GIGASTOR™

GigaStor User Guide

Trademark Notices

Open Source Copyright Notices

Limited Warranty—Hardware

Network Instruments, LLC. ("Network Instruments") warrants this hardware product against defects in materials and workmanship for a period of 90 days 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 Network Instruments' London, UK office. 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.

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.

End User License Agreement (EULA)

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE.

BY CLICKING ON THE "ACCEPT" BUTTON, OPENING THE PACKAGE, DOWNLOADING THE PRODUCT, OR USING THE EQUIPMENT THAT CONTAINS THIS PRODUCT, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DO NOT ACCEPT" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE, RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND, OR DO NOT DOWNLOAD THE PRODUCT.

The SOFTWARE is neither shareware nor freeware. The SOFTWARE is a commercial software package that is subject to international copyright laws.

Single User License Grant: Network Instruments, LLC ("DEVELOPER") and its suppliers grant to END-USER a nonexclusive and nontransferable license to use the DEVELOPER software ("SOFTWARE") in object code form solely on a single central processing unit owned or leased by END-USER or otherwise embedded in equipment provided by DEVELOPER.

Multiple-Users License Grant: DEVELOPER and its suppliers grant to END-USER a nonexclusive and nontransferable license to use the DEVELOPER SOFTWARE in object code form: (i) installed in a single location on a hard disk or other storage device of up to the number of computers owned or leased by END-USER for which END-USER has paid individual license fees purchased; or (ii) provided the SOFTWARE is configured for network use, installed on a single file server for use on a single local area network for either (but not both) of the following purposes: (a) permanent installation onto a hard disk or other storage device of up to the number of individual license fees purchased; or (b) use of the SOFTWARE over such network, provided the number of computers connected to the server does not exceed the individual license fees purchased. END-USER may only use the programs contained in the SOFTWARE (i) for which END-USER has paid a license fee (or in the case of an evaluation copy, those programs END-USER is authorized to evaluate) and (ii) for which END-USER has received a product authorization keys ("PAK"). END-USER grants to DEVELOPER or its independent accountants the right to examine its books, records and accounts during END-USER's normal business hours to verify compliance with the above provisions. In the event such audit discloses that the Permitted Number of Computers is exceeded, END-USER shall promptly pay to DEVELOPER the appropriate licensee fee for the additional computers or users. At DEVELOPER's option, DEVELOPER may terminate this license for failure to pay the required license fee.

END-USER may make one (1) archival copy of the SOFTWARE provided END-USER affixes to such copy all copyright, confidentiality, and proprietary notices that appear on the original.

EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, END-USER SHALL NOT: COPY, IN WHOLE OR IN PART, SOFTWARE OR DOCUMENTATION; MODIFY THE SOFTWARE; REVERSE COMPILE OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, SELL, OR CREATE DERIVATIVE WORKS OF THE SOFTWARE.

END-USER agrees that aspects of the licensed materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of DEVELOPER. END-USER agrees not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of DEVELOPER. END-USER agrees to implement reasonable security measures to protect such trade secrets and copyrighted material. Title to SOFTWARE and documentation shall remain solely with DEVELOPER.

SOFTWARE, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. END-USER agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import SOFTWARE.

This License shall be governed by and construed in accordance with the laws of the State of Minnesota, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This License constitutes the entire License between the parties with respect to the use of the SOFTWARE.

Restricted Rights - DEVELOPER's software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph "C" of the Commercial Computer SOFTWARE - Restricted Rights clause at FAR 52.227-19. In the event the sale is to a DOD agency, the government's rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202. Manufacturer is Network Instruments, 10701 Red Circle Drive, Minnetonka, MN 55343, USA.

Technical Support

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

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

UK and Europe at +44 (0) 1959 569880

By fax (depending on where you are located):

US & countries outside of Europe at (952) 358-3801

UK and Europe at +44 (0) 1959 569881

Or by e-mail at:

US & countries outside of Europe: support@networkinstruments.com

UK and Europe: support@networkinstruments.co.uk

Network Instruments provides technical support for a period of 90 days after the purchase of the product at no charge. After the 90-day initial support period, 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.

To subscribe to the Network Instruments e-mail newsletter (delivered in HTML format), send an e-mail to listserver@networkinstruments.com with the word "subscribe" in the subject line.

Contents

Chapter 3: Packet Capture or GigaStor Capture

Chapter 4: GigaStor Control Panel

Chapter 5: Using Observer with a WAN Probe

Chapter 6: Forensic Analysis using Snort

Chapter 1
About the GigaStor

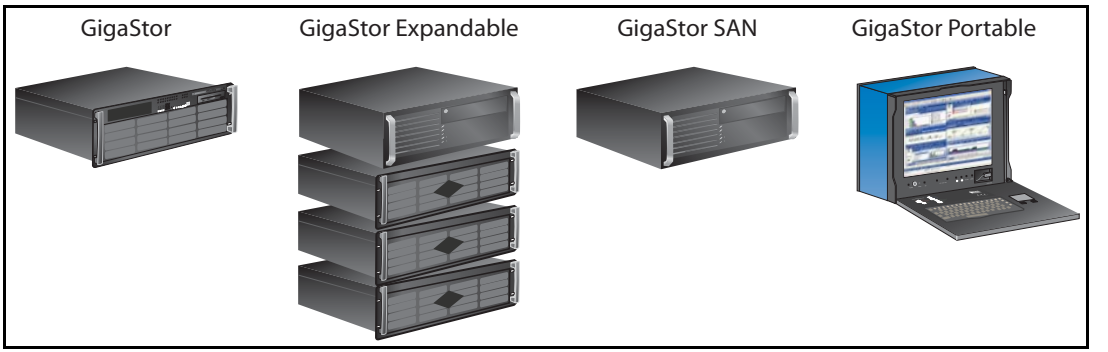
GigaStor versions

The GigaStor is an enterprise-strength network probe appliance. The GigaStor combines a multi-terabyte, high-performance Redundant Array of Independent Disks (RAID) with a dedicated, high-speed network capture card in a modular, easy-to-deploy appliance.

There are these versions of the GigaStor:

- GigaStor
- GigaStor Expandable: a controller PC along with one, two, or three disk expansion units that can store up to a total of 288 terabytes of data.
- GigaStor SAN: a controller PC that connects to your SAN to write its data. It uses a fibre channel host bus adapter that can operate at 1, 2, or 4 Gigabit speed for connectivity.
- GigaStor Portable: a portable GigaStor

Figure 1 GigaStor models



NOTE: Unless specifically noted, all information in this manual applies to all versions of the GigaStor: GigaStor, GigaStor Expandable, GigaStor SAN, and GigaStor Portable.

If your GigaStor is configured to monitor Gigabit Ethernet, 10Gb Ethernet, and Fibre Channel connections, the capture card is a Gen2 card with SFP (or XFP) modules. This allows you to hot-swap any SFP-compliant connectors into the your appliance. This makes it

possible to use the same probe to monitor different types of links as needed. For example, you can easily convert the capture card from optical to copper, allowing you to connect the GigaStor to different test access points (TAPs) or switch port analyzer (SPAN) or mirror interfaces.

If your GigaStor is configured to monitor WAN (such as E1, T1, E3, DS3, or HSSI) connections, your GigaStor has a specialized WAN capture card. It does not have SFP or XFP connectors.

The GigaStor can be used with the Expert Observer console or Observer Suite to troubleshoot your network. Alternatively, you can run the probe in "local console" mode, allowing you to analyze GigaStor-collected data locally.The local console on the GigaStor is Observer Expert. However, we recommend that you use Observer on a remote system to analyze the data.

Chapter 2
Installing Your GigaStor

The general steps to install your GigaStor are:

- ☐ "Unpacking and inspecting the parts" on page 18
- ☐ "Installing the GigaStor and connecting the cables" on page 19
- ☐ "Connecting Observer to the GigaStor" on page 22

Additional steps to complete the installation are:

- ☐ "Configuring Observer for your Gigabit device" on page 31
- ☐ "Configuring Observer for your WAN device" on page 33
- ☐ "Tapping an Ethernet or Fibre Channel connection" on page 37
- ☐ "Tapping a WAN connection" on page 42
- ☐ "Installing the drives in your GigaStor" on page 50

Unpacking and inspecting the parts

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

- ☐ One rack-mountable GigaStor system with an installed 10/100/1000 Ethernet network interface (management) card.
  - ☐ Appropriate capture interface (Gen2 or WAN).
  - ☐ The rack unit may also include a rail kit depending on which model was purchased.
  - ☐ Windows XP 64-bit operating system and a restore DVD specific for your GigaStor.
- ☐ TAP kits for your topology (Ethernet, Fibre Channel, or WAN), except for the GigaStor 2TE.
- ☐ Cables
  - ☐ Ethernet cable for each 10/100/1000 interface in your GigaStor.
  - ☐ Connection cables to connect your GigaStor to a TAP or switch.

Installing the GigaStor and connecting the cables

1. Install the GigaStor and any expansion units into your rack using the supplied rails. Instructions for installing the rail kits are provided in the rail kit box.
2. Install the drives into the GigaStor and any expansion units. See "Installing the drives in your GigaStor" on page 50.
3. Connect the GigaStor, TAP, and cables. See:
   - "Tapping an Ethernet or Fibre Channel connection" on page 37 for details about optical and copper Gigabit Ethernet, 10 Gigabit Ethernet, and Fibre Channel connections.
   - "Tapping a WAN connection" on page 42 for details about T1/E1 and DS3 connections.
   - "Connecting the GigaStor Expandable to the expansion units" on page 52.
   - See the fibre channel host bus adapter (QLogic or other third party) documentation included in the GigaStor packaging if you are using a GigaStor SAN.

Setting the GigaStor's IP address

At this point you have physically installed the hardware and connected all the cables. Now, you must turn on the GigaStor and configure the software.

1. Connect a monitor, keyboard, and mouse to the GigaStor and ensure the GigaStor 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 GigaStor to make these changes. The default IP address is 192.168.1.10.
2. If you are using a GigaStor Expandable, remember to start the disk expansion units.
3. Turn on the system. On the back of the GigaStor ensure the power switch is turned on. Then on the front of the GigaStor, press the power button until the system starts to turn on.

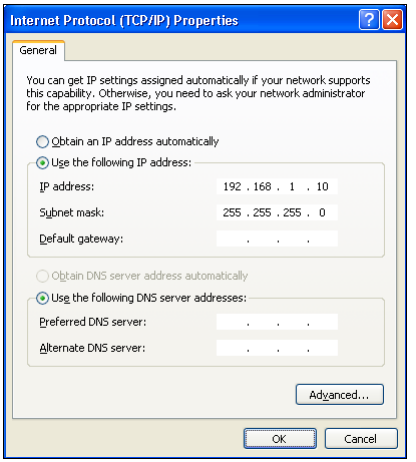
4 Ensure that each drive's power/activity light is lit. If a drive's light is not lit, it is likely that the drive is not seated properly. Turn off the GigaStor and reseat the drives. For more information, see "Installing the drives in your GigaStor" on page 50.

5 Log in using the Administrator account. The default Administrator password is **admin**.

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

7 Select Internet Protocol (TCP/IP) from the list and click Properties (Figure 2).

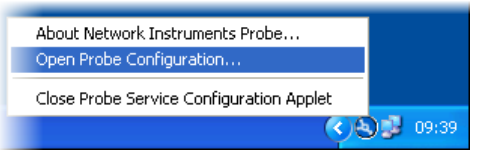
Figure 2 Default TCP/IP settings



8 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.

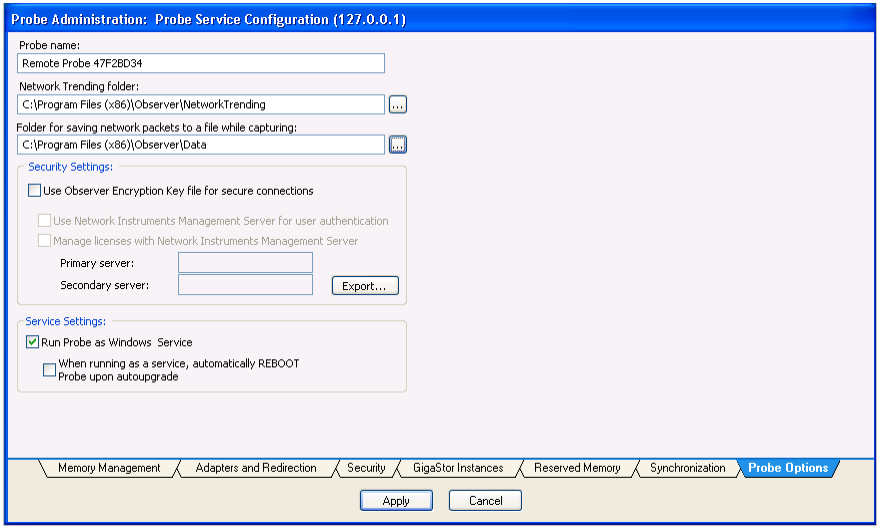
9 Right-click the Probe Service Configuration Applet in the system tray and choose Open Probe Configuration.

Figure 3 Probe Service Configuration Applet



10 The Probe Administration window opens. Click the Probe Options tab (Figure 4).

Figure 4 Probe Options



11 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 console on the GigaStor. You must connect to the GigaStor using Observer on a different system. If you want to use the Observer console locally, see "Using the Observer console locally on the GigaStor" on page 108.

Connecting Observer to the GigaStor

This section assumes you have already installed Observer on your desktop or laptop. If not, install the software. You can download from the Network Instruments website.

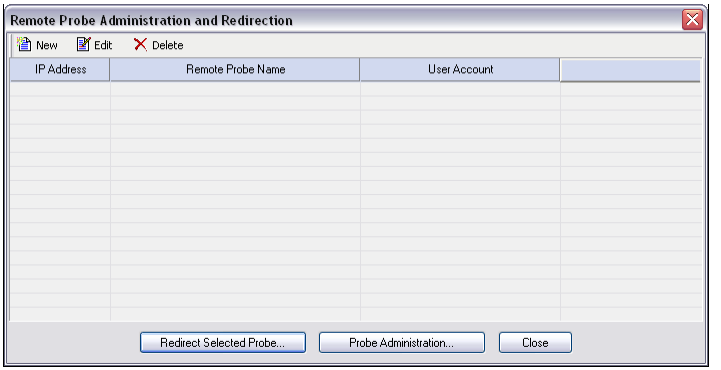
There are three main tasks to connect Observer to your GigaStor

- "Redirecting the GigaStor probe" on page 22
- "Probe administration" on page 24
- "GigaStor Capture Analysis" on page 29

Redirecting the GigaStor probe

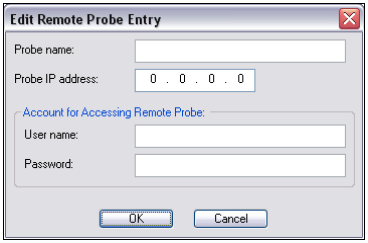
1. Choose Start →All Programs →Observer →Observer. Observer opens.
2. Select Actions →Redirect Probe (Figure 5).

Figure 5 Remote Probe Administration and Redirection



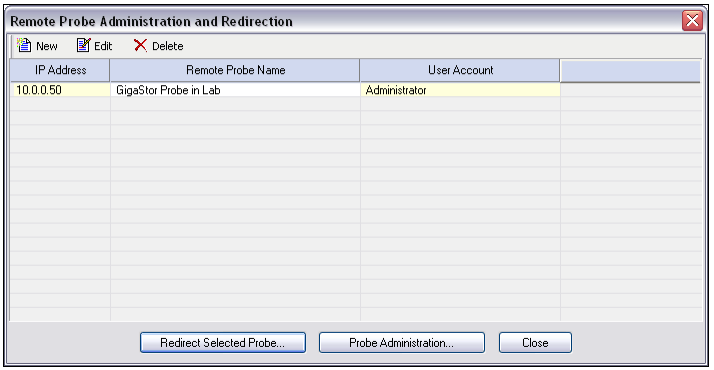
3. Click New to add the GigaStor to the Probe Administration and Redirection list. Figure 6 appears.

Figure 6 Edit Remote Probe Entry



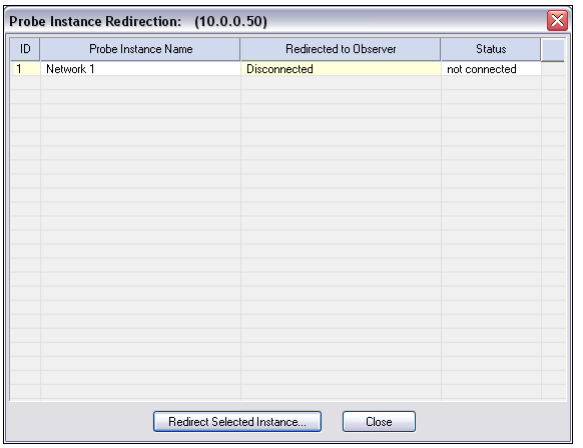
4 Type the IP address that you assigned to the GigaStor in step 7 in "Setting the GigaStor's IP address" on page 19 and click OK. You may leave the other fields blank. If you type a name, the name will change after Observer connects to the remote probe. The GigaStor appears in the list of probes available for redirection (Figure 7).

Figure 7 Probe added to Remote Probe Administration and Redirection



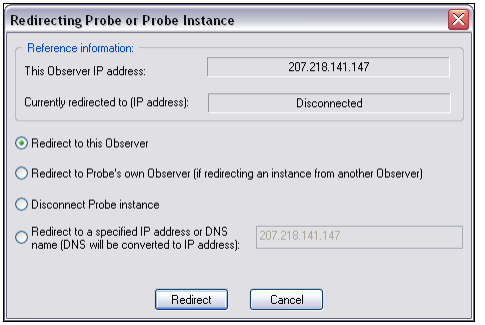
5 Select the GigaStor probe and then click Redirect Selected Probe (Figure 8).

Figure 8 Probe Instance Redirection



6 Select the probe instance and click Redirect Selected Instance. Figure 9 appears.

Figure 9 Redirecting Probe or Probe Instance



7 Choose the "Redirect to this Observer" option, then click the Redirect button. Within 30 seconds the GigaStor will connect to the local Observer. If you use NAT, see "NAT" on page 124.

8 Close the Probe Instance Redirection window.

Probe administration

Now that your GigaStor is connected to your Observer console, you can administer it.

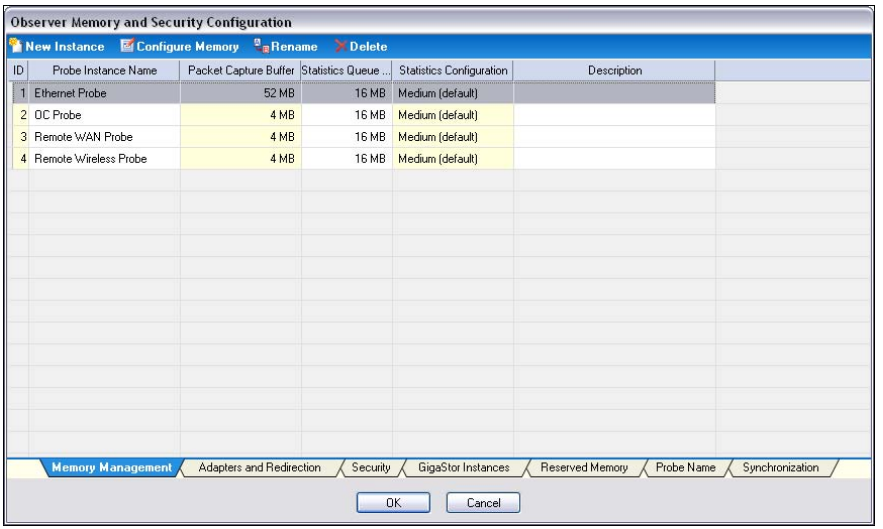
1 Click Probe Administration (see Figure 7). The Probe Administration Login window opens.

Figure 10 Remote Probe Administration

2 Ensure "Login using a user account configured for this Probe" is selected and click OK.

The Probe Administration window opens to the Memory Management tab (Figure 11).

Figure 11 Memory Management tab

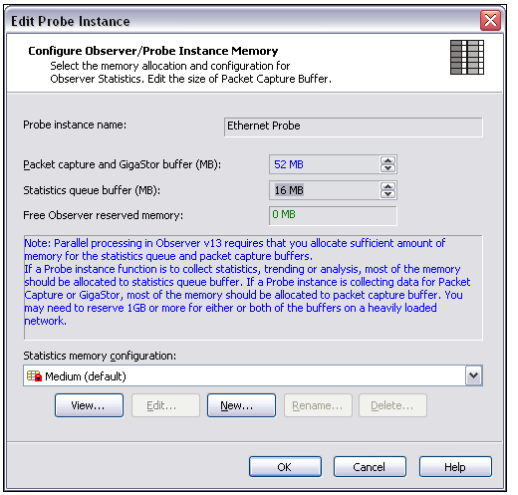


3 Select the Network 1 probe instance and click Rename. Choose a name that is meaningful to you for the probe instance name and click OK. By default, Network 1 is your active probe instance for your GigaStor. For details about active and passive probe instance, see "Probe Instances" on page 111.

By default all of the installed memory on the GigaStor is dedicated for one probe instance. You must first release the memory so that you can assign the freed memory to other probe instances.

4 With the newly renamed probe instance still selected, click Configure Memory (Figure 12) at the top of the window.

Figure 12 Edit Probe Instance: Capture Buffer Memory



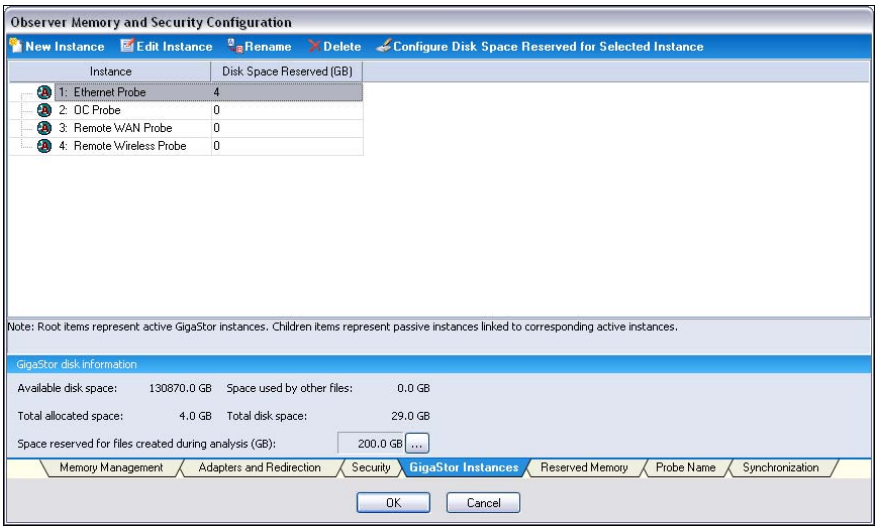
5 Use the arrows to release some memory. Free enough memory to create your probe instances and click OK. At a minimum each probe instance requires12 MB memory. It uses 4 MB for statistics and 8 MB for packet capture. Don't worry about freeing too much memory. If you determine you released too much, you can reallocate it later to the capture buffer or operating system.

Because Observer operates in real-time, its buffers must always remain in RAM; if the buffers resided in standard Windows user memory, nothing would prevent the buffer file from being swapped out to disk and subsequent packet loss. For this reason, the probe reserves its memory from Windows upon startup so that no other applications can use it and cause the buffer to be swapped out to disk.

For more information about buffers, see "Packet capture buffer and statistics buffer" on page 54.

