Ethernet Probe
Ethernet Probe

*Ethernet Probe*
### Table of Contents

- Change log.............................................................................................................6
- About GigaStor probes, Probe appliances, and probe instances..............................7
  - Introducing Probes.................................................................................................7
  - How probes work with switches...............................................................................8
  - Deploying probes in your network............................................................................8
    - Monitoring half-duplex and full-duplex Ethernet links...........................................9
    - Monitoring wireless traffic.....................................................................................10
- Deciding where to place probes in your network.....................................................10
- What is a probe instance?...........................................................................................12
- Ports used by Network Instruments products..........................................................15
- Installation................................................................................................................16
  - Unpacking and inspecting the parts..........................................................................16
  - Installing the Ethernet Probe....................................................................................16
  - Setting the probe’s IP address..................................................................................18
- Technical specifications.............................................................................................20
  - Ethernet Probe.......................................................................................................20
- Expert Probe software................................................................................................23
  - System requirements and installing or upgrading the software...............................23
    - Installing the wireless NIC driver on Windows 7/Vista..........................................24
    - Installing a third-party USB wireless adapter.......................................................25
    - Capture card driver requirements.........................................................................26
- Licensing and updating..............................................................................................28
- Upgrading the probe software....................................................................................29
  - Upgrading the probe software directly.....................................................................29
  - Remotely upgrading the probe software from within the Observer analyzer.............30
- Installing Windows updates and updating virus protection.......................................30
- Backing up your probe...............................................................................................31
- Using the NetFlow features in Observer....................................................................32
- Monitoring a wireless access point..........................................................................33
Configuring a probe's name and other probe options................................................................. 33
Probe Properties field-level descriptions.......................................................... 36
Configuring the probe's adapter speed, ToS/QoS precedence, and statistics sampling..................... 39
Enabling Network Trending and setting which statistics are collected........................................ 40
Configuring probes to collect data even when not connected to an analyzer................................. 41
Changing the monitored network adapter.............................................................................. 41
Connecting to a probe for the first time from the Observer analyzer........................................... 42
Connecting to a probe instance from an Observer analyzer..................................................... 42
Creating a probe instance....................................................................................................... 43
Connecting the probe to an Observer analyzer......................................................................... 44
Connecting the Multi Probe or Expert Probe to an Observer analyzer....................................... 44
When to use a virtual TAP........................................................................................................ 45
  Using the probe as a virtual TAP............................................................................................ 50
  Configuring VMware ESX Server............................................................................................ 51
Bonding probe instances to specific ports on the Gen2 card through virtual adapters.................. 53
Capturing full-duplex traffic...................................................................................................... 53
Switching between the probe and analyzer user interfaces......................................................... 53
Configuring access permissions for probe instances.................................................................. 54
Restricting access to probes with user accounts....................................................................... 55
Customizing statistics and capture buffers for probe instances.................................................. 56
Setting the total system memory reserved for probes............................................................ 56
Setting the probe’s time clock synchronization settings........................................................ 57
Configuring connections to multiple NICs or Observer analyzers........................................... 57
Using the Expert Probe software............................................................................................ 57
Using additional storage volumes for your GigaStor active instance........................................ 58
Creating GigaStor active and passive probe instances............................................................ 59
VoIP Expert, Application Performance Analysis, and Application Transaction Analysis................ 59
Creating an sFlow collector...................................................................................................... 60
Creating and configuring an MPLS probe instance.................................................................... 60
Creating a NetFlow collector or NetFlow Trending collector.................................................... 60
Forcing users to authenticate before connecting to a probe....................................................... 62
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 commitment by DEVELOPER. DEVELOPER assumes no responsibility or liability for any errors or inaccuracies that may appear in any SOFTWARE manual.

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

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

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

Liability

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

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

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

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

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

Ownership and Confidentiality

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

Technical Support

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

US & countries outside Europe at (952) 358-3800
UK and Europe at +44 (0) 1959 569880
By fax (depending on where you are located):
US & countries outside 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.
Chapter 1: Change log

In addition to fixing typographical and grammar errors, these changes were also made to the documentation:

These documentation changes were made:

February 12, 2013:
December 18, 2012:
Chapter 2: About GigaStor probes, Probe appliances, 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 1 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.
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.

Deploying probes in your network

You need visibility into every corner of the network, from the edge to the core. A distributed analysis solution can provide the coverage you need, but where should you deploy probes for maximum visibility at minimum cost? Because every network is different, the examples shown may not look like your network, but the concepts demonstrated will be applicable to most situations.
Successfully deploying a distributed analysis solution on your network requires that you understand some basic concepts about distributed analyzers and network technologies.

In deploying probes, make sure that you understand the visibility requirements unique to your deployment goals and the design of the network you are analyzing. For 100% visibility of traffic:

- Deploy TAPs and specialized high-speed probes on core switch connections to servers, server farms, and other critical network infrastructure.
- Deploy less-costly probe appliances on switch monitor (e.g., SPAN/mirror) ports at the edge of your network.

Most commercial packet analyzers, like Observer, are distributed. Packet captures and some analysis are performed by distributed agents called probes, which in turn send the packets (or the analysis results—e.g., bandwidth utilization statistics, most active stations, etc.) to analyzers for further processing and display. Distributed analysis is the only practical way to make different parts of a switched or wireless network visible and therefore manageable. From a single analyzer you can monitor and view traffic from anywhere on the network where a probe has been deployed, from any type of media or topology (Ethernet, wireless, and so on).

**Monitoring half-duplex and full-duplex Ethernet links**

If your IT department is typical, you have a limited budget. Therefore, before you spend any money on analyzers, TAPs, and probes, you should assess what kinds of traffic you need to see and what kinds of traffic you want to see for effective network management. This allows you to deploy the correct technology needed to meet your particular goals.

On wired networks with multiple switches, most of the stations are plugged into half-duplex ports, even if the backbone or server connections are Gigabit Ethernet or greater. Being able to see the traffic local to each switch at the edge can give you insight unavailable from tapping the core connections. For example, client-to-client communications are invisible from the backbone or server connections. It can also be useful to isolate a segment when troubleshooting client-to-core connection problems. The best way to achieve this kind of visibility is to configure SPAN/mirror sessions on each switch, and then direct the SPAN/mirror output to half-duplex probes.

A SPAN/mirror port duplicates the traffic on a switch port or a group of ports, and sends the copied data to an analyzer. Using a SPAN/mirror port and half-duplex probes are inexpensive and convenient, but cannot give you all the visibility you need to manage and troubleshoot a network that also includes gigabit, WAN, and wireless infrastructure. For networks that include these other topologies, other solutions are needed.

Because full-duplex Ethernet lies at the core of most corporate networks, ensuring completely transparent analyzer access to full-duplex Ethernet traffic is critical. A SPAN/mirror port access is fine for the half-duplex Ethernet connections to stations at the edge, but may be unable to keep up with the higher-traffic full duplex links to the core.

There are three common ways for a probe or analyzer to gain access to full-duplex streams of data flowing on Ethernet cables:

- Connect the probe to a SPAN/mirror port. A SPAN/mirror port can provide a copy of all designated traffic on the switch in real time, assuming bandwidth utilization is below 50% of full capacity.
Deploy a port aggregator (sometimes called an "Aggregator TAP") on critical full-duplex links.

Deploy a TAP (Test Access Port) on critical full-duplex links to capture traffic. For some types of traffic such as full-duplex gigabit links, TAPs are the only way to guarantee complete analysis, especially when traffic levels are high.

Connecting a probe to a switch SPAN/mirror port or aggregator can provide adequate visibility into most of the traffic local to the switch, assuming that bandwidth utilization is low. However, if the aggregate switch traffic ever exceeds 50% bandwidth saturation, SPAN/mirror ports and aggregators simply cannot transmit the data fast enough to keep up; dropped packets (and perhaps sluggish switch performance) will result. This is because SPAN/mirror ports and aggregators are designed to connect to a standard NIC, which allows them only one side of the full duplex link to transmit data. A TAP, however, is designed to connect to a dual-receive capture card. By sending data on both sides of the link to the capture card, a TAP has double the transmission capability of the other options, allowing it to mirror both sides of a fully saturated link with no dropped packets and no possibility of degrading switch performance. And regardless of utilization, SPAN/mirror ports filter out physical layer error packets, rendering them invisible to your analyzer.

The most critical parts of your network are almost by definition those that see the most traffic. If your network includes a business-critical link (for example, the gigabit link that connects the customer service database to the core switch), a TAP connected to a compatible probe or analyzer is the only way to ensure both complete visibility and complete transparency to the network, regardless of how saturated with traffic the link becomes.

### Monitoring wireless traffic

If you place an Ethernet Probe on a switch to which a wireless access point is connected, you will see the legitimate wireless station traffic connected to your wired network. What you will not see is the 802.11 headers crucial to understanding wireless-specific problems and security threats. You will also not be able to see rogue access points, or illegitimate stations trying to associate with access points. In short, to see all RF signals on the air at your site, you need a wireless probe. In fact, you usually need more than one such probe to see all of the access points and stations (legitimate or illicit) deployed on the site.

### Deciding where to place probes in your network

To guarantee that every packet passing between every device on the network, errors and all, is available to your analyzer is practically impossible on a network with multiple switches. It would require placing a TAP on every link to each switch. Fortunately, you need only place probes where the traffic is significant enough to warrant the expense, and a lot of traffic is not that critical.

Ultimately, where to deploy probes depends on the design of your particular network and where you require visibility. A probe only shows your analyzer the data that is visible to that probe. An Ethernet Probe's visibility, for example, is limited to what a particular switch's SPAN/mirror port can deliver. A specialized hardware probe connected through a TAP sees only the traffic traversing that link. If 100% coverage is important to you, install TAPs on all the high-speed critical links in or near the core of your network, and probes plugged into the SPAN/mirror ports of switches on the edge.
For example, placing TAPs on the full-duplex links that connect servers or server farms to core switches will give you complete visibility into all traffic between servers and their clients. Connecting additional half-duplex probe appliances to SPAN/mirror ports at the edge of the network will let you focus in on any segment or station on the network for detailed problem resolution.

Failure to deploy the right probes in the right place can result in “blind spots” on your network, and an incomplete picture can lead to inefficient troubleshooting and expensive mistakes.

<table>
<thead>
<tr>
<th>Gigabit Probe</th>
<th>Ethernet Probe</th>
<th>Wireless probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor server, link, and application</td>
<td>view top talkers</td>
<td>detect and respond to security</td>
</tr>
<tr>
<td>tweak or troubleshoot trunk performance</td>
<td>ensure corporate IT</td>
<td>detect and shut down rouge</td>
</tr>
<tr>
<td>troubleshoot workstation connections</td>
<td>troubleshoot workstation connections</td>
<td>troubleshoot 802.11 connections</td>
</tr>
</tbody>
</table>

Figure 1 shows where to places probes in a network. Figure 2 goes into greater detail about your options and what you gain or lose by placing probes at certain locations.

Figure 2: Where to place probes
Click to open a PDF diagram of your probe placement options.

**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 1 compares the features of active and passive probe instances with an Observer probe instance found on all non-GigaStor probes.
### Table 1: 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&lt;sup&gt;1&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better suited for troubleshooting</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Better suited for data capture</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start packet capture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Stop packet capture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Start GigaStor packet capture</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schedule packet capture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Change directories where data is stored</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Able to set permissions</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Able to redirect to different analyzer, etc.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<sup>1</sup> 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 4: GigaStor capture and packet capture through probe instances

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

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

Network Instruments probes and Observer use TCP port 25901 and 25903 to transfer data and commands between the probe and the Observer analyzer. You may need to modify your firewall rules to allow communication on these ports for Observer.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirection/connection request</td>
<td>TCP 25903</td>
</tr>
<tr>
<td>Probe administration</td>
<td>TCP 25903</td>
</tr>
<tr>
<td>Analyzer–Probe connection</td>
<td>TCP 25901</td>
</tr>
</tbody>
</table>
Chapter 3: Installation

Unpacking and inspecting the parts

Your probe includes a number of components. Take a moment after unpacking the kit to locate all of the parts.

- One rack-mountable probe system with a Gen2 card to capture traffic and an Ethernet network interface for management.
- One TAP kit for each link (two ports equal one link). Each TAP kit includes one nTAP, appropriate SFP media for your topology links, and the cables to connect the TAP to your probe. The SFP media is available as copper (TX) or optical (LX or SX).
- RJ-45 Ethernet cable for the management interface in your probe to connect to your switch.
- 64-bit Windows 7 restore DVD specific for your probe.
- Documentation and warranty information. Keep this information in a safe, accessible location.

Installing the Ethernet Probe

Getting your probe installed is the first step to greater visibility of your network. This topic covers installing your probe in the cabinet and connecting the probe to your network.

