS (General Packet Radio Service) Tunneling Protocol
TCP/IP - GTPv2 - GPRS Tunneling Protocol version 2
TCP/IP - HTTP - Hypertext Transfer Protocol
TCP/IP - HTTP 1.1 - Hypertext Transfer Protocol 1.1
TCP/IP - IAX2 (Inter-Asterisk eXchange version 2)
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP - ICMPv4</td>
<td>Internet Control Message Protocol Version 4 - RFC 2060</td>
</tr>
<tr>
<td>TCP/IP - ICMPv6</td>
<td>Internet Control Message Protocol Version 6 - RFC 2463</td>
</tr>
<tr>
<td>TCP/IP - IGMP</td>
<td>Internet Gateway Routing Protocol</td>
</tr>
<tr>
<td>TCP/IP - IGMPv2</td>
<td>Internet Group Management Protocol version 2</td>
</tr>
<tr>
<td>TCP/IP - IGMPv3</td>
<td>Internet Group Management Protocol version - RFC 3376</td>
</tr>
<tr>
<td>TCP/IP - IGRP</td>
<td>Internet Gateway Routing Protocol</td>
</tr>
<tr>
<td>TCP/IP - IIOP</td>
<td>Internet Inter-ORB Protocol</td>
</tr>
<tr>
<td>TCP/IP - IMAP4</td>
<td>Internet Message Access Protocol</td>
</tr>
<tr>
<td>TCP/IP - IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>TCP/IP - IP Compression</td>
<td></td>
</tr>
<tr>
<td>TCP/IP - IPFIX</td>
<td>Internet Protocol Flow Information eXport</td>
</tr>
<tr>
<td>TCP/IP - IPv6</td>
<td>Internet Protocol Version 6 - RFC 2460</td>
</tr>
<tr>
<td>TCP/IP - IPv6AUTH</td>
<td>Internet Protocol Version 6 Authentication Header - RFC 2402</td>
</tr>
<tr>
<td>TCP/IP - IRC</td>
<td>Internet Relay Chat</td>
</tr>
<tr>
<td>TCP/IP - ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>TCP/IP - iSCSI</td>
<td></td>
</tr>
<tr>
<td>TCP/IP - ISO TSAP</td>
<td>ISO Transport Service Access Point</td>
</tr>
<tr>
<td>TCP/IP - Kerberos</td>
<td>RFC 1510</td>
</tr>
<tr>
<td>TCP/IP - Kerberos Passwords</td>
<td>RFC 3244</td>
</tr>
<tr>
<td>TCP/IP - LDAPv1</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>TCP/IP - LDAPv2</td>
<td>LDAP Version 2</td>
</tr>
<tr>
<td>TCP/IP - LDAPv3</td>
<td>LDAP Version 3 - RFC 2251</td>
</tr>
<tr>
<td>TCP/IP - LMP</td>
<td>Link Management Protocol over IP</td>
</tr>
<tr>
<td>TCP/IP - Lotus Notes</td>
<td></td>
</tr>
<tr>
<td>TCP/IP - LPD</td>
<td>Line Printer Daemon Protocol</td>
</tr>
<tr>
<td>TCP/IP - LPR</td>
<td>Line Printer Daemon Protocol Remote</td>
</tr>
<tr>
<td>TCP/IP - LPP</td>
<td>ISO Services</td>
</tr>
<tr>
<td>TCP/IP - LSE Infolect</td>
<td>London Stock Exchange Infolect</td>
</tr>
<tr>
<td>TCP/IP - M2PA</td>
<td>MTP2 - Peer-to-Peer Adapt Layer</td>
</tr>
<tr>
<td>TCP/IP - MBGP</td>
<td>Multi-protocol BGP</td>
</tr>
<tr>
<td>TCP/IP - MINET</td>
<td>Mitel IP Terminal</td>
</tr>
<tr>
<td>TCP/IP - MIP</td>
<td>Mobile IP</td>
</tr>
<tr>
<td>TCP/IP - MIP RT</td>
<td>Mobile IP Reverse Tunneling</td>
</tr>
<tr>
<td>TCP/IP - MobileIP</td>
<td></td>
</tr>
<tr>
<td>TCP/IP - MODBUS</td>
<td>Modicon BUS</td>
</tr>
<tr>
<td>TCP/IP - MOSPF</td>
<td>Multicast Open Shortest Path First</td>
</tr>
<tr>
<td>TCP/IP - MSDP</td>
<td>Multicast Source Discovery Protocol</td>
</tr>
<tr>
<td>TCP/IP - Multicast DNS</td>
<td></td>
</tr>
<tr>
<td>TCP/IP - Multicast PITCH</td>
<td>BATS Multicast PITCH</td>
</tr>
<tr>
<td>TCP/IP - MYSQL</td>
<td></td>
</tr>
<tr>
<td>TCP/IP - NetBIOS</td>
<td>NetBIOS over TCP/IP</td>
</tr>
<tr>
<td>TCP/IP - NNTP</td>
<td>Network News Transfer Protocol</td>
</tr>
<tr>
<td>TCP/IP - NTP</td>
<td>Network Time Protocol -RFC 1305</td>
</tr>
<tr>
<td>TCP/IP - ODSI CP</td>
<td>Optical Domain Service Interconnect Control Protocol</td>
</tr>
<tr>
<td>TCP/IP - ODSI - SS</td>
<td>Optical Domain Service Interconnect Signaling Specification</td>
</tr>
<tr>
<td>TCP/IP - OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>TCP/IP - OSPF ext</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>TCP/IP - OSPF v6</td>
<td>OSPF for IPv6</td>
</tr>
<tr>
<td>TCP/IP - PIM-DM</td>
<td>Protocol Independent Multicast, Dense Mode</td>
</tr>
<tr>
<td>TCP/IP - PIM-SM</td>
<td>Protocol Independent Multicast, Sparse Mode</td>
</tr>
<tr>
<td>TCP/IP - POP2</td>
<td>Post Office Protocol v2</td>
</tr>
<tr>
<td>TCP/IP - POP3</td>
<td>Post Office Protocol v3 and extensions</td>
</tr>
<tr>
<td>TCP/IP - PPTP</td>
<td>Point to Point Tunneling Protocol</td>
</tr>
<tr>
<td>TCP/IP - PTP</td>
<td>Precision Time Protocol</td>
</tr>
<tr>
<td>TCP/IP - Profinet</td>
<td>-IEC 61158 and IEC 61784</td>
</tr>
<tr>
<td>TCP/IP - RADIUS Accounting</td>
<td>(obsoletes RFC2139)</td>
</tr>
</tbody>
</table>
TCP/IP - RADIUS Accounting Modifications for Tunnel Protocol Support
TCP/IP - RADIUS Attributes for Tunnel Protocol Support
TCP/IP - RADIUS Extensions
TCP/IP - RARP - Reverse Address Resolution Protocol
TCP/IP - REXEC - Remote Exec
TCP/IP - RIP - Routing Information Protocol
TCP/IP - RIP-2 - Routing Information Protocol v2
TCP/IP - RIPv6 - RIP for IPv6
TCP/IP - RLOGIN - Remote Login
TCP/IP - RLPR - Remote Print Routed Route daemon Protocol
TCP/IP - RSHELL - Remote Shell
TCP/IP - RSRB - Remote Source Route Bridging Protocol
TCP/IP - RSVP - Resource Reservation Protocol
TCP/IP - RTSP - Real Time Streaming
TCP/IP - RWHO - Remote Who
TCP/IP - SCMG - SCCP Management
TCP/IP - SSDPv1 - Simple Service Discovery Protocol
TCP/IP - Shoutcast
TCP/IP - SIMPLE - MSN / SIP for Instant Messaging and Presentation Leveraging Extensions
TCP/IP - SLPv1 - Service Location Protocol
TCP/IP - SLPv2 - Service Location Protocol Version 2 (RFC 2608)
TCP/IP - SMB - Server Message Block
TCP/IP - SMBv2 - Server Message Block version 2
TCP/IP - SMPP - Short Message Peer to Peer v3.4
TCP/IP - SMTP - Simple Mail Transport Protocol
TCP/IP - SMTPS - SMTP over SSL/TLS
TCP/IP - SNMP - Simple Network Management Protocol
TCP/IP - SNMP-Z - Simple Network Management Protocol version 2
TCP/IP - SNMP-2C - Simple Network Management Protocol version 2c
TCP/IP - SNMP-3 - Simple Network Management Protocol version 3
TCP/IP - SNMP - All Objects and Object Types MIB descriptions listed by name if MIB is loaded
TCP/IP - SOCKS
TCP/IP - SSH - Secure Shell
TCP/IP - TACACS - Terminal Access Controller Access Control System
TCP/IP - TACACS+ - Terminal Access Controller Access Control System Extensions
TCP/IP - TCP - Transport Control Protocol
TCP/IP - TDMoIP - Time Division Multiplexing over IP
TCP/IP - TELNET - Telnet
TCP/IP - Teradata - NCR Teradata
TCP/IP - Teredo - Tunneling IPv6 over UDP through Network Address Translations
TCP/IP - TFTP - Trivial File Transfer Protocol
TCP/IP - TIMED - Time Daemon Protocol
TCP/IP - UDP - User Datagram Protocol
TCP/IP - VISA Cardnet
TCP/IP - VRRP - Virtual Router Redundancy
TCP/IP - VTP - Virtual Trunking Protocol
TCP/IP - WCCP - Web Cache Communication Protocol
TCP/IP - WebSphere MQ - IBM WebSphere MQ
TCP/IP - WMP-NSS
TCP/IP - X-Windows
TCP/IP - IPv6 - (All lower TCP/Data functions)
TCP/IP - ISO - 8583 (AMEX)
TCP/IP - UPD - London Stock Exchange
WAN - Ethertype - Ethertype
WAN - Frame Relay - Frame Relay
WAN - GR303 TMC - Q.931 on T1-GR-303-CORE
WAN - HDLC - High level Data Link Control
WAN - LAPB - Link Access Procedure Balanced
WAN - LAPD - D channel Link Access Protocol
WAN - LAPV - Link Access Protocol v5
WAN - LMI Annex A - Local Management Interface A
WAN - LMI Annex D - Local Management Interface D
WAN - LMI Original - Local Management Interface
WAN - NODELOC - Node Location
WAN - PDU Bridged - Protocol Data Unit Bridged
WAN - RFC 1490/2427 - Frame Relay
WAN - SDLC - Synchronous Data Link Control
WAN - SLIP - Serial Line Interface Protocol
WAN - TOH - Transport OverHead
WAN - VoFR - Voice over Frame Relay
