

iMonitor User Guide

iDS Release 8.3

A component of iVantage NMS

August 29, 2008





Copyright © 2008 VT iDirect, Inc. All rights reserved. Reproduction in whole or in part without permission is prohibited. Information contained herein is subject to change without notice. The specifications and information regarding the products in this document are subject to change without notice. All statements, information, and recommendations in this document are believed to be accurate, but are presented without warranty of any kind, express, or implied. Users must take full responsibility for their application of any products. Trademarks, brand names and products mentioned in this document are the property of their respective owners. All such references are used strictly in an editorial fashion with no intent to convey any affiliation with the name or the product's rightful owner.

Document Name: UG_iMonitor User Guide iDS 8.3_082908.pdf

Document Part Number: T0000150

Contents

Figures	ix
Tables	x
The iVantage Network Management System	xi
1 Using this Guide	1
1.1 Intended Audience	1
1.2 Document Conventions	1
1.2.1 Typographical and Navigational Conventions	1
1.2.2 Informational Conventions	2
2 Overview of the NMS for iMonitor	3
2.1 Introduction	3
2.2 Components of the Network Management System	3
2.2.1 NMS Applications	3
<i>iBuilder</i>	3
<i>iMonitor</i>	4
<i>iSite</i>	4
2.2.2 Server Components	5
<i>Configuration Server</i>	5
<i>Real-time Data Server</i>	5
<i>Event Server</i>	5
<i>Latency Server</i>	5
<i>NMS Controller Server</i>	5
<i>PP Controller Servers</i>	5
<i>NMS Monitor Script</i>	5
<i>Consolidation Script</i>	5
<i>Database Backup Script</i>	5
<i>Database Restore Script</i>	6
2.3 Installing iBuilder, iMonitor, and iSite	6
2.3.1 System Requirements	6
2.3.2 Installation Procedure	6
2.4 Installing the Geographic Map	7
2.4.1 Components of the Geographic Map	7
2.4.2 Installing the License File on the NMS Server	8
2.4.3 Installing the Client Software and Map Data on Your PC	8
2.5 Launching iMonitor	9
<i>Logging On To Additional Servers</i>	10
<i>Multiple Users or PCs Accessing the NMS</i>	10

<i>Accepting Changes</i>	10
2.6 Overview of iMonitor Usage and Displays	11
2.6.1 iMonitor Time Frames in Requests	11
2.6.2 Saving Historical Time Ranges across Multiple Displays	11
2.6.3 Historical “Save to File” Capability	12
2.6.4 Types of iMonitor Displays	12
2.6.5 Multicolumn Details Displays	12
2.6.6 Multiple vs. Grouped Display Results	13
2.7 Using iMonitor’s Interface	14
2.7.1 Clicking on Elements: What Happens?	14
<i>Right-Clicking</i>	14
<i>Single-Clicking vs. Double-Clicking</i>	14
2.7.2 Globe Functions	15
<i>Using the Docking Feature</i>	15
<i>Hiding Elements</i>	15
<i>Expanding Tree</i>	15
<i>Collapsing Tree</i>	16
<i>Sorting Columns</i>	16
<i>Sorting the Tree</i>	17
2.7.3 Network Tree	19
2.7.4 Using the Interface Toolbars and Menu Options	19
<i>Title Bar</i>	19
<i>Menu Bar</i>	20
<i>Toolbar</i>	20
<i>Audio Notification</i>	20
<i>Acknowledging Conditions</i>	22
<i>View Menu</i>	22
<i>Find Toolbar</i>	23
<i>Workspace Toolbar</i>	25
<i>Saving and Reloading Workspaces</i>	25
<i>Operational Toolbar</i>	26
<i>Status Bar</i>	27
<i>Connection Details on Status Bar Icon</i>	27
<i>Conditions Pane</i>	27
<i>Legend Pane</i>	28
<i>Configuration Changes Pane</i>	29
<i>Viewing Real-Time Status</i>	29
2.7.5 Selecting Columns for Viewing	30
2.7.6 Monitoring iSCPC Links	31

3	Monitoring Conditions and Events	33
3.1	Conditions	33
3.1.1	Representing State of Element via Icons	33
3.1.2	Conditions Pane	34
3.1.3	Elements with Multiple Conditions	35
3.1.4	Offline State	36
3.1.5	Alarms and Warnings on Elements	36
3.2	Putting an Element under Observation for Conditions	39
3.2.1	Viewing Conditions or Events	42
	<i>Viewing Conditions</i>	42
	<i>Viewing Events</i>	42
3.2.2	Interpreting Conditions Results	48
3.3	Interpreting System Events	50
3.4	Snapshots	50
3.4.1	Network Condition Snapshot	50
	<i>Multiple Selection Options in Condition Snapshot View</i>	54
3.4.2	Network Data Snapshot	56
4	Obtaining Performance and Status Information	59
4.1	Monitoring Blades in iMonitor	59
4.2	Using the Remote Probe	61
	<i>Modifying the Timeout Duration for a CW or PN Carrier</i>	65
4.3	CPU Usage (Blades Only)	66
4.4	Timeplan	68
	<i>Pausing the Timeplan Graph and Highlighting Individual Entries</i>	71
4.5	Inroute Distribution	71
	<i>Networks</i>	72
	<i>Inroute Groups</i>	73
	<i>Performing ACQ Bounce</i>	73
4.6	Latency	74
4.7	Retrieving Information on Remotes using Probe Mesh	77
4.8	Satellite Link Information	79
4.8.1	Line Card Statistics	79
	<i>Identifying Remotes Causing Rx CRC Errors on iNFINITI Line Cards</i>	82
4.8.2	SATCOM Graph	82
	<i>Remote Status and UCP Info</i>	82
	<i>Display</i>	83
	<i>Procedure for Viewing SATCOM Graph, Remote Status and UCP Info</i>	83
	<i>Mesh UCP Tab</i>	86
	<i>Selecting Parameters in the Mesh UCP Tab</i>	87
	<i>Mesh UCP Parameter Definitions</i>	88

<i>Remote Status and UCP Info Tabs</i>	88
4.8.3 Group QoS Statistics	90
<i>Viewing QoS Statistics</i>	90
<i>Saving QoS Statistics to an Excel Spreadsheet or to a CSV Formatted File</i>	95
4.8.4 Control Panel	96
4.9 Connecting to Network Elements	98
<i>Examining IP Routing and HDLC Information on Remotes</i>	98
4.10 Monitoring Your Bandwidth with SkyMonitor	100
4.10.1 Viewing the Spectrum with SkyMonitor	100
4.10.2 Changing the SkyMonitor Settings	103
4.10.3 Capturing and Recalling SkyMonitor Data	104
<i>Saving SkyMonitor Data</i>	104
<i>Recalling and Viewing SkyMonitor Data</i>	105
<i>Capturing an Image of the SkyMonitor Display</i>	107
5 IP, SAT and Mesh Traffic Graphs	109
5.1 IP Statistics	109
5.2 SAT Statistics	109
5.3 IP Statistics vs. SAT Statistics	109
5.4 SAT Traffic Graph	111
5.5 IP Traffic Graph	114
5.6 Viewing Options	117
5.7 Bandwidth Usage	118
5.8 Mesh Statistics	120
5.8.1 Mesh Traffic Graph	121
6 Reporting on Networks	127
6.1 Reports	127
6.1.1 Long-Term Bandwidth Usage Report	127
6.1.2 IP, SAT and Mesh Long Term Bandwidth Usage Reports	127
<i>Results</i>	130
<i>Totals Tab</i>	130
<i>Averages Tab</i>	130
6.1.2.1 Interpreting the Report	132
<i>Percentage of Channel Capacity</i>	132
6.2 Remote and Line Card Availability Reports	133
7 Monitoring Remotes Using the Geographic Map	135
7.1 Launching the Geographic Map	135
7.2 The Map Toolbar	137
7.3 Tracking and Locating Mobile Remotes	140
<i>Enabling Remote Tracking and Clearing Remote Tracks</i>	141