Do not attempt in-cabinet repairs of the your probe. The probe is very heavy!

1. Take the probe and all other components out of their packing materials.
2. Attach the rail to the rack in your cabinet. Instructions for installing the rail kits are provided in the rail kit box. The rails are for installation purposes only and are not designed for in-cabinet repairs.
3. Insert the supplied SFP connectors from the TAP kit into the open slots on the back of the Gen2 card(s) in your probe.
4. Install the probe into rails in your cabinet. Caution! The probe is heavy. Lift with care. Do not turn on the probe yet.

5. Use the Ethernet cable to connect the management network interface card (NIC) in the probe to the network.

6. Install the TAP into your cabinet or some other location. (If you are using a switch’s SPAN/mirror port, no TAP is required. Simply plug any straight-through Ethernet cable into the SPAN/mirror port on the switch into the ports on the Gen2 capture card and skip TAP related steps.)

7. Connect the TAP to your probe. Connect the TX port from your server, firewall, router, or switch to the Link A port on the TAP. Connect the TX port from your Gigabit switch to the Link B port on the TAP. Use the two analyzer cables to connect the analyzer port on the TAP to the Gen2 capture card in the probe. If you have more than one TAP, repeat for each one.
After connecting the probe and TAP to your network, the next step is to set the probe's IP address.

### Setting the probe’s IP address

It is unlikely that the probe’s default address will be the one you want to keep for it. Configuring the probe’s IP address allows you to put the probe on your network and to connect to it using an Observer analyzer or Windows Remote Desktop, both of which can be very useful since most probes are in distant or physically secure locations.

At this point you have physically installed the hardware and connected all the cables. Now, you must turn on the probe and configure the software. After this is complete all of your interaction with the probe can now be done remotely by connecting to the probe using anObserver analyzer or Windows Remote Desktop depending on what you want to accomplish.

1. Connect a monitor, keyboard, and mouse to the probe and ensure the probe is plugged into a power outlet. These are only needed temporarily to set the IP address. You can disconnect them when you are finished. Alternatively, you can use Windows Remote Desktop to connect to the probe to make these changes. The default IP address is 192.168.1.10.

2. Turn on the system. For some probes, such as the GigaStor, you may need to ensure the power switch is in the “on” position on the back of the probe. Then on the front of the probe, press the power button until the system starts to turn on.

3. Log in to the Windows operating system using the Administrator account. The default Administrator password is admin. After logging in, you may change this. See the Windows documentation, if necessary.

4. Click Start >Control Panel > Network and Internet Connections > Network Connections. Choose Local Area Connection and right-click and choose Properties.

5. Select Internet Protocol (TCP/IP) from the list and click Properties.

   ![Figure 7: Default TCP/IP settings](image)

6. Set the IP address, subnet mask, gateway, and DNS server for your environment and click OK. Click OK again to close the Local Area Connection Properties dialog. Close the Network Connections window.
7. Right-click the Probe Service Configuration Applet in the system tray and choose Open Probe Configuration.

![Figure 8: Probe Service Configuration Applet](image)

8. The Probe Administration window opens. Click the Probe Options tab.

![Figure 9: Probe Options](image)

9. By default the probe’s name is a random mix of letters and numbers. Change the name of the probe to something meaningful to you. The name might be the physical location of the probe. Click Apply to save your changes and close the window.

By default the GigaStor runs the Expert Probe as a Windows service and starts automatically at system startup. This prevents you from using the Observer analyzer on the GigaStor. You must connect to the GigaStor using Observer on a different system.

**After completing this task:**

Now that the probe’s name is configured, there are several other settings you will need to configure before you connect the probe to an Observer analyzer. All probes share some common settings. There are also settings unique to the type of probe you are using. All common and unique settings are described in [Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling](#).


Chapter 4: Technical specifications

All hardware probe appliances connect to any Observer Expert or Observer Suite analyzer on your network. All probe appliance units include the required cabling, copper, or optical nTAPs (depending on configuration selected), a 10/100/1000 Ethernet management port, and DVD-RW drive. Each unit is a dual-processor system with Windows.

Designed for comprehensive analysis of full-duplex this probe provides a direct, passive link into high-speed data streams. Using the Observer analyzer and probes, you are able to capture every packet, conduct real-time and retrospective network analysis, and view reports to the packet to resolve the problem. Having access to actual data packets, as opposed to agentless solutions like NetFlow, allows for better understanding of problems and enhanced troubleshooting ability. Among other things that can be done with your probe, you can:

- Track dozens of VoIP-specific metrics
- Verify VLAN setups
- Collect NetFlow and sFlow data
- Create long-term trending reports
- Reconstruct web pages, e-mails, IM, and VoIP calls
- Isolate transaction and conversation delay
- Track application session flows and failed transactions

Ethernet Probe

Figure 10: Ethernet Probe
Figure 11: Ethernet Probe dimensions

Designed for moderately used gigabit networks. The appliance is available in five configurations, all in a 1.3U rack-mountable case:

- Single port capture card with Single Probe software. This provides a single session to view traffic on a single 10/100/1000 segment.
- Single port capture card with Multi Probe software. This provides multiple sessions for multiple users on a single 10/100/1000 segment.
- Dual port capture card with Multi Probe software. This provides multiple sessions for multiple users on two 10/100/1000 segments.
- Single port capture card with Expert Probe software. This provides multiple sessions for multiple users, and provides real-time expert processing at the probe (instead of the analyzer) on a single 10/100/1000 segment.
- Dual port capture card with Expert Probe software. This provides multiple sessions for multiple users, and provides real-time expert processing at the probe on two 10/100/1000 segments.

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>2.275in (H) x 16.75in (W) x 26 in (Mounting Depth) (19 inch rack mountable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range Input Voltage</td>
<td>90 to 264 VAC</td>
</tr>
<tr>
<td>Line Frequency</td>
<td>47 to 63 Hz</td>
</tr>
<tr>
<td>Input Current Load</td>
<td>1A at 115VAC</td>
</tr>
<tr>
<td>Operating Temperature Range</td>
<td>0° to 40° C</td>
</tr>
<tr>
<td>Non-Operating</td>
<td>-20° to 71° C</td>
</tr>
<tr>
<td>Operating Relative Humidity (non-condensing)</td>
<td>5% to 95%</td>
</tr>
<tr>
<td>Platform</td>
<td>19-inch rack-mountable probe appliance that monitors your low utilization edge or remote branch locations. Choose from Single, Multi or Expert software probe version to run on the appliance.</td>
</tr>
</tbody>
</table>
| Memory | Single probe: 2 GB  
Multi and Expert Probe: 8 GB (4 for operating system, 4 for Observer) |
<table>
<thead>
<tr>
<th>Specification</th>
<th>Details</th>
</tr>
</thead>
</table>
| 10/100/1000 Link Support              | *Single probe*: 1 port  
*Multi and Expert Probe*: 1 or 2 ports |
| Capture card                          | Custom-designed, full-duplex Gen2 Gigabit Capture Card                |
| Hard drive                            | 500 GB / 7200 RPM                                                     |
| Key Remote Capabilities               | Web-based management  
Pager and email alerts                                                     |
| Power consumption                     | Input voltage: 100V-240V auto select  
Input frequency: 50/60Hz                                                     |
| Operating Temperature Range           | 32°F (0°C) to 104°F (40°C)                                             |
| Dimensions                            | 19 in (W) x 2.28 in (H) x 18.5 in (mounting depth)  
(Full probe depth with handles: 20.4 in)  
48.26 cm (W) x 5.79 cm (H) x 46.99 cm (mounting depth)  
(Full probe depth with handles: 51.82 cm) |
| Weight                                | 40 lbs (18.1 kg)                                                      |
| Operating system                      | 64-bit Windows 7                                                      |
Chapter 5: Expert Probe software

System requirements and installing or upgrading the software

Prerequisite(s):

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

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

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

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

This section describes the installation process and minimum requirements if you are installing the Observer analyzer or probe on your system.

<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</td>
<td>2 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Operating system</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</td>
<td>Server-class</td>
<td>Intel server-class</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

3. Choose to install:
   
   ◆ Observer.

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

   ◆ Expert Probe

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

**After completing this task:**

- License your software. See Licensing and updating.

- If you are using a wireless network adapter to capture traffic, see Installing the wireless NIC driver on Windows 7/Vista.

- If you are using a USB wireless network adapter to capture traffic, see Installing a third-party USB wireless adapter.

**Installing the wireless NIC driver on Windows 7/Vista**

See the information in Monitoring a wireless access point, which contains details about raw packets and promiscuous mode for the network card.

Follow these instructions to install the wireless driver for your network card:

1. Click Start and then right-click on the ‘Computer’ icon and choose Properties.
2. Click Device Manager.
3. Right-click on the wireless adapter you want to use as your capture card and choose Update Driver Software.
4. Choose “Browse my computer for driver software.”
5. Choose “Let me pick from a list of drivers on my computer.”
6. Click Have Disk and use the drivers in this location:
   
   C:\Program Files\Observer\DRIVERS\Wireless\Atheros_Vista

7. Click Next and Windows installs the driver for your wireless card.

To confirm that you correctly installed the driver for the wireless network card, open Observer. If the probe instance shows (Wireless) behind it, then it is correctly configured.
If the probe instance shows (Ethernet), then either the network card driver was not correctly installed or the probe instance is not configured to use that network card. You can confirm the correct network card is selected, by choosing Actions > Select Network Adapter Card.

**After completing this task:**
- License your probe by following the instructions in Licensing and updating.
- If your wireless network uses an encryption key, you must add the encryption key information. See Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling

### Installing a third-party USB wireless adapter

The Belkin F9L1101v1 N600DB USB wireless adapter was tested for use with your systems. The USB wireless adapter is only supported on systems running Windows Vista or 7 (32- or 64-bit).

**Note:** Only Belkin N600DB USB wireless adapters with the revision number “F9L1101v1” are compatible. These adapters have a Broadcom chipset. The second revision, “F9L1101v2” does not have a Broadcom chipset and is incompatible.

**CAUTION!** For some wireless adapters you must install the software for the USB wireless adapter before you attach the adapter to your computer. This is not an Observer requirement, but one of the wireless adapter. If you attach the USB adapter before installing the software, unplug the USB adapter, uninstall the software, restart your system, and then proceed with step 1.

1. Install the software that came with your USB wireless adapter.
2. Attach the USB wireless adapter to your system.
3. Choose Control Panel > Network and Sharing Center > Change adapter settings and then select your USB wireless adapter. Right-click and choose Properties.
4. On the Networking tab, click Install > Service > Add. Click Have Disk and locate this file:NiNdisMon.inf
   - 64-bit: C:\Program Files\Observer\DRIVERS\Wireless
   - 32-bit:C:\Program Files(x86)\Observer\DRIVERS\Wireless
5. Click OK to install the software as Windows service.
6. Restart your system. This allows the software and the adapter to be fully recognized by your system and the Windows service to start. Observer will not be able to use the wireless adapter until you restart.
7. Start Observer, select the probe instance you want to associate with the USB wireless adapter, and choose Actions > Select Network Adapter Card.
8. Choose the USB Wireless Adapter you just installed.

The probe instance is now configured to use the USB wireless adapter. You can confirm this because the word "[Wireless]" appears after the probe instance name, and the **Wireless 802.11** tab of the probe instance is visible.

**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.
Licensing and updating

A non-trivial amount of customer concerns deal with licensing and updating issues. This section serves as a good resource for licensing and updating help, but do not hesitate to call our support team should you need further assistance.

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

Probes require two unique numbers for licensing: an identification number and a license number. The license number determines whether the probe is a Single Probe (one probe instance) or a Multi Probe (capable of running multiple probe instances and allowing multiple Observer analyzers to connect simultaneously).

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

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

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

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

What type of license do I have?

Look closely at the license you received; it should say which version of Observer the license key applies to. If it does not, or you notice any other error, please call our support team for assistance.

Why is my license not working?

Each license 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 keys are version specific. Each license works only within equal major version numbers of the product. For example, an Observer 14.0 license can be used to activate 14.0 and 14.1, but not 13.0, 13.1, etc.

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

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?

If you lost the original information containing your license key, please call our support team to have it resent. We verify all requesters of their authenticity.
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.

Upgrading the probe software

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

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

When upgrading to version 16, if your operating system is 64-bit, the 64-bit version ofObserver or GigaStor is installed. If you previously installed a 32-bit version, the same installation directory is used.

Use information from this section when upgrading to a new major version of the probe software.

Before upgrading have the following available:

- Your probe license information.

If you are using encryption keys with Observer, you can continue to use your existing keys or transfer them to your probe (and analyzer) as necessary.