WAN - VoFR Annex C - Voice over Frame Relay Annex C
WAN - VoFR Annex E - Voice over Frame Relay Annex E
WAN - VoFR Annex F - Voice over Frame Relay Annex F
WAN - VoFR Annex G - Voice over Frame Relay Annex G
WAN - VoFR Annex H - Voice over Frame Relay Annex H
WAN - VoFR Annex I - Voice over Frame Relay Annex I
WAN - X.25 - X.25
WAN - X.25 - XOT - RFC1613
WAN - Q.922 WAN - Q.931/Annex D (Frame Relay)
WAN - ISO8885 WAN - X.75 - X.75 WAN - MultiLink PPP
Xerox/XNS - Echo - XNS - Echo
Xerox/XNS - Error - XNS - Error
Xerox/XNS - RIP - Routing Information Protocol
Xerox/XNS - SPP - Sequenced Packet Protocol
Xerox/XNS - Xerox XNSIdp
VoIP - COPS - Common Open Policy Service for Packet Cable
VoIP - H.225.0 Version 2 - RAS
VoIP - H.225.0 Version 3 - Call signalling (Q.931/Q.932)
VoIP - H.235 - Security and encryption for H-series multimedia terminals
VoIP - H.245 Version 1 - Call Control for H.323 multimedia
VoIP - H.245 Version 2 - Call signaling for H.323 logical channels
VoIP - H.245 Version 3 - Call signaling for H.323 logical channels
VoIP - H.245 Version 5 - Control Protocol for Multimedia Communication
VoIP - H.248 MEGACO - ITU-T & IETF carrier-class VoIP signaling (text and binary)
VoIP - H.261 - Video CODEC used in H.323 - RFC2032
VoIP - H.263 - Video CODEC for low bit rate communication - RFC2250
VoIP - H.263-1998 - RFC2429, RFC3555
VoIP - H.263-2000 - RFC2429, RFC3555
VoIP - H.323v3 Annex E - Protocol for multiplexed call signaling transport E
VoIP - H.323v3 Annex F - Protocol for multiplexed call signaling transport F
VoIP - H.323v3 Annex G - Communication between administrative domains
VoIP - Megaco - Media Gateway Control Protocol
VoIP - MGCP - Media Gateway Control Protocol Version 1 - RFC 2705
VoIP - NCS - PacketCable - Network-Based Call Signaling Protocol
VoIP - Q.931 - Signaling for H.323
VoIP - RAS (H.225.0 V1) - RAS for H.323
VoIP - RTP - Real-time Transport Control Protocol
VoIP - RTCP - Real-time Transport Protocol
VoIP - SAP - Session Announcement Protocol
VoIP - SDP - Session Description Protocol - RFC 2327
VoIP - SGCP - Simple Gateway Control Protocol
VoIP - SIP - Session Initiation Protocol - RFC 2543, RFC 3261
VoIP - IAX VoIP - Nortel Unistim
VoIP - Avaya CCMS
VoIP - T.120/X.224 - DPMC
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP - T.122 - DPMC</td>
<td></td>
</tr>
<tr>
<td>VoIP - T.123 - DPMC</td>
<td></td>
</tr>
<tr>
<td>VoIP - T.124 (GCC) - Generic Conference Control</td>
<td></td>
</tr>
<tr>
<td>VoIP - T.125 - DPMC</td>
<td></td>
</tr>
<tr>
<td>VoIP - T.126 (SI) - Multipoint Still Image and Annotation</td>
<td></td>
</tr>
<tr>
<td>VoIP - T.127 (MBFT) - Multipoint Binary Transfer Protocol</td>
<td></td>
</tr>
<tr>
<td>VoIP - T.128 (AS) - Multipoint Application Sharing</td>
<td></td>
</tr>
<tr>
<td>VoIP - XGCP - Extended GCP</td>
<td></td>
</tr>
<tr>
<td>VoIP - XoIP - Media over IP</td>
<td></td>
</tr>
<tr>
<td>VoIP - CN - RFC3389</td>
<td></td>
</tr>
<tr>
<td>VoIP - 1016 - RTP Audio Payload</td>
<td></td>
</tr>
<tr>
<td>VoIP - G711/PCMU</td>
<td></td>
</tr>
<tr>
<td>VoIP - PCMA - G711 A-law - RFC 3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G721 - RTP Audio Payload</td>
<td></td>
</tr>
<tr>
<td>VoIP - GSM - RTP Audio Payload - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G722 - RTP Audio Payload - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G723 - Payload 4 - G.723 (Audio Playback)</td>
<td></td>
</tr>
<tr>
<td>VoIP - G.723.1-5.3</td>
<td></td>
</tr>
<tr>
<td>VoIP - G723.1A-5.3</td>
<td></td>
</tr>
<tr>
<td>VoIP - G723.1A</td>
<td></td>
</tr>
<tr>
<td>VoIP - DVI4 - RTP Audio Payload - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - LPC - RTP Audio Payload</td>
<td></td>
</tr>
<tr>
<td>VoIP - parityfec - RFC3009</td>
<td></td>
</tr>
<tr>
<td>VoIP - PCMA(G.711) - Payload 0 - G.711 PCMU u-law (Audio Playback)</td>
<td></td>
</tr>
<tr>
<td>VoIP - PCMU(G.711) - Payload 8 - G.711 PCMU A-law (Audio Playback)</td>
<td></td>
</tr>
<tr>
<td>VoIP - L8 - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - L16 - RTP Audio Payload - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - L20 - RFC3190</td>
<td></td>
</tr>
<tr>
<td>VoIP - L24 - RFC3190</td>
<td></td>
</tr>
<tr>
<td>VoIP - MPA - RTP Audio Payload - RFC3551, RFC2250</td>
<td></td>
</tr>
<tr>
<td>VoIP - MP4A-LATM - RFC3016</td>
<td></td>
</tr>
<tr>
<td>VoIP - mpa-robust - RFC3119</td>
<td></td>
</tr>
<tr>
<td>VoIP - G726</td>
<td></td>
</tr>
<tr>
<td>VoIP - G726-16 - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G726-24 - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G726-32 - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G726-40 - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G728 - RTP Audio Payload - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G729A - RTP Nortel Audio Payload (Audio Playback)</td>
<td></td>
</tr>
<tr>
<td>VoIP - G729B</td>
<td></td>
</tr>
<tr>
<td>VoIP - G729D - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - G729E - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - Ce1B - RTP Video Payload - RFC2029</td>
<td></td>
</tr>
<tr>
<td>VoIP - JPEG - RTP Video Payload - RFC2435</td>
<td></td>
</tr>
<tr>
<td>VoIP - Nv - RTP Video Payload - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - MPV - RTP Video Payload - RFC2250</td>
<td></td>
</tr>
<tr>
<td>VoIP - MP2T - RTP Audio/Video Payload - RFC2250</td>
<td></td>
</tr>
<tr>
<td>VoIP (FoIP) - T.30/T.38 Fax over UDP (H.323 Annex D)</td>
<td></td>
</tr>
<tr>
<td>VoIP - QCLEP VoIP - rtx - RFC-ietf-avt-rtp</td>
<td></td>
</tr>
<tr>
<td>VoIP - AMR - RFC3267</td>
<td></td>
</tr>
<tr>
<td>VoIP - AMR-WB - RFC3267</td>
<td></td>
</tr>
<tr>
<td>VoIP - DAT12 - RFC3190</td>
<td></td>
</tr>
<tr>
<td>VoIP - dsr-es201108 - RFC3557</td>
<td></td>
</tr>
<tr>
<td>VoIP - EVRC - RFC3558</td>
<td></td>
</tr>
<tr>
<td>VoIP - EVRC0 - RFC3558</td>
<td></td>
</tr>
<tr>
<td>VoIP - GSM-EFR - RFC3551</td>
<td></td>
</tr>
<tr>
<td>VoIP - RED - RFC2198, RFC3555</td>
<td></td>
</tr>
<tr>
<td>VoIP - red - RFC4102</td>
<td></td>
</tr>
<tr>
<td>VoIP - rtx - RFC-ietf-avt-rtp</td>
<td></td>
</tr>
</tbody>
</table>
VoIP - VDVI - RFC3551
VoIP - SMV - RFC3558
VoIP - SMVO - RFC3558
VoIP - t140c - RFC4351
VoIP - t38 - RFC4612
VoIP - telephone-event - RFC2833
VoIP - tone - RFC2833
VoIP - t140 - RFC4103
VoIP - BMPEG - RFC2343, RFC3555
VoIP - BT656 - RFC2431, RFC3555
VoIP - DV - RFC3189
VoIP - MP1S - RFC2250, RFC3555
VoIP - MP2P - RFC2250, RFC3555
VoIP - MP4V-ES - RFC3016
VoIP - pointer - RFC2862
VoIP - raw - RFC4175
VoIP - SMPT292M - RFC3497
VoIP - vc1 - RFC4425
VoIP - BV16 - RFC4298; BroadVo
VoIP - BV32 - RFC4298; BroadVo
VoIP - LRNB VoIP - LRWB
Other - Bridged Ethernet
Other - EIP - Extended Internet Protocol
Other - IKE - RFC2409
Other - IPSec - RFC2401
Other - DOI - Domain of Interpretation RFC 2407
Other - ESP - RFC2406
Other - AH - RFC 2402
Other - LLDP - Link Layer Discovery Protocol
Other - MNLP - Mobile Network Location Protocol
Other - PPP EAP TLS Authentication Protocol - RFC2716
Other - PPP LCP Internationalization Configuration Option - RFC2484
Other - PPP Extensible Authentication Protocol (EAP) - RFC2284
Other - sFlow
Other - Yahoo - Instant Messenger Protocol
Other - Yahoo - YMSG Messenger Protocol
Other - COPS (Common Open Policy Service)
Other - GSMP - General Switch Management Protocol
Other - VRRP (Virtual Router Redundancy Protocol)
Other - SNA over UDP Other - SCTP (Stream Control Transmission Protocol)
Chapter 12: Backup and Restoration