<i>Determining a Remote's Current Location and State</i>	141
<i>Determining a Remote's Past Locations at Specific Times</i>	141
7.4 Using the Map to Select from the Network Tree Menu	142
<i>Selecting from the Remote Submenu for a Single Remote</i>	142
<i>Selecting from the Remote Submenu for Multiple Remotes</i>	143
7.5 Geographic Map Filtering Based on Remote Status	144
<i>Applying Filters Using the Geographic Map Toolbar</i>	145
<i>Applying Filters Using the Filter Menu</i>	145
Appendix A Accessing the NMS Statistics Archive	147
A.1 Optimization of the Statistics Archive	147
A.1.1 Optimized NMS Statistics Archive Storage	147
A.1.2 Optimized NMS Statistics Archive Lookup	147
A.1.3 Archive Consolidation	148
A.2 NMS Database Overview	148
<i>Connecting to the NMS Archive Database with ODBC</i>	148
<i>Obtaining the ODBC Connection Library</i>	148
<i>Setting up a Simple ODBC Access Account</i>	148
A.3 Basic Archive Database Information	149
<i>Types of NMS Databases and Supported Access</i>	149
<i>Structure Changes between Releases</i>	149
<i>Accessing Remote and Network Names from Configuration Database</i>	150
<i>Timestamps</i>	150
<i>Overview of the Archive Database Tables</i>	150
A.4 Database Table Details	151
A.4.1 IP Stats Tables	152
<i>Consolidated IP Stats Tables</i>	153
<i>Statistics Consolidation Process</i>	154
A.4.2 Latency Measurements	154
A.4.3 Hub Line Card Statistics	155
A.4.4 Remote Status	156
A.4.5 Uplink Control Adjustments	157
A.4.6 Event Messages	158
A.4.7 Hub and Remote State Changes	159
A.4.8 Protocol Processor State Changes	161
A.4.9 Hub Chassis State Changes	162
A.4.10 Over-the-Air Statistics Tables	163
<i>Consolidated Over-the-Air Statistics Tables</i>	164
A.4.11 Over-the-Air Multicast Statistics Tables	165
<i>Consolidated Over-the-Air Statistics Tables</i>	165

A.4.12 Mesh Stats Tables	166
<i>Consolidated Mesh Tables</i>	166
A.5 NMS Statistics Archive Database Restructuring	167
A.5.1 Background	167
A.5.2 The New Archive Database Structure	168
A.5.3 The New Archive Process	169
A.5.4 Table Division Rules	170
A.5.5 Table Selection Process	171
A.5.6 Converting Data between Table Formats	172
<i>After the Upgrade to Release 6.1</i>	172
<i>Changing the 6.1 Table Structure</i>	173
A.5.7 Optimizing Archive Database Performance	174
<i>Copying the Archive Database Partitioning Calculator to Your PC</i>	174
<i>Using the Archive Database Partitioning Calculator</i>	175
A.5.8 Selecting from the Restructured Database	180
<i>Identifying the Location of the Result Set</i>	180
<i>Ignoring the Location of the Result Set Part One:</i>	181
<i>Ignoring the Location of the Result Set Part Two:</i>	182
 Appendix B Alarms and Warnings	 185
B.1 Alarms	185
B.2 Warnings	186
B.3 Acronyms	189
B.4 Default Warning Limit Thresholds	189
 Appendix C SNMP Proxy Agent	 191
C.1 How the Proxy Agent Works	191
C.2 The iDirect Management Information Base (MIB)	192
C.2.1 Resetting Statistical Data	195
C.2.2 iDirect MIB SNMP Traps	197
C.2.3 Setting up SNMP Traps	198
C.3 Working with HP OpenView	200
C.3.1 Linux SNMP Tools	200
 Appendix D Rx CRC Error Correlation	 203
 Index	 207

Figures

Figure 2-1: Desktop Shortcuts for NMS GUI Clients	6
Figure 2-2: Windows Start Menu Entries for NMS GUI Clients	7
Figure 2-3: iMonitor Main Window	14
Figure 2-4: Expand Tree Selection	16
Figure 2-5: Expanded Tree with Child Elements	16
Figure 2-6: Collapse Tree Selection	16
Figure 2-7: Collapsed Tree	16
Figure 2-8: The Workspace Toolbar in Action	25
Figure 3-1: Conditions Time Range	44
Figure 3-2: Events Time Range with Text Filter	45
Figure 3-3: Conditions Results in Multicolumn Format	46
Figure 3-4: Conditions Time Line Results in Graphical Format	46
Figure 3-5: Event Results	48
Figure 3-6: List and Details View of Network Condition Snapshot	51
Figure 3-7: Remote Submenu in Condition Snapshot	52
Figure 4-1: Mesh UCP Graph	86
Figure 4-2: Remote Status Raw Data	89
Figure 4-3: UCP Info Raw Data	89
Figure 4-4: SkyMonitor Initial View	101
Figure 4-5: Monitoring a Carrier with SkyMonitor	102
Figure 4-6: SkyMonitor Function Buttons	103
Figure 5-1: Collection Points for IP Usage Statistics	110
Figure 5-2: Real-Time Bandwidth Usage Display	119
Figure 5-3: Collection Points for Mesh, SAT, and IP Statistics	121
Figure 6-1: SAT Long Term Bandwidth Usage Report	131
Figure 6-2: IP Long Term Bandwidth Usage Report	132
Figure A-1: Default Table Set	168
Figure A-2: Release 6.0 and Earlier Stats Archiving Process	169
Figure A-3: Release 6.1 Stats Archiving Process	169
Figure A-4: Archive Database after Conversion to 6.1	172
Figure A-5: Retrieving the Database Partitioning Calculator Using Cygwin	175
Figure A-6: Archive Database Partitioning Calculator	177
Figure A-7: Segmented nms_remote_status archive tables	179
Figure C-1: SNMP Proxy Architecture	191