Upgrading the probe software directly

On the probe:

1. Run the ObserverSetup.exe installation program. Follow the on screen instructions and choose your probe type.
2. After the installer completes, restart the system. New major builds may have new drivers or other files that require a restart.
3. Connect the probe to an Observer analyzer.
Remotely upgrading the probe software from within the Observer analyzer

The Observer analyzer can push an upgrade of the probe software to the probe. When upgrading the probe software, you must restart the probe, and because of this, you should schedule the upgrade at a convenient time for the probe’s users.

If the probe software is running as a Windows service, you can choose to have the probe restart automatically. This is a configuration option in the probe’s settings and especially useful for remote probes where there is not a local administrator. See Configuring a probe’s name and other probe options.

1. In the Observer analyzer, select the probe instance you want to upgrade. Right-click and choose Probe or Device Properties. The Probe Properties window opens.
2. Click the Observer Autoupgrade tab. The Autoupgrade tab has three options:
   - Upgrading within minor versions (for instance, 15.0 to 15.1)
   - Upgrading within major versions (for instance, 15.0 to 16.0)
   - Forcing the autoupgrade of the probe
3. Select the second option: Autoupgrade Probe for major version release.
4. Click the Enter Licensing Information button.
5. Provide your probe’s license information. Click OK to close the licensing window.
6. Give the probe a few minutes to receive the new software version. The log window in the Observer analyzer shows that the analyzer is connecting to the probe and pushing the upgrade to the probe.
7. If the probe has not reconnected to the analyzer in about ten minutes, you may need to use Windows Remote Desktop to ensure that the probe is not displaying a Windows system message about restarting the system.

Installing Windows updates and updating virus protection

From time to time Microsoft releases updates for the operating system used for your probe or your virus protection software vendor updates their virus definitions. You should apply those updates as soon as feasible, however, you should always apply the updates manually. We do not recommend that you allow Windows to automatically install the updates and restart the system. By manually applying the updates you ensure that the system restarts properly and that the probe starts correctly whether running as a Windows service or as an application.

For your antivirus software, follow these guidelines:

- Ensure TCP ports 25901 and 25903 are open. All Network Instruments products communicate on these ports.
- Ensure UDP ports 25901 and 25903 are open if you use NIMS.
For all probes, disable any scanning of the Observer installation directory (typically C:\Program Files\Observer) and of D: (RAID) drive as scanning greatly diminishes the performance of writing data to disk.

The performance of the operating system may be greatly diminished when using antivirus software.

**Backing up your probe**

This section describes how to back up a system running the Observer analyzer. While your probe may not have all of these directories or files. If it does, you should back them up. Use whatever backup method or software is best for you, which, at a minimum, would be manually copying these to a different drive.

To make a complete backup of Observer and move it to a new machine you must do the following:

1. Install Observer on the new system.
2. Copy the files and directories in Table 1 from the backup location to the new system.

These are the default directories for:
- 32-bit Windows: C:\Program Files (x86)\Observer
- 64-bit Windows: C:\Program Files\Observer.

**Table 2: Directory or files to back up**

<table>
<thead>
<tr>
<th>Directory or file</th>
<th>Description</th>
</tr>
</thead>
</table>
| Network Trending | C:\Program Files\Observer\NetworkTrending  
This contains your Network Trending data. If you have changed the default location for Network Trending data, you must back up the new location. Use Options > Observer General Options > Folders tab to verify which folder is used for trending data. |
| Protocol Definitions | C:\Program Files\Observer\ProtocolDefs  
This contains any modifications or additions you have made to the protocol definitions list for each probe instance. Back up in all cases. |
| Multicast Definitions | C:\Program Files\Observer\MulticastDefinitions  
This contains the templates for defining trading multicast streams for Network Trending. Back up if you use trading multicasts in Network Trending. |
| Settings | C:\Program Files\Observer\Settings  
This contains alarms and triggers. Back up if you heavily use alarms or have alarm/trigger customizations that need to be retained. |
| SNORT Rules | C:\Program Files\Observer\Forensics  
This contains your SNORT information, such as rules, for detecting malicious activity in your packet captures. Back up if you use SNORT. |
| Expert Thresholds | C:\Program Files\Observer\ExpertSettings  
This contains your thresholds stored in Expert settings. These include TCP/UDP events and some triggers for problem identification. Back up if you have modified any Expert thresholds and want to retain those customizations. |
| SNMP | C:\Program Files\Observer\SNMP  
This contains any custom MIBs, compiled MIBs, request files and SNMP trending data. Back up if you have made SNMP changes or have SNMP trending data. Use... |
### Using the NetFlow features in Observer

Like many things in Observer a feature is not in just one place, but spread throughout the product. NetFlow is no different. Use this section as a starting place to find what you need regarding NetFlow in Observer.

- Choose the right probe for you.
- Ensure your ToS/QoS is set for your network so that your statistics are correct.
- There are two different types of NetFlow collectors. Learn the differences and see how to create one.
- If you are using a GigaStor probe, you can generate NetFlow statistics using it.
- Capturing NetFlow statistics does have some limitations that are different from packet capture.
- Decoding a NetFlow flow. This section also details how you may need to configure your NetFlow device so that Observer can see the flows.
- Open a saved NetFlow capture.
- Most NetFlow information comes from Network Trending.

<table>
<thead>
<tr>
<th>Directory or file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Tables</td>
<td>C:\Program Files\Observer\LocalAddressTable  &lt;br&gt;This contains your Discover Network Names list. Back up if you have run Discover Network Names and have saved the alias list.</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Observer\ProbeAddressTable  &lt;br&gt;This contains the Discover Network Names list from any remote probe that has connected to this Observer analyzer. Back up if you have run remote Discover Network Names and saved the alias list.</td>
</tr>
<tr>
<td>Scripts</td>
<td>C:\Program Files\Observer\Scripts  &lt;br&gt;This contains the scripts for Observer. Back up if you have created or modified a script.</td>
</tr>
<tr>
<td>Windows Registry</td>
<td>Using Regedit export the following key for 32-bit Windows:  &lt;br&gt;HKEY_LOCAL_MACHINE\SOFTWARE\Network Instruments  &lt;br&gt;64-bit Windows OS:  &lt;br&gt;HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Instruments</td>
</tr>
<tr>
<td>License</td>
<td>Make note of the license information in Help &gt; License Observer. You need the contact/department, company, identification number, and license number</td>
</tr>
</tbody>
</table>
Monitoring a wireless access point

You can capture all wireless traffic with a wireless network card on a laptop or any system with a wireless network card if you use the Network Instruments wireless driver. The default driver for your wireless card is not sufficient for Observer.

Standard network cards do not support “raw” wireless packets, nor do they enable “promiscuous” mode by default. Promiscuous mode captures all packets for the analyzer, not just those addressed to the network card. Both “raw” wireless packets and promiscuous mode are required by Observer. The Network Instruments wireless driver enables these options.

When a network card is running in promiscuous mode, it cannot connect to a wireless access point. It can only capture traffic. If you are using a laptop and want to capture traffic and at the same time connect to a wireless access point, your laptop must have two wireless cards.

If you are using the probe software on your laptop, you need two network adapters. Typically, one adapter is an Ethernet card for communication and one wireless adapter for analysis. You could also use two wireless cards. You may also need special drivers.

If your wireless network uses an encryption key or specific wireless channels, you can specify that information for the wireless adapter.

EAP/LEAP use private keys to authenticate with a RADIUS server, then dynamic keys are used to encrypt communication on a user by user basis, with no two users ending up with the same keys. Observer cannot decrypt the data from a site that implemented EAP/LEAP, but this does not mean Observer is not useful. Because all management and control packets are not encrypted, wireless troubleshooting is not affected even if you use EAP/LEAP.

Note: If you want to troubleshoot the actual data in the conversation, collect the data on the wired side where there is no encryption and all protocols can be decoded. Observer supports both wired topologies (i.e. Ethernet, Token Ring and FDDI) as well as wireless topologies to troubleshoot both sides of a conversation (wireless management+control AND full wired data) you only need one product.

Configuring a probe’s name and other probe options

The probe has many options that you can configure.

1. Choose Options > Probe Options. The Probe Options dialog opens, which lets you configure the probe.

2. Use this table to complete the settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe name</td>
<td>Allows you to specify a name for the probe which appears in the Observer analyzer probe list. The default name is a random mix of numbers and letters. We suggest renaming the probe to something meaningful to you. The name may be its physical location or any other standard you choose. The probe name is not the same as the</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>probe instance name, although with a Single Probe you only have one probe instance. You define the probe instance name elsewhere. See Creating a probe instance</td>
<td></td>
</tr>
<tr>
<td>Network trending folder</td>
<td>Allows you to specify where the network trending data is saved. The default is C:\Program Files\Observer\NetworkTrending. Unless you have a specific reason to use another directory, we suggest using the default.</td>
</tr>
<tr>
<td>Folder for GigaStor</td>
<td>Allows you to specify where the GigaStor and network packet data will be saved. The default is C:\Program Files\Observer\Data. Unless you have a specific reason to use another directory, we suggest using the default.</td>
</tr>
<tr>
<td>Maximum IP DNS resolution entries</td>
<td>Defines the maximum number of DNS entries the probe should maintain. The probe will keep up to the number of entries defined or what the probe can maintain in 10 MB, whichever is less. The probe keeps the first 1000 entries (or whatever amount you define) it sees; it does not keep a rolling list of the last 1000. After the limit is reached, no more entries are kept. They are discarded.</td>
</tr>
<tr>
<td>Use Observer Encryption Key file for secure connections</td>
<td>If selected, the probe will not connect with an analyzer unless a matching Observer Encryption Key (.oek) file is present. The .oek file must be in both the analyzer and probe installation directories. See “Encrypting the data sent between the probe and analyzer” for details.</td>
</tr>
<tr>
<td>Use Network Instruments Management Server at IP Address</td>
<td>Choose this option if you have licensed and installed NIMS. NIMS centralizes user/password administration superceding the probe security tab settings. Matching Observer Encryption Key files are required in the installation directory of both analyzer and probe for the connection to complete. Not available for the Single Probe.</td>
</tr>
<tr>
<td>Manage licenses with NIMS</td>
<td>Select this option if you are using NIMS to manage your licenses. Provide the primary and secondary server addresses. You may choose to export them for use on another system. Not available for the Single Probe.</td>
</tr>
<tr>
<td>Run Probe as Windows Service</td>
<td>Select this option if you want to run the probe as a Windows service. This allows the probe to start without requiring a user to log in and start the probe. The probe starts whenever the system starts, which can be especially important for a remote probe. The change takes effect on the next system restart. When running the probe as a Windows service, some options are available to you that you do not have when running the probe as an application. Specifically, you can set Networking Trending and see CPU load of each probe instance. In both modes, you can configure memory management, configure security for each probe instance, reserve Windows memory for the probe, adjust for time drifts through</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>When running as a service, allow autoupgrade</td>
<td>Allows you to elect to have the system restart automatically after the probe is upgraded. Will restart the probe only if probe runs as a Windows service.</td>
</tr>
<tr>
<td>Enable Probe HTTP responder</td>
<td>Allows you to enable the Web Probe Snapshot. The probe offers a “snapshot” of general data by connecting to the probe using a standard web browser. Information includes the state of the probe and the general network statistics that the probe displays within its own interface.</td>
</tr>
<tr>
<td>Auto-refresh Web page every 10 seconds</td>
<td>Allows you to configure the probe to refresh the browser display every 10 seconds.</td>
</tr>
<tr>
<td>Probe HTTP port (default = 80)</td>
<td>Allows you to specify which port to use for reporting of web information. For example, if your probe’s web server is configured to use port 3605, the URL is http://probe_host_name:3605.</td>
</tr>
<tr>
<td>GigaStor data analysis time slice</td>
<td>Available only when using Expert Probe software on a GigaStor. If your GigaStor is writing data to disk at near capacity of the disk speed and you then mine data from the disk, it is possible that the GigaStor will drop some packets from being written to disk. You can prevent this by reducing the data analysis percentage from 100% to something lower. Writing to disk will always be 100%, the reading or mining of data will be at the percentage you choose. The tradeoff is that all packets are captured, but data mining is slower. You must find that balance that is right for you and your users.</td>
</tr>
<tr>
<td>GigaStor Capture Payload Encryption</td>
<td>Available only when using Expert Probe software on a GigaStor. If you want the GigaStor payload to be encrypted using 256 bit AES encryption before it is stored, select the “Encrypt GigaStor network traffic...” option. An encryption key is needed on the GigaStor (or a location accessible by the GigaStor) to encrypt and decrypt the data. The AES key is not needed on workstations, probes, or other collection points; however you must generate the key from an Observer analyzer. A special license is required for this feature. Contact Network Instruments for this license.</td>
</tr>
</tbody>
</table>
# Probe Properties field-level descriptions

This section include details about many of the fields and options for a probe.