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 15: FIX Settings

<table>
<thead>
<tr>
<th>This option…</th>
<th>Allow you to do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIX Profile</td>
<td>Lists the name of the current profile. The current profile is the rest of the dialog window, including the General Settings and the Type/Message.</td>
</tr>
<tr>
<td>Edit</td>
<td>Use this button to rename, add a new, or delete a profile. If you have numerous GigaStor probes where you want to use the same FIX analysis options, modify or create the profiles on one system, export them, and import them into the other GigaStor probes.</td>
</tr>
<tr>
<td>Import</td>
<td>Use this button to import FIX profiles that was created and exported from another Observer analyzer.</td>
</tr>
<tr>
<td>Export</td>
<td>Use this button to export a FIX profile.</td>
</tr>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum tracked requests</td>
<td>Lists the maximum number of requests to be tracked during the time frame selected in the Detail Chart. The default is 1000 requests. Typically, 1000 requests should be sufficient to provide the information you seek. If it is not, you may increase or decrease it. By increasing the amount of requests, the amount of system resources needed to analyze the requests is also increased, which means the analysis will take longer to complete.</td>
</tr>
<tr>
<td>Ignore duplicate requests</td>
<td>If selected, duplicate requests are ignored. This is the default setting. If unchecked, duplicate requests may be present in the analysis and reduces the number of unique requests in the tracked requests.</td>
</tr>
<tr>
<td>Maximum displayed results</td>
<td>Defines the maximum number of results to display in the GigaStor Control Panel for the fastest or slowest responses.</td>
</tr>
<tr>
<td>Track not responded requests within</td>
<td>Amount of time used as the threshold that the GigaStor should wait for a response to a request before discarding the request from its analysis data set. If you want only requests that have received a response, uncheck this option.</td>
</tr>
<tr>
<td>This option…</td>
<td>Allow you to do this…</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Track/Type/Message</td>
<td>Type and Message are options defined in the FIX protocol specification. If Track is selected, the FIX transaction type will be part of this analysis profile. All untracked options are ignored for this profile.</td>
</tr>
</tbody>
</table>

Sharing alarms with others

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

How to import alarms

To import alarms, you need access to an exported *.ALM file. You must bring this file back into Observer using the import process described here:

1. Click the Alarms Settings button, near the bottommost portion of the Observer window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Click the Import Alarms button.
5. Navigate to, and select, your file; click Open.

You successfully imported an alarm file. The alarms contained within are now part of your local collection, including the triggers and actions associated with each alarm.

How to export alarms

To share alarms, the alarms must first be saved to a file. Create your file by following this export process:

1. Click the Alarms Settings button, near the bottommost portion of the Observer window. The Alarm Settings window appears.
2. Click a probe instance to highlight it.
3. Click the Selected Instance Alarm Settings button. The Probe Alarms Settings window appears.
4. Select each alarm you want to export.
5. Click the Export Checked Alarms button.
6. Give your file a name, and click Save.