Tables

Table 2-1: Toolbar Icons and Functions	20
Table 2-2: Operational Toolbar Icons and Functions	26
Table 2-3: Star Network vs. iSCPC Link Monitoring	31
Table 3-1: Elements and Types of Information Provided	33
Table 3-2: Real-Time States and Icons	33
Table 3-3: Explanation of Alarms by Element	36
Table 3-4: Explanation of Warnings by Element	37
Table 7-1: Geographic Map Toolbar Icons and Functions	138
Table A-1: Archive Database Tables	151
Table A-2: IP Stats Record Format	152
Table A-3: Additional Consolidated IP Stats Table Fields	153
Table A-4: lat_stats Record Format	154
Table A-5: nms_hub_stats Table Format	155
Table A-6: nms_remote_status Record Format	156
Table A-7: nms_ucp_info Record Format	157
Table A-8: event_msg Record Format	158
Table A-9: state_change_log Record Format	159
Table A-10: pp_state_change_log Record Format	162
Table A-11: chassis_state_change_log Record Format	163
Table A-12: OTA Stats Record Format	163
Table A-13: Additional Consolidated OTA Stats Table Fields	164
Table A-14: OTACAST Stats Record Format	165
Table A-15: Additional Consolidated OTACAST Stats Table Fields	165
Table A-16: Mesh Stats Record Format	166
Table A-17: Additional Consolidated Mesh Stats Table Fields	167
Table A-18: Default Data Striping	168
Table A-19: TABLE_INFO Format and Default Contents	170
Table B-1: Alarms	185
Table B-2: Warnings	187
Table B-3: Warning Limit Thresholds	189
Table C-1: iDirect MIB Contents	192
Table C-2: iDirect MIB Statistical Information	193
Table C-3: iDIRECT MIB Traps	197
Table C-4: SNMP Command Line Utilities	200

The iVantage Network Management System

iMonitor is a component of the iDirect iVantage Network Management System (NMS). The iVantage NMS is a complete suite of tools for configuring, monitoring, and controlling your iDirect satellite network.

The iVantage NMS consists of the following components:

- **iBuilder** enables rapid, intuitive configuration of any iDirect network. It allows you to easily add components to your network, change your current configuration, and download configuration and software to network elements. The iBuilder Revision Server provides automated management of software and firmware upgrades for your remote modems. The iBuilder Group QoS (GQoS) user interface allows advanced network operators a high degree of flexibility in creating subnetworks and groups of remotes with various levels of service tailored to their network requirements. The *iBuilder User Guide* provides detailed instructions for using iBuilder to configure and manage your network.
- **iMonitor** provides network operators with detailed information on real-time and historical performance of the network. Among its many capabilities, iMonitor allows you to analyze bandwidth usage; view remote status; view network statistics; monitor performance of networks, sub-networks and individual network elements; and manage alarms, warnings and network events. Alarms, warnings and statistics can be forwarded as SNMP traps. All events and performance statistics are automatically archived. Data displayed on the iMonitor GUI can be exported directly into Excel for further analysis. A Network Probe allows detailed investigation of network issues. The *iMonitor User Guide* provides instructions for using iMonitor.
- **iSite** allows you to monitor and configure iDirect devices in the field. It includes several features that aid in the remote commissioning process, including assistance for antenna pointing, antenna look angle calculation, and cross polarization. You can also use iSite to configure and manage point-to-point SCPC connections between dedicated remotes. An iSite API is available for custom development. For further information on these topics, see the *Installation and Commissioning Guide* for iNFINITI remotes and the *iSCPC User Guide*.
- The **Geographic Map** is an optional iMonitor feature that displays in real time the exact geographic location of all remotes within a given network on a world map. Functions include mobile remote tracking; the ability to zoom, pan in or out, and add or remove map features from the display; and filtering of remotes filter remotes by active state. The Geographic Map is described in detail in the *iMonitor User Guide*.
- **SkyMonitor** allows you to integrate one or more multi-port spectrum analyzers into your hub installation and then use iMonitor to view your iDirect carriers or other areas of the spectrum. SkyMonitor can be an invaluable tool for diagnosing performance issues from RF interference or other carrier-related anomalies. Network Operators can view, analyze, store and recall the spectral displays of any carrier from anywhere an iMonitor connection is supported. Configuration of SkyMonitor is described in the *iBuilder User Guide*. The use of SkyMonitor for spectrum analysis is described in the *iMonitor User Guide*.

- The **Web Services Tool Kit** (WST) provides a software interface along with engineering services that support iVantage integration with external systems. For example, you can integrate iVantage with external web applications or OSS/BSS systems such as billing, provisioning, reporting or customer access systems. Integrating the power of iVantage with other business tools allows Network Operators to generate revenue through new service offerings such as usage-based billing. WST also enables Network Operators to integrate iVantage with their service ordering and provisioning systems, greatly simplifying the process of adding new customers and sites. The use of the toolkit is described in the *Web Services Toolkit User's Guide*.
- A **Virtual Network Operator** (VNO) license enables network operators to view and manage only their own networks and remotes, independent of other operators delivering services out of the same hub. The VNO package makes it possible to scale investments to actual business growth, significantly reducing initial capital equipment expenses. Configuring VNOs is described in the *iBuilder User Guide*.
- A **Customer Network Observer** (CNO) license grants filtered read-only iMonitor access, allowing customers real-time and historical views into their own network performance while maintaining overall network privacy. Configuring CNOs is described in the *iBuilder User Guide*.

1 Using this Guide

This section discusses the purpose of this manual, its intended audience, and the document conventions used.

1.1 Intended Audience

This user guide is intended for all network operators using the iDirect iDS system, as well as network architects and any other personnel who may operate or monitor the networks from time to time. It is not intended for end users or field installers.

Some basic knowledge of TCP/IP concepts, satellite communications, and Windows operating systems is expected. Prior experience operating an iDS network, although desirable, is not a requirement.

1.2 Document Conventions

This section illustrates and describes the conventions used throughout the manual. Take a look now, before you begin using this manual, so that you'll know how to interpret the information presented.

1.2.1 Typographical and Navigational Conventions

- Information you type directly into data fields or at command prompts is in **courier font**.
- Windows menu selections are represented as **Menu → Command**, or in the case of cascading menus, **Menu → SubMenu → Command**.
- Menu selections made from items in the Tree View are represented as **<level in tree> → Command**. For example, the Tree menu item to modify a line card is shown as **Line Card → Modify**.
- Names of commands, menus, folders, tabs, dialog boxes, list boxes, and options are in **bold font**.
- Procedures begin with a feature description, followed by step-by-step, numbered instructions.

1.2.2 Informational Conventions



NOTE

When you see the **NOTE** symbol, the corresponding text contains helpful suggestions or references to material not contained in this manual.



WARNING

When you see this alert symbol with a **WARNING** or **CAUTION** heading, strictly follow the warning instructions to avoid personal injury, equipment damage or loss of data.

2 Overview of the NMS for iMonitor

iDirect's Network Management System (the iVantage NMS) is a powerful suite of applications and servers that provide complete control and visibility to all components of your iDirect networks. The NMS client/server system architecture consists of three series of components:

- Three NMS applications with Graphical User Interfaces (GUIs) that allow you to configure and monitor your network
- A database that stores the data entered by and displayed to users
- A middleware tier that manages access to the database on behalf of user operations

For a description of all iVantage NMS components see the [“The iVantage Network Management System” on page xi](#).

2.1 Introduction

This chapter provides some of the most important information you will need to understand how iMonitor works and how to use it as effectively as possible. This chapter discusses how to prepare for installation, what you will see when you first launch iMonitor, how to use the many powerful tools available in iMonitor, how to create, customize, and print reports, and how to determine the configuration status of network elements.

iMonitor provides complete visibility to real-time status and operational characteristics of network elements.

- **Status** refers to the real-time state of network elements (such as OK, Warning, Alarm). iMonitor notifies you asynchronously of warnings and alarms for all network elements, which are collectively called *conditions*.
- **Operational characteristics** are captured in a variety of network statistical data, such as IP traffic statistics, satellite link quality, and hardware component operating values.