## Table 3: General tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication timeout</td>
<td>Allows you to define how long Observer will wait for the Probe to communicate before it assumes the connection is lost. Values are from 2 to 60 seconds.</td>
</tr>
<tr>
<td>Probe report period or local Observer information refresh time</td>
<td>Allows you to set how often the Probe sends a refresh packet or how often the local Observer’s dialogs are refreshed. This value has a minimum of 2 seconds with no maximum.</td>
</tr>
<tr>
<td>Statistics report (refresh) period</td>
<td>Allows you to set the statistics display refresh period. This value has a minimum of three seconds with no maximum.</td>
</tr>
<tr>
<td>Vital signs report (refresh) period</td>
<td>Allows you to set the Network Vital Signs refresh period. Values are from 10 to 600 seconds.</td>
</tr>
<tr>
<td>Sampling Divider</td>
<td>On probes with less processing power, high traffic rates (such as those typical of gigabit connections) can overwhelm the probe’s ability to keep up. A sampling divider tells Observer to only consider one of every n packets when calculating statistical displays, where n is the sampling divider. This setting only affects statistical displays such as Top Talkers, Internet Observer, etc. (packet captures are unaffected). A sampling divider of 2 registers every other packet; a sampling divider of 10 registers every tenth packet. Some statistical displays consider every packet regardless of this setting. Bandwidth Utilization looks at traffic as whole, so does Wireless Site Survey.</td>
</tr>
<tr>
<td>Encapsulated Traffic Analysis</td>
<td>GRE (Generic Routing Encapsulation) and GTP (GPRS Tunneling Protocol) are two encapsulation protocols that may have been deployed on your network. To show the encapsulation IP addresses, leave the box unchecked; to show the nested IP addresses, check the box. This setting also applies to L2TP and IPv4.</td>
</tr>
<tr>
<td>Nortel OEL2 Metro Ethernet Analysis Settings</td>
<td>Choose if frame headers should be analyzed as OEL2 headers.</td>
</tr>
<tr>
<td>MPLS Analysis Settings</td>
<td>Choose whether Observer should auto determine IPv4 and IPv6, what all other traffic is (ATM or Mac Header), and whether to use a four byte pseudowire word. Also choose whether to use the MAC addresses from encapsulated MPLS header.</td>
</tr>
</tbody>
</table>

## Table 4: Parameters tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network type</td>
<td>Displays the probe’s network topology, such as Ethernet, Token Ring, wireless, and WAN.</td>
</tr>
<tr>
<td>Network speed</td>
<td>Displays the network speed. The distinction here is between the actual, measured speed of the network and the speed that the NIC card, possibly incorrectly, reads from its connection. For example, a 10/100Mb NIC card on a 10/100Mb connection to a switch on a network where all the other stations are running at 10Mb will report the network speed as 100Mb. This item is the actual number that the NIC card driver sends Observer, so 10Mb Ethernet will be reported as 10,000,000. 100Mb Ethernet will be reported as 100,000,000.</td>
</tr>
<tr>
<td>NIC card name</td>
<td>Displays the name of the card as reported by the NDIS driver to the registry.</td>
</tr>
<tr>
<td>Probe version</td>
<td>Displays the probe version used by the local Observer or probe.</td>
</tr>
</tbody>
</table>
### Table 5: Adapter Speed tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Network Speed</td>
<td>Your current speed reported by the network card.</td>
</tr>
<tr>
<td>Network Adapter Speed</td>
<td>Choose to let Observer and the NIC automatically determine the network speed, or to select from various values (in megabits per second) for the network speed to be used for calculations. The primary use of this is to correct a mistaken NIC’s impression of overall network speed. A network card connected to a 10 megabit hub on a gigabit network will think that the entire network is only 1% as fast as it actually is.</td>
</tr>
</tbody>
</table>

### Table 6: Autoupgrade tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoupgrade probe within minor version release</td>
<td>Activates the autoupdate feature for minor version (i.e., point) releases (which do not require a new license).</td>
</tr>
<tr>
<td>Autoupgrade probe for major version release</td>
<td>Activates the autoupdate feature for major version releases. You must supply an ID and license key to update probes with a major version release. If the probe includes a Gen2 capture card and the upgrade includes a Field Programmable Gate Array (FPGA) firmware update, the system must be manually shut down and restarted before the firmware update can take effect. A system restart will not complete the firmware upgrade (a shut down is required); however, the autoupgrade process will restart the probe system, thus completing the probe software upgrade. In most cases, the probe will still be operable with a software-only upgrade, but any of the benefits of the firmware update are not activated until you manually shut down and restart the probe.</td>
</tr>
<tr>
<td>Force Probe Autoupgrade to the current Observer version</td>
<td>This provides a manual mechanism for updating a probe.</td>
</tr>
</tbody>
</table>

### Table 7: ToS/QoS tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect Protocol Distribution by QoS</td>
<td>When enabled, QoS data is collected.</td>
</tr>
<tr>
<td>Use 802.11e Wireless TID/QoS</td>
<td>When enabled, QoS for wireless networks is collected.</td>
</tr>
</tbody>
</table>
### Ethernet Probe (pub. 20.Feb.13)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP ToS/QoS Standard     | This tab is used for NetFlow and VoIP analysis. IPv4 supports the Type of Service (ToS) byte, also known as the Precedence byte. Different RFCs define different ways to interpret the byte:  
  Default (RFCs 1349, 1195, 1123, and 791)  
  OSPF V2 (RFCs 1248 and 1247)  
  DSCP (RFC 2474)  
  User Defined  
  The information on the right shows the bit assignments. User-defined interpretations are also allowed, for the currently selected option. The User defined option displays entry fields that allow you to define the meaning of each bit position in the ToS byte. |

Table 8: Wireless 802.11 tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Profile</td>
<td>Site profiles allows you to save and retrieve wireless parameters, rather than re-keying the parameters every time you change sites.</td>
</tr>
</tbody>
</table>
| Monitor Wireless Traffic| Choose one of the following:  
  Scan Channels—Click the Channel Map button and choose which channels you want to scan, then choose how often you want to scan them.  
  Scan Interval—Define the scan interval.  
  Fixed Channel—Pick a channel to monitor.  
  BSSID—Specify the Basic Service Set ID of the Access Point you want to monitor.  
  ESSID—Specify the Extended Service Set ID of the network you want to monitor. |
| Use encryption keys     | If your wireless network is secured, you must provide an encryption key for Observer to be able to capture and decrypt the wireless traffic. Select the Edit Encryption Keys button and provide your wireless encryption key. |
| Antenna to use          | The type of antenna connected to your system. Specify one of the following:  
  Antenna Diversity—Use the stronger signal from the two antenna ports. This is the recommended setting for the standard snap-on antenna.  
  Primary Antenna Only—if you are not using the standard snap on antenna, choose this option if the antenna you are using is connected to the primary antenna port (see your NIC manual for details).  
  Secondary Antenna Only—if you are not using the standard snap on antenna, choose this option if the antenna you are using is connected to the secondary antenna port (see your NIC manual for details). |

Table 9: DS3/E3/HSSI tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Type</td>
<td>Choose DS3 (T3), E3 or HSSI to match the type of link you are analyzing, then choose the frame check sequence (FCS) standard: CRC-16 (the default) or CRC-32.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>You must set this to match the settings on the frame relay CSU/DSU.</td>
</tr>
<tr>
<td>Subprotocol</td>
<td>If ATM or LAPB is the selected encapsulation method, you must choose the sub-protocols on the link.</td>
</tr>
<tr>
<td>Fractionalized</td>
<td>Check if your link is configured for fractionalized operation. Fractionalized DS3 and E3 are not supported.</td>
</tr>
</tbody>
</table>
### Setting and Explanation

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth (HSSI)</td>
<td>Set to match the bandwidth and channel settings of the fractionalized HSSI link under analysis.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WAN/Frame Relay Type</th>
<th>Choose T1 or E1 to match the type of link you are analyzing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapsulation</td>
<td>You must set this to match the settings on the frame relay CSU/DSU.</td>
</tr>
<tr>
<td>Subprotocol</td>
<td>If ATM or LAPB is the selected encapsulation method, you must choose the sub-projects on the link.</td>
</tr>
</tbody>
</table>

**Link 1 and Link 2 Channel Settings (Note that for the link and settings to be activated, you must check the On check box for that link).**

<table>
<thead>
<tr>
<th>Fractionalized</th>
<th>Check if this link is configured for fractionalized operation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel selector check boxes</td>
<td>Choose the channels you want to be included in the analysis.</td>
</tr>
<tr>
<td>Include in Util. Thermometer</td>
<td>Check if you want to include statistics from this link in the Bandwidth Utilization Thermometer.</td>
</tr>
</tbody>
</table>

---

### Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling

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

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on Network Instruments hardware.

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

In the Observer analyzer:

1. Select a probe instance in the Probes list.
2. Right-click and choose Probe or Device Properties.
3. Use the following tabs to further configure the probe for your environment. Not all of these tabs are present at all times. What tabs are visible depends on the type of probe you are configuring. For instance, the Gigabit tab is only visible when you are configuring a Gigabit Probe. For details about the fields on each tab, see the online help.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Set the statistics sampling divider and MPLS settings. For field descriptions, see Table 1.</td>
</tr>
<tr>
<td>Adapter speed</td>
<td>Verify that the adapter speed is registering correctly. Change the adapter speed if necessary. Changing the adapter speed here may be useful and necessary, because statistics, graphs, and reports generated by Observer are set using the adapter speed as the maximum. If, for some reason, Observer is not able to</td>
</tr>
<tr>
<td>Tab</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Correctly identify your adapter speed your reports may be inaccurate. For field descriptions, see Table 3.</td>
<td></td>
</tr>
<tr>
<td>Autoupgrade</td>
<td>Choose whether you want your probe to be automatically upgraded when a newer version is available; that is, the Observer analyzer is a newer version than the probe to which it is connecting. See Remotely upgrading the probe software from within the Observer analyzer. For field descriptions, see Table 4.</td>
</tr>
<tr>
<td>ToS/QoS</td>
<td>Ensure these settings match your needs paying particular attention to the IP precedence bit for the ToS/QoS of your network. What you set here affects how the Observer analyzer displays information about VoIP, NetFlow, sFlow, and capture decodes. For field descriptions, see Table 5.</td>
</tr>
<tr>
<td>Gigabit</td>
<td>Define the maximum frame size for your network. The default is 1514 bytes (excluding the frame checksum), which is appropriate for standard Ethernet. If the network link you are analyzing is configured to support jumbo frames (frames larger than 1514 bytes), you may want to change this setting to match the frame size of the Gigabit network, up to a maximum size of 9014 bytes. Observer will then discard frames that exceed this maximum frame size, generating a “Frame too large” error.</td>
</tr>
<tr>
<td>Wireless 802.11</td>
<td>Define what channels you want to monitor, what antenna you use for the wireless card, and your wireless encryption key if you use one for your network. See Monitoring a wireless access point. For field descriptions, see Table 6.</td>
</tr>
<tr>
<td>D3/E3/HSSI</td>
<td>Choose your WAN type, then choose the frame check sequence standard. You must set encapsulation to match the frame relay settings on the CSU/CDU. If ATM or LAPB is selected, you must also choose a subprotocol. Set the bandwidth to match the channel settings of the fractionalized HSSI link. For field descriptions, see Table 7.</td>
</tr>
<tr>
<td>T1/E1</td>
<td>Choose your WAN type, then set encapsulation to match the frame relay settings on the frame relay router. If ATM or LAPB is selected, you must also choose a subprotocol. Pick a line frame that matches your network. If your link is fractionalized, select that option. For field descriptions, see Table 8.</td>
</tr>
<tr>
<td>Virtual adapters</td>
<td>See Configuring virtual adapters on the Gen2 card.</td>
</tr>
</tbody>
</table>

Your probe instance is now configured. You can begin collecting network traffic and statistics using it. Typically, this is done in the Observer analyzer by choosing Capture > Packet Capture and clicking the Start button. See Configuring probes to collect data even when not connected to an analyzer for details. You do not, however, need to start a packet capture to see statistics. See the list of statistics available under the Statistics menu in Observer.

**Enabling Network Trending and setting which statistics are collected**

A probe can provide many different statistics about your network, but you must enable the collection of those statistics. Network Trending does not capture packets, but collects statistics about the traffic on your network. Many reports in Observer use the trending information, and we recommend you enable Network Trending.

1. To turn on the collection of a specific statistic, in the Observer analyzer choose Statistics > and then select the statistic you want to have the probe collect and report.
2. To turn on Network Trending, in the Observer analyzer choose Trending/Analysis > Network Trending. The Network Trending window opens.
Configuring probes to collect data even when not connected to an analyzer

Probes (and probe instances) can be configured to collect data only when you tell it to—including manually starting/stoping the collection, having collection always running, or based on a schedule. The schedule and settings are saved with the probe instance. This means if you choose to have packet capture always running or running on a schedule that the probe instance does not need to be connected to an Observer analyzer.