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

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

How to export application definitions

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

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

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

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

How to import application definitions

Prerequisite(s):

To import application definitions, you need access to an exported *.protodefs file. See Exporting app definitions on page 35 for details.

To import application definitions, follow the import process:

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

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

How to export report data to XML

Sometimes it is advantageous to bring report data out of its native format and into third-party tools. If needed, you can accomplish this by exporting your report data to XML.

Your can generate hundreds of reports, all of which can be configured as you need and provide you visibility and analytics about your network. After creating a report, there may be times where you want the data from only part of a report so you can store the data elsewhere or manipulate it using another tool. Using settings only available from the report in your web browser, you can access the data on a report.

You can access report content in its raw format and then process the data with your tools. Just some of the raw data you can access includes SLA measurements for use in a MOM, security alerting inside a SIEM, or compliance monitoring data.

Unlike nearly every task described in this guide, which describes using the user interface to configure reports, this feature is only available after the report is created and you are viewing it in your web browser.

To export your report data to XML:

1. Open a web browser and type the following URL: http://Observer/Observer where Observer is the host name or IP address of the system running Observer.
2. In the upper left, ensure the desired probe instance is selected from the list.
3. Click Settings in the upper right. The Report Settings page opens.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Show Report Element Link when clicking on the report element title bar | Used for embedding report elements in a third-party tool. This allows you to click the title bar of any report element (graph, table, etc.) and obtain a link to that element and then embed the link in your tool. Hover your mouse over an element title and click it. This opens a pop up window from which you
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>can open the element in another browser window or use in your third party tool. The report (or report element — table, graph, etc.) you selected is processed and displayed in your third party dashboard. This report is from the source which it was generated, including any associated data sources and filters applied. In the URL, you may see a start time and end time for the report. This happens when you generate the report using a fixed time criteria. These fields are in epoch and can be modified within the URL to provide the report on whatever fixed time period you wish.</td>
</tr>
<tr>
<td>Show XML Export button</td>
<td>Allows the user to manually export the XML of a report (in its entirety, including all elements) to a XML file. An “XML Export” button appears at the top right. Click the button to generate an XML file which is saved to your hard drive. Use the XML file as you wish.</td>
</tr>
<tr>
<td>Show XML Report Link button</td>
<td>Similar to the Show XML Export button, but instead of needing to click the button to generate the XML, you can generate the URL once and then use the XML data request URL in your third party tool. The resulting XML will be for the entire report, including all elements. Similar to the “Show Report Element Link…”, the start and end times can be modified if using fixed time periods, and all business group sources and filters will apply.</td>
</tr>
</tbody>
</table>

**Private key locations per server**

**Microsoft Lync Server**

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

By default, the Lync Server key is not exportable. You must create an exportable key for Observer to use. Getting the Lync Server key is similar to that for the IIS Web Server. See Windows IIS Web Server on page 70.

**Apache Web Server**

Perform a search for the file with the name “server.key”. Check the format of the server.key file to ensure it is not an encrypted private key file. See Example of an encrypted private key file on page 71.
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):