You can also obtain and view data stored in the historical archive, which allows you to analyze anomaly conditions and perform trend analysis.

2.2 Components of the Network Management System

The NMS consists of several client/server components that work together to provide the functions and views necessary to control your network. These components are briefly discussed below.

2.2.1 NMS Applications

The iDirect NMS provides three GUI clients, each of which performs specific functions for networks operators, field installers, and end users.

iBuilder

The iBuilder application provides all configuration and control functions to network operators. **Configuration** options consist of creating network elements (e.g. networks, line cards, remotes)

and specifying their operational parameters, such as QoS profiles or IP addresses. **Control** options consist of applying the specified configurations to the actual network elements, retrieving active configurations, resetting elements, and upgrading element software and firmware. Refer to *Network Management System iBuilder User Guide* for more information.

iMonitor

The iMonitor application provides complete visibility to the real-time status and operational data of network elements. “Status” refers to the real-time state of network elements, such as OK, warning, or alarm. Operational data are captured in a variety of network statistical data tables and displays, revealing, for example, IP traffic statistics, satellite link quality, and hardware component operating values.

In addition to real-time visibility, iMonitor allows you to access state and statistics from the historical archive in order to analyze anomaly conditions and perform trend analyses. This guide has a complete list of real-time and historical data available through iMonitor.

iSite

The iSite application is used primarily for commissioning new sites and monitoring TDMA remotes from the local LAN side. It contains functions to help installers calculate antenna azimuth/elevation, perform antenna pointing, and put up a continuous wave (CW) carrier for antenna peaking, cross-polarization and 1 db compression tests. It also provides configuration and real-time state/statistical information for one or more remote units. Instead of interacting with the NMS middleware, it connects directly to each remote to perform all of its operations. iSite does not provide access to historical information. See the *Remote Installation and Commissioning Guide* for more on commissioning iNFINITI remotes using iSite.

In addition to its commissioning functions, iSite can be used to configure and monitor remote-to-remote SCPC connections. It also allows monitor-only capability to end-users, should you decide to provide it to them.



NOTE

End-users do not need iSite in order to receive or transmit IP data over the iDS system.



NOTE

Beginning with release 5.0.0, iSite replaces NetManager.

For more information about NMS applications, see [“The iVantage Network Management System” on page xi](#).

2.2.2 Server Components

The NMS server processes run on your NMS Linux Server machines. There are a number of NMS servers processes, each of which performs a specific set of back-end functions.

Configuration Server

The configuration server is the core component of the NMS server family. It manages access to the configuration database, which contains all the element definitions for your networks and their operational parameters. Additionally, the configuration server provides most network control functions (configuration apply, firmware download, resetting, etc.). The other servers also use this server to determine what the network components are.

Real-time Data Server

The real-time data server collects most of the network statistics produced by your network elements. These statistics include IP stats for each remote, remote status messages, timeplan slot assignments, line card statistics, etc. Additionally, the real-time data server provides these statistics to the GUI clients for real-time and historical display.

Event Server

The event server's primary job is to generate warnings and alarms and send them to iMonitor for display. Warnings and alarms are collectively known as "conditions". The event server also collects and archives all system events and provides them to iMonitor for display.

Latency Server

The latency server measures round-trip time, or latency, for every active remote in your networks. These measurements are stored in the archive and provided to iMonitor for display.

NMS Controller Server

The control server manages the PP Controller Server processes running on the NMS server.

PP Controller Servers

The PP Controller processes control the samnc process on each PP blade.

NMS Monitor Script

This simple script monitors all other servers and restarts them automatically if they terminate abnormally. It records a log file of its activities and can be configured to send e-mail to designated recipients when it restarts any of the other servers.

Consolidation Script

The consolidation process periodically consolidates records in the statistics archive to preserve disk space on the server machine. Default consolidation parameters are already entered into your configuration database; they can be tuned to your particular storage requirements if necessary.

Database Backup Script

This script runs nightly to back up the data in your primary databases and copy it to your backup NMS server. The database backup script must be custom-configured for each customer site.

Database Restore Script

This script runs nightly on your backup NMS server. It restores your primary NMS database into the backup database for NMS failover purposes.

2.3 Installing iBuilder, iMonitor, and iSite

This section provides the system requirements and procedures for installing your Network Management System components.

2.3.1 System Requirements

The NMS GUI clients are Windows PC-based applications that run under the following versions of Windows:

- Windows 2000 Service Pack 3 or later
- Windows XP

Windows NT, Windows 98 and Windows 95 are **NOT** supported. We do **NOT** support server-based versions of Windows.

2.3.2 Installation Procedure

A single client installer .exe file, *nms_clients_setup.exe*, installs all three GUI clients and associated library files for you.

To install, copy the .exe file to the target PC, double-click it, and follow the prompts.

By default, the clients are installed in the directory C:\Program Files\iDIRECT. The installer automatically places a shortcut to each GUI application on your desktop and adds the appropriate entries in the Windows **Start** menu. Click **Start** → **All Programs** → **iDirect** → **NMS Clients 7.1**. The iBuilder, iMonitor, and iSite clients are displayed, along with an **Uninstall** selection.

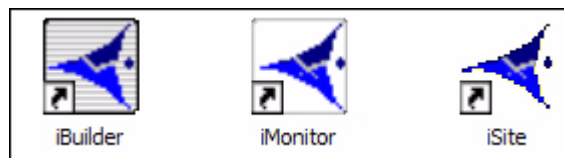


Figure 2-1: Desktop Shortcuts for NMS GUI Clients



Figure 2-2: Windows Start Menu Entries for NMS GUI Clients

2.4 Installing the Geographic Map

iMonitor's Geographic Map feature allows you to monitor the locations and status of your remotes in real time. Before you can use this feature, you must install your Geographic Map license on the NMS server and the map data on your client PCs.



NOTE

The Geographic Map is a licensed feature. Please contact your iDirect sales representative for pricing and ordering information.

To support this feature, your client PC or laptop should meet the following requirements:

- 1.6 gigahertz (GHz) Pentium processor or higher
- Microsoft Windows XP, Service Pack 2
- 512 megabytes (MB) of RAM or more
- At least 1 gigabyte (GB) of free disk space

2.4.1 Components of the Geographic Map

The Geographic Map feature has the following primary components:

- The *map license file* resides on the NMS server and allows or denies access to the map. When you purchase the Geographic Map feature, you will receive your license file from the iDirect Technical Assistance Center (TAC).
- The *mapx_setup.exe file* is the executable file that installs the MapX client software on your PC. It is a simple and quick InstallShield application that prepares your PC to run the Geographic Map software.
- The *map data files*, which are installed on your PC, supply the actual data for the map: names, roads, bodies of water, cities, and other map features. The map data is shipped to you on a read-only CD, and is quite large (approximately 1.13 GB uncompressed, 540 MB compressed).
- The *README file* contains instructions for installing the map software on your PC.

2.4.2 Installing the License File on the NMS Server

Once you have received your map license file from the iDirect TAC, you must copy it to the following location on both your primary and backup NMS servers:

`/home/nms/cfg/nmssvr_e.lic`



NOTE

Do not change the name of the map license file. The license file name must be **nmssvr_e.lic** for the Geographic Map software to operate.