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

1. In Observer, select a probe instance in the Probes list.
2. Choose Capture > Packet Capture. The Packet Capture window opens. Along the top of the window are several buttons, including Start, Stop, Settings, and Decode.
3. Click the Settings button. The Packet Capture Settings window opens.
4. Click the Schedule tab.
5. Choose the schedule you want (Always, daily, or specific days).
6. If you want to control the capture buffer’s size, click the Capture Options tab. The data is saved on the probe in C:\Program Files\Observer\Data.

Changing the monitored network adapter

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

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on Network Instruments hardware.

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

If you have a network card in your system, but it is not being seen or recognized by Observer, follow the instructions in No network adapter available.

If you are seeing only broadcast traffic, you do not have the correct network card selected or you do not have your switch port configured correctly as a SPAN/mirror port. Change the network adapter you are monitoring or configure the SPAN/mirror port.

1. When choosing the monitored adapter from within the Observer analyzer for all probe versions:
   a. In the Probes list, select the probe instance.
   b. Choose Actions > Select Network Adapter Card. The Select Network Adapter window opens.
   c. Select the network adapter you want to monitor and click Select.
2. When choosing the monitored adapter on the probe for Multi Probe and Expert Probe:
   a. Click the “Adapters and Redirection” tab.
b. Select your probe instance and click the Configure Adapter/Redirection button. The Edit Probe Instance window opens.
c. In the Selected Network Adapter section, change the network card you are monitoring.

The probe instance is now using the newly selected adapter.

**Connecting to a probe for the first time from the Observer analyzer**

1. In the Observer analyzer, select Actions > Redirect Probe.
2. Click New to add the probe to the Probe Administration and Redirection list.
3. Type the IP address that you assigned to the probe and click OK. You may leave the other fields blank. If you type a name, the name will change after the Observer analyzer connects to the probe. The probe appears in the list of available probes.
4. Select the probe and then click Redirect Selected Probe.
5. Select the probe instance and click Redirect Selected Instance.
6. Choose the “Redirect to this Observer” option, then click the Redirect button. Within 30 seconds the probe will connect with the analyzer.

   Probe redirection can be password protected or disabled. Please see Connecting the Multi Probe or Expert Probe to an Observer analyzer for details. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.

7. Close the Probe Instance Redirection window.

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

*Prerequisite:* Multi or Expert Probe.

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

1. In Observer, select Actions > Redirect Probe.
2. Select the probe instance you want to redirect and click the Redirect Selected Probe Instance button at the bottom. The Edit Probe Instance window opens.
3. If this is the first time you are connecting to the probe from the Observer analyzer, you must add the probe to your list. See Connecting to a probe for the first time from the Observer analyzer.
4. If the probe is not connecting, Probe redirection might be password protected or disabled. Please see Connecting the Multi Probe or Expert Probe to an Observer analyzer for details. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa.
5. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.
Creating a probe instance

Prerequisite: Multi or Expert Probe.

When you open a Multi Probe for the first time, you assign memory to a probe instance. You can choose to use this one probe instance, or you can create other probe instances. See “Configuring connections to multiple NICs or Observer analyzers” for why you would want to use multiple probe instances.

Note: There are several different probe instance types. These include a packet capture-based probe instance used to capture packet traffic, two NetFlow collectors, an sFlow collector, and a MPLS probe. This section describes creating a packet-based probe instance, but the process is similar for the other probe instances, some of which are only available on the Expert Probe. For NetFlow, see Creating a NetFlow collector or NetFlow Trending collector. For MPLS, see Creating and configuring an MPLS probe instance. For sFlow, see Creating an sFlow collector.

To set up a probe instance, follow these steps:

1. Do one of the following:
   - On the probe: Click the Adapters and Redirection tab.
   - In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Adapters and Redirection tab.

2. In the upper left, click New Instance. The Edit Probe Instance wizard opens.
   - If the New Instance button is grayed out, it probably means you do not have enough Observer-allocated memory to add another instance.
   - If you get a message that says that there is not enough reserved memory to create a probe instance, you must reduce the amount of memory used by another probe instance. By default all of the reserved memory on a GigaStor is assigned to the “Instance 1” active instance. By releasing some of the reserved memory you re-allocate memory from one probe to the pool of reserved memory from which you can create other probe instances, including passive probe instances on the GigaStor. Click the Configure Memory button and reduce the amount of memory for the packet capture buffer.

   You must have a minimum of 256 MB RAM to run the probe with a single instance, plus 12 MB for each additional probe instance. See Setting the total system memory reserved for probes for details on allocating memory for Observer probes.

3. Ensure “Probe” is selected in the Instance type. Type a name and description and click Next.

4. Choose an appropriate capture buffer size given the local system’s available memory and how much traffic you plan on capturing from the given network.

   Statistical reporting uses different memory—and much less of it—than packet capture.

   Although it is possible to customize the amounts of memory used by various Observer statistical displays (by choosing a statistics memory configuration), for most situations the defaults work perfectly well. For additional information, see Customizing statistics and capture buffers for probe instances.
a. If you need to create your own memory configuration, click New. The New Statistics Memory Configuration window opens.
b. Type a name and choose a default memory configuration to use. Click Finish. After choosing the memory configuration, you can change how the memory is allocated.
c. Select your newly created memory configuration and click Edit. The Edit Statistics Memory Configuration window opens.
d. Choose your network type. For each Observer statistic, choose how much memory is allocated for it. Click OK.
e. Click Next to continue, and the Select Network Adapter and Redirection configuration dialog is displayed
5. Ensure the correct network adapter is selected and type the IP address of your Observer analyzer. Click Finish.
6. If you are creating a probe instance on any probe except a GigaStor, you are done. If you are creating a probe instance on a GigaStor probe, then see Creating GigaStor active and passive probe instances.

**Connecting the probe to an Observer analyzer**

There are two ways to connect the probe to an Observer analyzer. The method described here shows you from the perspective of the probe. The second way is described in Connecting the Multi Probe or Expert Probe to an Observer analyzer. All actions are done on the probe itself.

1. Choose **Options > Probe Redirection Settings**. The Probe Redirection Settings dialog opens.
2. Use Table 8 to complete the settings. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa.

<table>
<thead>
<tr>
<th>Observer IP address</th>
<th>Type the address of the Observer analyzer you want this probe to connect to.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Probe redirection for remote users</td>
<td>Allows remote users to redirect the probe to their Observer analyzer. If you want the probe to be able to connect to only one Observer analyzer, leave this option unchecked.</td>
</tr>
<tr>
<td>User name</td>
<td>By default any user can connect to the probe and no password is required.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the user account.</td>
</tr>
</tbody>
</table>

3. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.

**Connecting the Multi Probe or Expert Probe to an Observer analyzer**

**Prerequisite:** Multi or Expert Probe.

There are two ways to connect the probe to an Observer analyzer. The method described here is from the perspective of the probe. All actions are done on the probe itself.

Each probe instance can be connected to only one Observer analyzer at a time. Connecting the probe instance with the analyzer is called “redirecting” it. This is because the probe instance may not be connected to any Observer analyzer or it may be connected to a different Observer than the one you want to connect it to. The connection can be done from within the analyzer or from the probe.
This section describes how to redirect a probe instance from the probe and assumes that the probe software is running and that you already have a probe instance.

1. Click the Adapters and Redirection tab.
2. Select the probe instance you want to redirect and click the Configure Adapter/Redirection button at the top. The Edit Probe Instance window opens.
3. Select the “Redirect to a specified IP address or DNS name” option and provide the IP address or DNS name. When the probe instance is connected the “Redirected to” column lists the IP address of the Observer analyzer system. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa.
4. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling.

**When to use a virtual TAP**

Monitoring network and application traffic in a virtualized environment containing one-to-many relationships between physical hardware devices (virtual hosts) and virtual application servers (virtual machines) presents a number of concerns.

Virtual environments are designed to include a virtual adapter (vNIC) for each virtual machine within the system. The vNIC is logically connected to a virtual switch, which is managed by the virtual host system (see the diagram below). This addresses communication which would remain in the VM host. In order to enable communication into and out of the VM host, a logical connection between the vNIC and the pNIC must be established.

Depending on the virtual server technology you have decided to implement, you have a number of options for network and application traffic visibility, and for the use of external devices for analysis. If all virtual machine communications take place between the virtual machines and the “outside” (i.e., outside the physical host), then monitoring the data flow from outside the host server may be the least complicated method by which to gain flow visibility. If there is any internal communication between virtual machines, the only way to monitor this data is by using a monitoring virtual machine (separate or existing) with an analysis service (i.e., probe) gathering data from the internal virtual switch. Should you need to analyze or store data on an external purpose-built device, installing a virtual TAP within the monitoring virtual machine provides complete visibility into all data flowing on the internal virtual switch.

Within the VMware ESX and ESXi environments, a virtual adapter can be set in “promiscuous mode.” When promiscuous mode is enabled on a virtual adapter, all traffic flowing through the virtual switch—including local traffic between virtual machines and remote traffic originating from outside the virtual host—is sent to the promiscuous virtual adapter.
A number of challenges are presented when attempting to monitor applications with a virtualized environment.

1. **Lack of visibility.** Traffic between virtual machines within a virtual host will not be visible outside of the host. This causes a number of problems:
   a. Network engineers cannot monitor multi-tier applications partially or wholly located on multiple virtual machines within a single host.
   b. Should a virtual machine be compromised by malicious code or security breach, other virtual machines within the same host may also be compromised.

2. **Lack of analysis functionality.** A separate solution is required to push data streams flowing within virtual machines out to an external tool or a purpose-built device. This functionality is necessary for network and application monitoring and analysis, compliance, and security audits. Virtual TAPs (software applications placed inside a virtual machine to export all data through a designated pNIC to an external device) can alleviate this problem.

**Options**

The goal is to not only see all traffic flowing within a VM host but also export that data for powerful analytics and reporting. There are three primary ways to monitor both traffic flow from within applications on virtual machines and from the virtual host:

1. Monitor the host using an external analysis device as you would any other system, via SPAN technology or a physical TAP. This option works well for environments not needing to track internal virtual machine-to-machine traffic within a host. However, it may not catch a security breach compromising multiple virtual machines within a host.
2. Monitor all virtual machines in a host by establishing a new virtual machine within the host. This option assumes the ability to SPAN or set in promiscuous mode the virtual switch within the host. This option provides visibility at the statistics and packet levels of all traffic within a virtual host. It does not, however, allow packet-level traffic to be analyzed by an external physical device (IDS, retrospective analysis device, etc.).
3. Use a virtual TAP to collect and redirect all internal virtual machine traffic to a dedicated virtual NIC within the monitoring virtual machine that is connected to an external purpose-built device for analysis or compliance enforcement. Depending on the functionality of the external device the traffic is being copied to, this option may provide all the functionality of option two while taking advantage of the physical capabilities of the purpose-built external device.
Option two combined with option three offers the most extensive and comprehensive monitoring solution. In a VMware environment, you can use promiscuous mode on the internal virtual switch and direct a copy of all traffic from all virtual machines to a virtual machine monitoring instance. This allows you to collect metrics and perform real-time analysis; and using a virtual TAP, you can re-direct packet streams out a separate NIC to a GigaStor probe.

**Benefits of a virtual TAP**

Mirroring all traffic within a virtual host to an external device provides a number of advantages, including total visibility into VM application traffic and the ability to run greater analytics for comprehensive reporting and faster problem resolution. For example:

- **Application Performance Monitoring.** Feed VM traffic to an enterprise reporting engine for comprehensive monitoring of virtualized environments. Set and track performance baselines and respond quickly when performance deviates from the norm. Tracking VM traffic over time helps determine if your VM server load has increased to the point of requiring action.

- **Application Performance Troubleshooting.** The virtual TAP can also output data to a GigaStor probe, which stores it for later access. The GigaStor can help isolate problems within your virtual environment and troubleshoot these issues using Application Analytics.

The Virtual TAP option bridges the visibility gap, allowing complete real-time analysis, Retrospective Network Analysis, and full-scale reporting on all virtualized traffic.
Using the probe as a virtual TAP

Prerequisite: Multi or Expert Probe.

The Virtual TAP (sometimes called a vTAP) allows you to configure a virtual tap to monitor traffic within a virtual host environment.

Most virtual environments provide virtual adapters for each virtual machine, and these virtual adapters are logically connected to a virtual switch managed by the virtual host system. The virtual switch manages traffic flow to and from the virtual adapters by mapping each virtual adapter to a physical adapter in the host. When promiscuous mode is enabled on a virtual adapter (or virtual switch), all traffic flowing through the virtual switch—including local traffic between virtual machines and remote traffic from outside the virtual host—is sent to the promiscuous virtual adapter and can be monitored by Observer.