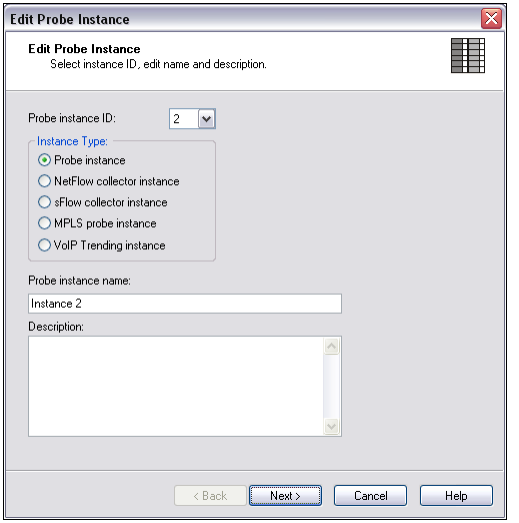
6 Click the GigaStor Instances tab (Figure 13).

Figure 13 GigaStor Instances



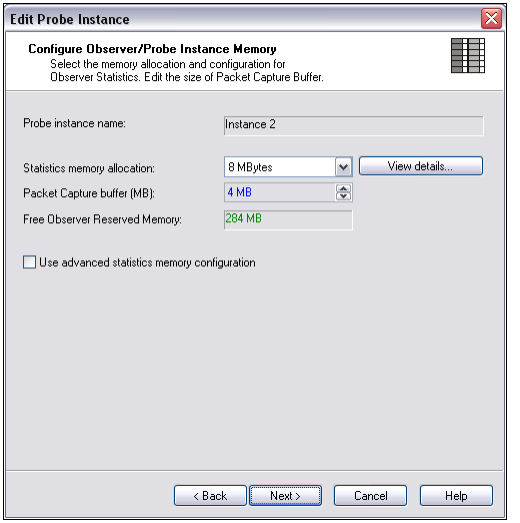
7 Click New Instance. Figure 14 appears.

Figure 14 Edit Probe Instance: Name



8 You are configuring a GigaStor probe to capture data and write it to the hard drive. Therefore ensure "Probe instance" is selected in the Instance type. Type a name and description and click Next.

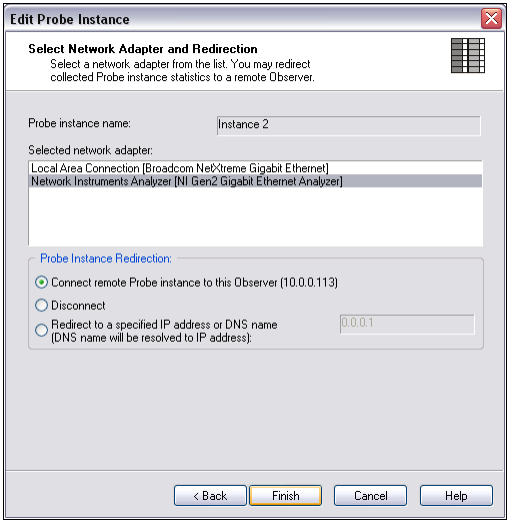
Figure 15 Edit Probe Instance: Configure Memory



9 From the RAM that you released earlier, assign some of it to this probe instance and click Next.

10 Ensure the correct network adapter is selected and click Finish to redirect the GigaStor to your local Observer console.

Figure 16 Edit Probe Instance: Connect to Console



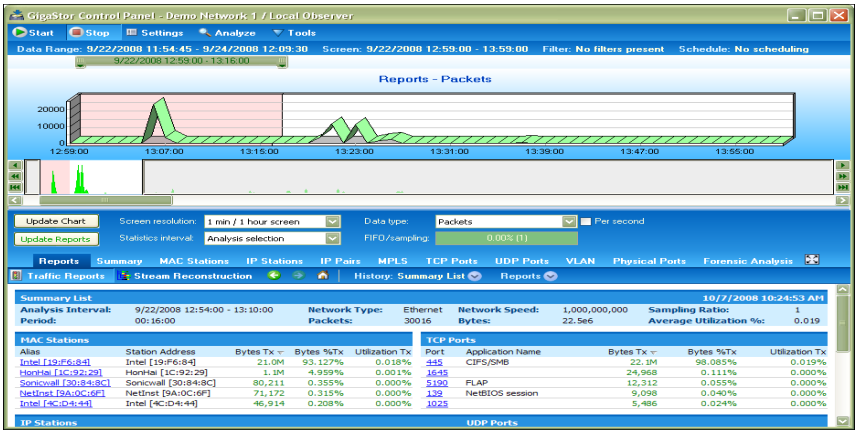
11 Repeat step 7 through step 10 until you have created all of your probe instances. Any unused memory should be reallocated to the packet capture buffer of the active probe instance or to the operating system.

12 Click OK to close the Probe administration windows. After a moment the GigaStor probe and any probe instances appear in the Observer Probe list found along the left side of the main Observer window.

GigaStor Capture Analysis

1 Click Capture →GigaStor Capture Analysis to begin viewing network traffic that passes through the GigaStor probe. The GigaStor Control Panel opens (Figure 17).

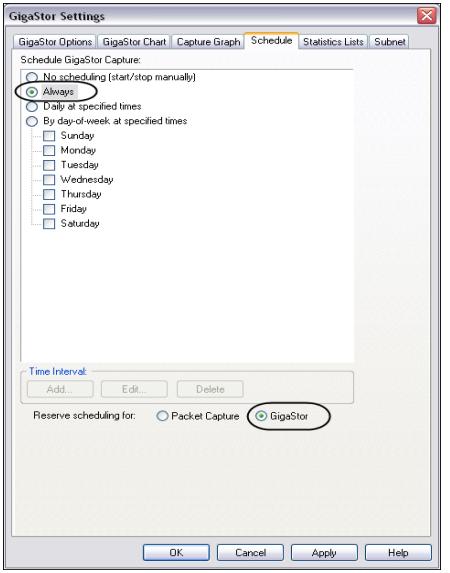
Figure 17 GigaStor Control Panel



At this point the data is not being written to disk unless you manually click the Start button. With most GigaStor installations, you want the GigaStor probe to always be writing its data to disk.

2 Click Settings in the middle of the top menu bar. The GigaStor Settings window opens. Click the Schedule tab.

Figure 18 GigaStor Settings Schedule tab



3 In the Schedule GigaStor Capture section, select Always. For more information about a packet capture vs. GigaStor capture, see "Packet Capture or GigaStor Capture" on page 53.

4 In the Reserve scheduling for section, select GigaStor and click OK. You may receive a notice about scheduling reservation. If you do, click Yes to change the scheduling.

You have installed your GigaStor! Now you must configure some settings in Observer before getting the maximum results from your new network analysis tool.

- If you are monitoring a Gigabit connection, you must configure the WAN device. See "Configuring Observer for your Gigabit device" on page 31 for details.
- If you are monitoring a WAN connection, you must configure the WAN device. See "Configuring Observer for your WAN device" on page 33 for details.
- If you are monitoring any other connection, begin using Observer to analyze the data. To get started, take use the GigaStor Control Panel. It is described in "GigaStor Control Panel" on page 57.

Configuring Observer for your Gigabit device

Depending on your probe and your network, you may need to make some changes from the factory defaults.

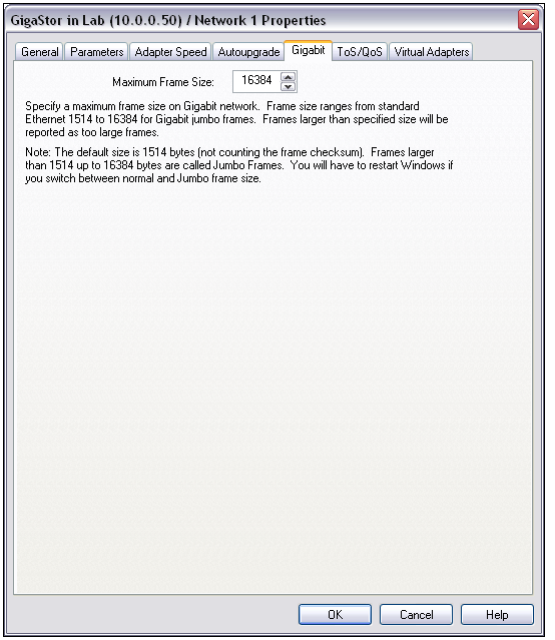
- "Jumbo Frame Support (Gigabit Ethernet)" on page 31
- "Configuring Terms of Service and Quality of Service settings" on page 32

Jumbo Frame Support (Gigabit Ethernet)

When a Gigabit Ethernet GigaStor is the selected probe, Observer displays an additional Gigabit tab on the Probe or Device Setup dialog. This allows you to adjust the maximum frame size. 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 (i.e., 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.

1. Select the gigabit probe and right-click. A menu appears. Choose Probe or Device Settings.
2. Click the Gigabit tab (Figure 19).
3. Change the frame size to suit your needs and click OK.

Figure 19 Gigabit tab

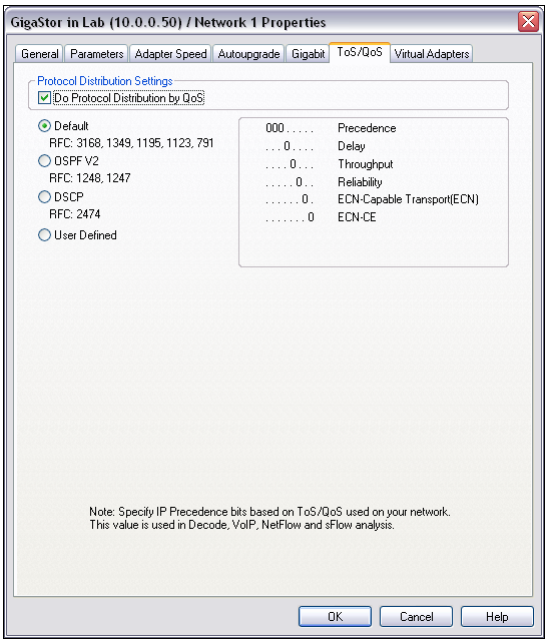


Configuring Terms of Service and Quality of Service settings

The ToS/QoS settings are configured for each probe.

1. Select the gigabit probe and right-click. A menu appears. Choose Probe or Device Settings.
2. Click the ToS/QoS tab (Figure 20).
3. Specify the IP precedence bits for the terms of service/quality of service for your network.

Figure 20 ToS/QoS tab



Configuring Observer for your WAN device

There are a number of setup options and statistical displays unique to WAN Observer, which are described in the following subsections.

Before you can analyze the WAN link, you must set some device options. You must also have the appropriate administrative privileges to change WAN device settings.

- “Digital DS3/E3/HSSI Probe Settings” on page 34
- “Digital T1/E1 Probe Settings” on page 35
- “Serial T1/E1 Probe Settings” on page 36

After configuring your connection, you should begin using Observer to monitor your connections. To get started, use the information in “Using Observer with a WAN Probe” on page 79.

Digital DS3/E3/HSSI Probe Settings

To access the probe settings, select the probe, right-click and choose Probe or Device Settings. Then click the DS3/E3/HSSI tab (Figure 21).

Figure 21 DS3/E3/HSSI Probe Settings

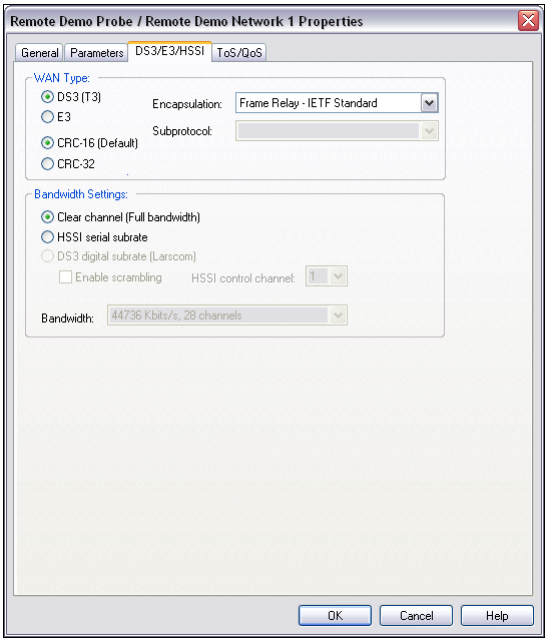


Table 1 describes fields in Figure 21.

Table 1 DS3/E3/HSSI probe settings

Setting	Explanation
WAN Type	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.
Encapsulation	You must set this to match the settings on the frame relay CSU/DSU.
Subprotocol	If ATM or LAPB is the selected encapsulation method, you must choose the sub-protocols on the link.
Fractionalized	Check if your link is configured for fractionalized operation. Fractionalized DS3 and E3 are not supported.
Bandwidth (HSSI)	Set to match the bandwidth and channel settings of the fractionalized HSSI link under analysis.

Digital T1/E1 Probe Settings

To access the probe settings, select the probe, right-click and choose Probe or Device Settings. Then click the T1/E1 tab (Figure 22).

Figure 22 T1/E1 WAN Probe Settings

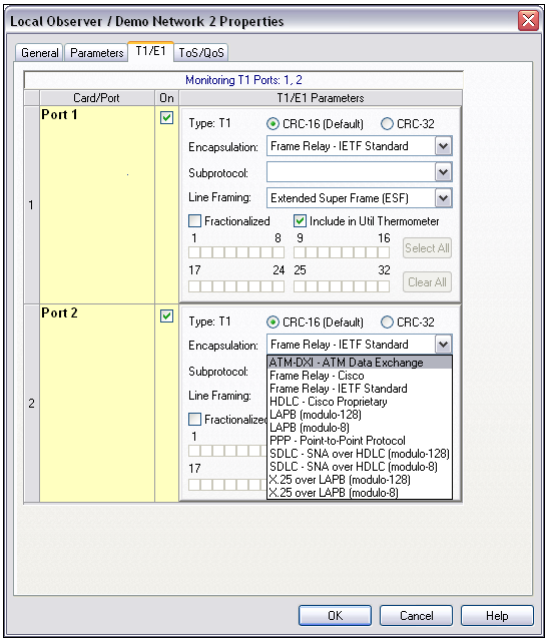


Table 2 describes fields in Figure 22.

Table 2 T1/E1 WAN Probe Settings

Setting	Explanation
WAN/Frame Relay Type	Choose T1 or E1 to match the type of link you are analyzing.
Encapsulation	You must set this to match the settings on the frame relay CSU/DSU.
Subprotocol	If ATM or LAPB is the selected encapsulation method, you must choose the sub-projects on the link.
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).	
Fractionalized	Check if this link is configured for fractionalized operation.
Channel selector check boxes	Choose the channels you want to be included in the analysis.
Include in Util. Thermometer.	Check if you want to include statistics from this link in the Bandwidth Utilization Thermometer.

Serial T1/E1 Probe Settings

Table 3 describes fields for a serial T1/E1 connection.

Table 3 Serial T1/E1 probe settings

Setting	Explanation
WAN/Frame Relay Type	Choose T1 or E1 to match the type of link you are analyzing.
Encapsulation	You must set this to match the settings on the frame relay router.
Fractionalized	Check if your link is configured for fractionalized operation.
Bandwidth	Set to match the bandwidth setting of the link you are analyzing.

Tapping an Ethernet or Fibre Channel connection

This section describes how to connect the cables for these environments:

- "10/100/1000, 10GbE Optical, and Fibre Channel" on page 37
- "Gigabit copper" on page 40

10/100/1000, 10GbE Optical, and Fibre Channel

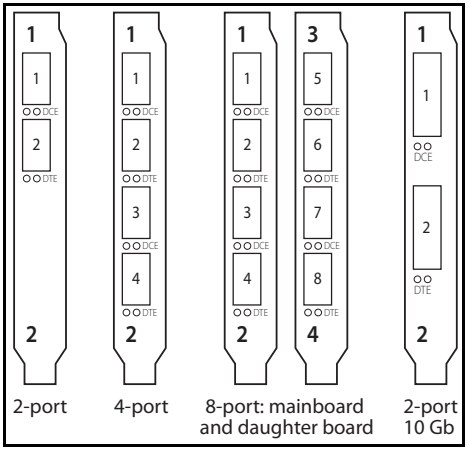
The optical Ethernet kit includes:

- Optical TAP
- One, two, or four full duplex optical cables depending on which Gen2 card you purchased.
- One, two, or four optical Y-analyzer cables

To connect the TAP to the GigaStor:

1. Insert the supplied SFP connectors (XPF connectors for 10GbE) into the open slots on the back of the Gen2 card(s).
2. If you have a GigaStor Expandable, see "Connecting the GigaStor Expandable to the expansion units" on page 52 for details about connecting the expansion units. After connecting them, continue with step 3.
3. Connect the TX Data Circuit-terminating Equipment (DCE) or SAN port to the Link A port on the *n*TAP.
4. Connect the TX port on the Gigabit switch (DCE) or Fibre Channel Fabric to the Link B port on the *n*TAP.
5. Use the Y-analyzer cable to connect the *n*TAP to the Gen2 capture card in the GigaStor. If you have more than one *n*TAP, repeat for each additional *n*TAP.

Figure 23 Gen2 card port assignments



6 Use the supplied Ethernet cable to connect the network interface card in the GigaStor to the network.

NOTE: STRAIGHT-THROUGH CABLE

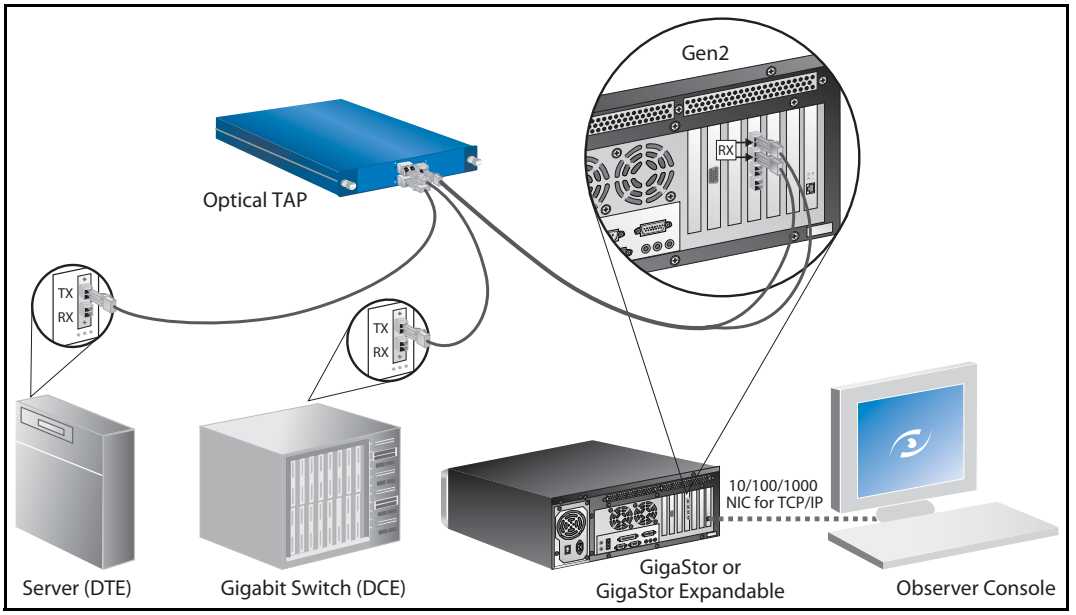
If you are using a switch's SPAN/mirror port, no *n*TAP is required. Simply plug any straight-through or Fibre cable between the SPAN/mirror port and one of the ports on the Gen2 capture card.

Fibre Channel has auto-negotiation disabled by default. You must enabled it first, then connect it to the SPAN or mirror port on your switch.

Now that you have physically connected the cables for the GigaStor, you must now configure its software. See "Setting the GigaStor's IP address" on page 19.

Figure 24 shows the GigaStor cabled to analyze a server. The TAP can replace the connection between any DCE (Data Circuit-terminating Equipment) and DTE (Data Terminal Equipment) device or connection.

Figure 24 GigaStor with an optical *n*TAP



Gigabit copper

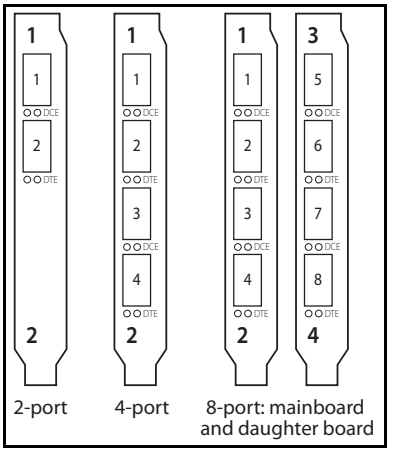
The Gigabit copper kit includes:

- Copper *n*TAP
- 1, 2, or 4 standard Ethernet cables
- 2, 4, or 8 analyzer cables

To connect the TAP to the GigaStor:

1. Insert the supplied SFP connectors into the open slots on the back of the Gen2 card(s).
2. If you have a GigaStor Expandable, see "Connecting the GigaStor Expandable to the expansion units" on page 52 for details about connecting them. After connecting them, continue with step 3.
3. Connect the TX Data Circuit-terminating Equipment (DCE) or SAN port to the Link A port on the *n*TAP.
4. Connect the TX port Gigabit switch (DCE) to the Link B port on the *n*TAP.
5. Use the two analyzer cables to connect the analyzer port on the *n*TAP to the Gen2 capture card in the GigaStor. If you have more than one *n*TAP, repeat for each additional *n*TAP.

Figure 25 8-port Gen2 card port assignments



6 Use the supplied Ethernet cable to connect the network interface card in the GigaStor to the network.

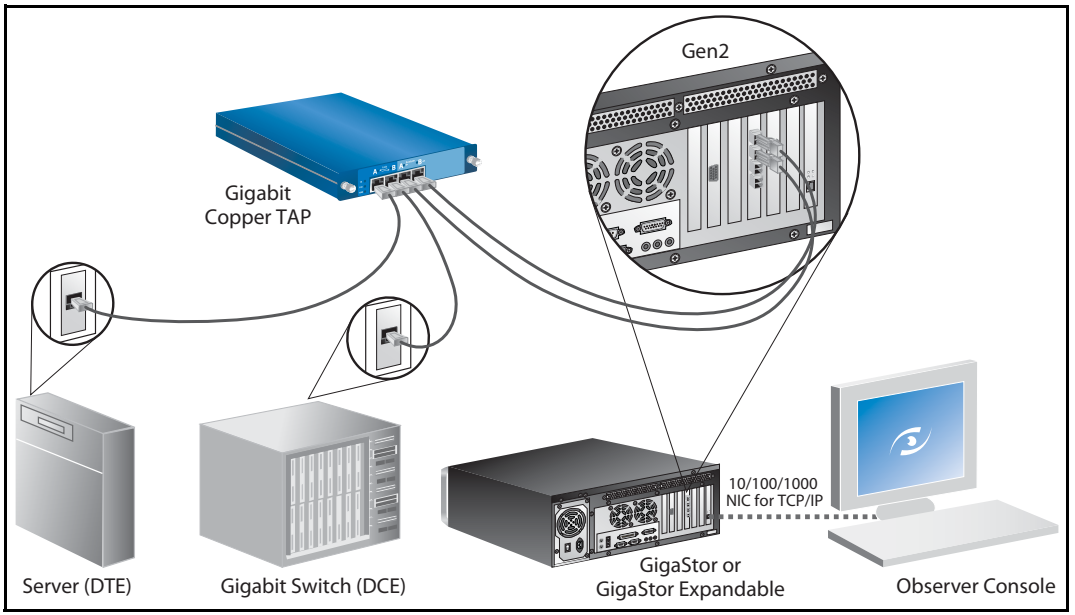
NOTE: PASS-THROUGH CABLE

If you are using a switch's SPAN/mirror port, no *n*TAP is required. Simply plug any straight-through Ethernet cable into the SPAN/mirror port on the switch and one of the ports on the Gen2 capture card.

Now that you have physically connected the cables for the GigaStor, you must now configure its software. See "Setting the GigaStor's IP address" on page 19.

Figure 26 shows the GigaStor as it would be cabled to analyze a server. The TAP can replace the gigabit connection between any DCE (Data Circuit-terminating Equipment) and DTE (Data Terminal Equipment) device or connection.