It is not necessary to restart any of the NMS servers; the new license will be enabled immediately.

2.4.3 Installing the Client Software and Map Data on Your PC

Once you have purchased the Geographic Mapping license, you must install the client software and the map data on each PC that will use the map. There is no limit to the number of PCs that can run the map client software when connected to an NMS server with a valid license.

To install the client software and map data on your PC:

- Step 1 Close any programs currently running on your PC.
- Step 2 Insert the distribution CD into the CD-ROM drive on your PC. The CD contains the following files:
 - **README.txt**
 - **mapx_setup.exe**
 - **WorldPlaces.zip**
- Step 3 Copy the above files to your PC and perform the remaining steps from your PC.
- Step 4 Double-click the **mapx_setup.exe** command and follow the instructions to install the software on your PC.
- Step 5 Verify that the folder **C:\Program Files\MapInfo\MapX 8.3\Maps** contains only the following two files: **GeoDict.DCT** and **World4NMS.gst**.
- Step 6 From the folder **C:\Program Files\MapInfo\MapX 8.3**, execute the following commands:

RegTypLib.exe mdatasetint.tlb
regsvr32 MAPX50.dll
- Step 7 Using WinZIP or another zip file utility, open the WorldPlaces.zip file and extract its contents to the following folder on your PC:

C:\Program Files\MapInfo\MapX 8.3\Maps

For instructions on using the Geographic Map to monitor your remotes, see [Section 7 “Monitoring Remotes Using the Geographic Map” on page 135](#).

2.5 Launching iMonitor

iMonitor is initially installed with two default accounts: “admin” and “guest”. The admin user has full access privileges to all iMonitor functionality, while the guest account has read-only access. The passwords for these two accounts are identical to their associated user names. For information on setting up user accounts, see the chapter titled [“Creating and Managing User Accounts and User Groups”](#) in *Network Management System iBuilder User Guide*.

iDirect strongly recommends that you modify the **admin** user password as soon as possible after the installation. This is especially important if your NMS Server is accessible via the public Internet.

- Step 1 To launch iMonitor, double-click the desktop shortcut or select it from the Windows **Start** menu.
- Step 2 Enter your user name and password in the **Login Information** dialog box.
- Step 3 Click **Server** and select the IP address or host name of your primary NMS Server machine. The Server box holds up to three IP addresses. If yours does not exist, enter the IP Address in the Server box.
- Step 4 Click **OK** to complete the login process.



NOTE

The NMS server version must match the iMonitor version in order for you to log in. For example, version 6.0.0 of iMonitor may connect only to version 6.0.0 of the NMS servers.

Login Information

Enter a user name and password that is valid for this application.

User name:

Password:

OK Cancel Server <<

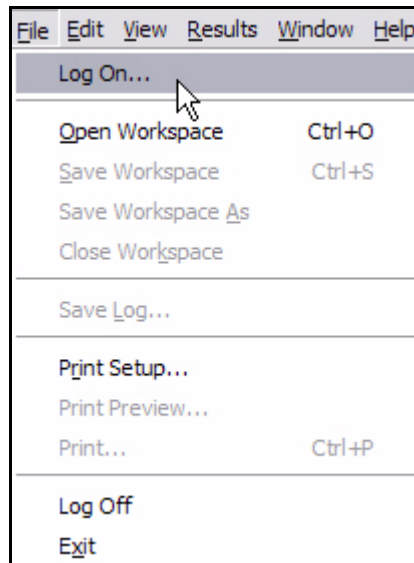
Enter the IP Address or Host Name of the Network Management Server.

Server:

The iMonitor application automatically connects to the NMS server processes that are required to perform the NMS functions. If this connection is lost for any reason, iMonitor automatically reconnects to the servers when they become available.

Logging On To Additional Servers

In the event that there are multiple NMS servers in the same teleport or multiple teleports under the network operator's control, you may need to log out of one NMS server and log in to another one. You can do this without exiting iMonitor. From the Main Menu, select **File → Log Off** to log out of your current session and **File → Log On** to open the **Login Information** dialog box again.



Multiple Users or PCs Accessing the NMS

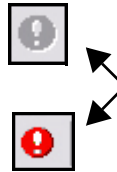
Multiple users or multiple sessions may run simultaneously on the NMS database. For example, the NMS offers the following capabilities:

1. You may run multiple simultaneous sessions of iMonitor on a single PC. These versions may be connected to different servers or the same server.
2. Multiple PCs may run the same session of iMonitor at any given time and connect to the same server at the same time.

Accepting Changes

When two iBuilder users are connected to the same server, and one of them modifies the network configuration, the *other* user cannot modify the configuration suite until he accepts the changes, which will automatically refresh his configuration view to reflect the latest changes.

When another user changes the configuration, or when you make a change that affects other network elements, the **Accept Changes** button on your toolbar changes color from gray to red. (For more information, see [Table 2-1, “Toolbar Icons and Functions,” on page 20.](#))



Before you accept the changes, you may view the other user's changes by selecting **View → Configuration Changes** (see [Section “Configuration Changes Pane” on page 29](#)). To accept the changes and update your view of iMonitor, click **Accept Changes**. Any modifications the other user has made are now displayed in your copy of iMonitor.

2.6 Overview of iMonitor Usage and Displays

2.6.1 iMonitor Time Frames in Requests

iMonitor provides three basic time periods for requesting data: real-time, historical, and Get Past.

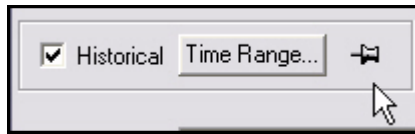
- **Real-time** requests display data as it arrives into the NMS back-end in real-time. These requests have no ending time period—they continue displaying data as long as you keep the display running. Closing either the specific display or the iMonitor application automatically cancels real-time requests.
- **Historical** requests retrieve data purely from the historical archive based on the start and end times you specify. These requests are active in the back-end only until the data is completely delivered to iMonitor.
- **Get Past** requests represent a hybrid of real-time and historical: when you request Get Past data, iMonitor retrieves the most recent data from the archive, and then continues to give you real-time data until you cancel the request.

2.6.2 Saving Historical Time Ranges across Multiple Displays

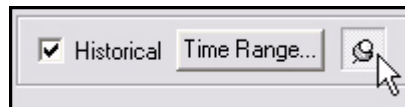
Occasionally you are faced with a situation that requires you to launch multiple different displays for the same time range. iMonitor makes this task much simpler by allowing you to save a specified time range and re-use it in as many displays as necessary. You may save purely historical time ranges and Get Past ranges independently.

To save a specified time range, use the following procedure:

1. Launch the first display and specify the time range for the time period you are investigating. Notice the pushpin located next to the **Time Range** button (or the **Get Past** drop-down list for **Get Past** requests).



2. Next, press the pushpin located next to the **Time Range** button (or the **Get Past** drop-down list for **Get Past** requests). The pushpin will change to appear undepressed.



3. All future requests will automatically use the time range you just saved, until you “take down” the time range by clicking on the pushpin again.

2.6.3 Historical “Save to File” Capability

You may specify a disk file name for iMonitor to save historical or real-time results into. This feature is useful if you have requested a large amount of data for a large number of remotes. You may specify a file name in the following parameters dialogs:

- Latency
- Line card statistics
- Events
- Conditions
- Remote Status/UCP

2.6.4 Types of iMonitor Displays

The two data display types used in iMonitor are graphical displays and multicolumn lists. Events are shown only in multicolumn lists. Network statistical data and conditions may be displayed in both graphical format and/or multicolumn lists, depending on the type of data you are viewing.