To use the virtual tap you must monitor all virtual machines in a host from a virtual machine within the host. This assumes you can use a SPAN/mirror port or the virtual NIC has a “promiscuous mode” setting. This functionality is available in VMware’s ESX and ESXi. It may also be available in other virtual server products.

Using the virtual TAP, you can then collect and re-direct all traffic internal to the virtual switch to a dedicated virtual NIC within the monitoring virtual machine that is then connected to Observer.

If there is any internal communication between virtual machines, the only way to monitor this data is by using a separate monitoring virtual machine with an analysis service (for instance, probe) gathering data from the internal virtual switch. Should you need to analyze or store data on a GigaStor, installing a Virtual TAP within the monitoring virtual machine provides complete visibility into all data flowing on the internal virtual switch.

You can create a port group on a switch and use a virtual machine (VM1) to monitor traffic of a second virtual machine (VM2) that resides on the same switch but in different port.

If you already have a 64-bit Windows virtual machine, we suggest you use it, because installing the probe there will be less resource intensive on the host than installing a new virtual machine on the host.

1. Do one of the following:
   - On the probe: Click the Virtual TAP tab.
   - In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Virtual TAP tab.

2. Click Modify to set the source and destination adapters for the virtual tap.

3. Choose your source and destination adapters and select the Enable Virtual Tap option.
   - You have now configured what you need to within Observer to enable the virtual tap feature, but you must modify a setting for your virtual switch.

4. Set the virtual NIC on the virtual switch within the host in SPAN/mirror mode, sometimes also called promiscuous mode. See your virtual machine’s documentation for further details.
Configuring VMware ESX Server

**Prerequisite:** Multi or Expert Probe.

A free physical NIC is required on the VMware ESX server to perform this configuration. In the virtual switch to be monitored, add a virtual port group and set it to run in Promiscuous Mode. Do not choose the same source and destination for the Virtual TAP Settings. This could cause broadcast/multicast loops and would noticeably impact your network.

The default policy for Promiscuous Mode for the vSwitch itself should remain in the Reject setting. Only the new port group within the vSwitch should be set to Accept Promiscuous mode.

You can use the virtual machine properties dialog to identify the Network Connection, listed in the Windows Network Connections dialog, by unchecking the “connected” option.

1. Open VI Client and highlight the VMware ESX Server Entry.
2. Click to the Configuration tab.
3. Click Hardware – Choose Networking.
4. Find the vSwitch for which you would like to monitor traffic and choose Properties.
5. In the vSwitch Properties dialog (Ports tab), click Add.
6. In the Add Network wizard, choose Virtual Machine [port group], give the group a name (“Promiscuous Port Group”), and finish the wizard.
7. In the vSwitch Properties dialog, highlight the new port group and click Edit.
8. Click the Security tab.
9. Select the Promiscuous Mode Policy Exception option and change the list to Accept.

![Figure 13: VMware ESX Server](image)
10. Setup a second virtual switch and bind a second physical NIC to that virtual switch. See Figure 2 Virtual Infrastructure Client > Configuration tab. Then see Figure 4 Add Networking > Add Network Wizard > Virtual Machine.
11. Create a virtual switch.
12. Select the appropriate NIC entry (i.e. Physical NIC 2 on ESX Server).
13. Name the vSwitch (i.e. “vTAP OUT to GigaStor”) and finish.

The result should be similar to Figure 3. See your VMware ESX Server documentation if you need more detailed information on adding a virtual switch.

14. Edit the Virtual Machine that contains the Observer to use the Port Monitor Group and second vSwitch.
15. Select the first network adapter.
16. Change the Network label to the new Port Monitor Group, and add a 2nd virtual NIC if needed.
17. Select the second virtual NIC and change the Network label to the second vSwitch (i.e., vTAP OUT to GigaStor) and click OK.
18. Verify that the Virtual Machine containing Observer is located in both virtual switches.
19. Within the virtual machine, setup Observer to VTAP Local Area Connection 1 to Local Area Connection 2.

20. Connect the cable from “NIC 2” on the VMware ESX Server to the GigaStor Gen2 capture card.

**Bonding probe instances to specific ports on the Gen2 card through virtual adapters**

**Prerequisite:** Multi or Expert Probe.

Some probes available from Network Instruments come with a special capture card called the Gen2 capture card. Any probe equipped with a multi-port Gen2 card may be configured to use virtual adapters to bind specific port to specific probe instances.

**Capturing full-duplex traffic**

**Prerequisite:** Multi or Expert Probe.

Using a Gen2 capture card, you can capture full-duplex traffic. You can also bond probe instances to specific ports on the Gen2 card.

**Switching between the probe and analyzer user interfaces**

**Prerequisite:** Multi or Expert Probe.

Depending on how you want or need to use your Expert Probe, it can be either an Observer analyzer to help you view your network data or it can be a probe to capture data and to which other Observer analyzers can connect. The Expert Probe software cannot simultaneously be an analyzer and a probe.

To change the Expert Probe interface to load as a fully-featured Observer analyzer, choose Options > Switch Between Observer and Expert Probe Interface. You must restart the application to see the change.

For a GigaStor, the Expert Probe software is running as a Windows service. You must stop the Expert Probe service before you can change its interface.

1. Right-click the Probe Service Configuration Applet in the system tray and choose Open Probe Configuration.
2. The Probe Administration window opens. Click the Probe Options tab.
3. In the Service Settings section, clear the “Run Probe as a Windows Service” option and click OK. This removes the Network Instruments Expert Probe service from Windows.
5. Choose Options > Switch between Observer and Expert Probe Interface. The Choose Program Interface window opens.
6. Choose Observer and click OK. You must close Observer and restart it to switch into the analyzer interface. Click OK on the message dialog.
7. Click Start >All Programs > Network Instruments Observer > Observer to open the analyzer interface.

After completing this task:
When switching back to an Expert Probe on the GigaStor, you must reverse these steps and then you must manually start Expert Probe from the Windows Service Control Manager. It may take a moment before the service starts. You may need to restart the GigaStor for the setting changes to fully set.

Configuring access permissions for probe instances

Prerequisite: Multi or Expert Probe.

Note: If you have purchased and configured the NIMS option, user authentication is configured through NIMS rather than the probe’s Security tab, which is unavailable if the Use Network Instruments Management Server option is selected in Options > Probe Options.

Tip! To display security information by probe instance instead of by user account, click the Probe Instances button in the upper left. This lets you see what permissions each user on the probe has for the probe instance.

If you have already created user accounts described in Restricting access to probes with user accounts, then you are ready to continue with configuring access permission for the probe instances.

1. Do one of the following:
   - On the probe: Click the Security tab.
   - In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Security tab.

2. Use the check boxes to fine-tune the permissions that each user has on each account by clicking on the check boxes to select or deselect the particular option. The different types of access permissions are described in Table 1.
If there is a green check mark, the feature is enabled. If the option is unchecked, the feature is unavailable. If the option is grayed out, the user does not have access to that probe instance.

Table 11: Probe instance security options

<table>
<thead>
<tr>
<th>Permission</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt data</td>
<td>Data sent to the analyzer is Triple DES encrypted during transmission. By making Triple DES encryption passes, it increases the effective key length to 168 bits. Only use this option if you need strong encryption, because it imposes a significant performance cost. Even with this option turned off, the probe does not send raw, easily-readable data; the data is concealed by a proprietary compression algorithm.</td>
</tr>
<tr>
<td>Configure</td>
<td>User is allowed to change the probe's configuration options (such as memory usage, etc.).</td>
</tr>
<tr>
<td>Redirect</td>
<td>User is allowed to change the destination analyzer for probe analysis data.</td>
</tr>
<tr>
<td>Select Adapter</td>
<td>User is allowed to change the capture adapter for the probe.</td>
</tr>
<tr>
<td>Capture Packets</td>
<td>User is allowed to view captured packets from the probe's network.</td>
</tr>
<tr>
<td>Network Trending</td>
<td>User is allowed to view Network Trending data from the probe's network.</td>
</tr>
<tr>
<td>Internet Patrol</td>
<td>User is allowed to run Internet Patrol on the probe's network.</td>
</tr>
<tr>
<td>WAN Configuration</td>
<td>User is allowed to change WAN probe settings such as encapsulation type and Committed Information Rate (CIR). Only applicable to Network Instruments WAN hardware probes.</td>
</tr>
<tr>
<td>Modify Partial Packet</td>
<td>User is allowed to change the partial packet capture setting in the Packet Capture Settings dialog for this probe.</td>
</tr>
<tr>
<td>Modify Protocol Definitions</td>
<td>Protocol Definitions: User is allowed to modify user-defined protocol definitions. These definitions can be shared with other Observer analyzers through NIMS.</td>
</tr>
<tr>
<td>Modify Shared Filters</td>
<td>Shared Filters: User is allowed to modify shared filters. This feature works in conjunction with NIMS and modifying filters must also be enabled in NIMS.</td>
</tr>
<tr>
<td>Reconstruct Data</td>
<td>User is allowed to reconstruct data and view the data in Reconstruct Stream or TCP Dump.</td>
</tr>
<tr>
<td>Replay VoIP</td>
<td>User is allowed to replay audio or video VoIP data.</td>
</tr>
<tr>
<td>Transfer Capture Files</td>
<td>User is allowed to move capture files.</td>
</tr>
</tbody>
</table>

**Restricting access to probes with user accounts**

**Prerequisite:** Multi or Expert Probe.

If you wish to restrict access to packet captures and reporting provided by a probe instance, you can define security attributes of the probe by clicking the Security tab.

To display security information by user account, click the User Account button to the right of the Probe Instances button. This lets you see what permissions the currently selected user has access to on each instance of the probe.

When displaying a user account’s permissions, you can use the check boxes to fine-tune the permissions that each user has on each account by clicking on the Permissions check boxes.

By default there is an “Anyone” account with administrator rights. That means that anyone, regardless of user name, can connect to the probe instance and use it. We suggest you delete or limit
this account after you have created other user accounts. The Anyone account does not require a password.

**Note:** You cannot delete the Anyone account for a Single Probe. If you are having connection issues, see the issue about the Anyone account in *A probe is not connecting to the analyzer or vice versa.*

1. Do one of the following:
   - On the probe: Click the Security tab.
   - In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Security tab.
2. Click the New User Account button. To edit an existing account, select the account and click Edit User Account. The setup options are the same whether you are creating a new account or editing an existing account.
3. Type a user name and password. The user cannot change this password. If it is feasible you may wish to have the user type their own password.
4. If you want the user to have administrator rights, enable the option.
5. Select which probe instances the user will be allowed to use and click OK. By default, any new probe instances are accessible by all user accounts.
6. Select which access permissions the user will have for the probe instance. See Configuring access permissions for probe instances.

**Customizing statistics and capture buffers for probe instances**

**Prerequisite:** Multi or Expert Probe.

Before changing any of the buffer sizes, you should understand how any changes you make affects the probe. See *How an Observer probe uses RAM.*

- To change memory allocation for probe instances, see Running Observer with reserved memory.
- To fine-tune the Statistics Memory Configuration, see Tweaking the statistics memory configuration.

**Setting the total system memory reserved for probes**

**Prerequisite:** Multi or Expert Probe.

Memory use is an important and vital part of using an Observer probe successfully. Before changing any of the reserved memory, you should understand how any changes you make affects the probe.
Setting the probe’s time clock synchronization settings

At times your capture card drivers time clock may drift. They can be synchronized with the system clock, if you wish. Unless you notice a reason to enable this feature, we recommend that you do not synchronize your capture card’s time clock. Some Other things to consider:

- The capture card synchronizes itself with the system clock at when the system starts.
- Generally, you are interested in relative time between packets, not the actual time a packet was seen. If you need to have very accurate times, then consider using an external time server on your network, or by using the optional GPS timing device for Network Instruments’ Gen2 cards. See .

1. Do one of the following:
   - On the probe: Click the Synchronization tab.
   - In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Synchronization tab.

2. Click the Edit Schedule button.
3. Choose when and how you want the capture card’s time clock to synchronize with the system clock and click OK.

Configuring connections to multiple NICs or Observer analyzers

Prerequisite: Multi or Expert Probe.

With a Multi Probe, you can configure the probe to view multiple networks if multiple NICs are installed on the local system and to provide multiple Observer analyzers with views of the local network interfaces.

The probe accomplishes these capabilities by allowing multiple instances of itself. A probe instance is a virtual probe with attributes that define:

- Which network interface on the local system to capture data from.
- Which Observer analyzer (local or remote) to direct the data to.