Figure 26 GigaStor with a copper TAP



Tapping a WAN connection

This section describes how to connect the cables for these environments:

- "T1/E1" on page 42
- "DS3/E3" on page 46

T1/E1

See "Digital" on page 42 or "Serial" on page 44 depending on your needs.

Digital

The digital T1/E1 kit includes:

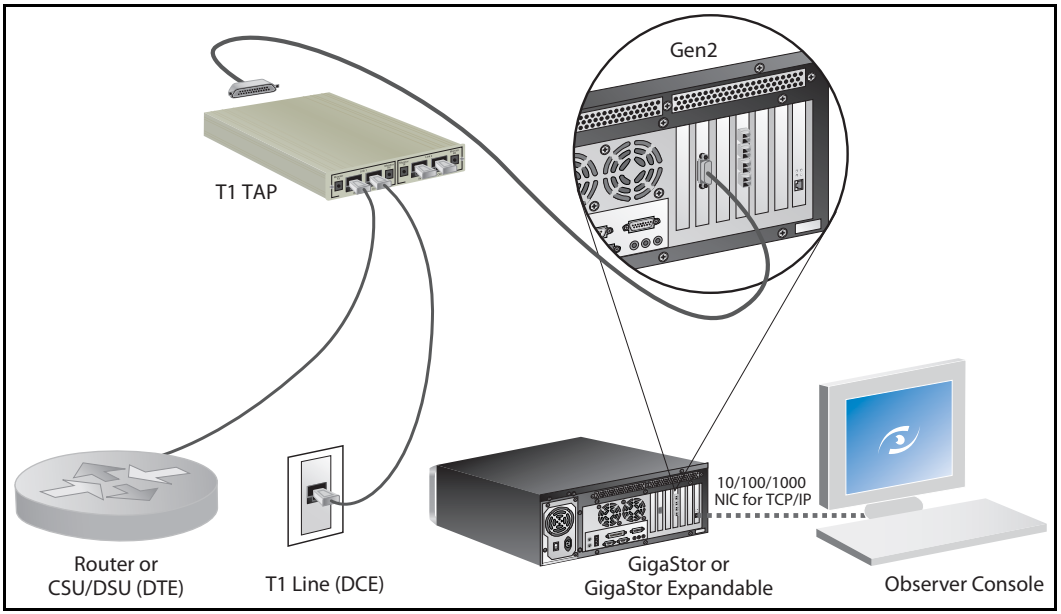
- One T1/E1 dual link TAP
- One T1/E1 WAN analyzer cable
- Two T1/E1 Ethernet cables

1. If you have a GigaStor Expandable, see "Connecting the GigaStor Expandable to the expansion units" on page 52 for details about connecting them. After connecting them, continue with step 2.
2. Connect the TAP to the GigaStor using the T1/E1 WAN analyzer cable.
3. From your T1/E1 cable that connects the DCE to your CSU/DSU, unplug the CSU/DSU end and plug it into the Link 1 IN port on the TAP.
4. Using one of the supplied T1/E1 Ethernet cables, connect the Link 1 OUT port of the TAP to the CSU/DSU.
5. If you have a second T1 you want to monitor, repeat step 3 and step 4 using Link 2.
6. Use the supplied Ethernet cable to connect the network interface card in the GigaStor to the network.

Now that you have physically connected the cables for the GigaStor, you must now configure its software. See “Setting the GigaStor’s IP address” on page 19.

Figure 27 shows the GigaStor as it would be cabled to analyze T1/E1 link with a Channel Service Unit/Data Service Unit (CSU/DSU)[1].

Figure 27 Digital T1/E1 Tap



1. The 4-Port version of this system has an additional PC interface card and an additional TAP and cable kit. Connect the second TAP kit as shown in the diagram.

Serial

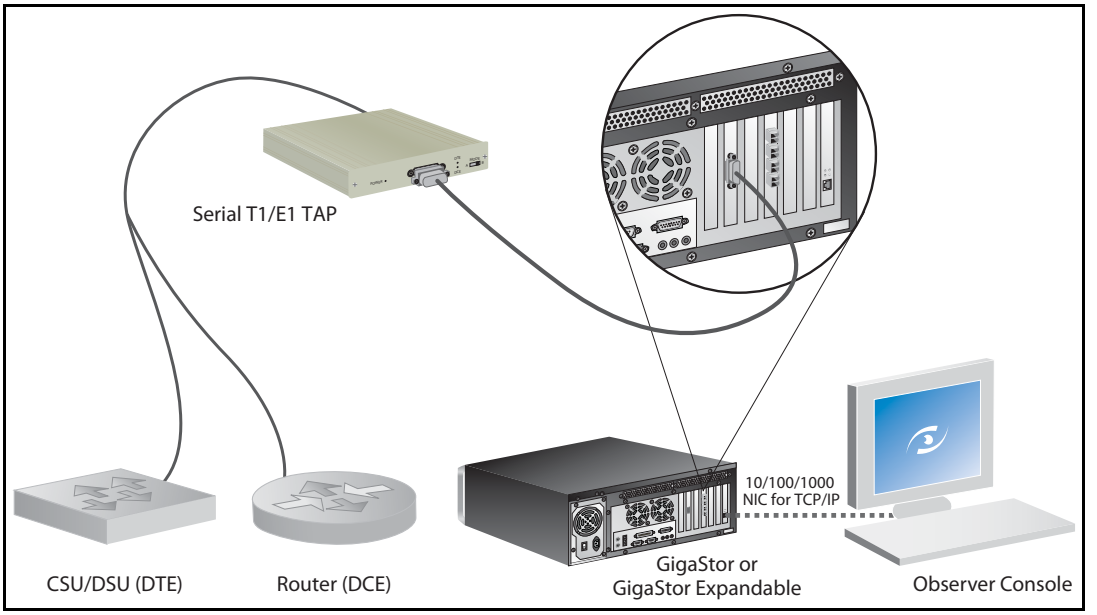
The serial T1/E1 kit includes:

- One serial T1/E1 WAN TAP
- One serial Y cable
- One serial T1 WAN cable

1. If you have a GigaStor Expandable, see “Connecting the GigaStor Expandable to the expansion units” on page 52 for details about connecting them. After connecting them, continue with step 2.
2. Connect the TAP to the GigaStor using the serial T1/E1 WAN cable.
3. Using the serial Y cable, connect it to the TAP and then to your CSU/DSU and your router.
4. Use the supplied Ethernet cable to connect the network interface card in the GigaStor to the network.

Now that you have physically connected the cables for the GigaStor, you must now configure its software. See “Setting the GigaStor’s IP address” on page 19.

Figure 28 WAN Serial T1/E1 TAP



See “Digital” on page 46 or “Serial/HSSI” on page 48 depending on your needs.

Digital

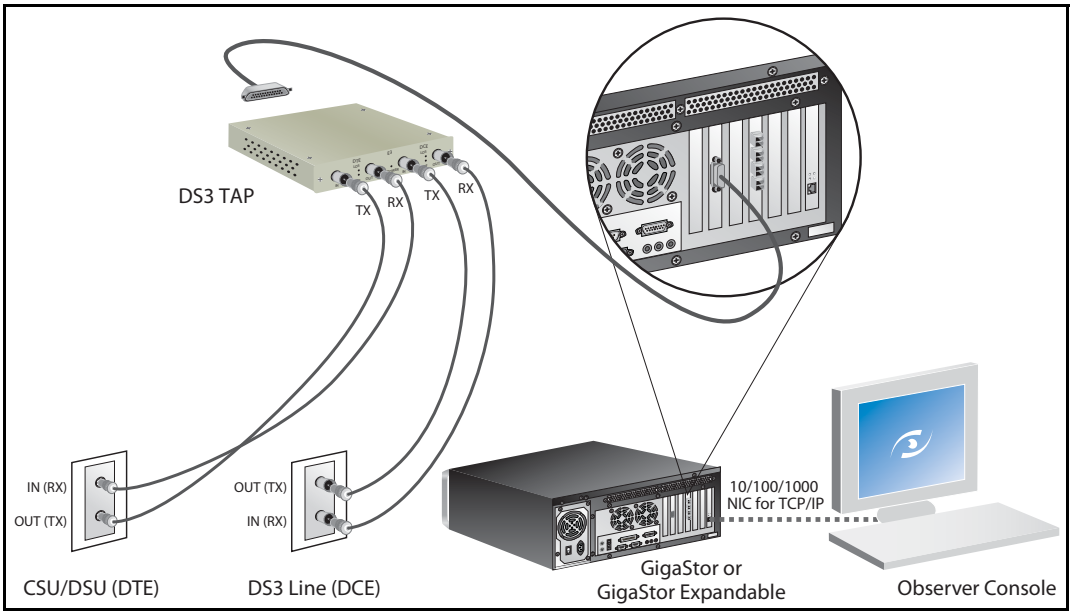
The digital DS3/E3 kit includes:

- One digital DS3/E3 TAP
- One digital DS3/E3 WAN cable
- Two full-duplex DS3/E3 coax cables

1. If you have a GigaStor Expandable, see “Connecting the GigaStor Expandable to the expansion units” on page 52 for details about connecting them. After connecting them, continue with step 2.
2. Connect the TAP to the GigaStor using the supplied digital DS3/E3 WAN cable.
3. From your coax cables that connects the router to your CSU/DSU, unplug the ends of both cables connected to the CSU/DSU and plug them into the IN ports on the TAP.
4. Using the supplied coax cables, connect them from the OUT ports on the TAP to the CSU/DSU.
5. Use the supplied Ethernet cable to connect the network interface card in the GigaStor to the network.

Now that you have physically connected the cables for the GigaStor, you must now configure its software. See “Setting the GigaStor’s IP address” on page 19.

Figure 29 DS3/E3 TAP



Serial/HSSI

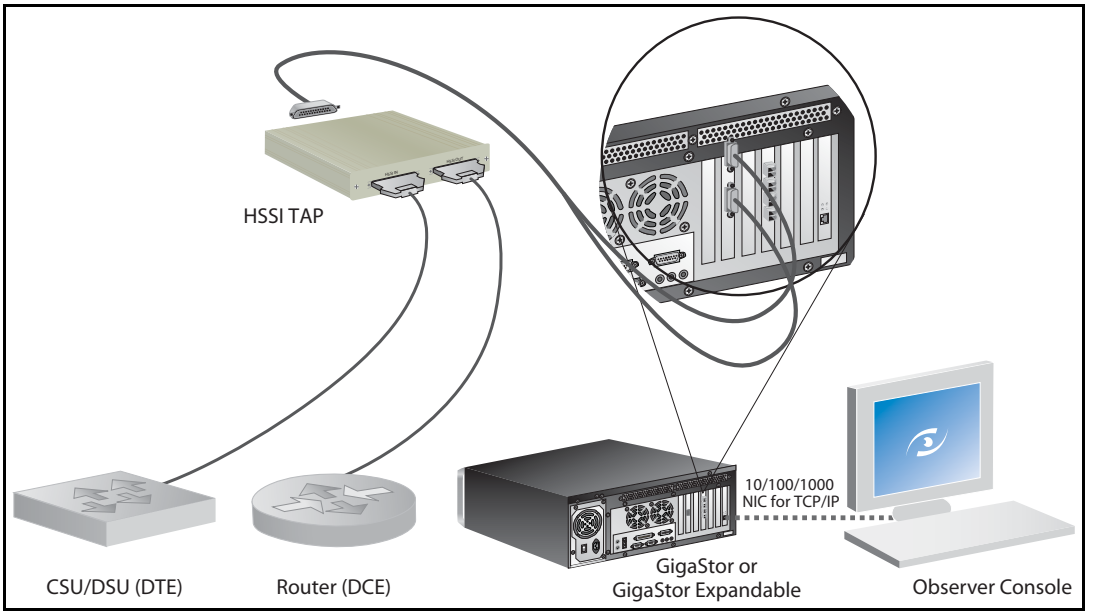
The serial DS3 kit includes:

- One serial DS3/E3 TAP
- One HSSI Y-cable
- One HSSI cable
- One Ethernet cable

1. If you have a GigaStor Expandable, see "Connecting the GigaStor Expandable to the expansion units" on page 52 for details about connecting them. After connecting them, continue with step 2.
2. Connect the TAP to the GigaStor using the supplied HSSI Y-cable.
3. From your serial HSSI cable that connects the router to your CSU/DSU, unplug the CSU/DSU end and plug it into the IN port on the TAP.
4. Using the supplied HSSI cable, connect it to OUT port on the TAP.
5. Use the supplied Ethernet cable to connect the network interface card in the GigaStor to the network.

Now that you have physically connected the cables for the GigaStor, you must now configure its software. See "Setting the GigaStor's IP address" on page 19.

Figure 30 WAN HSSI



Installing the drives in your GigaStor

CAUTION HANDLING THE DRIVES

Be especially careful when handling and installing the hard drives. Proper handling is paramount to the longevity of the unit. The internal mechanism of the hard drive can be seriously damaged if the hard drive is subjected to forces outside its environmental specifications.

When transporting the hard drive, always use the original packaging in which the hard drive was delivered to you, and avoid exposing the hard drive to extreme changes in temperature to minimize the risk of condensation.

- Never drop the unit. Handle it with care.
- Never place the hard drive in the vicinity of equipment giving off strong magnetic fields, such as CRT monitors, televisions, or loudspeakers.
- Always use an anti-static mat and wrist strap when handling the hard drive. Hold the hard drive by the base and never touch the components on the circuit board assembly.
- If the temperature difference between the storage location and installation location exceeds 50°F/10°C, for temperature acclimation purposes, leave the hard drive in the new location for at least two hours before turning it on.

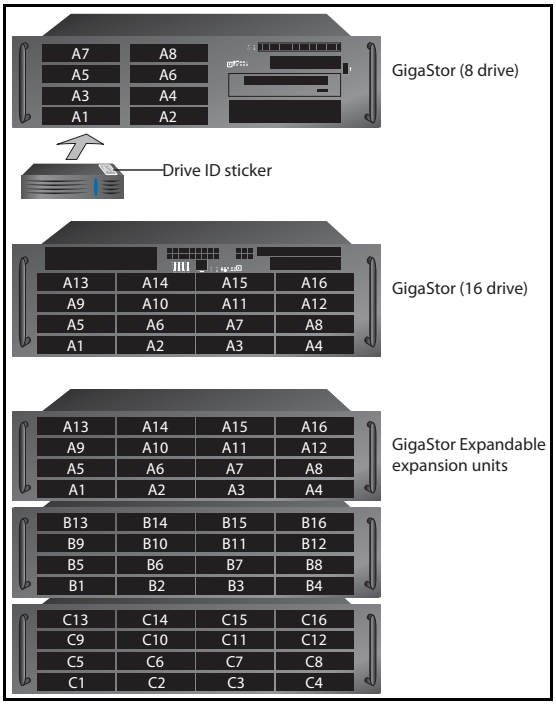
Each drive for the GigaStor is packed in shock-resistant boxes. The tray that holds each drive has two optical pipes that run along the right side. These pipes are connected to the indicator lights on the front of the tray and are prone to cracking or breaking if you squeeze the sides of the tray too tightly.

Stickers on each drive identify which slot (and expansion unit) it should be installed in. The drive labeled A1 must be installed in the lower left slot. The disk expansion units for the GigaStor Expandable are labeled A, B, or C on the back of the expansion unit's case.

1. Open the locking latch by pushing the release tab until the tray panel pops out.
2. Gently, but firmly, push the A1 drive into the appropriate slot until you feel the pins engage and the latch closes slightly.

Figure 31 shows how the drive numbers correspond to slot locations.

Figure 31 GigaStor drive locations



CAUTION GIGASTOR EXPANDABLE DRIVE LOCATION

It is important that you install the drives in the correct drive slot, and in correct expansion unit if you have a GigaStor Expandable. Failure to install the drives in the proper order will result in poor read/write performance or possibly RAID array failure.

3 Push the latch in all the way until it clicks.

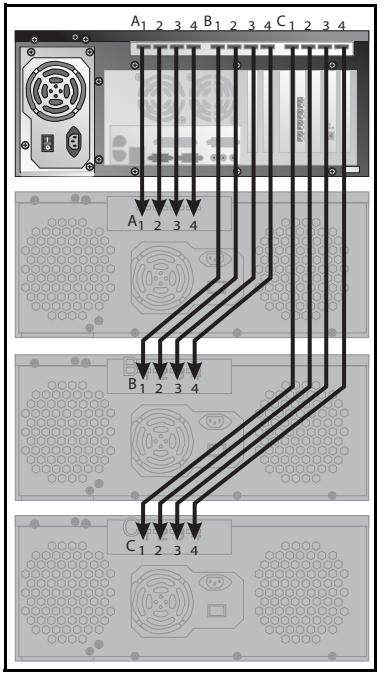
4 Repeat until all drives are in the chassis. For the GigaStor Expandable continue with B1-B16 and C1-C16 as appropriate.

5 If you are installing a GigaStor Expandable, you must also connect the cables. See "Connecting the GigaStor Expandable to the expansion units" on page 52. Otherwise, continue with "Installing the GigaStor and connecting the cables" on page 19.

Connecting the GigaStor Expandable to the expansion units

After you have installed the drives Use the supplied cables to connect the expansion units to the GigaStor Expandable. Figure 32 shows how to cable the GigaStor Expandable to the expansion units.

Figure 32 Cable diagram for the GigaStor Expandable



Otherwise, continue with "Installing the GigaStor and connecting the cables" on page 19.

NOTE: GIGASTOR EXPANDABLE

When turning the GigaStor Expandable components on and off, follow this order to ensure proper drive recognition and operation:

- Start the disk expansion units before turning on the capture/controller PC unit.
- Shut down the capture/controller PC unit before turning off the disk expansion units.

Chapter 3

Packet Capture or GigaStor Capture

Capturing Packets with the GigaStor

A GigaStor can accumulate terabytes of stored network traffic. To manage the sheer volume of data, the GigaStor includes an alternative, specialized capture and analysis control panel. The GigaStor Control Panel manages the capture, indexing, and storage of large numbers of packets over long periods of time. While the GigaStor control panel is active, standard packets captures are unavailable. You cannot run the two types of captures simultaneously.

While actively capturing packets, the GigaStor control tracks network statistics and indexes them by time as it saves the packets to disk. This allows you to quickly scan the traffic for interesting activity and create filters to focus on specific traffic using the slider controls and constraint options.

The GigaStor control panel also automates storage management by deleting the oldest data before storage runs out. This maintains a multi-terabyte "sliding windows" of time within which you can review and decode traffic. It also allows for passive (in other words, virtual) probe instances, which allow users to have their own instances (and security credentials) without duplicating data collection or storage.

You can view the sliding window as a time line chart. Depending on what constraint are in effect and your display options determine what appears on the chart. By using time selection sliders and other options, you can quickly acquire and analyze the packets by clicking the Analyze button. This opens the standard packet decode and analysis window. From there you can view packets, save them, and perform further filtering if desired.

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 the system on which the probe is installed 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 passive probe instances doing packet captures.)

Network Speed × Average Throughput (MB/second) = Seconds of data storeable in RAM

Tip! Capture Buffer

You want a buffer that will handle your largest, worst case burst.

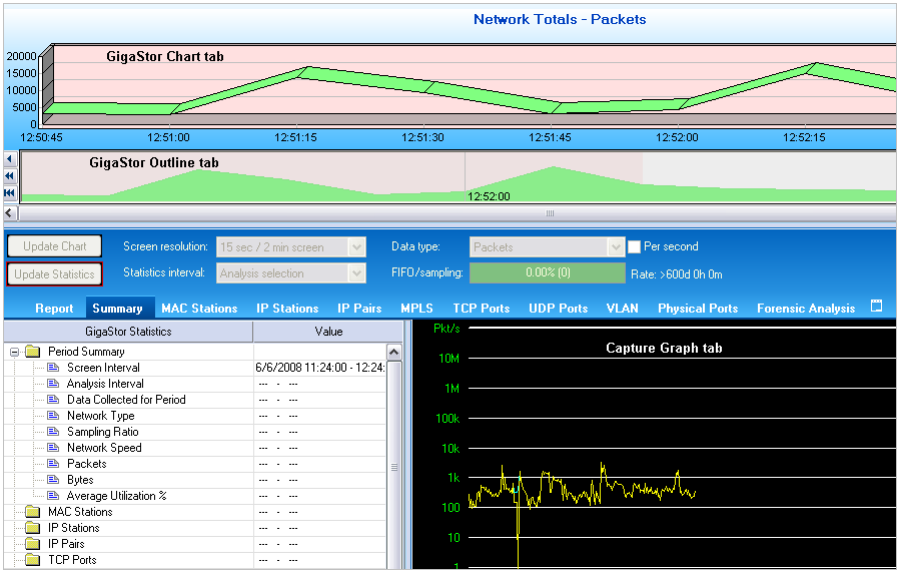
Chapter 4

GigaStor Control Panel

Once the GigaStor is up and running on the network, you can run Expert Observer or Observer Suite to connect to the GigaStor running as a probe to begin analyzing the network, or you can run the GigaStor in Console mode via Windows Terminal Server (or a monitor and keyboard that are physically attached). Observer works with the GigaStor just as it does any other Network Instruments probe, with some GigaStor-specific enhancements (described below).

The GigaStor Control Panel is available from the probe itself (when running in Console Mode), and also from any Observer Expert or Observer Suite console when it is connected to a GigaStor. In either case, choose GigaStor Capture Analysis from Observer's Capture menu, and a screen like the following is displayed:

Figure 33 GigaStor Control Panel



The GigaStor Control Panel shows traffic on a time line graph, allowing you to select packets for decoding, analysis, and display by defining the time period you want to view, and the types of packets you want to include.

Use the sliders at the top of the time line chart to select the time period you are interested in analyzing. If desired, you can further constrain the display of packets by MAC Stations, IP Stations, IP Pairs,

etc., by clicking on the appropriate tab and selecting the items you want to see on the time line chart.

Display Controls

Charts and statistical tables are refreshed only when you click the Update Chart or Update Statistics button. The buttons will flash with a red border when a refresh is necessary. You can also have the display auto-update. For details, "GigaStor Options tab" on page 64.

You can change the Screen resolution (in other words, the time scale) and which Data type (i.e., packets or bytes, either per second or totals) to chart by using the drop-down controls and per second check box. The Statistics interval control lets you display network statistics based on the entire visible chart, or only show data derived from the time interval you have selected to analyze.

The FIFO gauge on the right side of the control pane tracks how well GigaStor's disk hardware is keeping up with the current traffic load; if the FIFO gauge shows 90% or greater, you should consider reducing the load using one or more of the following methods:

- Allocate more memory to the GigaStor instance. See the instructions in "Probe administration" on page 24 for details about allocating memory for the probe instance.
- Activate dynamic sampling, or increase the fixed sampling ratio. See details about packet capture in "Packet capture buffer and statistics buffer" on page 54.
- Activate partial packet capture or reduce the size of portion captured. See details about partial packet capture in "Capture partial packets" on page 65.

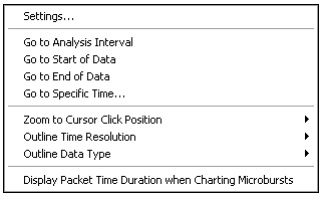
The Rate: field shows how much traffic the GigaStor will be able to archive given the active instance's current disk usage rate. It is updated dynamically as the usage rates change. To increase the archivable time window, activate partial packet capture and sampling as described above, or apply pre-filtering.

Right-click menus

As with other Observer displays, the charts and tables of the GigaStor control panel offer many right-click shortcuts.