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

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

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

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

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD7uhNyamd6WOCRqH0rp5zs4FEwCX2JrKtm0dmTf44SVaGvFLF1
vakeOYP/sFs4aa20aNo0FcbFaSzW3IZWum4sCtqtvb8Zi1+13VCdyR+2SRx9Gmbu
SnoL/6Fl86m+C0hQ6G0LoiTAlJnY+M0EC2bwbMykzljPVUOXE91EG0AQIDAAQAB
AoGAFQOyqWEVmQrPzNW6YXnJkxVGBCzrPdrWfgC0/ITXhYUtlt2I47QLd+ni
-----END RSA PRIVATE KEY-----
```
Example of an encrypted private key file

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

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,7BC....
JHQ8U0pDbeFM9h2jZSmiuqxdqOa2q/MiX43Xa4Es6nKmzu9oI/ZfpIdAHi8qwtsD
m25bQRIXD9AnExxRy0tG2ibUaphQEsV995PVUsh8N9dVumsqykmMXSwND7tkbHB
io/VVSAAD9bV3db15nBMwMnPG+YC3S90GAK42R1qrHRQ94fd/ZAvP8kV9i1wCmX6
swFLNBLGuKFllJ9gkryr+OOQul1AyZAB2UThGCGJJetELFtV4mLmIaHdgD1cUqPj==
-----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. Choose Options > Protocol Definitions and Server Application Discovery.
2. Click the TCP Application Definitions tab to ensure it has focus.
3. Click the Tools button, and click Restore Predefined TCP Applications. A confirmation prompt appears.
4. Click OK to confirm.
5. (Optional) Select Apply Changes Across All Probe Instances if you want to apply these changes to all probe instances.
6. Click OK to apply and save your changes.

Your TCP application definitions list is now restored.

How to restore UDP application definitions

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

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

**Importing and exporting Observer Alias (.adr) files**

Observer Infrastructure can exchange alias lists with Observer. To import an alias list from (or export an alias list to) Observer, select Tools > Observer Integration > Import Alias list from (or Export alias List to...).

A file dialog is then displayed, allowing you to select the file to import (or supply a filename to export).

Alias list files must have the extension .adr for Observer and Observer Infrastructure to recognize them.

**Importing or exporting a server profile**

You can import or export servers that you monitor from one Observer analyzer to another. This can save time and reduce typing errors if you have several Observer analyzers which you want to have the same servers be analyzed for application transaction analysis.

**Tip!** You can also logically group server applications and switch between profiles quickly by choosing a profile from the Profiles list.

1. Choose **Trending/Analysis > Application Transaction Analysis**.
2. Click the Settings button to define any application servers you want to monitor.
3. Click the Import or Export button.

   First you must define the server applications and then export the server to create the *.ata file that you can later import.

**Creating a Forensic Settings profile**

Forensics profiles provide a mechanism to define and load different pairings of settings and rules profiles. Settings profiles define pre-processor settings that let you tune performance; rules profiles define which forensic rules are to be processed during analysis to catch threats against particular target operating systems and web servers. Because Observer performs signature matching on existing captures rather than in real time, its preprocessor configuration differs from that of native Snort. When you import a set of Snort rules that includes configuration settings, Observer imports rules classifications, but uses its own defaults for the preprocessor settings.

There is a difference between enabling the preprocessor and enabling logs for the preprocessor. For example, you can enable IP defragmentation with or without logging. Without logging, IP fragments are simply reassembled; only time-out or maximum limit reached messages are noted in
the Forensics Log and in the Forensic Analysis Summary window. If logging is enabled, all reassembly activity is displayed in the Forensics Log (but not displayed in the Forensic Analysis Summary).

1. In Observer, choose Capture > GigaStor Control Panel > Forensic Analysis tab.
2. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.
3. Choose your profile and click Edit. The Forensic Settings window opens.
4. From the Forensic Settings window, complete the following:
   - Import Snort rules
   - Define Forensic Settings.
   - Define Rule Settings—Select the rules you want to enable.
5. Close all of the windows, then right-click anywhere on the Forensic Analysis tab and choose Analyze from the menu.

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 16: Forensic Settings options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings Profile</td>
<td>Settings Profiles provide a mechanism to save and load different preprocessor settings, and share them with other Observer analyzers.</td>
</tr>
<tr>
<td>IP Flow</td>
<td>Packets belong to the same IP flow if they share the same layer 3 protocol, and also share the same source and destination addresses and ports. If this box is checked, forensic analysis identifies IP flows (also known as conversations), allowing Snort rules to isolate packets by direction and connection state via the flow option. If this pre-processor is disabled, flow keywords are ignored, but the rest of the rule is processed. The remaining settings allow you to throttle flow analysis by limiting the number of flows tracked, and by decreasing the time window within which a flow is considered active.</td>
</tr>
<tr>
<td>IP Defragmentation</td>
<td>Some types of attacks use packet fragmentation to escape detection. Enabling this preprocessor causes forensic analysis to identify and reconstruct fragmented packets based on the specified fragment reassembly policy. Rules are then run against the reconstructed packets during forensic analysis. The fragment reassembly policy mimics the behavior of various operating systems in what to do when ambiguous fragments are received. Choose the policy to match the OS of the server (or servers) being monitored. If the buffer contains traffic targeting hosts with different operating systems, use post-filtering to...</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>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></td>
<td>Refer to <a href="http://www.snort.org">http://www.snort.org</a> for more detailed version-specific information. The remaining options allow you to enable logging of alerts and reconstruction progress, limit the number of active packet segments to track, and change the length of fragment inactivity that causes the fragment to be dropped from analysis.</td>
</tr>
</tbody>
</table>

TCP Stream Reassembly

Another IDS evasion technique is to fragment the attack across multiple TCP segments. Because hackers know that IDS systems attempt to reconstruct TCP streams, they use a number of techniques to confuse the IDS so that it reconstructs an incorrect stream (in other words, the IDS processes the stream differently from that of the intended target). As with IP fragmentation, forensic analysis must be configured to mimic how the host processes ambiguous and overlapping TCP segments, and the topology between attacker and target to accurately reassemble the same stream that landed on the target. Re-assembly options are described below:

TCP Stream Reassembly (Continued)

Log preprocessor events—Checking this box causes forensic analysis to display all activity generated by the TCP stream assembly preprocessor to the log. |
| Maximum active TCP streams tracked—if this value is set too high given the size of the buffer being analyzed, performance can suffer because of memory consumption. If this value is set too low, forensic analysis can be susceptible to denial of service attacks upon the IDS itself (i.e., the attack on the target is carried out after the IDS has used up its simultaneous sessions allocation). |
| Drop TCP streams inactive for this duration—a TCP session is dropped from analysis as soon as it has been closed by an RST message or FIN handshake, or after the time-out threshold for inactivity has been reached. Exercise caution when adjusting the time-out, because hackers can use TCP tear-down policies (and the differences between how analyzers handle inactivity vs. various operating systems) to evade detection. |