Using the Expert Probe software

Prerequisite: Expert Probe

The Expert Probe is a step above the Multi Probe software and is the only probe software that runs on the GigaStor. The Expert Probe includes all the functionality of the Multi Probe, plus it displays remote expert analysis in real time for faster troubleshooting. If you are using the Expert Probe on a GigaStor(rather than a non-GigaStor probe) there are even more features available. Just like the Multi Probe, the Expert Probe has a number of tabs that allow you to control probe network connections and memory usage, administer probe security, and monitor probe activity.
An Expert Probe transfers decode data to an Observer analyzer only when you select the packet from the one-line summary pane, which is updated with packet header information in real time. This conserves network bandwidth by analyzing all data locally and sending only the results. This eliminates the need to transfer data packets over the wire. This differs from the Single Probe and Multi Probe because those probes send the entire buffer to the analyzer and the decoding and analysis happens on the analyzer.

Another feature exclusive to the Expert Probe is its ability to switch between being a probe or an analyzer. This can be very useful depending on your needs. This gives you flexibility in using the probe both remotely and on site.

### Using additional storage volumes for your GigaStor active instance

**Prerequisite:** Expert Probe

The maximum NTFS disk volume is 256 TB, but with a GigaStor you can have more storage than that by using the expanded disk arrays or striping through Windows. If you have expanded your disk array beyond 256 TB, for performance reasons you will want to add the additional volumes to your GigaStor active instance.

**Note:** This feature requires a special license key. Contact your Network Instruments sales person for that key. After you have the license key, enter it on the GigaStor probe by choosing Help > License probe. This enables the necessary feature.

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

**Prerequisite:** Expert Probe

This feature is only available when you are using the Expert Probe on a GigaStor probe. If your GigaStor RAID has more than 256 TB, see Using additional storage volumes for your GigaStor active instance before continuing.

By default, the GigaStor has an active probe instance called “Instance 1” but does not have any passive probe instances. We recommend that you

- Rename the active probe instance by selecting Instance 1 and clicking Rename. Choose a name that is meaningful to you for the probe instance name and click OK. A typical name might be the physical location of this GigaStor.
- Have only one active GigaStor instance, unless you have specific reasons to have more.
- Create passive probe instances to use.
- See details about active and passive probe instances discussed in [What is a probe instance?](#).
- After creating your active instance, if you want to change how much disk space is reserved for that active instance, click Configure Instance Storage.

To create a passive probe instance, follow the steps in Creating a probe instance. When you create a probe instance for an Expert Probe on GigaStor, it is automatically created as a passive probe instance.

If you want to change a passive probe instance to an active probe instance, follow these steps.

1. Do one of the following:
   - On the GigaStor probe: Click the GigaStor Instances tab.
   - In Observer analyzer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the GigaStor Instances tab.
2. Select the passive probe instance you want to promote to an active instance and right-click.
3. Choose Make Instance Active. Your passive probe instance is now an active probe instance.

**After completing this task:**

You should then create passive probe instances for it.

**VoIP Expert, Application Performance Analysis, and Application Transaction Analysis**

**Prerequisite:** Expert Probe

The Expert Probe provides unique insight into your OSI Model Layer 7 applications that the Multi Probe and Single Probe cannot provide. This is especially true for VoIP.

There is nothing that you need to configure on the probe to enable these features, but this information is only available when viewing the probe instance of an Expert Probe.
To use and configure VoIP, ATA, or APA:

1. In the Observer analyzer, choose **Trending/Analysis > Network Trending**. The Network Trending window opens.
2. Use the General, Application Transaction Analysis, Application Performance Analysis, and VoIP tab to configure your options.
3. Click the Start button to begin monitoring.
4. After you have collected some data, click the Analysis button. The View Network Trending data dialog opens.
5. Choose “Transfer and view current day statistics” and click OK. This opens the Network Trending Viewer in a new tab where you can see your data.

**Creating an sFlow collector**

**Prerequisite:** Expert Probe

See Creating a probe instance for details about creating an sFlow collector or a NetFlow Trending collector. In step 3 choose sFlow collector and follow the on screen instructions. After the probe instance is created, there is no other configuration you must do and it is ready to use.

**Creating and configuring an MPLS probe instance**

**Prerequisite:** Expert Probe

See Creating a probe instance for details about creating an MPLS probe instance. In step 3 choose MPLS Probe and follow the on screen instructions.

After the probe instance is created, you may want to configure the probe to tell it what type of traffic is seen.

1. In Observer analyzer, select a probe instance, right-click and choose Probe or Device Properties. The Probe Properties window opens.
2. On the General tab, use the options in the MPLS Analysis Settings to choose whether Observershould auto determine IPv4 and IPv6, what all other traffic is (ATM or Mac Header), and whether to use a four byte pseudowire word.
3. Click OK.

**Creating a NetFlow collector or NetFlow Trending collector**

**Prerequisite:** Expert Probe

**Note:** If you want to have scheduled collection of your NetFlow devices, use the settings on the Schedule tab.

NetFlow and sFlow collectors support the following versions of these technologies:

- NetFlow: 1, 5, 7, 9, and 10
sFlow: 2, 4, and 5

There are two types of NetFlow collectors in Observer. Choose the correct one for your needs, or create two different probe instances—one for the NetFlow collector and another for the NetFlow Trending collector. In most cases, it will likely be the NetFlow Trending collector. The NetFlow Trending collector supports up to 512 NetFlow devices, whereas the NetFlow collector only supports one NetFlow device. That means you must add and configure a NetFlow collector for each NetFlow device in your environment.

<table>
<thead>
<tr>
<th>Feature</th>
<th>NetFlow Trending collector</th>
<th>NetFlow collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>One flow per collector</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Up to 512 flows per trending collector</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Collects live statistics</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Collects historical trending²</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

1) Live statistics are details about the flow that appear in Observer in as few as five seconds.
2) Historical trending data collection interval can be as few as 60 seconds.

See Creating a probe instance for details about creating a NetFlow collector or a NetFlow Trending collector. In step 3 choose NetFlow collector or NetFlow Trending collector and follow the on screen instructions. After the probe instance is created, there is no other configuration you must do and it is ready to use.

After the probe instance is created, you may want to configure the probe to tell it what type of traffic is seen.

1. In Observer analyzer, select a probe instance, right-click and choose **Probe or Device Properties**. The Probe Properties window opens.
2. On the General tab, configure the Timing and Statistics Packet Sampling sections for your needs and Click OK.
3. Choose **Trending/Analysis > Network Trending**. The Network Trending window opens. If you have already configured the settings for the NetFlow collector, skip to step 7.
4. Click the Settings button.
5. In the Collection Settings section, choose a sampling divider and how often you want flow data collected.
   - **Sampling divider**—specifies how many packets should be sampled. The default is one in 10 packets is analyzed. Choosing 1 ensures every packet is analyzed, but increases the amount of CPU required. Choosing a larger number means not every packet is analyzed, but CPU use is reduced. A larger sampling rate still produces statistically accurate information. If you experience high CPU use, make the divider a larger number.
   - **Collection interval**—specifies how often data is collected. The default is 60 minutes. The minimum is one minute.
   - **Use current filter**—If you have a filter defined and you want to use it, select this option. Otherwise, leave it blank.
6. Click OK to close the Network Trending Settings window.
7. Click the Start button to begin monitoring the NetFlow devices.
8. After you have collected some data, click the Analysis button. The View Network Trending data dialog opens.

9. Choose “Transfer and view current day statistics” and click OK. This opens the Network Trending Viewer in a new tab. In the Network Trending Viewer you can see for your NetFlow devices:
   - Station Activity Time
   - Top Talkers
   - Packet Size Distribution
   - Bandwidth Utilization
   - Protocols

**Forcing users to authenticate before connecting to a probe**

**Prerequisite:** Expert Probe

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

Note that to enable user authentication, you must first tell Observer to encrypt all connections. Also note that user authentication is conceptually different than creating user accounts in Observer and setting user permissions.

**Encrypting the data sent between the probe and analyzer**

**Prerequisite:** Expert Probe

Connections to probes and probe units are secured end-to-end using the Triple DES (3DES) encryption algorithm, making Observer’s transmissions over the network highly resistant to eavesdropping and any meaningful interpretation of data. These secured connections are facilitated by the Observer analyzer and cannot be disabled—only improved.

You can further enhance the security by enabling probe to analyzer communication by turning on the “Encrypt Data” feature. See Configuring access permissions for probe instances

Along with securing your connections, if you have NIMS we recommend authenticating your users. See Forcing users to authenticate before connecting to a probe for more information.

After completing this task:

After the option is enabled, you must then create or obtain an Observer Encryption Key file:

- If you have an existing Observer Encryption Key file (*.OEK)
  - You must copy the encryption key file into the installation directory (usually C:\Program Files\Observer) of each probe or analyzer that you want to authorize.

- If you do not have an Observer Encryption Key file (*.OEK)
  - Generate a key file; click the “Launch Encryption Key Generator” button. Its online help explains its use and how to set up the keys it generates.
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 1 describes the two different ways that Observer runs.
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 2** shows what options in Observer control the size of various portions of memory.
Packet capture buffer and statistics buffer

There are two kinds of buffers that a probe uses to store data in real-time: capture buffers and statistical buffers. The capture buffer stores the raw data captured from the network while the statistical buffer stores data entries that are snapshots of a given statistical data point.

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

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

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

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

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

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

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

Use this formula to determine your RAM buffer size:

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

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.

\[
\frac{(\text{HDD Write Speed} / 8 \text{ bit}) \times 3600 \text{ Seconds}}{1024 \text{ bytes}} \text{ Gigabytes per hour}
\]
For instance:

\[
\frac{\text{(6 Mbps HDD write speed / 8 bit)} \times 3600 \text{ Seconds}}{1024 \text{ bytes}} \approx 2.63 \text{ GB per hour}
\]

Running Observer without reserved memory

This section discusses how Observer uses the protected memory for packet capture. It applies to all versions of Observer and NetFlow probes. This is the default, but not recommended, configuration. It is the default because each network is unique and you must determine how you want Observer to be configured for your system.

This section does not apply to the GigaStor or other hardware products from Network Instruments. They are properly configured at the factory.

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

After you install Observer and first open the program it does not have any reserved memory. Observer allocated a portion of the available protected memory for its use. This creates a “Windows memory pool” for Observer of about 50 to 80 MB (depending on the amount available from Windows, and cannot be increased).

1. Click the Memory Management tab to display the list of probe instances and their buffer sizes.
2. Click the Configure Memory button at the top of the window to view and modify how Observer uses the protected memory for this probe instance. The Edit Probe Instance window opens.

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

- 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.

## 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.

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 1 shows how much memory is required by the operating system. Anything beyond this amount may be reserved for Observer.

Table 12: 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 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.

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:

- For a 1 Gb Gen2 card, you need a minimum of 100 MB for the probe instance that monitors any Gen2 card. Allocating less than 100 MB for a probe instance monitoring a Gen2 card may cause instability.
- 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.)
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.

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 ? 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 23: 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.
Chapter 7: FAQ and Troubleshooting

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.

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.

- Ports 25901 and 25903 are open on your 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. Check any local system firewall as well as any network firewall. See also the information in Suspected NAT or VPN issues

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

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

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

- The probe and Observer analyzer are within the same minor build range. You can have the Observer analyzer automatically force an upgrade of an older probe version. See Upgrading the probe software
- 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 step 7.
   - If the VMONI driver is listed, remove it. Select VMONI Protocol Analyzer and click the Uninstall button. After the VMONI driver is removed, restart the system and continue with step 7.
7. From the Local Area Connection Properties (step 5), choose Install > Protocol > Add > 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 for explanation/resolution before proceeding.

**Solutions:** If you are using a Gigabit NIC to capture the traffic and you have checked the switch configuration, then try using this solution. For BCM5751M NetXtreme Gigabit chips found in IBM T43, HP laptops, and Dell Latitude laptops; there is a registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet can cause the driver and chip not to strip the 802.1Q headers. To set that key, you must find the correct instance of the driver in Windows registry and change it.

1. Open the Windows registry editor. Start > Run > Command and type regedit.
2. Search for “TxCoalescingTicks” and ensure this is the only instance that you have.
3. Right-click the instance number (e.g., 0008) and add a new string value.
4. Type PreserveVlanInfoInRxPacket and give it the value 1.
5. Restart the computer.

The Gigabit NIC no longer strips VLAN tags, so the symptom in Observer is resolved.

VLAN Statistics tool is not working

**Symptoms:** “No VLAN” is the only VLAN ID that shows up in the VLANs column in VLAN Statistics. You are not seeing all VLANs you have on the network.
Causes: To display VLAN Statistics, Observer checks each packet for a VLAN tag; if no tag is present, the packet is logged as “No VLAN.” Both 802.1Q or ISL VLAN tags are stripped unless the SPAN destination port to which the analyzer is attached has been configured to include VLAN tags.