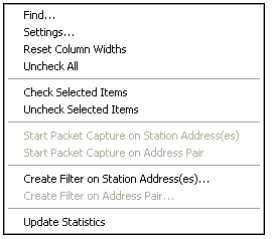
- Right-clicking on the chart portion of the Control Panel displays the following options for navigating and displaying traffic data:

Figure 34 Chart right-click menu



- Settings brings up GigaStor Control panel settings; the Zoom to Cursor Click Position options let you select from different chart resolutions, centering the display at the current cursor position.
- Right-clicking on any table (such as Summary, TCP, UDP, etc.) presents a context-sensitive menu. The TCP right-click menu is typical:

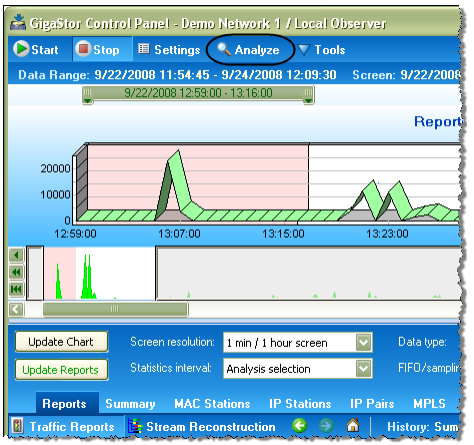
Figure 35 TCP right-click menu



- The options themselves are self-explanatory. Filtering options displayed depend on which table you right-clicked on.

Analyze button

Figure 36 GigaStor Control Panel Analyze button



When you click the Analyze button to view the results, you are prompted to select how to filter the packet capture for display (Figure 37).

After you click OK, any filters you have chosen are applied, and a standard decode window is displayed, unless you have checked the "Display selected filter before starting analysis" option, in which case the filter editor is displayed.

Figure 37 GigaStor Analysis Options window

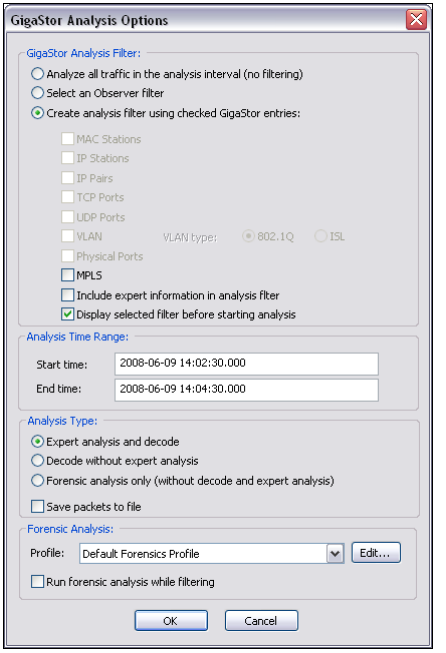


Table 4 describes what the fields in the various sections control.

Table 4 GigaStor Analysis Options

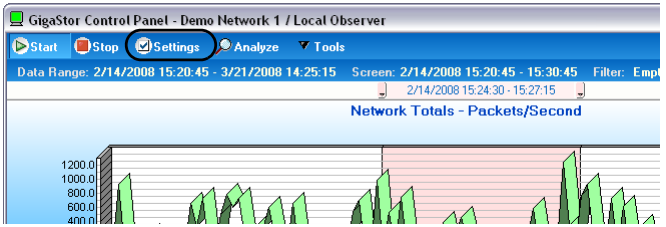
Field section	Description
GigaStor Analysis Filter	Choose whether to Analyze all traffic in the analysis period, Select an Observer filter to apply before decoding, or Create an analysis filter using checked GigaStor entries (in other words, based on the constraints you have selected using the GigaStor control panel). Subsequent check boxes let you choose which criteria from the Control Panel selection to include in the analysis. The Include expert information in analysis filter option should be checked if you plan on using Observer's Expert Analysis on the packet buffer; otherwise leave it unchecked.
Analysis Time Range	Set the start and end time for analysis. The fields are pre-filled based on the time slider selections made from the GigaStor Control Panel.
Analysis Type	Choose between Expert analysis and decode, Decode without expert analysis, or Forensic analysis only. Load time is significantly reduced (especially with large files) by bypassing analysis processing for features you are not interested in.
Forensic Analysis	Select a Forensic Analysis profile. See "Starting Forensic Analysis using Snort rules" on page 92 for details on using this Snort-compatible feature.

Configuring the GigaStor through the Control Panel

Just as with the standard Observer packet capture interface, you can set the colors of the capture graph and schedule captures to be automatically launched (or to run all the time). In addition, there are a number of GigaStor-specific settings that allow you to fine-tune performance based on your particular needs.

1. Open the GigaStor Control Panel (Capture →GigaStor Capture Analysis).
2. Click the Settings button.
3. Click the tab for the settings you want to change.

Figure 38 GigaStor Control Panel Analyze button



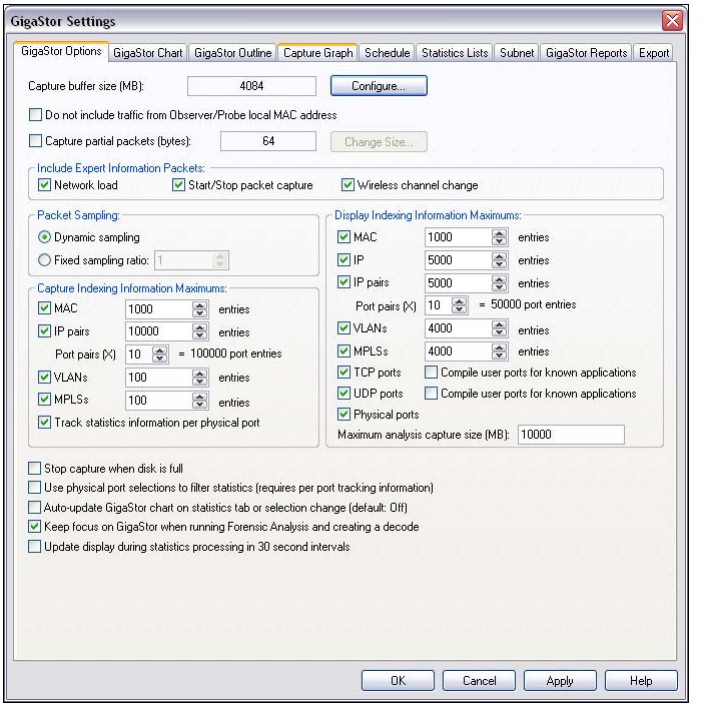
These options and settings are described in

- "GigaStor Options tab" on page 64
- "GigaStor Chart tab" on page 67
- "GigaStor Outline" on page 67
- "Capture Graph tab" on page 69
- "GigaStor Schedule tab" on page 70
- "Statistics Lists tab" on page 71
- "Subnet" on page 72
- "GigaStor reports" on page 75
- "Export" on page 77

GigaStor Options tab

This tab lets you configure many options for the GigaStor. Follow the instructions in “Configuring the GigaStor through the Control Panel” on page 63 to open the GigaStor Options tab (Figure 39).

Figure 39 GigaStor Options tab



See Table 5 for a description of each field of the GigaStor Options tab.

Table 5 GigaStor Options tab

Field	Description
Capture Buffer size	Allows you to set the amount of Windows memory that Observer will dedicate to the capture buffer cache for this instance. Values are in megabytes. This configuration value has been pre-set for optimum performance given a single GigaStor collection instance. The factory settings also allow enough memory to set up a number of passive or virtual instances, which will allow multiple users to view the analysis results while avoiding redundant processing, memory, and disk storage consumption. If you wish to run multiple collection instances to monitor multiple links or networks, you can decrease the capture buffer size dedicated to GigaStor collection which will release some memory for creating other probe collection instances, but be careful. Inadequate memory allocation to GigaStor collection can affect performance and result in dropped packets during high load periods. A GigaStor Instance can be as large as the physical memory installed on your system after subtracting the memory dedicated to Windows and other probe Instances. To change the allocation for this probe instance, click the Configure button, which will display the probe Instance, Memory and Security Administration dialog. In all cases, the actual buffer size (Max Buffer Size) is also reduced by 7% for memory management purposes. Should you try to exceed the Max Buffer Size an error dialog will be displayed indicating the minimum and maximum buffer size for your Observer (or probe) buffer.
Do not include traffic from Observer/ Probe local MAC address	Excludes packets sent and received from the station running Observer or probe (the MAC address of the station from which you are capturing packets).
Capture partial packets	By default, Observer will capture the entire packet. This option allows you to define a specific amount of each packet to capture to the buffer. For example, a setting of 64 bytes will result in Observer only capturing the first 64 bytes of every packet. Most of the pertinent information about the packet (as opposed to the information contained in the packet) is at the beginning of the packet, so this option allows you to collect more packets for a specific buffer size by only collecting the first part of the packet. In some forensic situations, a warrant may only allow an officer/agent to collect, for example, e-mail headers. Also, if the system is having trouble keeping up with bandwidth spikes, collecting partial packets can resolve the issue. To change the number of bytes captured in each packet, click the Change Size... Note that this setting affects all consoles that connect to this probe. You cannot change this setting unless you have administrative privileges to do so.
Network Load	When checked, Observer will not strip out the informational markers used by Expert Time Interval and What If analysis modes. Leave this box unchecked unless you intend to use these modes.

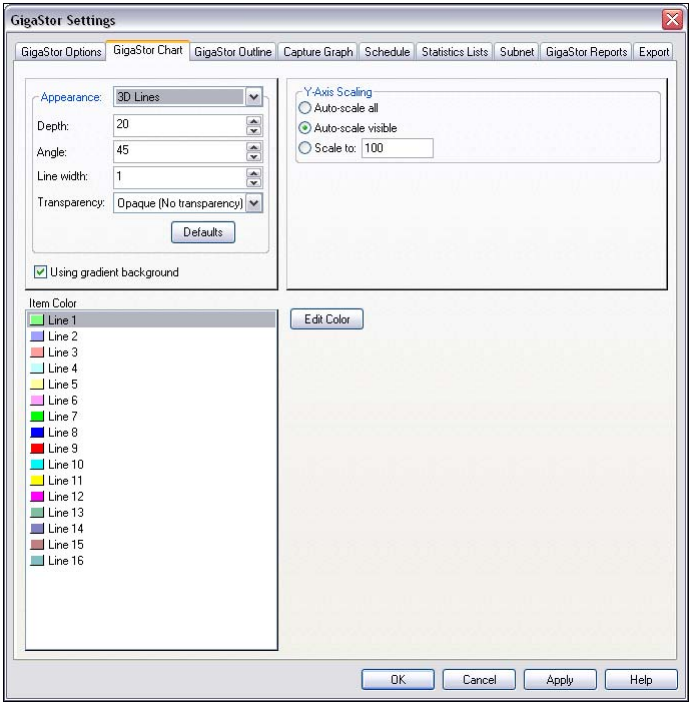
Table 5 GigaStor Options tab

Field	Description
Start/Stop Packet Capture marker frames	When checked, saved packet capture buffers will include markers that timestamp when packet captures were started and stopped.
Wireless Channel Change	When checked, saved packet capture buffers will include markers that show what channel was currently being listened to. This is useful if you are using Wireless Site Survey to scan channels.
Packet Sampling	Packet sampling applies to the control panel statistical displays, not saved packets. On probes connected to highly-saturated networks (especially multi-port probes), sometimes it is desirable to adjust the rate of statistical indexing to conserve probe processing and storage resources. The default (and recommended) setting is for Observer to automatically scale back the packets it uses to update the console display based on system load. Alternatively, you can specify a Fixed Sampling Ratio to consider when updating the GigaStor Control Panel Charts and statistical displays.
Capture Indexing Information Maximums	Depending on what kinds of information you are interested in tracking, you can conserve probe processing and espeically storage resources by only indexing the information that is useful to you. Of special note is the "Track statistics information per physical port" option. When selected, causes the GigaStor to index the data it collects by Gen2 capture card physical ports. You can then display GigaStor Control Panel statistics by physical port (see the next bullet item).
Display Indexing Information Maximums	Depending on what kinds of information you are interested in tracking, you can conserve probe processing and resources by only indexing the information that is useful to you.
Collect and Show GigaStor indexing information by	Depending on what kinds of information you are interested in tracking, you can conserve probe processing and storage resources by only indexing the information that is useful to you.
Track statistics information per physical port	When selected, causes the GigaStor to index the data it collects by Gen2 capture card physical ports. You can then display GigaStor Control Panel statistics by physical port (see the next bullet item).
Use physical port selections to filter statistics (requires per port tracking information)	If the previous check box is selected, you can choose this option to display, within the GigaStor Control Panel, statistics sorted by Gen2 Capture Card physical port. This is useful, for example, when you want to troubleshoot the individual links without having to load the capture buffer by clicking Analyze.
Stop capture when disk is full	When activated, the GigaStor stops capturing packets when the disk array is full. The default behavior is to use circular (i.e. FIFO) disk writes, causing the oldest buffer files to be overwritten as newer traffic is captured.
Auto-update GigaStor chart on statistics tab or selection change	When selected, causes the listed actions to have the same effect as clicking the Update Chart/Statistics buttons.
Keep focus on GigaStor when running Forensic Analysis and creating a decode	Keeps the focus in the GigaStor Control Panel instead of switching to the decode pane.
Update display during statistics processing in 30 second intervals	When selected all charts will received updates in 30 second intervals when processing statistics.

GigaStor Chart tab

This tab lets you choose the appearance, colors, and scale of the GigaStor Control Panel's time line chart. Follow the instructions in "Configuring the GigaStor through the Control Panel" on page 63 to open the GigaStor Chart tab (Figure 40).

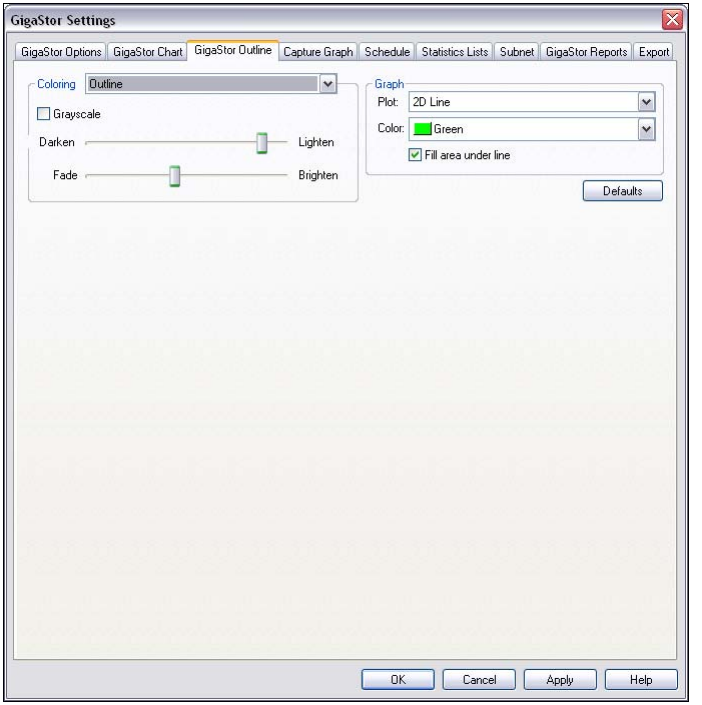
Figure 40 GigaStor Chart tab



GigaStor Outline

Click Settings and the GigaStor Outline tab to modify the display of the GigaStor outline graph. See Figure 33 on page 58 for an example of the GigaStor outline graph. Follow the instructions in "Configuring the GigaStor through the Control Panel" on page 63 to open the GigaStor Outline tab (Figure 41).

Figure 41 GigaStor Outline



Capture Graph tab

Click Settings and the tab for the type of graph or chart for which you want to set the display properties. Follow the instructions in "Configuring the GigaStor through the Control Panel" on page 63 to open the Capture Graph tab (Figure 42).

Figure 42 Capture Graph tab

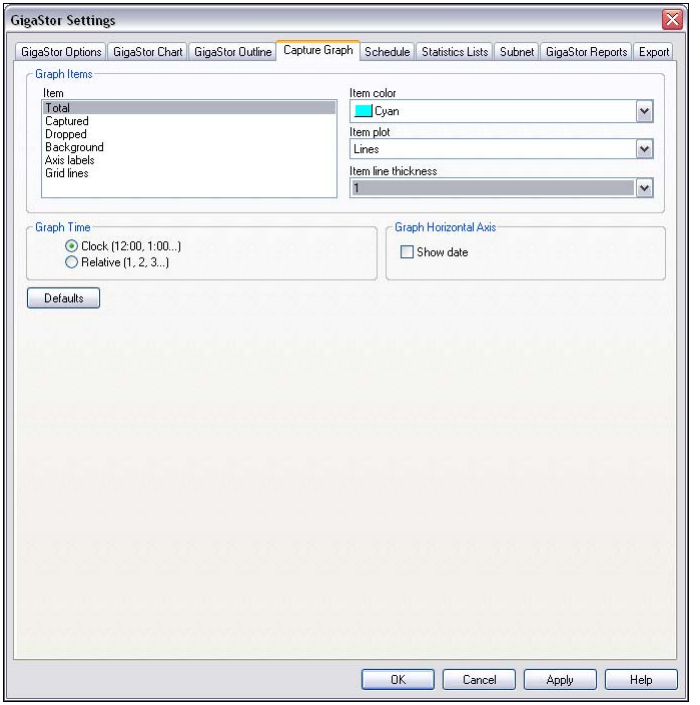


Table 6 Capture Graph fields

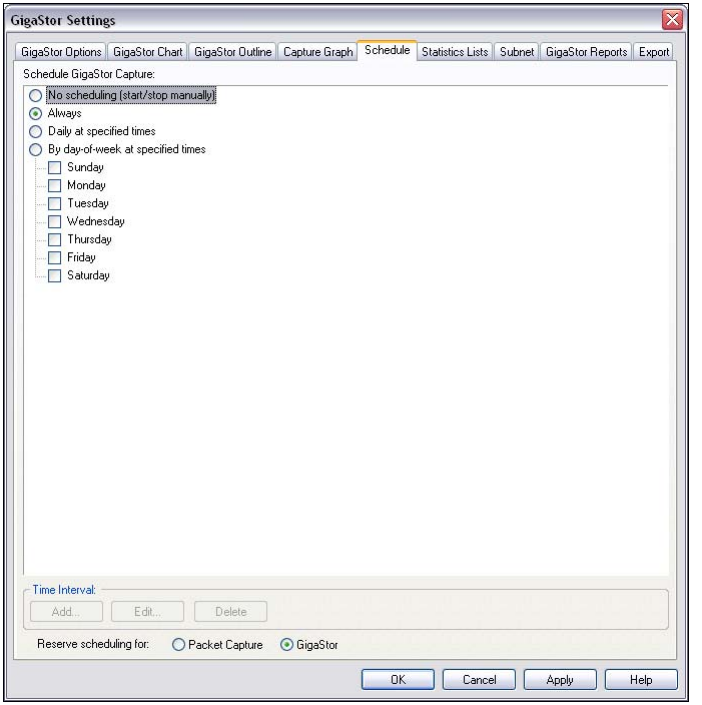
Field	Description
Item	allows you to select which item will be configured.
Item color	allows you to select the color of the display item.
Item plot	allows you to select the item to be displayed as Lines or Bars. This dropdown will only be active if "Lines" is selected in the "Item plot" dropdown.
Item line thickness	allows you to select the thickness of the displayed item (in pixels).
Graph Time option buttons	allows you to set how the "X" axis will be displayed. Clock time will show times using a 24-hour clock (i.e., the current time). Relative time will display times from the start of the activation of the mode.

GigaStor Schedule tab

This tab lets you schedule GigaStor packet captures to occur at preset times and days of the week. Although the dialog looks identical to the standard Packet Capture schedule tab, the two types of schedules can not be in effect at the same time. If you attempt to schedule GigaStor packet captures when standard packet captures are already scheduled (or the reverse), an error message is displayed.

Follow the instructions in "Configuring the GigaStor through the Control Panel" on page 63 to open the Schedule tab (Figure 43).

Figure 43 Schedule tab



- Choose No Scheduling to turn off any automatically scheduled packet captures for the selected probe or probe instance.
- Choosing Always causes the selected probe or probe instance to capture packets whenever the probe is running.

- Choose Daily at specified times or By day-of-week at specified times to automatically schedule packet captures during the specified time intervals (which you can add by clicking the Add button at the bottom of the dialog; see below).

Adding, Modifying, and Deleting Time Intervals

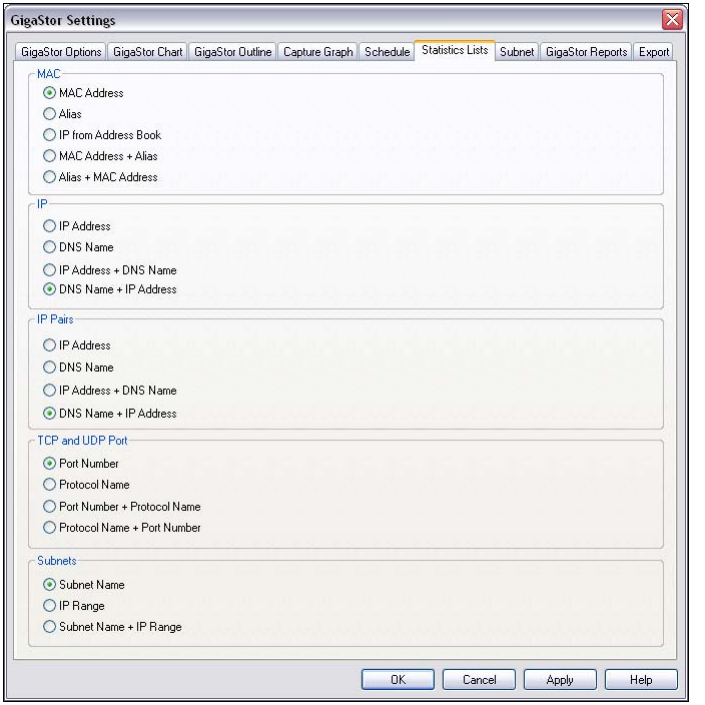
To add or modify a time interval to a schedule option, choose that option (in other words, Daily or the day-of-week for which you want to schedule a capture) and click the appropriate button. A time interval specification dialog is displayed that allows you to set the time period for the capture to be performed. To delete a time interval from a schedule option, simply highlight the interval you wish to delete and click the Delete button.

Time intervals include the last minute of the interval. All time periods are specified in 24-hour (also known as military) time.

Statistics Lists tab

Observer tracks and makes many statistics available to you. You can control how those statistics are displayed for your GigaStor. This tab lets you customize how MAC address, IP address, IP Pair, and port information are displayed in the various constraint tab statistical listings. Follow the instructions in "Configuring the GigaStor through the Control Panel" on page 63 to open the Statistics Lists tab (Figure 44).

Figure 44 Statistics Lists tab



Subnet

You can specify subnet properties for the GigaStor. Follow the instructions in “Configuring the GigaStor through the Control Panel” on page 63 to open the Subnet tab (Figure 45).

Use the Add, Delete, Modify, and Delete All buttons to configure the subnet settings for the GigaStor. When you define subnets in the GigaStor, Observer adds that subnet information to the index files. All future data analyzed will have subnet filtering readily available as well as statistical data. On the IP stations tab you see your subnets and you can perform statistical analysis based on subnets.

When you analyze data from captures with index files without any subnets defined, there will be no subnet available in the IP stations tab even if the analyzed data includes some index files with the new subnet information.