| TTL delta alert limit—Some attackers depend on knowledge of the target system's location relative to the IDS to send different streams of packets to each by manipulating TTL (Time To Live) values. Any large swing in Time To Live (TTL) values within a stream segment can be evidence of this kind of evasion attempt. Set the value too high, and analysis will miss these attempts. Setting the value too low can result in excessive false positives. |
| Overlapping packet alert threshold—the reassembly preprocessor will generate an alert when more than this number of packets within a stream have overlapping sequence numbers. |
| Process only established streams—Check this box if you want analysis to recognize streams established during the given packet capture. |
| Reconstruct Client to Server streams—Check this box to have analysis actually reconstruct streams received by servers.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconstruct Server to Client streams—Check this box to have analysis actually reconstruct streams received by clients.</td>
<td></td>
</tr>
<tr>
<td>Overlap method—Different operating systems handle overlapping packets using one of these methods. Choose one to match the method of the systems being monitored.</td>
<td></td>
</tr>
<tr>
<td><strong>TCP Stream Reassembly (Continued)</strong></td>
<td>Reassembly error action—Discard and flush writes the reassembled stream for analysis, excluding the packet that caused the error. Insert and flush writes the reassembled stream, but includes the packet that caused the error. Insert no flush includes the error-causing packet and continues stream reassembly.</td>
</tr>
<tr>
<td></td>
<td>Reassembled packet size threshold range—Some evasion strategies attempt to evade detection by fragmenting the TCP header across multiple packets. Reassembling the stream in packets of uniform size makes this easier for attackers to slip traffic past the rules, so forensic analysis reassembles the stream using random packet sizes. Here you can set the upper and lower limits on the size of these packets.</td>
</tr>
<tr>
<td></td>
<td>Reassembled packet size seed value—Changing the seed value will cause forensic analysis to use a different pattern of packet sizes for stream reassembly. Running the analysis with a different seed value can catch signature matches that would otherwise escape detection.</td>
</tr>
<tr>
<td></td>
<td>Port List—Enabling the Port List option limits analysis to (or excludes from analysis) the given port numbers.</td>
</tr>
<tr>
<td><strong>HTTP URI Normalization</strong></td>
<td>Many HTTP-based attacks attempt to evade detection by encoding URI strings in UTF-8 or Microsoft %u notation for specifying Unicode characters. This preprocessor includes options to circumvent the most common evasion techniques. To match patterns against the normalized URIs rather than the unconverted strings captured from the wire, the VRT Rules use the uricontent option, which depends on this preprocessor. Without normalization, you would have to include signatures for the pattern in all possible formats (using the content option), rather than in one canonical version.</td>
</tr>
<tr>
<td></td>
<td>Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the HTTP preprocessor to the log, but not the Forensic Summary Window.</td>
</tr>
<tr>
<td></td>
<td>Maximum directory segment size—Specifies the maximum length of a directory segment (i.e., the number of characters allowed between slashes). If a URI directory is larger than this, an alert is generated. 200 characters is reasonable cutoff point to start with. This should limit the alerts to IDS evasions.</td>
</tr>
<tr>
<td></td>
<td>Unicode Code Page—Specify the appropriate country code page for the traffic being monitored.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>HTTP URI Normalization (Continued)</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lookup Unicode in code page</td>
<td>Enables Unicode codepoint mapping during pre-processing to handle non-ASCII codepoints that the IIS server accepts.</td>
</tr>
<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 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.</td>
</tr>
</tbody>
</table>
## Importing Snort rules

After getting the Snort rules from [http://www.snort.org](http://www.snort.org), follow these steps to import them into Observer.

1. In Observer, choose Capture > GigaStor Control Panel > Forensic Analysis tab.
2. Right-click anywhere on the Forensic Analysis tab and choose Forensic Settings from the menu. The Select Forensic Analysis Profile window opens.
3. Choose your profile and click Edit. The Forensic Settings window opens.
4. At the bottom of the window, click the Import Snort Files button.
5. Locate your Snort rules file and click Open. Close all of the windows. After you import the rules into Observer you are able to enable and disable rules and groups of rules by their classification as needed.

   Observer displays a progress bar and then an import summary showing the results of the import. Because Observer’s forensic analysis omits support for rule types and options not relevant to a post-capture system, the import summary will probably list a few unrecognized options and rule types. This is normal, and unless you are debugging rules that you wrote yourself, can be ignored.

6. To use the Snort rules you just imported, right-click anywhere on the Forensic Analysis tab and choose Analyze from the menu.
Chapter 13: Change Log

Recent documentation changes

In addition to fixing typographical and grammar errors, these changes were also made to the documentation:

July 19, 2013 Observer

- Added instructions for how to enable 256-bit AES encryption for at-rest captured data. See How to encrypt captured data on page 97.
- Added network port information that was originally listed in a separate publication. See Ports used by Network Instruments products on page 8.
- Added instructions for exporting web report data to XML or third-party tools. See How to export report data to XML.
- Added conceptual information about the "Track only new connections in each collection interval" setting. See What is Application Performance Analysis?
- Added new information to the table listed in Choosing your network trending types, including a setting to automatically delete old trending data after a set length of days.
- Updated information for deleting trending data. See Deleting your network trending data files.
## Numerics

<table>
<thead>
<tr>
<th>Numerics</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>25901 (port)</td>
<td>8, 8, 114, 121, 121</td>
</tr>
<tr>
<td>25903 (port)</td>
<td>8, 114, 121</td>
</tr>
<tr>
<td>32-bit</td>
<td>108, 108</td>
</tr>
<tr>
<td>64-bit</td>
<td>108, 108</td>
</tr>
<tr>
<td>64-bit, RAM</td>
<td>108</td>
</tr>
<tr>
<td>802.11</td>
<td>100, 100, 103</td>
</tr>
<tr>
<td>802.1Q</td>
<td>117</td>
</tr>
</tbody>
</table>

## Default

<table>
<thead>
<tr>
<th>Default</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>33, 119</td>
<td></td>
</tr>
</tbody>
</table>

## A

<table>
<thead>
<tr>
<th>Access point statistics</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>17, 17, 20, 20</td>
</tr>
<tr>
<td>activate and dectivate</td>
<td>61, 61</td>
</tr>
<tr>
<td>active instance vs. passive instance</td>
<td>101</td>
</tr>
<tr>
<td>Activity Display</td>
<td>30</td>
</tr>
<tr>
<td>Activity Display tool</td>
<td>30</td>
</tr>
<tr>
<td>adapter</td>
<td></td>
</tr>
<tr>
<td>see network adapter</td>
<td>19, 19</td>
</tr>
<tr>
<td>see network adapter</td>
<td>19, 19</td>
</tr>
<tr>
<td>Add Rename Filter Profile</td>
<td>56</td>
</tr>
<tr>
<td>Add/Edit Protocol Filter</td>
<td>56</td>
</tr>
<tr>
<td>adding</td>
<td>35, 35</td>
</tr>
<tr>
<td>adding derived definitions</td>
<td>35, 35</td>
</tr>
<tr>
<td>Address Filter</td>
<td>56</td>
</tr>
<tr>
<td>AES 97</td>
<td></td>
</tr>
<tr>
<td>Alarm Settings</td>
<td>83</td>
</tr>
<tr>
<td>configuring</td>
<td>83, 83, 87</td>
</tr>
<tr>
<td>customizing</td>
<td>87, 87, 87, 87, 87, 87</td>
</tr>
<tr>
<td>enabling</td>
<td>83, 83, 84, 84</td>
</tr>
<tr>
<td>exporting</td>
<td>88, 88, 136, 136</td>
</tr>
<tr>
<td>filter-based, creating</td>
<td>85, 85</td>
</tr>
<tr>
<td>high latency</td>
<td>84</td>
</tr>
<tr>
<td>importing</td>
<td>89, 89, 136, 136</td>
</tr>
<tr>
<td>resetting</td>
<td>86, 86, 86</td>
</tr>
<tr>
<td>retransmissions, excessive</td>
<td>84</td>
</tr>
<tr>
<td>alias files</td>
<td>142</td>
</tr>
<tr>
<td>allocating</td>
<td>111</td>
</tr>
<tr>
<td>analyzer connection</td>
<td>114</td>