- **Graphical displays** represent data in graphical charts.
- **Multicolumn lists** represent data arranged in tabular format with rows and columns.

2.6.5 Multicolumn Details Displays

All of iMonitor’s multicolumn lists share certain characteristics in common. Among them are:

- Data in multicolumn lists can be sorted in ascending or descending order by clicking on the column heading containing the data you want to sort by.
- The default sort order is normally “ascending by time stamp.”
- All scrollbars function identically:

- If the slider is at the bottom of the pane, the pane scrolls to continually show you new data as it's added to the display.
- If the slider is positioned somewhere other than the bottom of the display, data continues to be added at the bottom, but the display position remains constant at the current point. This is based on the assumption that you're viewing data in the middle of the display and you don't want the pane scrolling away from that data.
- Multiple rows of data may be selected and copied/pasted into another application such as Excel for offline viewing and analysis.
- Multicolumn lists may be printed to any printer you have configured on your PC. Select **File→Print** to print the contents of a list.
- By using your mouse button inside the multicolumn list, you may select either the **Expand All** or **Fit to Window** options. These options work as follows:
 - Expand All resizes each column to be the width of either the widest data in that column, or the width of the column heading, whichever is wider.
 - Fit to Pane resizes all columns to fit inside the current width of the pane (so that no scroll bar is required).
 - copy this data to a file
 - copy it without the headers to a file

2.6.6 Multiple vs. Grouped Display Results

When you request element data from a higher node level, iMonitor provides you with an interim dialog where you can select which remotes for which to request data. How the data is displayed depends on the type of data you are requesting. Two different behaviors are possible:

- When the data makes sense only for a single network element, iMonitor launches multiple displays, one for each element.
- When the data from multiple elements can be shown together, iMonitor launches a single pane and displays all data in that pane.

2.7 Using iMonitor's Interface

iMonitor's main window is comprised of several toolbars and panes which are described below.

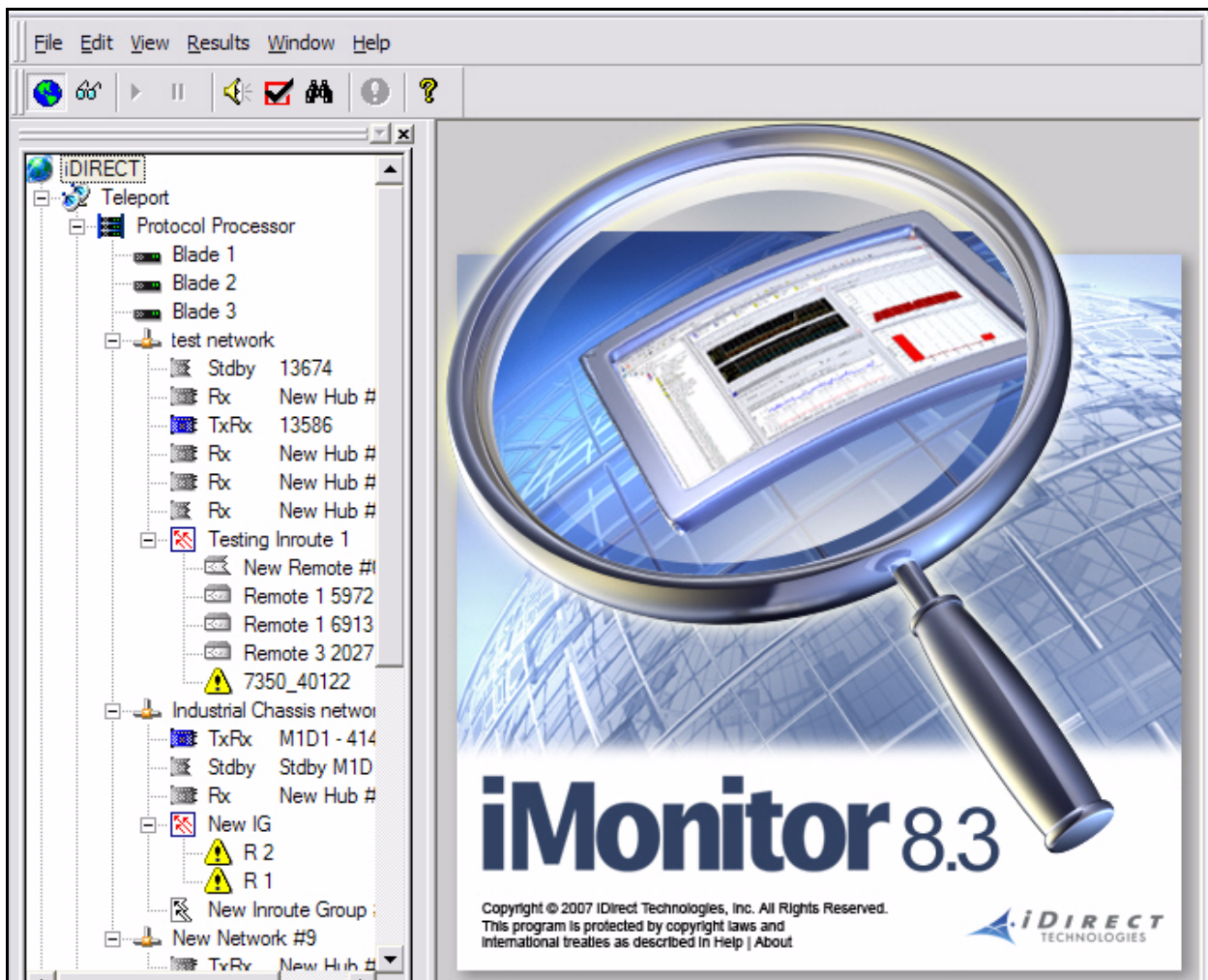


Figure 2-3: iMonitor Main Window

2.7.1 Clicking on Elements: What Happens?

Right-Clicking

In general, you must right-click on your mouse or use the task bar to display any list of options in submenus that can be performed on the element you currently have selected.

Single-Clicking vs. Double-Clicking

You can single-click a plus (+) or minus (-) sign next to an element in the Tree to expand or contract the branches to the next level down in the tree for that element. You can double-click a remote or iSCPC line card in the tree to open the Control Panel for that element.

You can double-click any element in the Tree that has been expanded to automatically contract the branches below that node.

2.7.2 Globe Functions

Right-clicking the Globe in the Tree allows you to move dockable panes, sort columns hide elements, expand the Tree and Collapse the Tree.

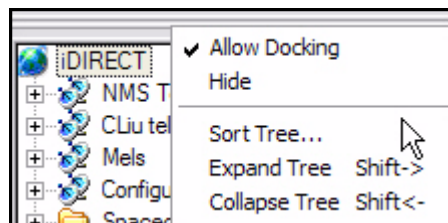
Using the Docking Feature

Docking refer to the ability to move a window pane of the NMS interface to another location on the screen or to detach it from the screen entirely and place it somewhere else on your monitor. In iDirect's NMS, the dockable panes have double-ridge lines at the top of the pane.