Figure 45 GigaStor Subnet tab

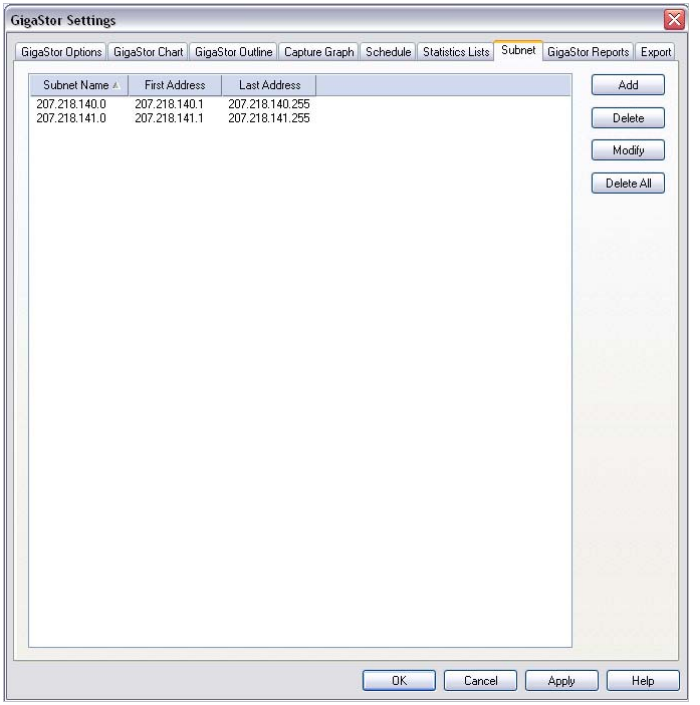
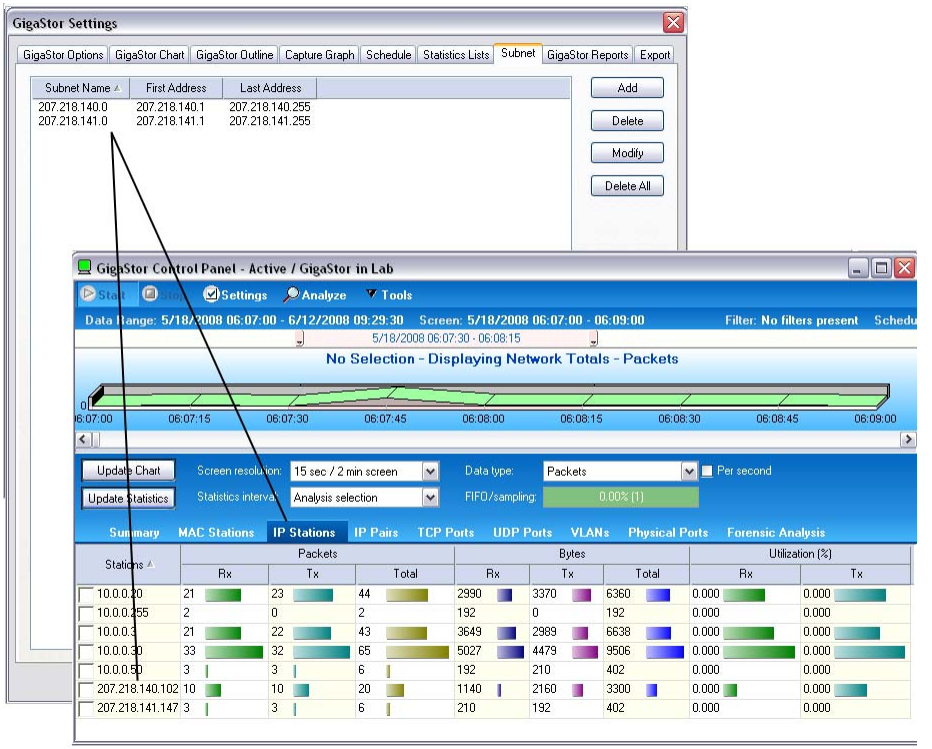


Figure 46 shows how the subnet settings show up in the GigaStor Control Panel. They appear on the IP Stations tab.

Figure 46 Subnet and IP Stations

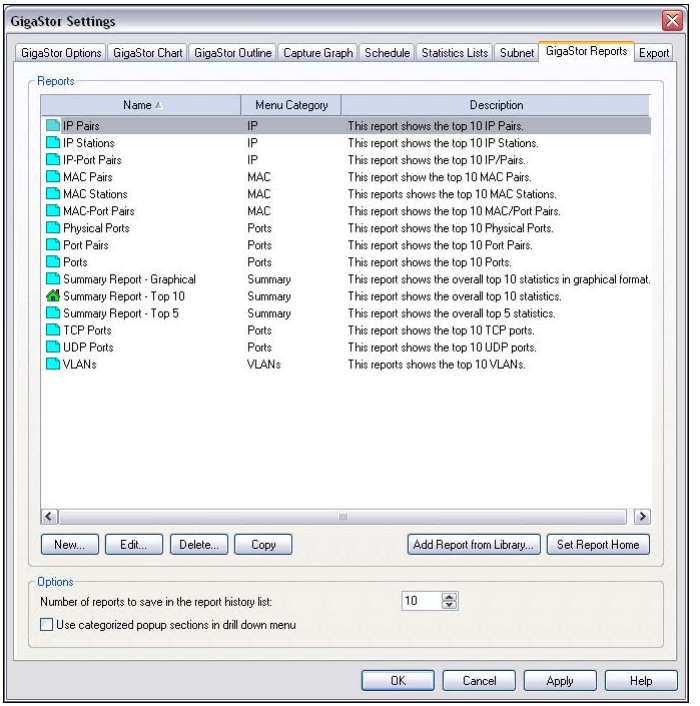


GigaStor reports

There are several default reports available for you.

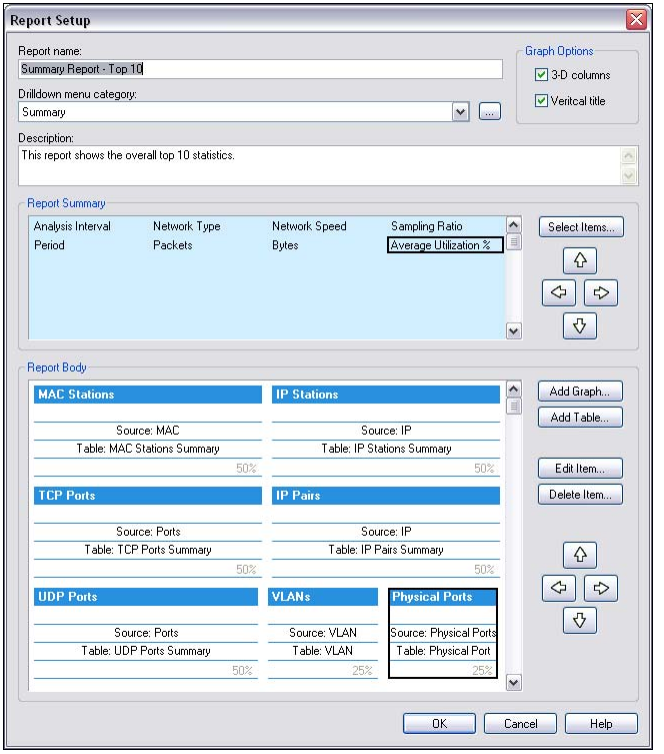
1 Follow the instructions in "Configuring the GigaStor through the Control Panel" on page 63 to open the GigaStor Reports tab (Figure 47).

Figure 47 GigaStor Reports tab



2 Select a report name and click Edit to change the report's characteristics (Figure 48).

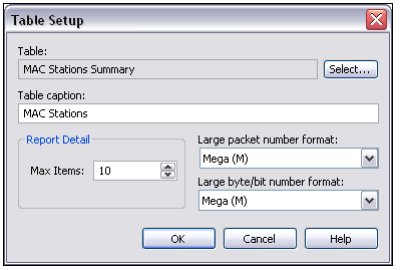
Figure 48 Report Setup



3 Use the arrow buttons to position graphs and tables on your report.

4 Double-click a section of the report to modify its caption, detail, and number format (Figure 48).

Figure 49 Table Setup

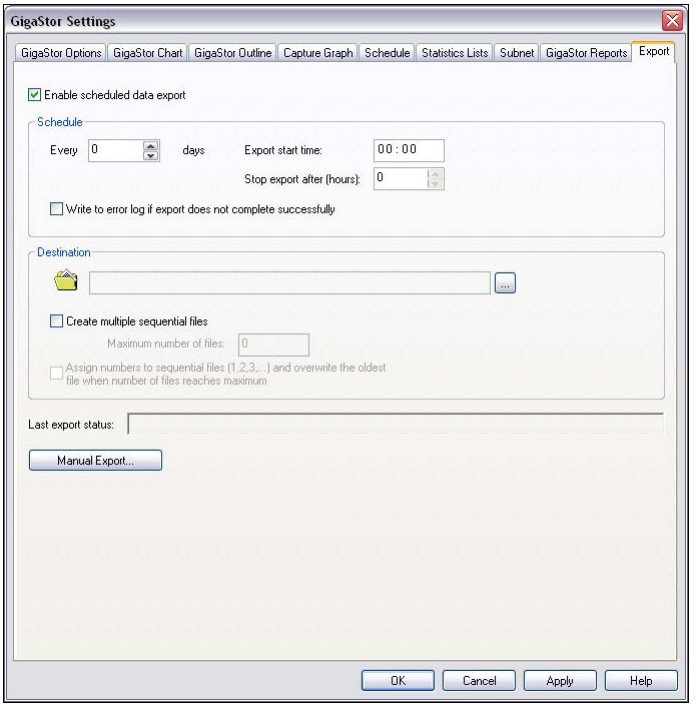


Export

You can export your GigaStor-collected data on a scheduled basis. Use the Export tab to configure when and to where your data is saved or to manually export your data.

Follow the instructions in “Configuring the GigaStor through the Control Panel” on page 63 to open the Export tab (Figure 50).

Figure 50 Exports tab



Chapter 5

Using Observer with a WAN Probe

In general, the WAN analysis works much like Ethernet analysis. One difference is that, when appropriate, Observer identifies WAN links by their Data Link Connection Identifier (DLCI) rather than by MAC address as is done with standard protocol analysis. In addition, many WAN statistical modes break out the data by DCE, DTE, and summary to reflect the full-duplex nature of WAN links. Modes unrelated to WAN analysis are greyed out and unavailable.

The following sections describe how the available Observer modes operate to analyze a WAN link.

Discover Network Names

To access this mode, choose Tools →Discover Network Names

Discover Network Names mode will show DLCIs instead of MAC addresses. You can also define the Committed Information Rate for each DLCI you are monitoring with WAN Observer.

Setting the Committed Information Rate (CIR) for a DLCI

The Committed Information Rate defines the guaranteed bandwidth for a WAN connection. If you want Observer's WAN Vital Signs and WAN Load by DLCI to monitor CIR compliance, you must specify the CIR. A number of WAN triggers and alarms also use this information, allowing you to be notified if the link is not performing to the CIR.

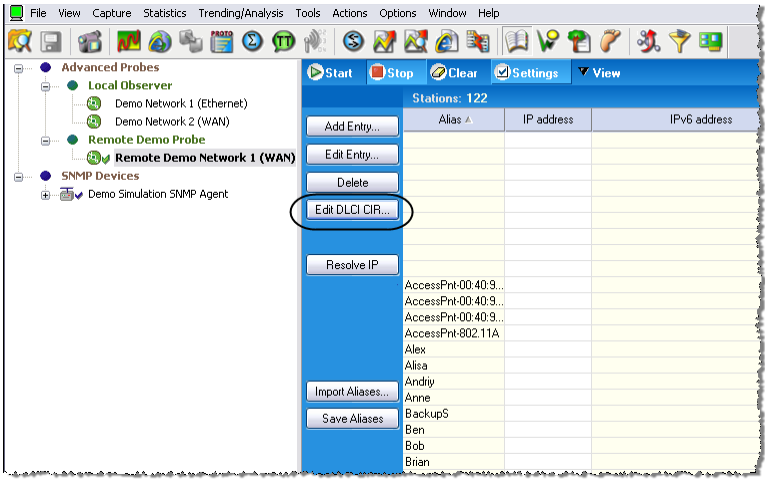
For encapsulations that do not use DLCI (such as X.25), just use the address scheme for your encapsulation.

To set the CIR for a DLCI or group of DLCIs

1 Choose Tools → Discover Network Names. The Discover Network Names pane opens.

2 In the pane, click the edit DLCI CIR button on the Discover Network Names mode window (Figure 51).

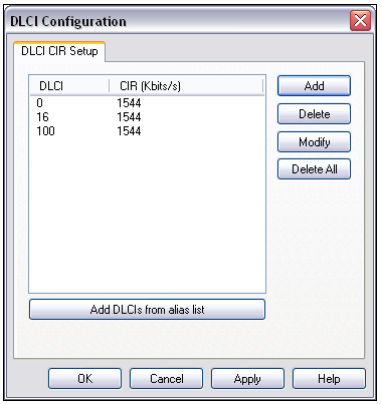
Figure 51 Edit DCLI



3 Click Add to add a new DLCI.

4 Type the CIR in Kbits/sec for the DLCI.

Figure 52 DLCI Configuration dialog

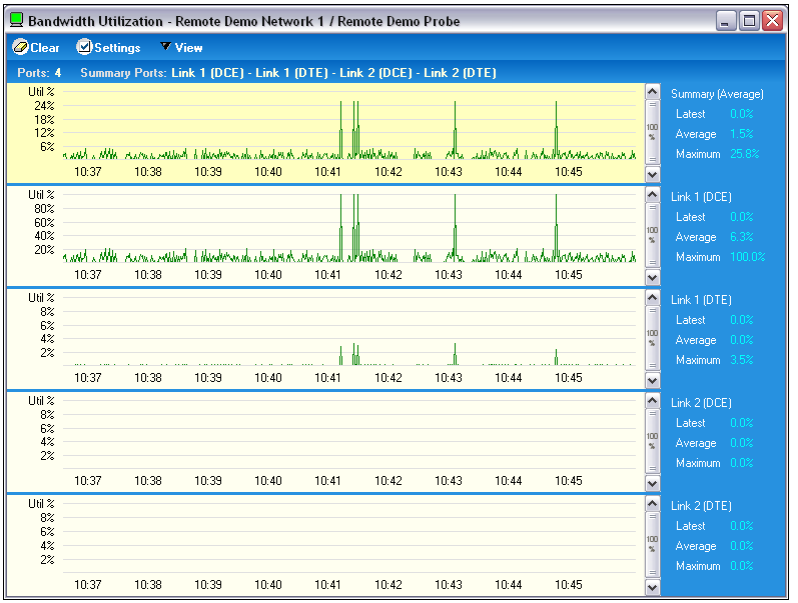


5 Click OK when you are done. For encapsulations that do not use DLCI (such as X.25), the correct address value is shown even though it is still labeled DLCI.

WAN Bandwidth Utilization

To see the percentages of bandwidth saturation on DCE, DTE and DCE+DTE (Summary) for each configured link, choose Statistics → Bandwidth Utilization. The mode starts automatically:

Figure 53 WAN bandwidth utilization



WAN links have two ports (DCE and DTE), so for a dual link T1, you could display up to 5 charts (including the summary). The mode is available in chart, pie, graph, and dial views. The display setup dialog (click Settings to access), lets you choose what ports to display as well as color and scale options.

NOTE: BANDWIDTH UTILIZATION AND FILTERS

The Bandwidth Utilization display is not subject to any filters as it compares the actual activity on the network to the network's theoretical capacity.

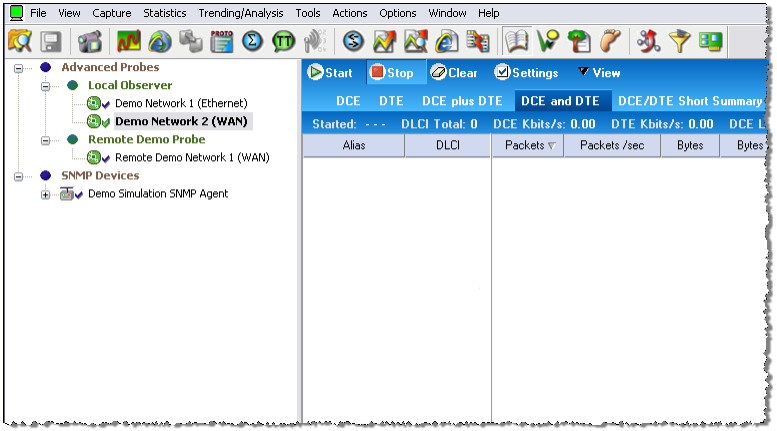
WAN Vital Signs by DLCI

In Observer, the Network Vital Signs display is replaced by the WAN Vital Signs by DLCI mode. This mode provides a summary of the errors occurring on a WAN link (E1/T1/DS3/E3).

Choose Statistics → WAN Vital Signs by DLCI.

You can choose what portion of traffic you wish to view from the list box in the upper left corner of the window: DCE, DTE, DCE plus DTE, and so forth.

Figure 54 WAN Vital Signs by DLCI pane



DTE (Data Terminal Equipment), in the context of a WAN link, refers to the DSU/CSU. DCE (Data Circuit-terminating equipment) refers to the WAN switch (which may reside remotely at the line provider's site). Summary view shows a concatenation of traffic from both ends of the link.

The following statistics are shown, broken down by DLCIs (which are listed in the left most column). You can change the sort order by clicking on any of the column headings:

Table 7 WAN statistics

Column	Description
DLCI	Data Link Connection Identifier of the statistics that follow. For encapsulations that do not use DLCI (such as X.25), the correct address value is shown even though it is still labeled DLCI.
DCE KBits/s Max	The maximum bit rate sensed so far from the DCE side of this DLCI, in Kbits per second.
DTE KBits/s Max	The maximum bit rate sensed so far from the DTE side of this DLCI, in Kbits per second.
DCE Kbits/s Avg	The average bit rate sensed on the DCE side of this DLCI, in Kbits per second.
DTE Kbits/s Avg	The average bit rate sensed on the DTE side of this DLCI, in Kbits per second.
DCE FECN under CIR	The number of packets seen on the DCE side of the link that had the Forward Explicit Congestion Notification bit set, even though the bandwidth usage was within the Committed Information Rate (CIR). Normally this number should be zero. If bandwidth usage exceeds CIR, congestion is expected.
DTE FECN under CIR	The number of packets seen on the DTE side of the link that had the Forward Explicit Congestion Notification bit set, even though the bandwidth usage was within the Committed Information Rate (CIR). Normally this number should be zero. If bandwidth usage exceeds CIR, congestion is expected.
DCE BECN under CIR	The number of packets seen on the DCE side of the link that had the Backward Explicit Congestion Notification bit set, even though the bandwidth usage was within the Committed Information Rate (CIR). Normally this number should be zero. If bandwidth usage exceeds CIR, congestion is expected.
DTE BECN under CIR	The number of packets seen on the DTE side of the link that had the Backward Explicit Congestion Notification bit set, even though the bandwidth usage was within the Committed Information Rate (CIR). Normally this number should be zero. If bandwidth usage exceeds CIR, congestion is expected.

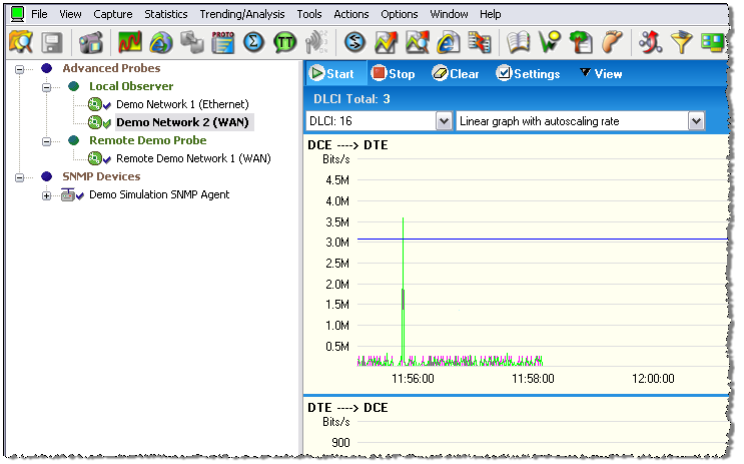
WAN Load by DLCI

In a WAN installation, Observer's Network Activity Display is called WAN Load by DLCI. This mode shows critical WAN transfer rate and congestion statistics in a number of formats. This display can show you the health of a WAN link at a glance and can warn of impending slowdowns due to congestion or other error conditions.

1 Choose Statistics → WAN Load by DLCI.

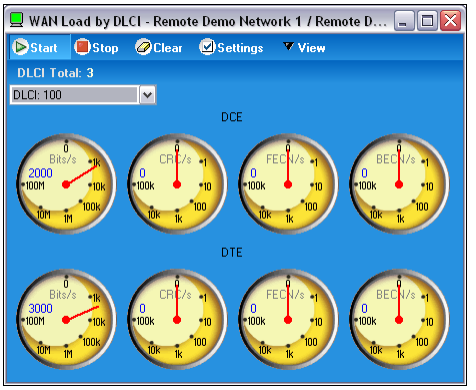
2 Press Start to begin capturing load data.

Figure 55 WAN Load by DLCI



The WAN Load by DLCI mode can be viewed as a dial, graph, or list display. Except for list view, there are no setup options for WAN Load by DLCI mode. Every view includes a dropdown box that lets you select which DLCI you want to monitor.

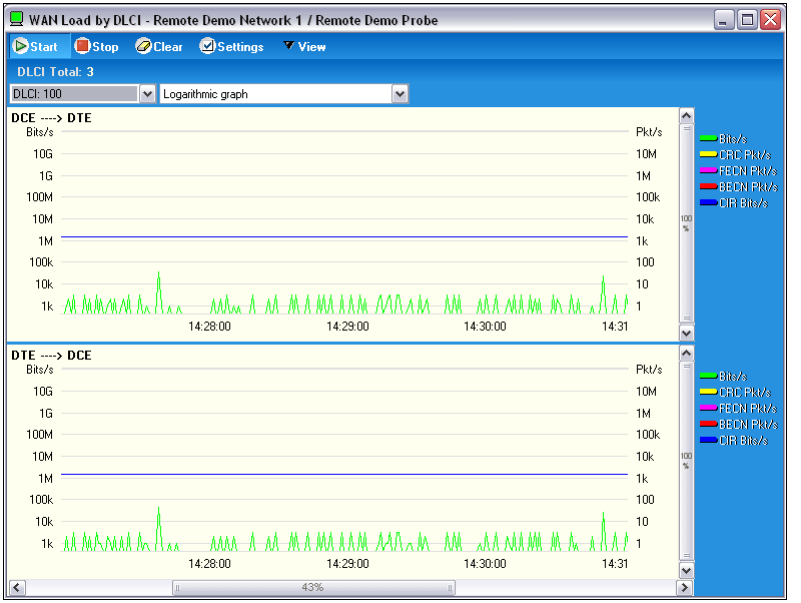
Figure 56 WAN Load by DLCI Dial View



The WAN Load by DLCI mode in dial view shows transfer rate, CRC error rate, FECN/BECN frame rates graphed on dial meters.

For encapsulations that do not use DLCI (such as X.25), the correct address value is shown even though it is still labeled DLCI.

Figure 57 WAN Load by DLCI Graph View



The WAN Load display in graph view shows these same statistics (transfer rate, CRC error rate, and FECN/BECN frame rates) as superimposed spike meters. The Committed Information Rate (CIR) is also shown, allowing you to view the network activity against the baseline performance you have contracted to receive from your WAN service provider

You can select line, point, or bar-style meter, and the colors for each statistic by right-clicking on the chart. The dropdown menus at the top of the display let you select what DLCIs to view, and how the chart should be scaled (linearly, logarithmically, or auto-scale). For linear scales, you can also set the CIR or the line rate as the maximum value for the chart.

WAN Top Talkers

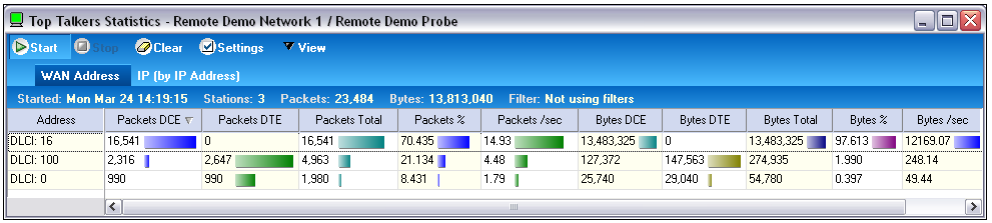
Just as in standard Observer, Top Talkers shows the IP and MAC address of stations on your network sorted by volume of traffic generated and received. In WAN Observer, the MAC Address tab shows DLCIs sorted by volume of traffic. Also, the sorting and charting statistical criteria (such as percentage of packets, packets per

second, etc.) that apply to WAN is a subset of those available for standard network analysis. For encapsulations that do not use DLCI (such as X.25), the correct address value is shown even though it is still labeled DLCI.