</tr>
<tr>
<td>Anyone account</td>
<td>114, 114</td>
</tr>
<tr>
<td>Apache Web Server</td>
<td>70, 139</td>
</tr>
</tbody>
</table>

## B

<table>
<thead>
<tr>
<th>Backup</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>installation</td>
<td>2</td>
</tr>
<tr>
<td>bad TCP checksums</td>
<td>116</td>
</tr>
<tr>
<td>troubleshooting</td>
<td>116</td>
</tr>
<tr>
<td>Bandwidth Utilization</td>
<td>19</td>
</tr>
<tr>
<td>Bandwidth Utilization - Full Duplex Display</td>
<td>19</td>
</tr>
<tr>
<td>Bandwidth Utilization tool</td>
<td>19, 19, 20</td>
</tr>
<tr>
<td>Bandwidth Utilization with Filter</td>
<td>20</td>
</tr>
<tr>
<td>best practices</td>
<td>101</td>
</tr>
<tr>
<td>BFR</td>
<td>13, 53, 53, 53</td>
</tr>
<tr>
<td>BIOS memory hole</td>
<td>108</td>
</tr>
<tr>
<td>broadcast and multicast storms</td>
<td>30</td>
</tr>
<tr>
<td>buffer</td>
<td>107</td>
</tr>
<tr>
<td>buffer size</td>
<td>101</td>
</tr>
<tr>
<td>buffer statistics</td>
<td>107</td>
</tr>
<tr>
<td>buffer, see capture buffer and statistics buffer</td>
<td>107</td>
</tr>
<tr>
<td>buffers</td>
<td>101, 103, 103, 103, 108, 110</td>
</tr>
<tr>
<td>circular</td>
<td>49, 49</td>
</tr>
<tr>
<td>configuring</td>
<td>41, 47</td>
</tr>
<tr>
<td>replaying</td>
<td>71</td>
</tr>
</tbody>
</table>

## C

<table>
<thead>
<tr>
<th>Calculate Cumulative Bytes</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>72</td>
<td></td>
</tr>
<tr>
<td>CAP</td>
<td>53</td>
</tr>
<tr>
<td>capture buffer</td>
<td></td>
</tr>
<tr>
<td>32-bit Windows</td>
<td>107</td>
</tr>
<tr>
<td>64-bit Windows</td>
<td>107</td>
</tr>
<tr>
<td>IP defragmentation</td>
<td>142</td>
</tr>
<tr>
<td>Max Buffer Size</td>
<td>107</td>
</tr>
<tr>
<td>RAM limitations</td>
<td>107</td>
</tr>
<tr>
<td>size</td>
<td>107</td>
</tr>
<tr>
<td>TCP stream</td>
<td>142</td>
</tr>
<tr>
<td>capture card</td>
<td></td>
</tr>
<tr>
<td>driver requirements</td>
<td>3</td>
</tr>
<tr>
<td>capture card</td>
<td>3</td>
</tr>
<tr>
<td>Capture Decode</td>
<td>74</td>
</tr>
<tr>
<td>Capture Graph</td>
<td>47</td>
</tr>
</tbody>
</table>
Capture Internet Observer 14
Capture Pairs (Matrix) 16
Capture Protocols 17
Capture Summary 24
Capture Top Talkers 21
Capture VLAN 32
captures
  see packet captures 51
see packet captures 51
capturing 50
CAPWAP Control 33
CAPWAP Data 33
CIR 83
circular 49, 49
Cisci 6xxx switches
troubleshooting 120
Cisco 6xxx switches 120
CME RLC 33
collision test 119, 119
command line 63, 63
command line, enabling 63, 63
Committed Information Rate 83
common issues 113
common problems with 114, 114
Configure IP Application List for Internet Observer
Statistics Dialog 14
Configure IP Application Ports Dialog 15
configuring 19, 41, 41, 41, 47, 47, 49, 49, 51, 83, 83, 87
  Expert Information 47
  partial packets 49, 49, 49
Connection Dynamics 67
connections 14, 14, 14, 14, 16, 16, 16, 21
creating 50, 61
customizing 87, 87, 87, 87, 87

D
dashboard 6, 6
  see Observer 6
see Observer 6
daylight savings time 119
Daylight Savings Time 119, 119
decodes
keyboard shortcuts 76
decoding 67, 67, 72, 78, 79, 79, 103, 103, 103
  expert analysis 67
  geolocation 13
NetFlow 79
  packet captures 67, 67, 67, 67, 78
  encrypted 70, 70, 139, 139
sFlow 79
  user interface 72, 72, 74, 74
  using third party decoder 13, 13
defining its purpose 111
definition 100
definitions, restoring 38, 141
denial of service 142
derived application definitions 35
derived applications 9
disabling 81
Discover Network Names 118, 118, 118
VLANs 118
Display Protocols for Selected Station 17
Display Stations sending Selected IP 67
DLCI Address Filter 56

DLCl CIR Setup 83
DMP 53, 68
DNS 54
driver error support 24
driver requirements 3, 3, 3
duplicate, removing 50, 68, 68
dynamic 36

E
Edit IP Application Port Dialog 14
Edit Pager Entry Dialog 67
Edit Probe User Account Dialog 67
Edit Statistics Memory Configuration 67
editing 37
effects of packet capture 110
efficiency 96
enabling 83, 83, 84, 84
ENC 53
encrypted 70, 70, 139, 139
encryption 9, 9, 9, 9, 9, 91, 91, 91, 91, 91
  AES 97
  see also security 97
encryption key 114
Error Filter 56
ers 24, 25, 25, 25, 28
  Ethernet 28
Errors by Station 25
Errors by Station tool 25
ErrorTrak 1
Ethernet 28, 100, 100, 103
  ARP inspection 142
  errors 28
  full-duplex 103
Ethernet Physical Port Filter 56
Ethernet Vital Plot Properties 24
Ethernet Vital Signs 24
Ethernet Vital Signs and Collision Expert 24
  expert analysis 67
  Expert Connection Dynamics 67
  Expert Fibre Events 67
  Expert Global Settings 67
  Expert Global Settings - Connection Dynamics 67
  Expert Global Settings - General 67
  Expert Global Settings - IP Range 67
  Expert Global Settings - TCP IP 67
  Expert Global Settings - Time Interval Analysis 67
  Expert Global Settings - What-if Analysis 67
  Expert ICMP Events 67
  Expert IPX Events 67
  Expert NetBIOS Events 67
  Expert Probe 103, 103, 103
  Expert Reconstruct Streams 67
  Expert Server Analysis 67
  expert summary 103
  Expert Summary 67
  Expert TCP Dump 67
  Expert TCP Events 67
  Expert Time Interval Analysis 67
  Expert UDP Events 67
  Expert VoIP 67
  Expert VoIP Analysis 67
  Expert VoIP Events 67
  Expert VoIP Settings - General 67
Expert VoIP Settings - MOS 67
Expert What-If Analysis 67
Expert Wireless Events 67
exporting 39, 39, 88, 88, 136, 136, 137, 137
server applications 35, 39, 39, 137, 137

F
FDC 53
FDDI 53, 53, 53, 53, 67
FDDI Errors by Station 24
FDDI Vital Signs 24
feature suitability 50
Federal Information Processing Standards 90
Fibre Channel Vital Signs 24
Filter Names 56
filter-based, creating 85, 85
filtering 56
post-filters
applying 63, 63, 78
command line 63
command line, enabling 63
pre-filters
"exclude" rules 56
creating 56, 56, 61
exporting 56
importing 56
scope 61
pre-filters, scope 62
filters
activate and deactivate 61, 61
command line 63
command line, enabling 63
see also filtering 56
partial packets 50
Filters 56, 57
Find Packet 78
FIPS 90, 90
firewall 8, 121
firewall, ports 114
FIX 74
forensic analysis 142
format
XML 53
formats 53
BFR 53
CAP 53
DMP 53, 68
ENC 53
FDC 53
PCAP 53
TRC 53
from multiple sources 51
from unknown sources 69, 69
FTP 37, 37, 37
full-duplex 103
full-duplex Ethernet 103

G
Gen2 22, 42
Gen2 card
passive probe instance 101
performance 101
probe instance warning 101
recommendations 112
GeoIP Settings 13
geloocation 13, 13
Gigabit 103
gigabytes 107, 107
GigaStor 111
collision test 119
RAM 111
recommendations 112
reserved memory 111
traffic generation 119
GigaStor capture 101, 103
GigaStor Control Panel
forensic analysis 142
Snort 142
Snort rules 147
Graph Display Properties 67
Graph Display Properties - Graph Time 67

H
H.323 67
hardware acceleration 112
hardware requirements 1
high latency 84

I
ICMP Expert 67
IIS Web Server, Windows 70, 139
importing 34, 34, 39, 39, 39, 89, 89, 136, 136, 137, 137
alarms 88, 88, 89, 89, 89, 136, 136, 136, 136
server applications 39, 137
in a switched environment 105
individual stations 16, 16, 16, 21
installation 2
Interface Properties 67
interface switching 103
Internet Observer 14
Internet Observer Internet Patrol 14
Internet Observer IP Subprotocols View 14
Internet Observer Settings 14
Internet Observer tool 14, 14, 14
Internet Patrol 14
Internet Patrol - Pair Circle 14
IP address
IPv6 142
NAT 119
IP defragmentation 142
IP flow 142
IP Fragment Bits Filter 56
IP Fragment Offset Filter 56
IP masquerading, see NAT 119
IP Pairs - Pair Circle 67
IP Properties 67
IP Subprotocols 67
IPv4 Options Filter 56
IPv4 TOS Precedence 50
IPv6 12, 142, 142
IPv6 Address representation 67
IPv6 Flow Label 50
IPv6 Options Filter 56
IPv6 Traffic Class 50
Jitter 67

K
keyboard shortcuts 76

L
Layer 3 Switch 118
LDAP 61, 61
licenses
  redeeming 2
  troubleshooting 2
List Bar Display Properties 67
List Display Properties 67
load 18
  preprocess settings 142
load, preprocessor 101
load, testing 22, 22, 22, 22, 22
loading 53
local probe 5
Log Window Settings - Event Filter 81
Log Window Settings - Log Files 80
logging 80
  disabling 81

M
MAC addresses 118
MAC Properties 67
matching between probe and analyzer 114
Max Buffer Size 107
Mean Opinion Score (VoIP Expert) 67
megabytes 101
memory management 107
memory tuning 107
memory, see RAM 110
Microsoft Lync Server 70, 139
mirror port 105
mirror port, see also SPAN ports 105
missing 52, 115
Modify Observer Reserved Memory dialog 67
MOS Settings 67
moving through RAM 110
MPLS 103
MPLS Filter 56
Multi Probe 103, 103
Multicast Pitch 33
Multiple Filters 56

N
NAT 119, 119, 119
NetFlow 79, 103, 119
decoding 79
  TAPs and 119