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

If connecting the Observer analyzer to a Cisco switch, see the following link (it does require a TAC account): http://www.cisco.com/en/US/customer/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml.

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 | nongotiate] [vlan_range] [isl | dot1q | negotiate]
set span
source_port
destination_port [rx | tx | both]
```

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

```
switch (enable) set trunk 6/2 nonegotiate dot1q
switch (enable) set span 6/1 6/2
```

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

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

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

```
C4000 (config) # monitor session 1 source interface fastethernet 0/2
C4000 (config) # monitor session 1 destination interface fastethernet 0/6 encapsulation dot1q
```

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

```
C6500(config)#Interface Type slot/port
C6500(config-if)#Switchport
C6500(config-if)#Switchport trunk encapsulation { ISL | dot1q }
C6500(config-if)#Switchport mode trunk
C6500(config-if)#Switchport nonnegotiate
```

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

```
C6500 (config) # interface fastethernet 0/6
C6500 (config-if) #switchport
C6500 (config-if) #switchport trunk encapsulation dot1q
C6500 (config-if) #switchport mode trunk
C6500 (config-if) #switchport nonnegotiate
C6500 (config-if) #exit
C6500 (config) # monitor session 1 source interface fastethernet 0/2
C6500 (config) # monitor session 1 destination interface fastethernet 0/6
```
Using Discover Network Names on a Layer 3 switch that uses VLANs

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

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

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

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

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

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

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

**Suspected NAT or VPN issues**

If you use network address translation (NAT) in your environment, you must make some configuration changes in Observer. Using the TCP/IP port information in Ports used by probes and Observer, 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**

Network Instruments probes and Observer use TCP port 25901 and 25903 to transfer data and commands between the probe and the Observer analyzer. You may need to modify your firewall rules to allow communication on these ports for Observer.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirection/connection request</td>
<td>TCP 25903</td>
</tr>
<tr>
<td>Probe administration</td>
<td>TCP 25903</td>
</tr>
<tr>
<td>Analyzer–Probe connection</td>
<td>TCP 25901</td>
</tr>
</tbody>
</table>
Index

Numerics
25901 (port) 15, 15, 75, 81, 81
25903 (port) 15, 15, 75, 81, 81
32-bit 69
3DES 62
64-bit 69
64-bit, RAM 68
802.11 7, 10, 40
802.1Q 78

Default
10, 11, 11

A
adapter speed 39
address tables 32
AES 35
alarms 75
Anyone account 55, 75
Application Performance Analysis 60
Application Transaction Analysis 60
ATM 38, 40, 60
autoupgrade 35
Autoupgrade tab 30

B
backup
installation 29
backups 31
bad TCP checksums
troubleshooting 77
bandwidth saturation 10
bandwidth utilization 9
BIOS memory hole 69
broadcast traffic 41
buffer statistics 66
buffer, see capture buffer and statistics buffer 66
buffers 13, 68, 73

capture buffer 66, 66
32-bit Windows 66
64-bit Windows 66
limitations 66
Max Buffer Size 66
RAM limitations 66
size 66
capture card
driver requirements 26
capture card driver 26
capture decodes 40
CDU 40
Cisci 6xxx switches
troubleshooting 80
Cisco EAP/LEAP 33
collision test 80
Committed Information Rate (CIR) 55
configuring
network trending folder 34
probe name 33
CRC-16 38
CRC-32 38
CSU 40
encapsulation 38, 39

D
D3 40
data analysis time slice 35
data reconstruction 55
data transfer 58
Daylight Savings Time 80, 80
Discover Network Names 79, 79
VLANs 79
DNS resolution 34
driver requirements 26
drivers, wireless 24
DS3
fractionalized 38
DSUencapsulation 38, 39

E
E1 40
WAN relay type 39
E3 40
fractionalized 38
EAP/LEAP 33
Edit Probe Instance 67
capsulation 38, 39, 39, 40, 55
cryption 35, 62
cryption key 29, 33, 34, 62
ErrorTrak 23
Ethernet 7, 40
cables 16
full-duplex 9, 10
half-duplex 9
jumbo frames 40
port aggregator 10
Expert Probe 28, 35, 58
as probe or analyzer 53
changing NIC 41, 41
configuring 39, 39
connecting to analyzer 44
data transfer 58
GigaStor 57
NetFlow 60
port bonding 53
redirection 44

F
filters 55, 61
firewall 15, 81
firewall, ports 15, 75, 81
fractionalized 38, 39
frame check sequence 40
frame checksum 40
frame relay 11, 40
frame size 40
Frame too large 40
full-duplex 53

G
Gen2 card
  full-duplex 53
Gigabit copper 16
GPS 57
  passive probe instance 13
  performance 13
  probe instance warning 13
  recommendations 70, 70
  time synchronization 57
Gigabit 40
  jumbo frames 40
gigabytes 66, 66
GigaStor
  AES 35
  collision test 80
  data analysis time slice 35
  encryption 35
  Expert Probe 57
  RAM 70
  recommendations 70
  reserved memory 70
  traffic generation 80
  virtual machine with 50
GigaStor capture 14
GPS 57

H
hardware probes
  10Gigabit 20
  Gigabit 20
hardware requirements 23
HSSI 39, 40
HSSI, fractionalized 40

I
installing 16
IP address
  GigaStor 18, 42
  NAT 79
  setting 18, 18
  IP masquerading, see NAT 79
  IP precedence 40
  IPv4 60
  IPv6 60

J
jumbo frames 40

L
LAPB 40
laptop
  NICs 33
  using as probe 33
  wireless 33
Layer 3 Switch 79
license 32
licenses 28, 28, 28
  redeeming 28
  troubleshooting 28, 28, 28
Licensing Observer 28
line frame 40
load, preprocessor 13

M
MAC addresses 79
Mac Header 60
man-in-the-middle, preventing 62
Max Buffer Size 66
megabytes 13
memory management 66
memory, see RAM 72
Microsoft 30
mirror port 8
mirror port, see also SPAN ports 8
MPLS 11, 39, 43, 60
  ATM 60
  IPv4 60
  IPv6 60
  Mac Header 60
  pseudowire word 60
Multi Probe 28
  changing NIC 41, 41
  configuring 39, 39
  connecting to analyzer 44
  data transfer 58
  limitations of 59
  redirection 44
  multicast 31

N
NAT 79, 79
NetFlow 20, 40
  TAPs and 80
  versions supported 60
NetFlow collector 60
NetFlow Trending collector 60
Network 1 probe instance 59
network adapter, see also NIC 41
Network Instruments Management Server 34
network masquerading, see NAT 79
network traffic 11
network trending 40, 75
  filters 61
  sampling divider 61
  securing 55
Network Trending 31
network visibility 9
NIC 24
  broadcast traffic 41
  changing 41
  missing 41, 76
  missing from Observer 41
  multiple in a system 57
  with packet analyzers 10
NIMS 34, 54, 62, 62
NIProbe.exe 28

O
Observer
Index

no network card 41
ports used 15, 81
system requirements 23, 23
updating 29
observer.exe 28
OSI Layer 2 11
OSI Layer 7 59

P
packet capture 14, 40, 72
80
active instance vs. passive instance 13
buffer 66
daylight savings time 80
memory 67
RAM 72
securing 55, 55
packet captures
wireless 23, 33
packets
moving through RAM 72
RAM 72
partial packet capture 55
port aggregator 10
ports 15, 81
ports used 15, 81
Probe administration, port required 15, 81
probe instance 8, 13, 14
active 12, 13, 13, 66
active vs. passive 12
best practices 13
configuring 40
configuring statistics memory 56
connecting 42
connecting to analyzer 57
defining its purpose 70
definition of 12
memory allocation 56
memory tuning 66
naming 59
passive 12, 13, 14
redirecting 42
reserving memory 66
security 54
specifying NIC 57
Probe Options 19
probe redirection 44
Probe Service Configuration Applet 19, 53
probes
Adapter Speed tab 39
as Windows service 30
Autoupgrade tab 40
autoupgrading 35, 40
backing up 31
clock synchronization 57
collecting data 41
common problems with 74, 75
configuring 33
connecting to analyzer 44, 44
D3/E3/HSSI 40
definition 7
encryption keys 29
General tab 39
Gigabit tab 40
hardware 67

in a switched environment 8
IP precedence 40
MPLS 39, 60
name, changing 33
not connecting 75
options 34
placing in your network 8
port bonding 53
ports used 15, 81
protecting 30
running as Windows service 34
securing 55
security 55
statistics sampling divider 39
T1/E1 tab 40
updating 30
upgrading 29, 29
Virtual Adapters tab 40
virtual TAPs 50
VLAN access 76
WAN 40
wireless 40
Wireless 802.11 tab 40
promiscuous mode 8, 23, 33, 50
protected memory 64, 64, 67, 67, 67, 69, 72
pseudowire word 60

Q
QoS 40

R
RAID 13, 13, 14, 14
RAM 64, 64, 72
allocating 70
buffer size 13
effects of packet capture 72
formula 66
GigaStor 70
limitations 66
packet capture 13, 66
see also buffer 66
see also protected memory, user memory, and
reserved memory 64
recommendations 68
reserving for Observer 56
resizing 64
statistics 66
tuning 66
used in Observer 64
Windows 66
Random Access Memory, see also RAM 64
Reconstruct Stream 55
redirecting, see probes 44
redirection 44
requirements, hardware/software 23
reserved memory 64, 64, 64, 67, 67, 68, 68, 73
see also RAM 64
RF signals 10
RMON 8
running Observer or Probe 53

S
scripts 32
security
Index

Anyone account 55
authentication 62
encrypting data 55
encryption key 62, 75
filters 55
man-in-the-middle 62
matching between probe and analyzer 75
NIMS 62
partial packet capture 55
permissions 55
personal information 28
probe configuration 55
probe instances 54
Probe redirection error 75
reconstructing data 55
users 55
VoIP 55
sFlow 20, 40, 43
sFlow collector 60
sFlow, versions supported 61
SFP 16
Single Probe 28
Anyone account 56, 75
changing NIC 41, 41
configuring 39, 39
data transfer 58
redirection 44
security 56
VoIP 59
SNMP 8, 31
SNORT 31
software probes 29
software requirements 23
SPAN
VLANs 78
SPAN ports
bandwidth utilization 9
broadcast traffic 41
cost-effectiveness 9
Ethernet 9
settings 8
see also mirror port 8
traffic duplication 9
using 11
virtual machine 50
visibility 10
where to use 9
statistics 39, 40
collection interval 61
memory 67
packet capture 40
RAM needed for busy networks 70
sampling divider 61, 75
statistics buffer 66, 66, 66
statistics memory configuration 71
statistics queue buffer 65, 68, 68, 70, 72, 73
synchronization 57, 80
T
T1 40
WAN relay type 39
TAP 16
full-duplex Ethernet 10
NetFlow 80
where to use 9
TAPs
placing 11
TCP 18, 79
TCP 25901 15, 81
TCP 25903 15, 81
TCP Dump 55
TCP/IP 18, 79
TCP/IP settings 18
third-party capture card
driver requirements 26
time synchronization 80
time synchronization 57
Top Talkers 66
topologies 7
802.11 7
Ethernet 7
ToS 40
traffic generation 80
triggers 75
Triple DES 55, 62
see also encryption 55
troubleshooting
analyzer connection 75
bad TCP checksums 77
Cisco 6xxx switches 80
common issues 74
licenses 28, 28, 28, 28
probe connection 75
slow probe system 74
VLAN Statistics tool 77, 77
VLAN visibility 79
U
updating
Observer 29
updating virus protection 30
upgrading 29
upgrading, encryption keys 29
user memory 64, 64, 64
users 75
administrator 55
Anyone 55
V
virtual adapter 14, 40, 50, 53
virtual IP 11
virtual machine 23, 50, 50
virtual NIC 50
virtual TAP 50
virus protection 30
VLAN 20, 77, 78
"No VLAN" 77, 77
VLAN Statistics 77
VLANs 77
Discover Network Names 79
SPAN port 78
VMONI 76
VMONI Protocol Analyzer 76
VoIP 11, 40, 55, 60
VPN 11, 79
W
WAN 11, 40
encapsulation 55
fractionalized 40
security 55
WAN Type 38, 39
Windows 24
  32-bit 31, 69
  64-bit 31, 50, 66, 69
registry 32
Remote Desktop 18
  reserved memory in Observer 56
service 19, 34
services 54, 54
Windows memory pool 67, 67
Windows protected memory 64
Windows updates 30
wireless 7, 10, 40
wireless access point 10, 10, 11, 33
wireless driver 24
wireless network, encryption key 33
wireless packets, raw 23, 33
wireless probe 11