1 Choose Statistics → Top Talkers Statistics.

2 Press Start to begin capturing load data.

Figure 58 WAN Top Talkers



Address	Packets DCE	Packets DTE	Packets Total	Packets %	Packets /sec	Bytes DCE	Bytes DTE	Bytes Total	Bytes %	Bytes /sec
DLCI: 16	16,541	0	16,541	70.435	14.93	13,483,325	0	13,483,325	97.613	12169.07
DLCI: 100	2,316	2,647	4,963	21.134	4.48	127,372	147,563	274,935	1.990	248.14
DLCI: 0	990	990	1,980	8.431	1.79	25,740	29,040	54,780	0.397	49.44

TIP!

If you are looking to identify additional top talkers beyond the DLCI, using Ethernet Top Talkers may be more beneficial for you.

WAN Filtering

In addition to the standard Observer packet filtering rules (station address, pattern matching, etc.), there are two WAN-specific filtering rules available for use with WAN probes:

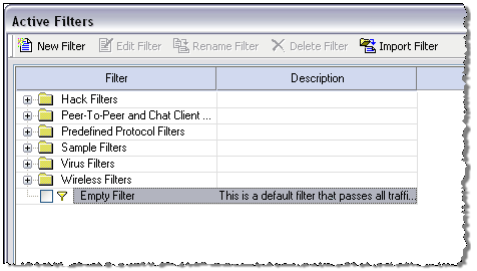
- DLCI Address, which lets you enter the number of the DLCI address you wish to include or exclude.
- WAN Conditions, which let you include or exclude frames based on flow direction, forward and backward congestion, and discard eligibility.

To create a WAN filter rule:

1 Choose Actions →Filter Setup for Selected Probe.

2 Select an existing filter or click New Filter to create your own. See the filtering information in the Observer manual for full details about creating a custom filter from scratch.

Figure 59 Active Filters

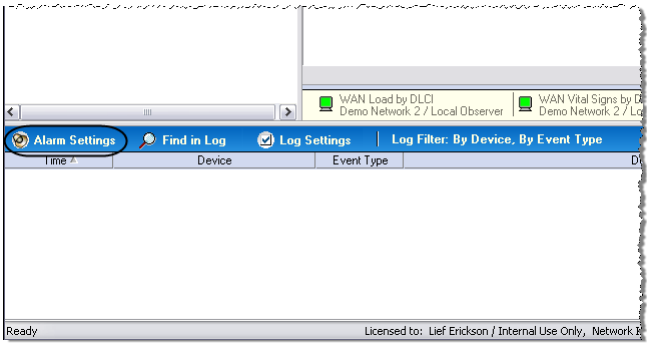


Triggers and Alarms

WAN Observer adds WAN-related criteria to the standard Triggers and Alarms mode.

1 Click the Alarm Settings button located in the lower left corner of Observer's main window.

Figure 60 Alarm Settings

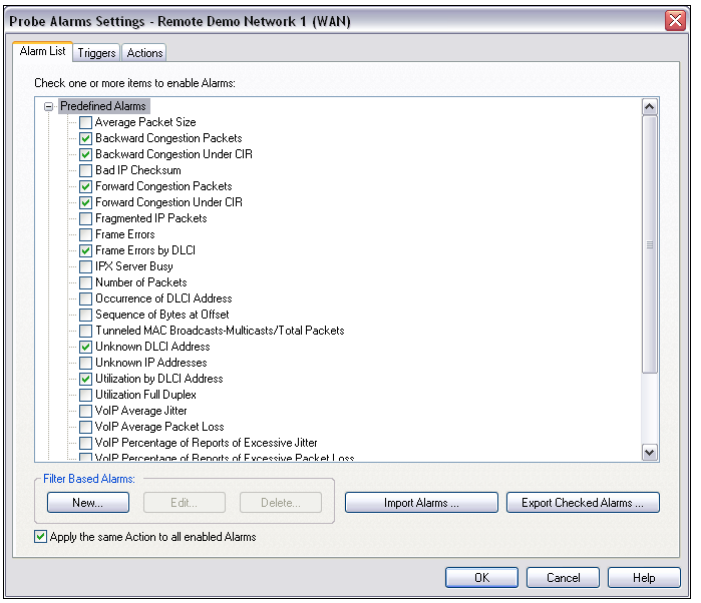


A dialog appears that allows you to select the probe or probes for which you want to set alarms.

2 Check the probes you wish to set.

3 Select an probe for which you want to set alarms and then click the Selected Instance Alarm Settings button. Figure 61 appears.

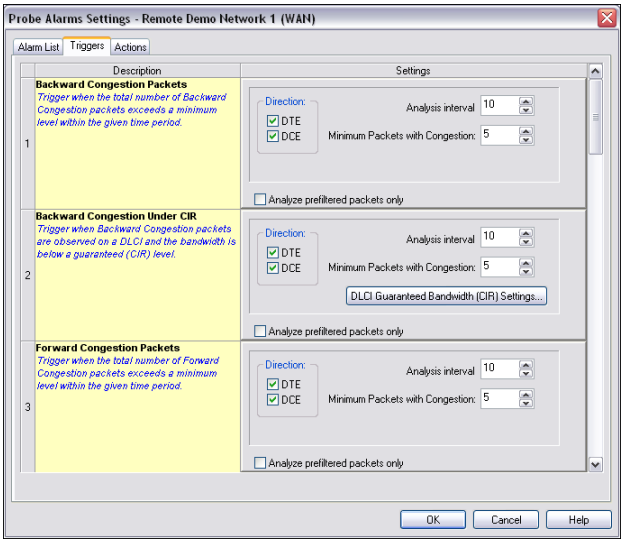
Figure 61 Probe Alarm Settings



4 Select the alarms you want set.

5 Click the Triggers tab to set the criteria by which the alarms will be triggered.

Figure 62 Triggers tab



Most WAN alarms can be set on the DTE or DCE side or both. The Committed Information Rate displayed is that which you set in Discover Network Names mode. See "Setting the Committed Information Rate (CIR) for a DLCI" on page 80.

6 Click the Actions tab to define actions to launch if an alarm is triggered. You can log messages, send e-mail, or even send a pager alarm.

Chapter 6

Forensic Analysis using Snort

Forensic Analysis, exclusive to the GigaStor version of Observer, is a powerful tool for scanning high-volume packet captures for intrusion signatures and other traffic patterns that can be specified using the familiar Snort rule syntax. You can obtain the rules from www.snort.org, or, if you know the Snort rule syntax, you can write your own rules.

Snort began as an open source network intrusion detection system (NIDS). Snort's rule definition language is the standard way to specify packet filters aimed at sensing intrusion attempts.

Snort rules (or Snort-style rules) imported into Observer operate much like Observer's Expert conditions, telling Observer how to examine each packet to determine whether it matches specified criteria, triggering an alert when the criteria is met. They differ from Expert conditions in that they only operate post-capture, and the rules themselves are text files imported into Observer.

NOTE:

Only rules with alert actions are imported. Rules with log, activate, dynamic, or any actions other than alert are simply ignored. Except for RULE_PATH, variable declarations (Snort var statements) are imported. Rule classifications (config classification) are imported, but any other config statements are ignored. Another difference is that Observer, unlike Snort, supports IPv6 addressing.

After you import the rules into Observer you are able to enable and disable rules and groups of rules by their classification as needed.

Starting Forensic Analysis using Snort rules

Forensics profiles provide a mechanism to define and load different pairings of settings and rules profiles. *Settings profiles* define pre-processor settings that let you tune performance; *rules profiles* define which forensic rules are to be processed during analysis.

Observer lets you configure preprocessor settings to tune performance, and to perform specialized processing designed to catch threats against particular target operating systems and web servers. Because Observer performs signature matching on existing captures rather than in real time, its preprocessor configuration differs from

that of native Snort. When you import a set of Snort rules that includes configuration settings, Observer imports rules classifications, but uses its own defaults for the preprocessor settings.

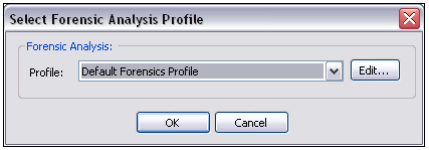
NOTE:

There is a difference between enabling the preprocessor and enabling logs for the preprocessor. For example, you can enable IP defragmentation with or without logging. Without logging, IP fragments are simply reassembled; only time-out or maximum limit reached messages are noted in the Forensics Log and in the Forensic Analysis Summary window. If logging is enabled, all reassembly activity is displayed in the Forensics Log (but not displayed in the Forensic Analysis Summary).

Forensics analysis is available from both the Decode/Analysis window displayed when you load a saved capture buffer locally from GigaStor, and also from the GigaStor control panel. In either case, if you have not yet imported any rules, or if you wish to add or modify rules, click Edit to display the Forensic Settings dialog.

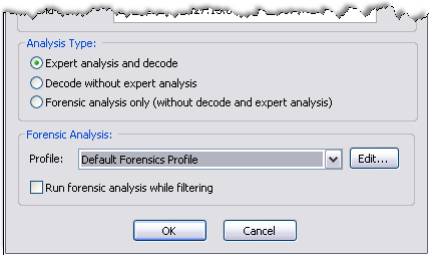
- From the Decode/Analysis Display: After loading a previously-saved capture buffer, click the Forensics tab. The Select Forensics Analysis dialog is displayed:

Figure 63 Select Forensic Analysis Profile dialog



- From the GigaStor Control Panel: Select the time window you wish to analyze, then click Analyze. At the bottom of the GigaStor Analysis Options dialog you can select or edit a Forensics profile. This is described in detail in "Creating a forensic analysis profile from the GigaStor control panel" on page 94.

Figure 64 GigaStor Analysis Options - Forensic Analysis section



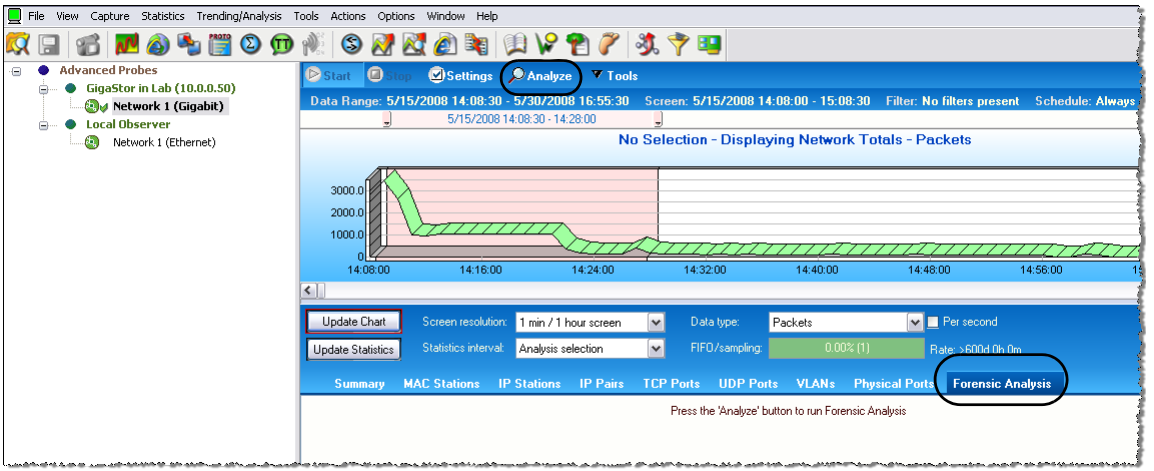
If you already have a forensic analysis profile, you choose the profile from the Profile list (Figure 64) and click OK. For more information about the analysis output, see:

- "About Forensic Analysis tab" on page 98
- "About the Forensic Analysis Log tab" on page 99

Creating a forensic analysis profile from the GigaStor control panel

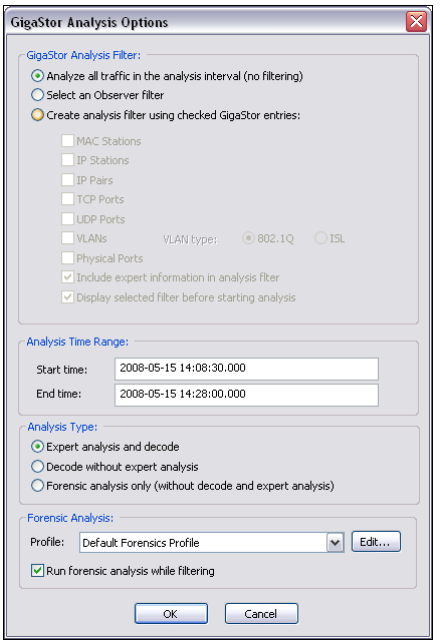
1 Click the Forensics Analysis tab on the far right of the screen.

Figure 65 Forensic Analysis tab



2 Click the Analyze button at the top of the screen. The GigaStor Analysis Options dialog opens.

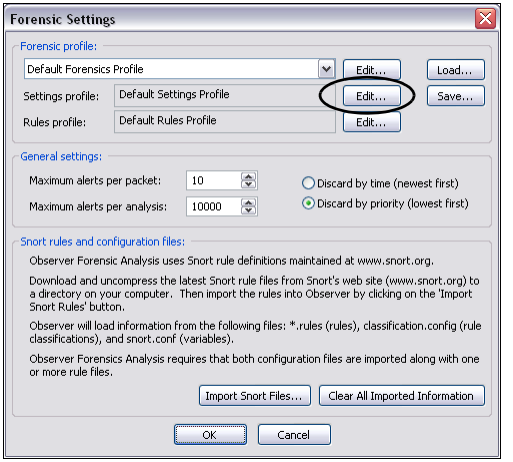
Figure 66 GigaStor Analysis Options



3 Select the profile that you want or click Edit.

4 Click the Settings Profile Edit button to view and define the fields as you need. The fields are described in full in "Forensic Analysis Profile Settings tab" on page 100.

Figure 67 Forensic Settings



If this is the first time forensic analysis has been run, you must import some rules.

5 Click the Import Snort Files button to display a file selection dialog. Browse to the directory where the rules you wish to import are located and select them. You can select multiple files using either CTRL-clicks or by simply dragging the cursor across the files you wish to select. If you do not yet have the Snort rules, see "Rules tab" on page 106.

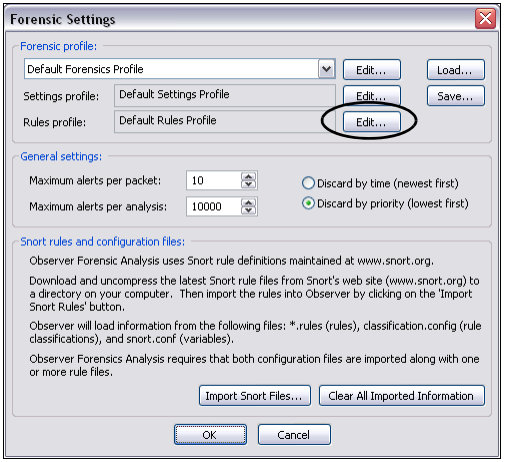
6 Click OK when you are done selecting files.

Observer displays a progress bar and then an import summary showing the results of the import. Because Observer's forensic analysis omits support for rule types and options not relevant to a post-capture system, the import summary will probably list a few unrecognized options and rule types. This is normal, and unless you are debugging rules that you wrote yourself, can be ignored.

7 Close the Import Summary Window.

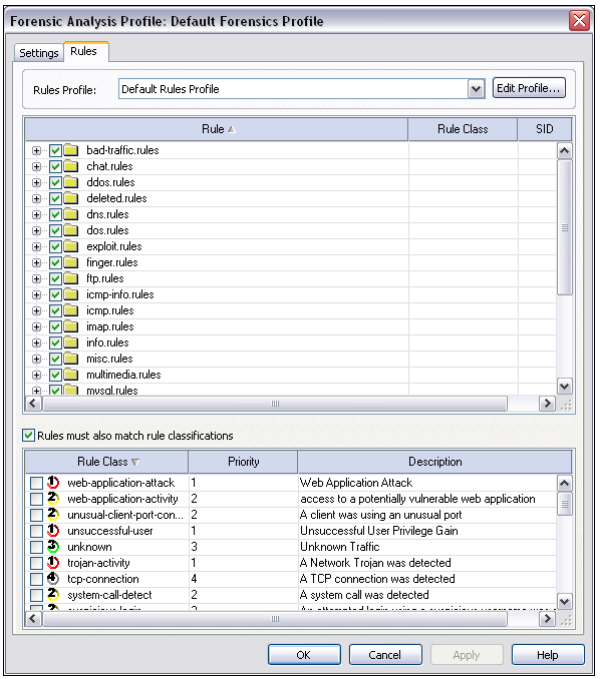
8 Click the Edit button to the right of the Rules profile dropdown menu.

Figure 68 Forensic Settings



The Rule Settings dialog is displayed (Figure 69). The top portion of the window lists the rules that were imported, grouped in a tree with branches that correspond to the files that were imported.

Figure 69 Rules tab



9 Select the boxes next to the rules you want to enable. The right-click menu has options to enable/disable all rules, and to show the actual Snort rule that was imported. It also lets you jump to web-based threat references such as bugtraq for further information about the alert.

Rule classifications offer another level of control. Check the "Rules must also match rule classifications" box to display a list of defined rule classifications. Classifications are defined at import time by parsing the Snort config classification statements encountered in the rule set. Rules are assigned a classification in the rule statement's classtype option.

Select the rule classification(s) you want to enable. If classification matching is enabled, a rule and its classification must both be enabled for that rule to be processed. For example, suppose you want to enable all policy violation rules: simply right-click on the rule list, choose Enable all rules, and then enable the policy violation classification.

10 Click OK to close the Forensic Analysis Profile dialog. Click OK again to close the Forensic Settings dialog. Click OK to close the GigaStor Analysis Options dialog.

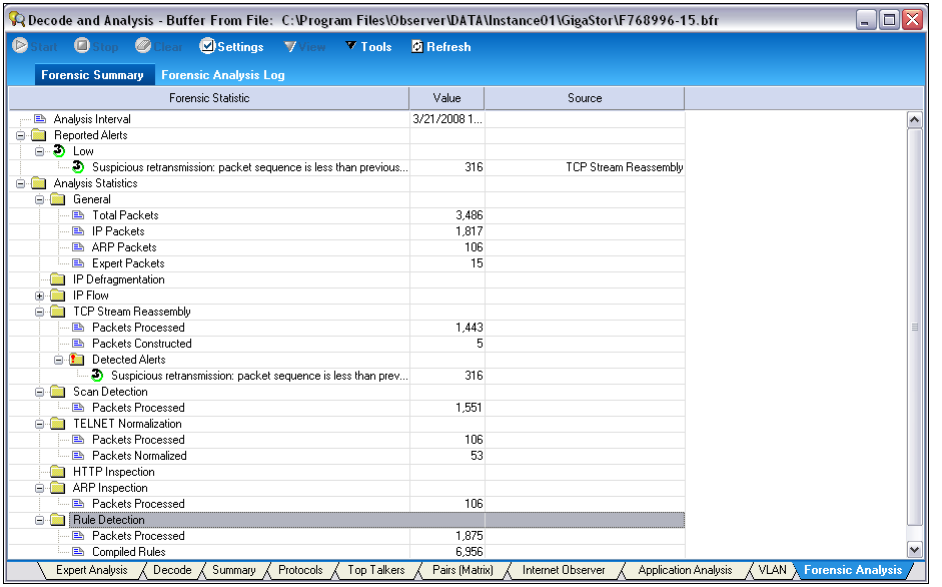
Observer applies the rules and filters to the capture data and displays the results in the Forensics Summary tab. A new tab is also opened that contains the decode. For details about the tabs, see:

- "About Forensic Analysis tab" on page 98
- "About the Forensic Analysis Log tab" on page 99

About Forensic Analysis tab

This display summarizes alerts and preprocessor events in a navigable tree.

Figure 70 Forensic Summary



TIP! PREPROCESSOR MAXIMUMS

It is important to examine the preprocessor results to ensure that time-outs and other maximum value exceeded conditions haven't compromised the analysis. In Figure 70, both the IP Flow and TCP Stream Reassembly preprocessors have timed out on hundreds of flows and streams. If you see similar

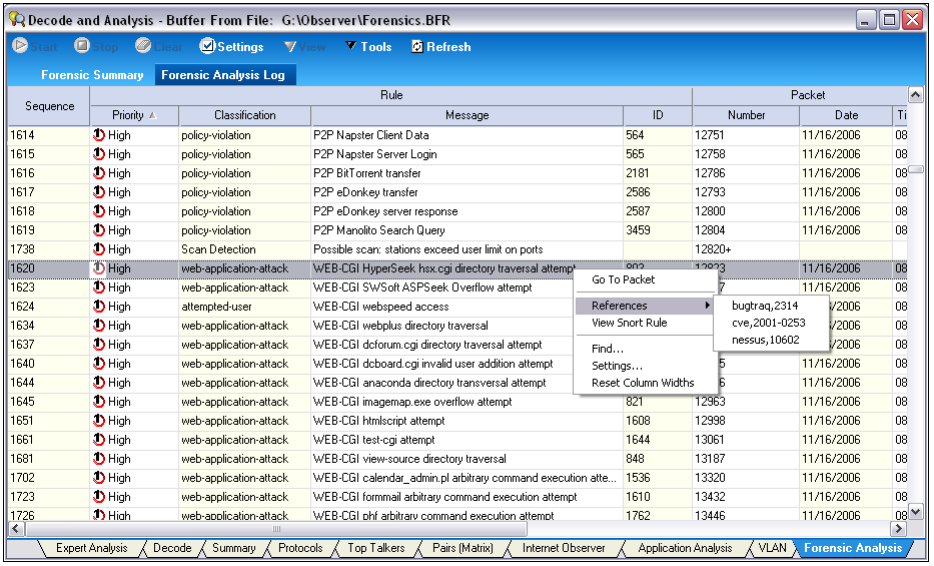
results, you may want to adjust preprocessor settings to eliminate these conditions. Intruders often attempt to exceed the limitations of forensic analysis to hide malicious content.

The right-click menu lets you examine the rule that triggered the alert (if applicable). It also lets you jump to web-based threat references such as bugtraq for further information about the alert. These references must be coded into the Snort rule to be available from the right-click menu.

About the Forensic Analysis Log tab

The Forensic Analysis Log comprehensively lists all rule alerts and preprocessor events in a table, letting you sort individual occurrences by priority, classification, rule ID, or any other column heading. Just click on the column heading to sort the alerts by the given criteria.

Figure 71 Forensic Analysis Log tab



The right-click menu lets you examine the rule that triggered the alert (if applicable). It also lets you jump to web-based threat references such as bugtraq for further information about the alert. These references must be coded into the Snort rule to be available from the

right-click menu. You can also jump to the Decode display of the packet that triggered the alert.