network 22, 22, 24, 24, 24, 25, 26, 30
  errors 25
  load 18
  load, testing 22, 22, 22, 22, 22
  summary 24, 24
troubleshooting 24, 24, 24, 24
utilization 18, 19, 19, 20, 20, 23, 23, 24, 24
Network Activity Display Properties 30
network adapter
  configuring 19
  Gen2 22, 42
Network Errors Settings 25
network load 18, 22, 22, 22, 22, 22
network masquerading, see NAT 119
Network Summary 24
Network Summary tool 24
network trending 103, 114
server profiles 142
Network Trending Settings - MOS 67
Network Vital Signs tool 24
NIC 103
  missing 115
NIMS 9, 9, 9, 9, 9, 9, 9, 94, 103
NIProbe.exe 2
  not connecting 114
Notify Probe User 50
Numeric Value Filter 56

O
Observer 91
  alias files 142
dashboard 6, 6
  encryption 9, 91
feature suitability 50
password protecting 93
ports used 8, 121
regulation compliance 90
security 91
supported protocols 122
switching to probe 103
system requirements 1
user interface 5, 7
Observer General Options - folders 67
Observer General Options - IPv6 67
Observer General Options - Security 67
Observer General Options Tab 67
observer.exe 2
OpenView 84
OR filter example 62

P
packet 142
packet alert threshold 142
packet captures
  from unknown sources 69
packet capture 110
  119
    active instance vs. passive instance 101
    buffer 107
daylight savings time 119
    decoding 103
    RAM 110
    reassembling 142
Packet Capture on Multiple Instances Settings 51
Packet Capture Options 47
Packet Capture Schedule 51
  configuring 41, 41, 47, 47, 49, 49, 51
    Expert Information 47
    partial packets 49, 49, 49
creating 50
decoding 67, 67, 72, 78
efficiency 96
encrypted 70, 70, 139, 139
filtering 56
from multiple sources 51
from unknown sources 69
loading 53
replaying 71
saving 53, 53, 77
scheduling 51, 51
security 96
sharing 95
timestamps 47
transferring 52
wireless 1
packet fragmentation 142
Packet Length Filter 56
packet storms 30
Packet Time Filter 56
Packet View Settings - Column Order 67
Packet View Settings - Configure SNMP MIBs 67
Packet View Settings - General 67
Packet View Settings - Protocol Forcing 67
Packet View Settings - Summary 67
packets 21, 50
capturing 50
duplicate, removing 50, 68, 68
Expert Information 47
Expert Information, excluding 47
missing 52
moving through RAM 110
RAM 110
saving 77
searching for 78
sizes 21
Pair Statistics (Matrix) 67
Pair Statistics Settings 67
Pair Statistics Settings - List 67
Pair Statistics Settings - Pair Circle 67
Pair Statistics Settings - Statistics Settings 67
Pair Statistics tool 16
Partial Packet Capture for TCP/UDP Payload Filter 95
partial packets 49, 49, 49, 50
passive probe instance 101
password protecting 93
Pattern Filter 56, 57
PCAP 13, 53, 53, 53
performance 101
Phone Pager Schedule 67
port bonding 103
Port Filter 56
ports 34, 34, 36, 36, 36, 36, 37
dynamic 36
ports used 8, 121
Post Capture Filtering 63
post-filters
applying 63, 63, 78
command line 63
command line, enabling 63
pre-filters
creating 56, 61
scope 61, 62
preprocess settings 142
Probe administration, port required 8, 121
Probe Alarms Settings - Actions 87
Probe Alarms Settings - Alarm List 84
Probe Alarms Settings - Triggers 87
probe connection 114
probe instance
active 101, 107
active vs.passive 101
best practices 101
defining its purpose 111
definition of 101
memory tuning 107
passive 101
reserving memory 107
probe instance warning 101
probe instances
redirecting 54, 54
user accounts 93
Probe redirection error 114
probe, local 5
probes 50, 54, 91
common problems with 114, 114
definition 100
hardware acceleration 112
in a switched environment 105
not connecting 114
see probe instances 54
securing 91
software, versions 103
SPAN ports 103
switching to analyzer 103
VLAN access 114
see probe instances 54
promiscuous mode 1, 105
protected memory 105, 108, 110
Protocol Filters 57
Protocol Definitions and Server Application Discovery 67
Protocol Distribution 17
Protocol Distribution Settings 17
Protocol Distribution Statistics 17
Protocol Distribution Statistics Switched 17
Protocol Distribution tool 17
Protocol Filter 56
protocols 15, 15, 17, 17, 17, 122
statistics 17
protocols supported 122

Q

Quality of Service (QoS) 67

R

RAID 101, 101
RAM 110, 110, 110, 111
allocating 111
buffer size 101
effects of packet capture 110
formula 107
GigaStor 111
limitations 107
packet capture 101, 107
see also buffer 107
see also protected memory, user memory, and reserved memory 105
recommendations 108
resizing 105
statistics 107
TCP stream reassembly 142
tuning 107
used in Observer 105
sampling divider 114

top talkers 21, 21, 21, 21
utilization 19, 20, 23, 24
VLAN 32, 32, 32
wireless 17, 26, 26

statistics buffer 107, 107
Statistics Memory Allotment Page 67
statistics queue buffer 105, 108, 110, 110, 111, 112
stream reconstruction 67
Stream Reconstruction 67

Subnet mask 50

summary 24, 24

supported protocols 122, 122

switching to analyzer 103
switching to probe 103
synchronization 119

system requirements 1

T

TAP

NetFlow 119

TAPs and 119
TCP 119, 142, 142, 142, 142, 142, 142, 142, 142, 142, 142, 142
TCP 25901 8, 121
TCP 25903 8, 121
TCP Expert 67
TCP stream 142
TCP stream reassembly 142
TCP/IP 119
testing

network load 22, 22, 22, 22, 22
third party decoder 13
third-party capture card
driver requirements 3

Time Interval Analysis

using 67
time synchonization 119
timestamps 47

packet captures 47

Tivoli 84

Token Ring Errors by Station 25
Token Ring Vital Signs 24

Toolbar Setup 7
top talkers 21, 21, 21, 21
Top Talkers 30, 107
Top Talkers Statistics 21
Top Talkers tool 21, 21
top talkers, defined 21
topologies 100, 103

802.11 100

Ethernet 100

traffic generation 119, 119

Traffic Generator 22
Traffic Generator Settings 22
Traffic Generator tool 22
transferring 52
transferring packet captures 52

TRC 53

triggers 103, 114

troubleshooting 24, 24, 24, 24, 24, 116, 120

analyzer connection 114
bad TCP checksums 116
broadcast and multicast storms 30
Cisco 6xxx switches 120

common issues 113

network 22, 22, 24, 24, 24, 25, 26, 30

packet storms 30

probe connection 114

slow probe system 114

VLAN Statistics tool 116, 117
VLAN visibility 118

TTL Hop Limit 50

U

UDP 25903 8, 121
UDP Expert 67

updating

Observer 2

user accounts 93, 93, 93, 93, 94

security 93, 93, 93, 94

user interface 5, 7, 72, 74

see Observer 5

user memory 105

see user accounts 94

user permissions

see user accounts 94

users 103, 114

simultaneous 103

using 67, 67, 67

using third party decoder 13, 13

utilization 18, 19, 19, 19, 20, 20, 20, 20, 23, 23, 23, 24, 24

Utilization History 23

Utilization History tool 23

Utilization Thermometer Mode 23

Utilization Thermometer tool 24

V

variable name 142

virtual adapter 101

virtual machine 1

Virtual Tap 67

Virtual Tap Settings Dialog 67

VLAN 32, 32, 32, 117, 117

"No VLAN" 116, 117

VLAN access 114

VLAN Filter 56

VLAN ISL Filter 56

VLAN Properties 32

VLAN Statistics 32, 32, 117

VLAN Statistics tool 32, 116, 117

VLAN visibility 118

VLANS 117, 117, 118

Discover Network Names 118

SPAN port 117

VMONI 115

VMONI Protocol Analyzer 115

VoIP 67, 103

VoIP RTP RTCP Graph 67

VPN 119

W

WAN 53

WAN alarms 83

WAN Conditions Filter 56

WAN Load 30

WAN Port Filter 56

WAN vital plot properties 24
WAN Vital Signs 30
WAN Vital Signs by DLCI 24
Web Observer 16
WEB Observer Settings 16
Web Observer tool 16
Web Server, Apache 70, 139
Web Server, Windows IIS 70, 139
Windows
- 32-bit 108
- 64-bit 107, 108
- reserved memory from 103
Windows IIS Web Server 70, 139
Windows protected memory 105
wireless 1, 17, 17, 20, 20, 26, 26, 100, 103, 103
- access point statistics 17, 17, 20, 20
- signal strength conversion 26
- site survey 26
Wireless Access Point Filter 56
Wireless Access Point Load Monitor 17
Wireless Access Point Settings 17
Wireless Access Point Settings - List 17
Wireless Access Point Statistics 17
Wireless Access Point Statistics tool 17
Wireless Channel Filter 56
Wireless Data Rate Filter 56
wireless interference 26
Wireless Network Errors by Station 25
wireless packets, raw 1
Wireless QoS 50
Wireless Signal Strength Filter 56
Wireless Site Survey 26
Wireless Site Survey - Channel Scan 26
Wireless Site Survey - Ctrl. Frames 26
Wireless Site Survey - Data Frames 26
Wireless Site Survey - Frame Types 26
Wireless Site Survey - General Info 26
Wireless Site Survey - Mgmt. Frames 26
Wireless Site Survey - Signal 26
Wireless Site Survey - Speeds 26
Wireless Site Survey tool 26
Wireless Vital Signs 24
Wireshark 13, 53
Word Report Options 67

X
- XML 53, 53

Symbols
- "No VLAN" 116, 117