To dock a window pane somewhere else on the NMS interface or on your monitor, follow the procedure below:

- Step 1 Point to and right-click the double-ridge lines of the pane you want to move and select **Allow Docking**.



- Step 2 Place the pointer (mouse arrow) on the double-ridge lines and drag the pane wherever you want it. Depending on where you drag it, the pane may change shape (for example, from a vertical display to a horizontal display).
- Step 3 If you want to move the pane back into its original place or to another location, start by grabbing the double-ridge lines with your pointer. Then, you can click the **Name** toolbar at the top of the pane to move it around, and you can place your pointer at the edges of the pane to resize the pane.
- Step 4 To detach the pane completely, double-click the double-ridge lines. The pane becomes separately parented and you may move it independently from the main iMonitor window.

Hiding Elements

You can click **Hide** to remove iMonitor Network Tree from view.

Expanding Tree

To expand the Tree to view all of the children elements, select **Expand Tree**. The Tree will expand to show all of the child elements.

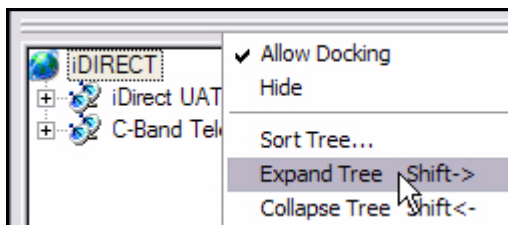


Figure 2-4: Expand Tree Selection

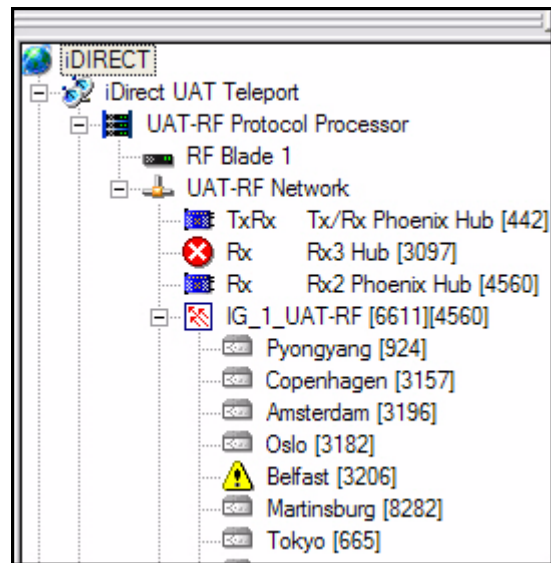


Figure 2-5: Expanded Tree with Child Elements

Collapsing Tree

To collapse the Tree to view only the top level elements, select **Collapse Tree**. The Tree will contract to show only the top level elements.

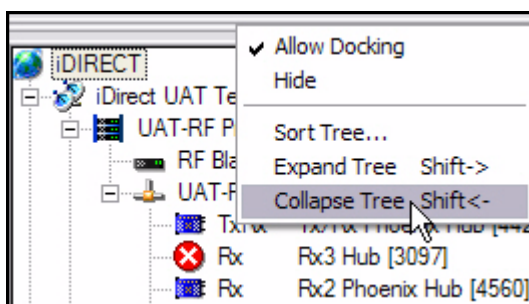


Figure 2-6: Collapse Tree Selection

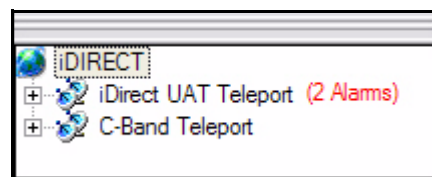


Figure 2-7: Collapsed Tree

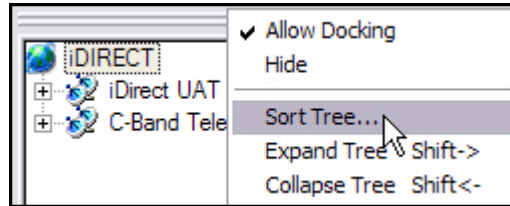
Sorting Columns

In any pane with columns or list controls, you can sort the entries in the pane by clicking on the heading of the given column.

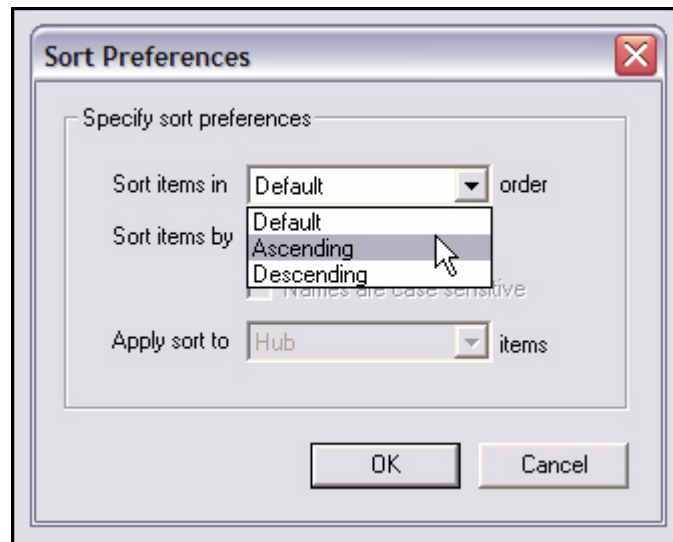
Sorting the Tree

To sort the Tree, follow the steps below:

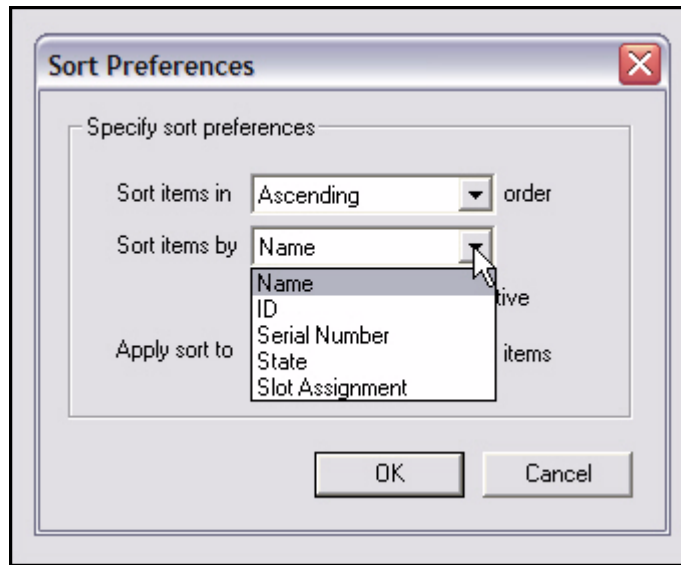
- Step 1 Right-click in the Tree pane (or right-click the double-ridge lines above the Tree pane) and select **Sort Tree**. You can also select **Edit → Sort Tree**.



- Step 2 The **Sort Preferences** dialog box is displayed.
- Step 3 Click the **Sort items** in drop-down list and select either **Ascending** or **Descending**.