Forensic Analysis Profile field descriptions

This section describes in detail the fields on the Settings and Rules tab. See:

- "Forensic Analysis Profile Settings tab" on page 100
- "Rules tab" on page 106

Forensic Analysis Profile Settings tab

Figure 72 Forensic Analysis Profile Settings tab

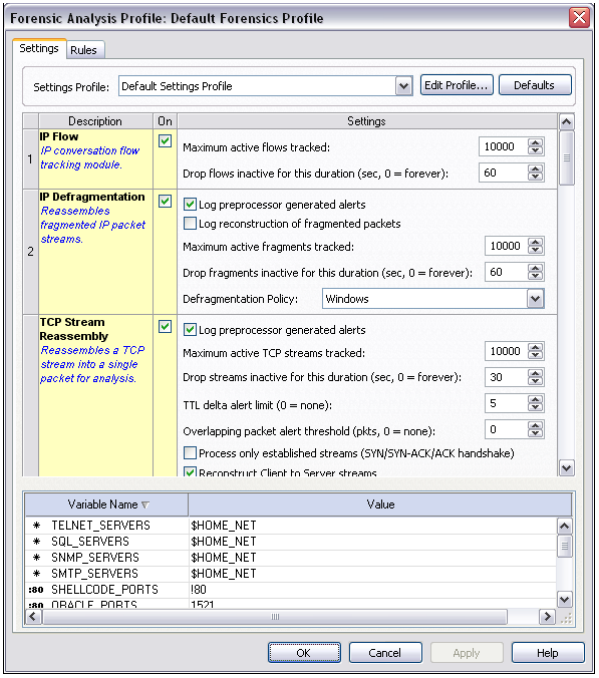


Table 8 describes the fields in the Forensic Analysis Profile Settings tab.

Table 8 Forensic Analysis Profile Settings tab

Field	Description
Settings Profile	Settings Profiles provide a mechanism to save and load different preprocessor settings, and share them with other Observer consoles.
IP Flow	Packets belong to the same IP flow if they share the same layer 3 protocol, and also share the same source and destination addresses and ports. If this box is checked, forensic analysis identifies IP flows (also known as conversations), allowing Snort rules to isolate packets by direction and connection state via the flow option. If this pre-processor is disabled, flow keywords are ignored, but the rest of the rule is processed. The remaining settings allow you to throttle flow analysis by limiting the number of flows tracked, and by decreasing the time window within which a flow is considered active.
IP Defragmentation	Some types of attacks use packet fragmentation to escape detection. Enabling this preprocessor causes forensic analysis to identify and reconstruct fragmented packets based on the specified fragment reassembly policy. Rules are then run against the reconstructed packets during forensic analysis. The fragment reassembly policy mimics the behavior of various operating systems in what to do when ambiguous fragments are received. Choose the policy to match the OS of the server (or servers) being monitored (see the table below). If the buffer contains traffic targeting hosts with different operating systems, use post-filtering to isolate the traffic before forensic analysis so that you can apply the correct policy. Defragmentation Policy is: BSD = AIX, FreeBSD, HP-UX B.10.20, IRIX, IRIX64, NCD Thin Clients, OpenVMS, OS/2, OSF1, SunOS 4.1.4, Tru64 Unix, VAX/VMS Last data in = Cisco IOS BSD-right = HP JetDirect (printer) First data in = HP-UX 11.00, MacOS, SunOS 5.5.1 through 5.8 Linux = Linux, OpenBSD Solaris = Solaris Windows = Windows (95/98/NT4/W2K/XP) Refer to www.snort.org for more detailed version-specific information. The remaining options allow you to enable logging of alerts and reconstruction progress, limit the number of active packet fragments to track, and change the length of fragment inactivity that causes the fragment to be dropped from analysis.
TCP Stream Reassembly	Another IDS evasion technique is to fragment the attack across multiple TCP segments. Because hackers know that IDS systems attempt to reconstruct TCP streams, they use a number of techniques to confuse the IDS so that it reconstructs an incorrect stream (in other words, the IDS processes the stream differently from that of the intended target). As with IP fragmentation, forensic analysis must configured to mimic how the host processes ambiguous and overlapping TCP segments, and the topology between attacker and target to accurately reassemble the same stream that landed on the target. Re-assembly options are described below:

Table 8 Forensic Analysis Profile Settings tab (Continued)

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

Table 8 Forensic Analysis Profile Settings tab (Continued)

Field	Description
TCP Stream Reassembly (Continued)	• Reassembly error action—Discard and flush writes the reassembled stream for analysis, excluding the packet that caused the error. Insert and flush writes the reassembled stream, but includes the packet that caused the error. Insert no flush includes the error-causing packet and continues stream reassembly. • Reassembled packet size threshold range—Some evasion strategies attempt to evade detection by fragmenting the TCP header across multiple packets. Reassembling the stream in packets of uniform size makes this easier for attackers to slip traffic past the rules, so forensic analysis reassembles the stream using random packet sizes. Here you can set the upper and lower limits on the size of these packets. • Reassembled packet size seed value—Changing the seed value will cause forensic analysis to use a different pattern of packet sizes for stream reassembly. Running the analysis with a different seed value can catch signature matches that would otherwise escape detection. • Port List—Enabling the Port List option limits analysis to (or excludes from analysis) the given port numbers.
HTTP URI Normalization	Many HTTP-based attacks attempt to evade detection by encoding URI strings in UTF-8 or Microsoft `%u` notation for specifying Unicode characters. This preprocessor includes options to circumvent the most common evasion techniques. To match patterns against the normalized URIs rather than the unconverted strings captured from the wire, the VRT Rules use the uricontent option, which depends on this preprocessor. Without normalization, you would have to include signatures for the pattern in all possible formats (using the content option), rather than in one canonical version. • Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the HTTP preprocessor to the log, but not the Forensic Summary Window. • Maximum directory segment size—Specifies the maximum length of a directory segment (i.e., the number of characters allowed between slashes). If a URI directory is larger than this, an alert is generated. 200 characters is reasonable cutoff point to start with. This should limit the alerts to IDS evasions. • Unicode Code Page—Specify the appropriate country code page for the traffic being monitored. • Normalize ASCII percent encodings—This option must be enabled for the rest of the options to work. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because such encoding is considered standard, logging occurrences of this is not recommended.

Table 8 Forensic Analysis Profile Settings tab (Continued)

Field	Description
HTTP URI Normalization (Continued)	• Normalize percent-U encodings—Convert Microsoft-style %u-encoded characters to standard format. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because such encoding is considered non-standard (and a common hacker trick), logging occurrences of this is recommended. • Normalize UTF-8 encodings—Convert UTF-8 encoded characters to standard format. The second check box allows you to enable logging when such encoding is encountered during preprocessing. Because Apache uses this standard, enable this option when monitoring Apache servers. Although you might be interested in logging UTF-8 encoded URIs, doing so can result in a lot of noise because this type of encoding is common. • Lookup Unicode in code page—Enables Unicode codepoint mapping during pre-processing to handle non-ASCII codepoints that the IIS server accepts. • Normalize double encodings— This option mimics IIS behavior that intruders can use to launch insertion attacks. Normalize bare binary non ASCII encodings—This an IIS feature that uses non-ASCII characters as valid values when decoding UTF-8 values. As this is non-standard, logging this type of encoding is recommended. • Normalize directory traversal—Directory traversal attacks attempt to access unauthorized directories and commands on a web server or application by using the /./ and /../ syntax. This preprocessor removes directory traversals and self-referential directories. You may want to disable logging for occurrences of this, as many web pages and applications use directory traversals to reference content. • Normalize multiple slashes to one—Another directory traversal strategy is to attempt to confuse the web server with excessive multiple slashes. • Normalize Backslash—This option emulates IIS treatment of backslashes (i.e., converts them to forward slashes).

Table 8 Forensic Analysis Profile Settings tab (Continued)

Field	Description
ARP Inspection	Ethernet uses Address Resolution Protocol (ARP) to map IP addresses to a particular machine (MAC) addresses. Rather than continuously broadcasting the map to all devices on the segment, each device maintains its own copy, called the ARP cache, which is updated whenever the device receives an ARP Reply. Hackers use cache poisoning to launch man-in-the-middle and denial of service (DoS) attacks. The ARP inspection preprocessor examines ARP traffic for malicious forgeries (ARP spoofing) and the traffic resulting from these types of attacks. ● Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the ARP Inspection preprocessor to the log, but not the Forensic Summary Window. ● Report non-broadcast requests—Non-broadcast ARP traffic can be evidence of malicious intent. Once scenario is the hacker attempting to convince a target computer that the hacker's computer is a router, thus allowing the hacker to monitor all traffic from the target. However, some devices (such as printers) use non-broadcast ARP requests as part of normal operation. Start by checking the box to detect such traffic; disable the option only if analysis detects false positives.
Telnet Normalization	Hackers may attempt to evade detection by inserting control characters into Telnet and FTP commands aimed at a target. This pre-processor strips these codes, thus normalizing all such traffic before subsequent forensic rules are applied. ● Log preprocessor events—Checking this box causes forensic analysis to save any alerts generated by the Telnet Normalization preprocessor to the log, but not the Forensic Summary Window. ● Port List—Lets you specify a list of ports to include or exclude from Telnet pre-processing. The default settings are appropriate for most networks.
Variable Name	A scrollable window located below the preprocessor settings lists the variables that were imported along with the Snort rules. Variables are referenced by the rules to specify local and remote network ranges, and common server IP addresses and ports. You can edit variable definitions by double-clicking on the variable you want to edit. The VRT Rule Set variable settings (and those of most publicly-distributed rule sets) will work on any network without modification, but you can dramatically improve performance by customizing these variables to match the network being monitored. For example, the VRT rules define HTTP servers as any, which results in much unnecessary processing at runtime. Address variables can reference another variable, or specify an IP address or class, or a series of either. Note that unlike native Snort, Observer can process IPv6 addresses. Port variables can reference another variable, or specify a port or a range of ports. To change a variable, simply double-click the entry. The Edit Forensic Variable dialog shows a number of examples of each type of variable which you can use as a template when changing values of address and port variables.

Rules tab

The web site www.snort.org provides Snort rule documentation, and downloadable rule sets. There are three sets of rules available at www.snort.org: Community Rules (which are available to anyone with a web browser), and three versions of the Vulnerability Response Team (VRT) Certified Rule Set. The most recent rule updates are available to paid subscribers only; non-paying registered users have access to the VRT Rule Set 30 days after subscribers, and unregistered users have access to snapshots of the rule sets that are distributed with Snort releases. All of the rule sets are distributed as tar archives; download the desired rule set and extract the archive to a directory that is accessible to the Observer console.

Although it is recommended that you eventually register for at least the Certified Rule Set, here are the steps for obtaining the Snort release snapshot distribution. If you need archive software that can extract tar files, www.7-zip.org has a free, open source utility that handles most of the popular archive formats, including tar.

1. Go to www.snort.org. Click the Rules link on the left side banner. This displays the VRT rules main page.
2. Click the Download Rules link located on the right side banner.
3. Click the link to Sourcefire VRT Certified Rules (unregistered user release).
4. Click the Download button for the most recent unregistered user release. Save the file (which should have a name something like snortrules-pr-2.4.tar.gz).
5. Extract the rules directory from the archive you downloaded to a directory that is accessible to the GigaStor.

Chapter 7

Observer on the GigaStor

Using the Observer console locally on the GigaStor

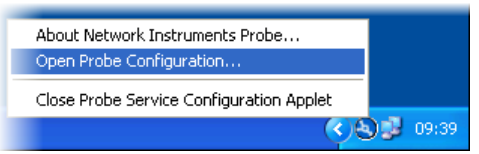
Depending on how you want or need to use Observer it can be either a graphic console to help you analyze your network data or it can be a probe to capture data and to which other Observer consoles can connect. Observer cannot simultaneously be a console and a probe.

In some situations you may want to run Observer locally on your GigaStor instead of using a separate system. This is not the default behavior for a GigaStor. This section describes how to stop the probe that runs as a Windows service and launch Observer.

On the local GigaStor system

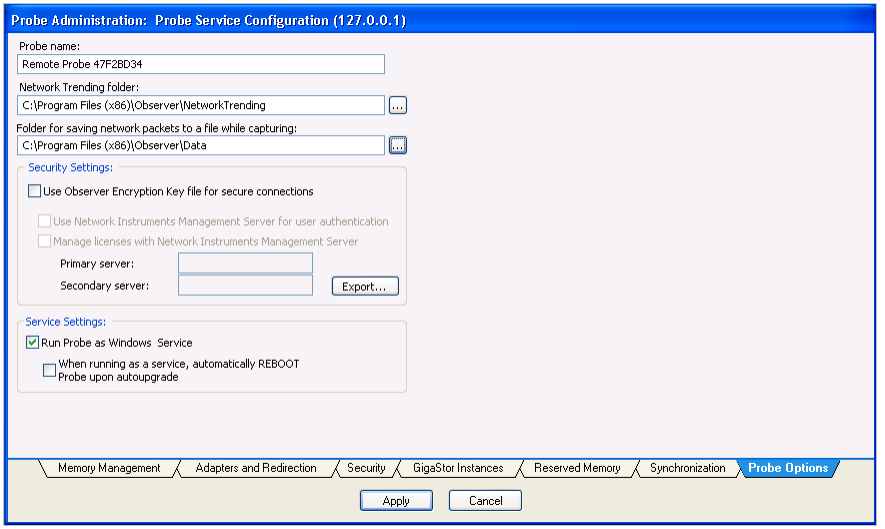
1. Right-click the Probe Service Configuration Applet in the system tray and choose Open Probe Configuration.

Figure 73 Probe Service Configuration Applet



2. The Probe Administration window opens. Click the Probe Options tab (Figure 74).

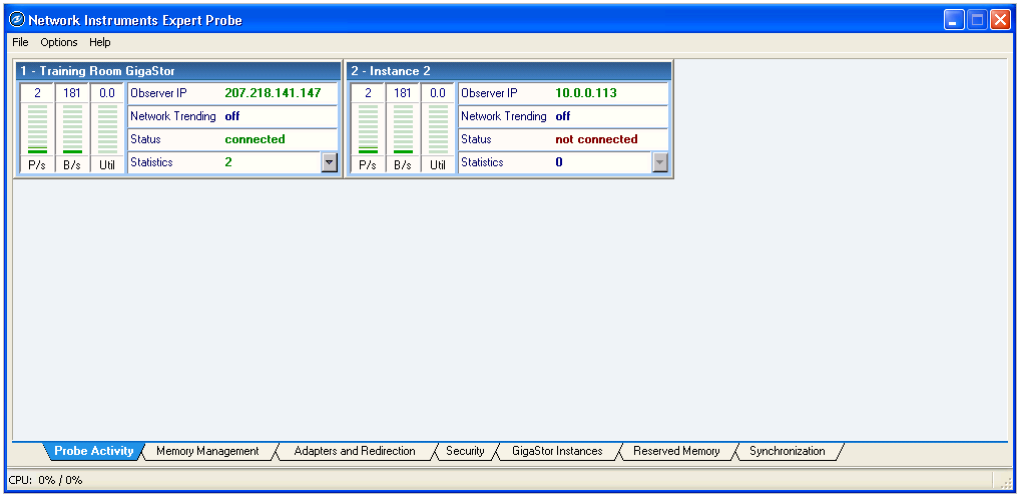
Figure 74 Probe Options



3 In the Service Settings section, clear the "Run Probe as a Windows Service" option and click OK. This uninstalls the Network Instruments Expert Probe service from Windows.

4 Click Start →Programs →Observer →Observer. The Network Instruments Expert Probe window opens.

Figure 75 Expert Probe interface



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 console interface. Click OK on the message dialog.

7 Click Start →Programs →Observer →Observer to open the console interface.

Tip! Switching back to Expert Probe

In Observer, choose View →Switch between Observer and Expert Probe Interface.

After the Expert Probe interface is open, choose Options → Probe Options to select the Run Probe as Windows Service option. You must manually start Network Instruments Expert Probe from the Windows Service Control Manger. It may take a moment before the service starts. You may need to restart the GigaStor for the setting changes to fully set.

Chapter 8

Probe Instances

What is a probe instance?

TIP!

For instructions on setting up a probe instance, see "Probe administration" on page 24.

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

Observer has only one kind of probe instance: the *passive probe instance*. If you have a GigaStor you have an additional probe instance type available to you: the *active probe instance*.

Table 9 compares the features of active and passive probe instances.

Table 9 Active probe instance compared to passive

	GigaStor Active	GigaStor Passive	Observer
Start packet capture			
Stop packet capture			
Start GigaStor packet capture			
Schedule packet capture			
Change directories where data is stored			
Able to set permissions			
Able to redirect to different console, etc.			
Better suited for troubleshooting			
Better suited for data capture			

A passive probe instance captures 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 whatever adapter a passive probe instance is bound to without affecting any active probe instance.

CAUTION : PASSIVE PROBE INSTANCE AND THE GEN2 CARD

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 are 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, it can mine data that has already been written to the RAID disk by 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 an 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. A 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 running.

Tip! Active probe instance best practices

- 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.

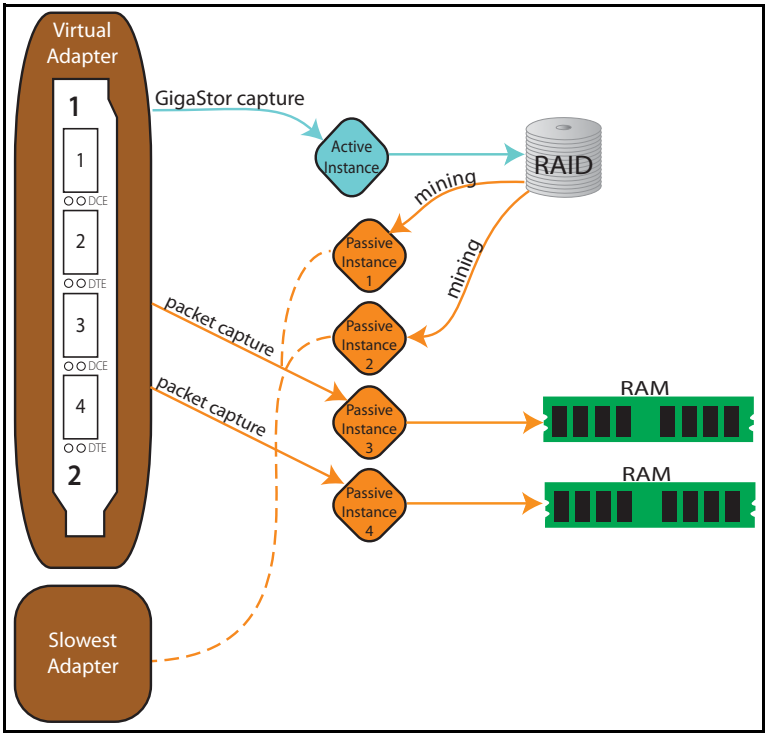
NOTE:

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. See "Configuring virtual adapters on the Gen2 card" on page 116.

Figure 76 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 each are 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.

Figure 76 GigaStor capture and packet capture through probe instances



Chapter 9
Gen2 Capture Card

The Gen2 card is designed and manufactured by Network Instruments and is optimized for the GigaStor. The Gen2 card comes in two, four, or eight port models.

This section describes

Swapping the Gen2 card's SFP or XFP interfaces

To connect the probe to a monitoring interface (TAP or SPAN/mirror) different from that shipped with the unit, simply obtain the necessary SFP for your application, remove the installed SFPs, and insert the desired interface.

The SFPs can be hot-swapped, but you should disconnect any cables before changing the SFP modules. As with any electronic components, you should follow electrostatic discharge precautions (i.e., use a grounding strap or touch the chassis power supply before handling SFPs) to avoid damaging components. In addition, you should be careful to avoid exposure to laser radiation from optical components by keeping the dust plugs installed until you are ready to install cables.

Configuring virtual adapters on the Gen2 card

NOTE: Only GigaStor's equipped for 10 Gigabit Ethernet, Gigabit Ethernet, and Fibre Channel use a Gen2 capture card.

By default Observer recognizes a Gen2 capture card as a single adapter, regardless of how many ports are present. Sometimes this is desirable (as when monitoring a trunk that consists of multiple links), but for many applications it is more convenient for Observer to recognize a subset of Gen2 ports as a single adapter. For example, suppose you are deploying an 8-port Gen2 as follows:

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

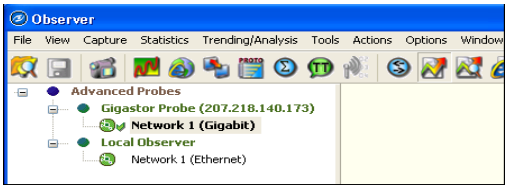
In this scenario, it makes sense for Observer to view Ports 1-4 as a single data stream and to separate each of the four remaining ports into separate data streams.

Virtual adapters are a convenient way to accomplish this separation in real time, rather than depending on filters to sort through the traffic post-capture. A physical port cannot belong to more than one virtual adapter.

To define a subset of Gen2 ports as a single virtual adapter,

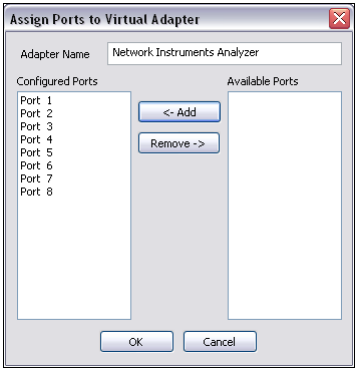
1 Right-click the Gen2-equipped probe from Observer's probe list and choose Probe or Device Properties from the menu.You can tell the probe is a GigaStor probe because (Gigabit) appears after the probe name (Figure 77).

Figure 77 GigaStor probe



2 Click the Virtual Adapters tab and click Edit Adapter. By default all of the ports are assigned to the adapter. You must remove ports if you want to have multiple virtual adapters. See Figure 23 for a diagram of the physical ports assignments.

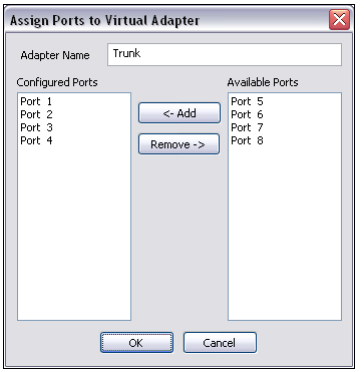
Figure 78 Assign Port to Virtual Adapter: Default view



3 Select the ports to remove and click Remove. This places them in the Available Ports list.

4 Change the name of the adapter to something meaningful to you and click OK (Figure 79).

Figure 79 Assign Ports to Virtual Adapter: Trunk



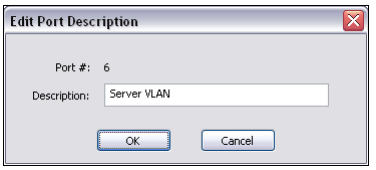
5 Click New Adapter. The Assign Ports to Virtual Adapter window opens.

6 Type a name in the Adapter Name box.

7 Select the ports you want to assign to this virtual adapter from the Available Ports list and click OK.

8 Select the port and click Edit Port. Type a useful description and click OK. This description appears in the GigaStor Control Panel in Observer.

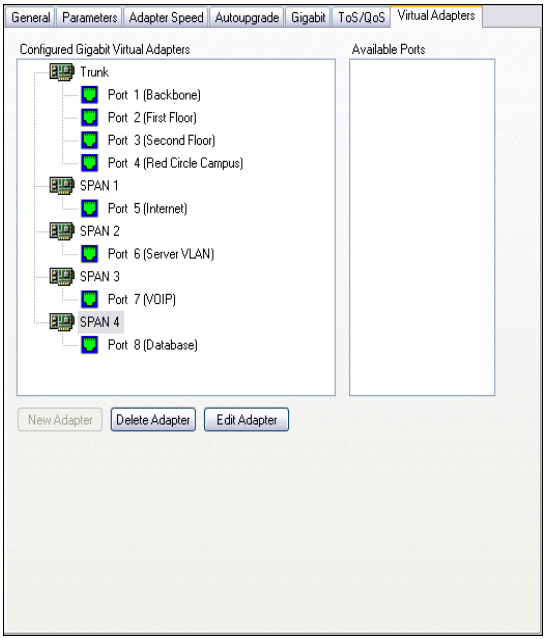
Figure 80 Edit Port Description



9 Repeat step 5 through step 8 until you have created all of your virtual adapters and given descriptions to your ports. The adapters appear in the list of adapters presented when you create a probe instance. This allows you to bind the probe instance to a virtual adapter.

Figure 81 shows the example of the trunk with four ports assigned to it and four more adapters each with its own port.

Figure 81 Virtual Adapters tab



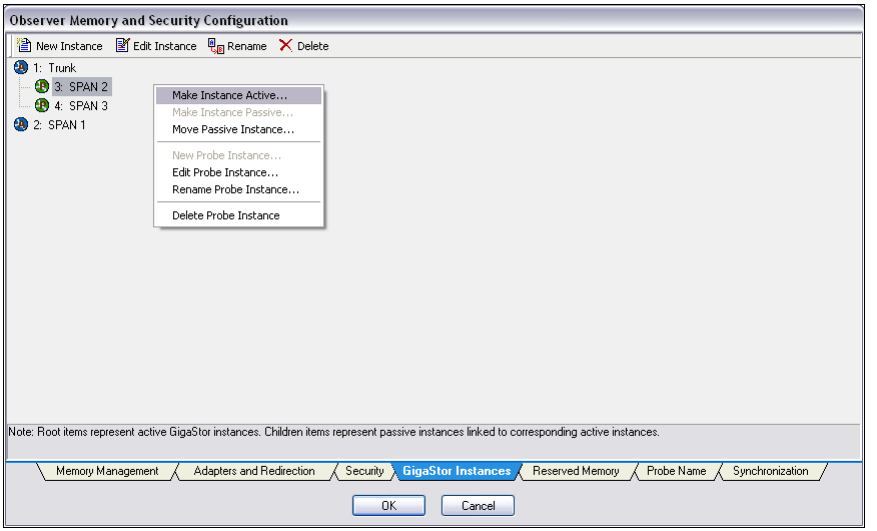
For each virtual adapter you must create an active probe instance and bind the virtual adapter to that probe instance. By default, new virtual adapters are not bound to any probe instance, so no data is collected on those ports until assigned to a probe instance.

10 Right-click the GigaStor probe and choose Administer Selected Probe from the menu. Log in to the probe.

11 Click the GigaStor Instances tab along the bottom.

12 For each virtual adapter listed as a passive probe instance that you want to promote to an active probe instance, select it, right click and choose Make Instance Active.

Figure 82 Make Instance Active



13 A message appears with information about the change. Click Yes to accept the changes.

Your virtual adapters are now configured.

Viewing the Gen2 card's properties and finding the board's ID

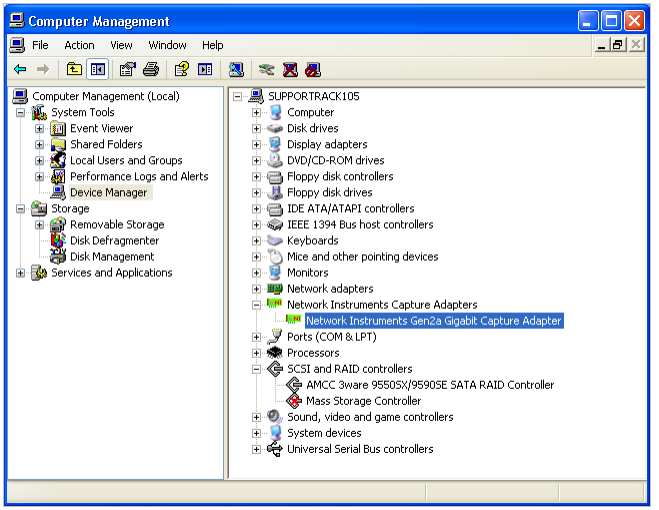
To retrieve the board's ID or view the Gen2 card's properties:

1 On the GigaStor system, choose Start → All Programs → Accessories → Windows Explorer. Choose My Computer and right-click and choose Manage. The Computer Management window opens.

2 In the tree on the left, select Device Manager.

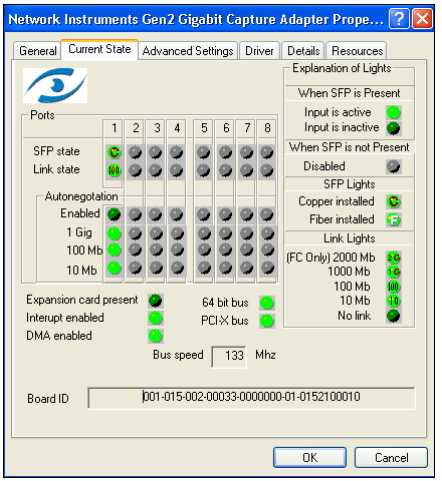
3 In the tree on the right, expand Network Instruments Capture Adapters (Figure 83).

Figure 83 Computer Management window



4 Choose Network Instruments Gen2 Gigabit Capture Adapter, right-click and choose Properties. Click the Current State tab (Figure 84).

Figure 84 Gen2 Card Properties – Current State tab



This tab shows all active physical ports on the Gen2 card and the board's ID. The "Interrupt enabled" and "DMA enabled" lights are light green when Observer is running and dark green when Observer is not running.

CAUTION ADVANCED SETTINGS TAB

Do not make any changes to the settings on the Advanced Settings tab unless directed by the Support department! The DMA buffer size and DMA copy size are optimized at the factory for your specific motherboard and Gen2 card.

Appendix A

TCP/IP ports, NAT, and VPN

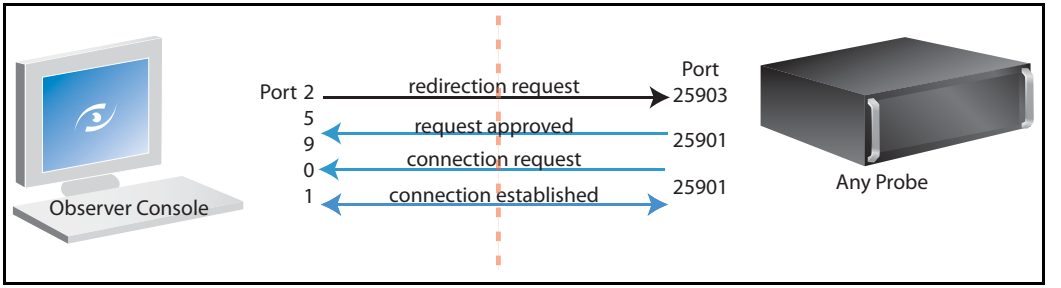
This section discusses the TCP/IP ports, NAT, and VPN.

TCP/IP ports

Observer and all Network Instruments probes use ports 25901 and 25903 to communicate. These ports are registered ports to Network Instruments.

All Network Instruments probes initiate connection with Observer using port 25901. Observer listens on port 25901. After a connection is established all communication between Observer and the probes occurs on port 25901, except probe redirection and administration, which uses port 25903.

Figure 85 Port connections



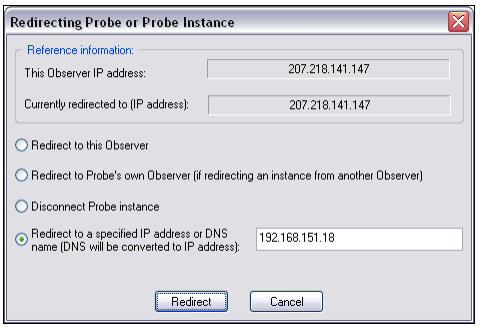
NAT

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 “TCP/IP ports” on page 124, 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 (Figure 86).

Figure 86 NAT



If the Observer is outside the network where the probe is running, you must forward port 25903 from the Observer's address. You must use the NAT outside IP address as the probe's IP address when trying to redirect and/or administer the probe from Observer.

VPN

Using VPN is an easy way to get access to a probe on a remote LAN. The most common configuration change is when redirecting the probe. You must manually enter the Observer IP address. By default, Observer will use the LAN IP address configured to Observer. You must enter your VPN client's IP address by selecting "Redirect to a specified IP address" in the probe redirection dialog.

Select "Redirect to a specified IP address" in the Redirecting Probe or Probe Instance dialog (Figure 86) and type the VPN client's IP address.

Appendix B

GigaStor, GigaStor Expandable, and Expansion Unit Cases

GigaStor

Figure 87 shows the front of the GigaStor.

Figure 87 GigaStor

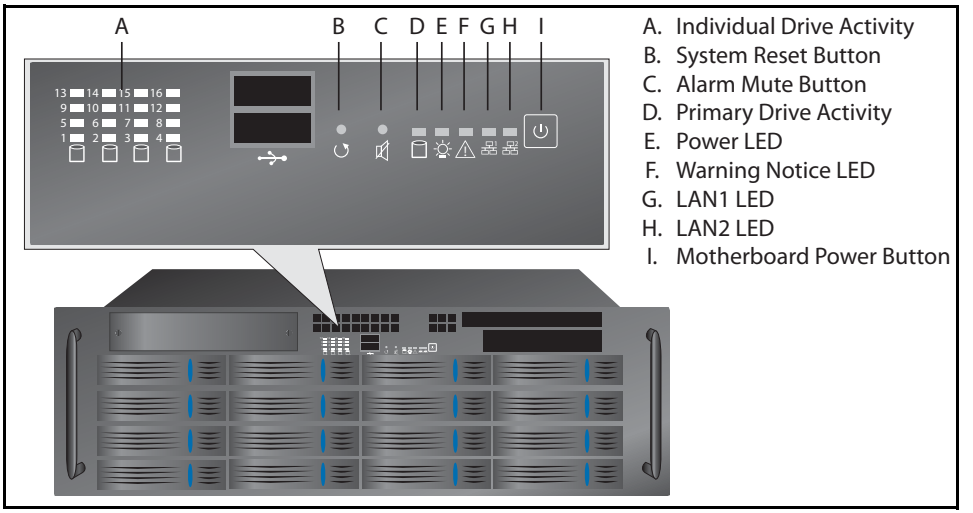


Table 10 GigaStor LEDs and Buttons

LED/Button	Description
Individual Drive Activity	These LEDs blink whenever there is activity on the drive in the RAID array. The lights are red when there is a problem with the drive, otherwise they are green.
System Reset Button	When pushed, the system resets.
Alarm Mute Button	When an error or warning is detected the LED blinks and an alarm sounds. Pushing this button silences the alarm. This button is used in conjunction with the Warning Notice LED.
Primary Drive Activity	This LED blinks whenever there is activity on the main drive. This drive is where the operating system is installed.
Power LED	This LED is lit whenever the unit and motherboard are powered on and running.
Warning Notice LED	When the unit detects a problem such as a fan failure or excessively high temperature, the alarm sounds and this LED blinks. Even if the alarm is silenced, this LED will blink until the alarm condition is resolved.
LAN1 LED	Not used.
LAN2 LED	Not used.
Motherboard Power Button	The motherboard button works only when the power button on the rear of the GigaStor is on. Press to turn on the GigaStor. If you press and hold this button for a few seconds, the unit will do a a hard shut down.

GigaStor Expandable

Controller unit

Figure 88 GigaStor Expandable controller

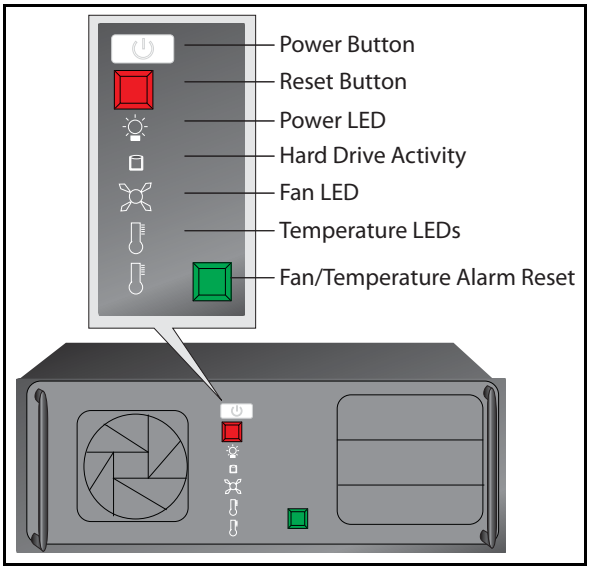
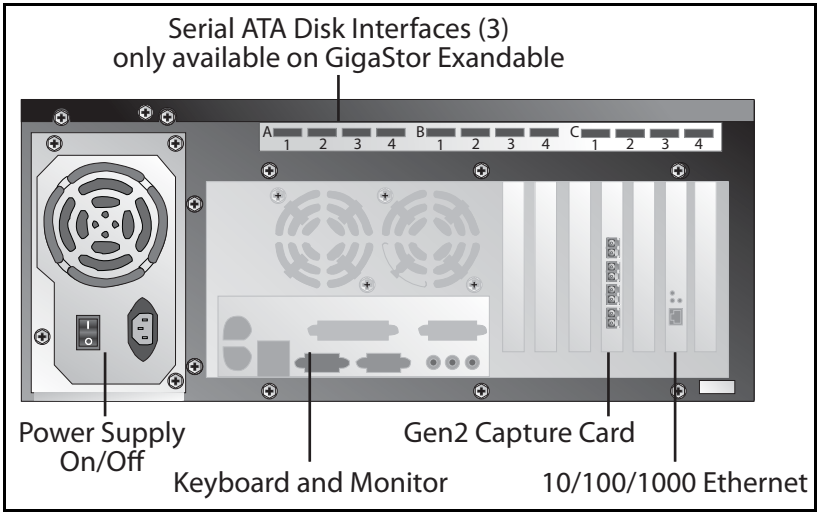


Table 11 GigaStor Expandable LEDs and Buttons

LED/Button	Description
Power Button	The power button works only when the power switch on the rear of the unit is on. Press to turn on the GigaStor. If you press and hold this button for a few seconds, the unit will do a a hard shut down.
Reset Button	When pressed, the unit will do a hard restart of the GigaStor Expandable.
Power LED	This LED is lit whenever the unit and motherboard are powered on and running.
Hard Drive Activity	This LED blinks whenever there is activity on the drive. This drive is where the operating system is installed.
Fan LED	When green, the fan is operating as expected. If it is red, there is a problem with the fan. The removable filter may need to be cleaned. Works in conjunction with the Alarm button. Even if the alarm is silenced, this LED will blink until the alarm condition is resolved.
Temperature LEDs	When lit green the unit's temperature is within normal operating conditions. If it is red, then the unit is too hot. Works in conjunction with the Alarm button. Even if the alarm is silenced, this LED will blink until the alarm condition is resolved.
Fan/Temperature Alarm Button	When pressed, it silences the on board alarm. Alarms may sound with the unit is too hot or the fan has a problem. Even if the alarm is silenced, this LED will blink until the alarm condition is resolved.

Figure 89 shows the back of the GigaStor Expandable.

Figure 89 GigaStor Expandable rear view



Expansion unit

Figure 90 Expansion unit

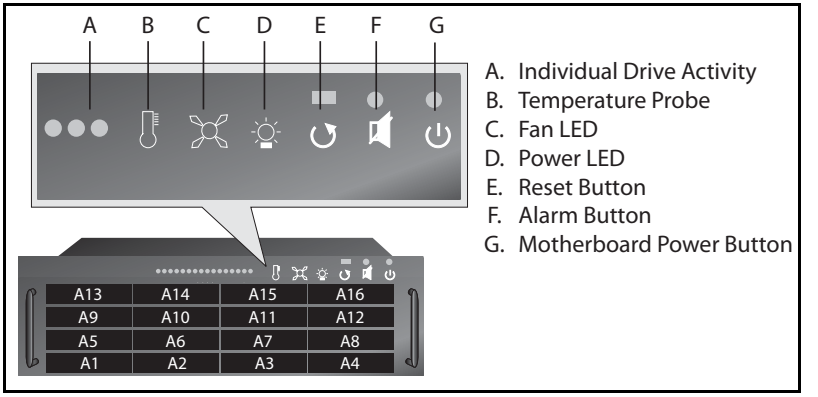
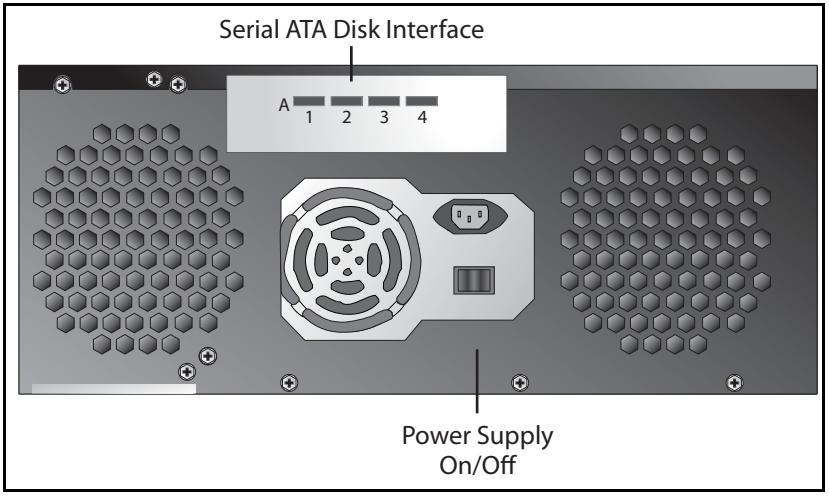


Table 12 Expansion Unit LEDs and Buttons

LED/Button	Description
Individual Drive Activity	These LEDs blink whenever there is activity on the drive in the RAID array. The lights are red when there is a problem with the drive, otherwise they are green.
Temperature probe	When lit green the unit's temperature is within normal operating conditions. If it is red, then the unit is too hot. Works in conjunction with the Alarm button. Even if the alarm is silenced, this LED will blink until the alarm condition is resolved.
Fan LED	When green, the fan is operating as expected. If it is red, there is a problem with the fan. The removable filter may need to be cleaned. Works in conjunction with the Alarm button. Even if the alarm is silenced, this LED will blink until the alarm condition is resolved.
Power LED	This LED is lit whenever the unit and motherboard are powered on and running.
Reset Button	This button is flush with the case. When pressed, the unit will do a hard restart.
Alarm Button	This button is flush with the case. When pressed, it silences the on board alarm. Alarms may sound with the unit is too hot or the fan has a problem. Even if the alarm is silenced, this LED will blink until the alarm condition is resolved.
Motherboard Power Button	The motherboard button works only when the power button on the rear of the GigaStor is on. Press to turn on the expansion unit. If you press and hold this button for a few seconds, the unit will do a a hard shut down.

Figure 91 shows the back of the expansion unit.

Figure 91 Expansion unit rear view



Appendix C

GigaStor Portable

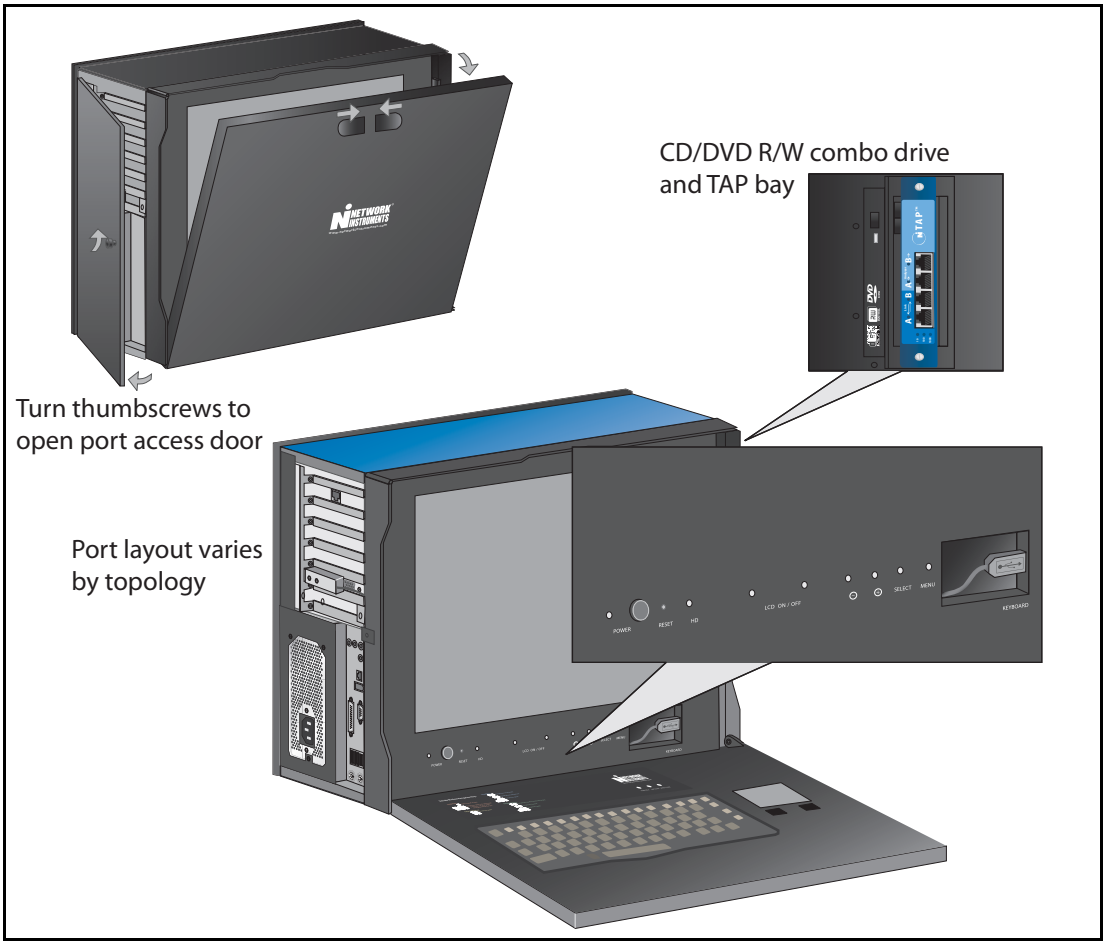
The portable GigaStor offers full-duplex packet capture and analysis at wire speed. Depending on which version you ordered, the system includes everything you need to perform continuous, in-depth analysis of one of the following topologies:

- Gigabit Ethernet
- 10 Gigabit Ethernet
- Fibre Channel
- Wide Area Networks (WAN), in any of a number of different encapsulations

The Portable Analysis Platform includes an internal probe that provides access to the network to which it is connected. The internal probe not only provides a point of visibility for the local Observer console, but also for remote Observer consoles that have been given administrative permission. In other words, the Portable Analysis Platform can double as a secure, remote probe, which can be indispensable for multi-site troubleshooting.

All Ethernet and Fibre Channel versions of the platform feature Small Form-factor Portable (SFP or XFP) technology, allowing you to hot-swap any SFP-compliant connectors into the system. This makes it possible to use the same system to monitor different types of links as needed without having to open the case to swap interface cards. For example, you can easily convert the capture card from optical to copper, allowing you to connect the system to different TAPs and Switch Port Analyzer (SPAN) interfaces.

Figure 92 Portable Analysis Platform System Tour



Your GigaStor includes a number of components. Take a moment after unpacking the system to ensure that you received all the parts.

- A ruggedized “portable” PC system with Observer Suite hardware interfaces and drivers for the relevant topology pre-installed:

Figure 93 Portable GigaStor

Gigabit and Fibre Channel systems have an appropriate copper or optical *n*TAP installed in the drive bay on the right side of the system. WAN system TAPs are shipped separately.

Running Observer passively

When analyzing a link using a TAP, Observer runs "passively." Passive operation guarantees that analysis will not affect the link; however, it does have some implications when running Observer. 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

The Portable GigaStor includes a standard 10/100/1000 Ethernet interface in addition to the WAN, Gigabit, or Fibre Channel interface(s). The standard Ethernet interface allows you to use the system on non-gigabit networks by simply connecting it to an Ethernet hub or switch using a standard Ethernet cable. The TCP/IP driver has been set to automatically obtain an IP address through the

Dynamic Host Control Protocol (DHCP). For most applications of Observer, you should assign an address to the analyzer rather than depending on the DHCP assignment.

Using the portable GigaStor as a probe

Although most administrators usually run the Observer console directly from the portable GigaStor, in some cases you may want to use the system as a distributed probe system. The probe software is included for this purpose.

Index

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

www.networkinstruments.com