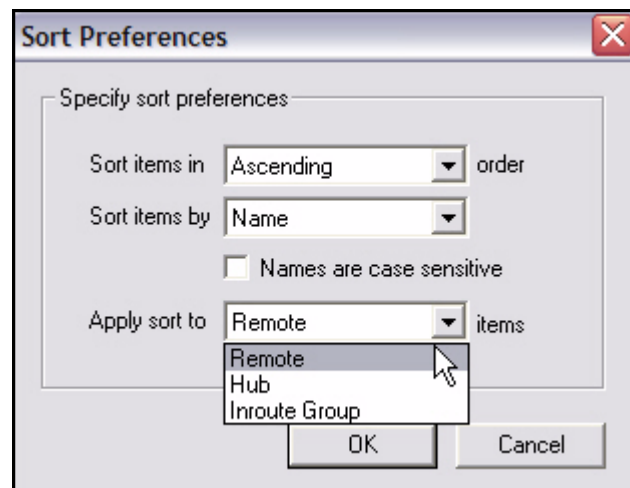
- Step 4 Click the **Sort items by** drop-down list and select one of the options. Depending on what you select in this field, your choices in the **Apply sort to** field will change.



Step 5 If you select **Name**, either click the **Names are case sensitive** check box or clear it.

Step 6 Select the element to which you want to apply the Sort feature. The options are:

- Remote
- Hub
- Inroute Group

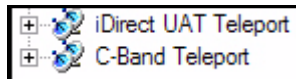


Step 7 Click **OK**. The next time you log in, iMonitor will remember and display the last sort preference you chose.

2.7.3 Network Tree

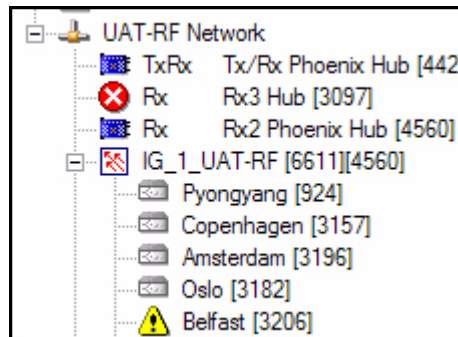
By right-clicking a tree element, a submenu of options appears, which you may click to view various types of data and other information used to monitor and troubleshoot your network. For specific information on how to use and interpret the information you view, see the section on that particular option. Use the **Contents** or **Index** to locate this information if you do not readily see it. Below is a description of the menu options for each element in the tree.

A *plus sign* (+) next to an element in the Tree indicates that additional elements exist at the next level, or branch, of the Tree. Click the *plus sign* (+) to expand the element to view the next level of the Tree.



A *minus sign* (-) next to an element indicates that the element has been expanded and children are visible at the next level, or branch, in the Tree.

In the figure below, the UAT-RF Network has been expanded as far as possible. The UAT-RF Network cannot include children in another network; therefore, its only children are the TxRx and Rx line cards, and the IG_1_UAT-RF Inroute Group. The Inroute Group is a parent element that can be expanded by clicking its *plus sign* (+) to reveal its children elements at the next level of the Tree.



2.7.4 Using the Interface Toolbars and Menu Options

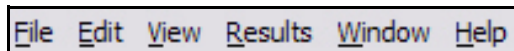
Title Bar

The **Title** bar identifies the name of the application (in this case, iMonitor), the iDS software version, and the IP address of the server to which you are connected.



Menu Bar

The **Menu** bar at the top of the display provides access to log in, log out, quit, and other high-level functions.












Toolbar

The main **Toolbar**, shown below, contains context-sensitive buttons, allowing you to perform a variety of operations on a currently-selected element without using its context menu. Their functions are described in [Table 2-1](#).



Table 2-1: Toolbar Icons and Functions

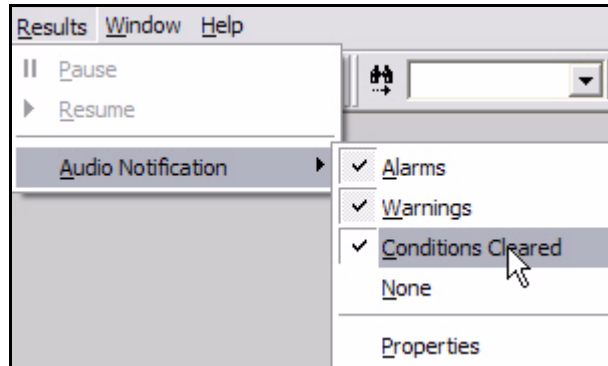
Toolbar Icon	Functionality
	Allows you to view elements in the Tree Menu hierarchy
	Allows you to view Conditions. The Conditions pane has two tabs you can select to view different aspects of the conditions: Conditions Log and Observation View. See Section 3.1.2 “Conditions Pane” on page 34 for more information.
	Allows you to pause the Timeplan Graph.
	Allows you to resume the Timeplan Graph.
	Allows you to turn audio on or off when a new alarm or condition is presented or when a condition is cleared.
	Allows you to acknowledge a condition.
	Opens the Find Toolbar next to the Main Toolbar
	Allows you to accept any changes made to the system by another user. This does not mean that you approve of or agree with the changes; it simply updates your GUI with the latest database information.
	Allows you to view the version number of the NMS and system information.

Audio Notification

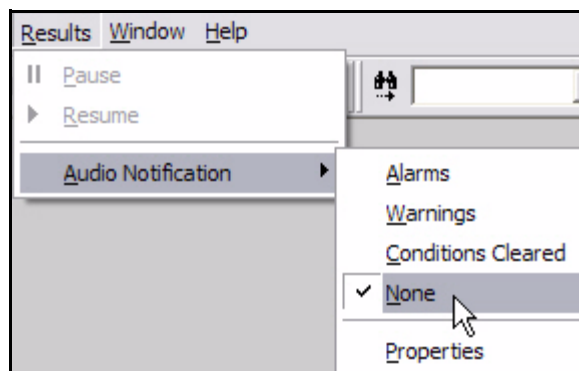
You can choose to turn on audio notification to alert you whenever a new alarm or condition is raised. When you select audio notification, you are only notified of newly-raised conditions by

default. When you acknowledge conditions, the audio notification will stop, even if the alarm has not yet cleared.

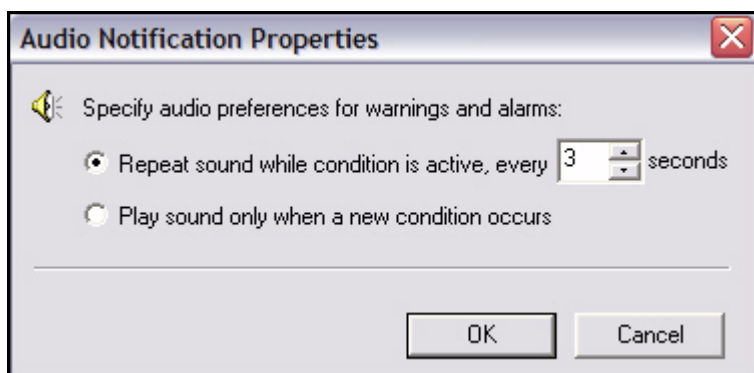
To configure audio notification, select **Results → Audio Notification** from the main menu. You can select any of the three conditions under which you would like to have an audio notification raised.



You may select one, two, or all three. If you wish to have no audio notification, select **None**.



To set up how often you want the audio notification to be repeated, or to specify that the notification should play only when a new condition occurs, select **Results → Audio Notification → Properties** from the main menu. Then configure one of the two choices in the dialog box.

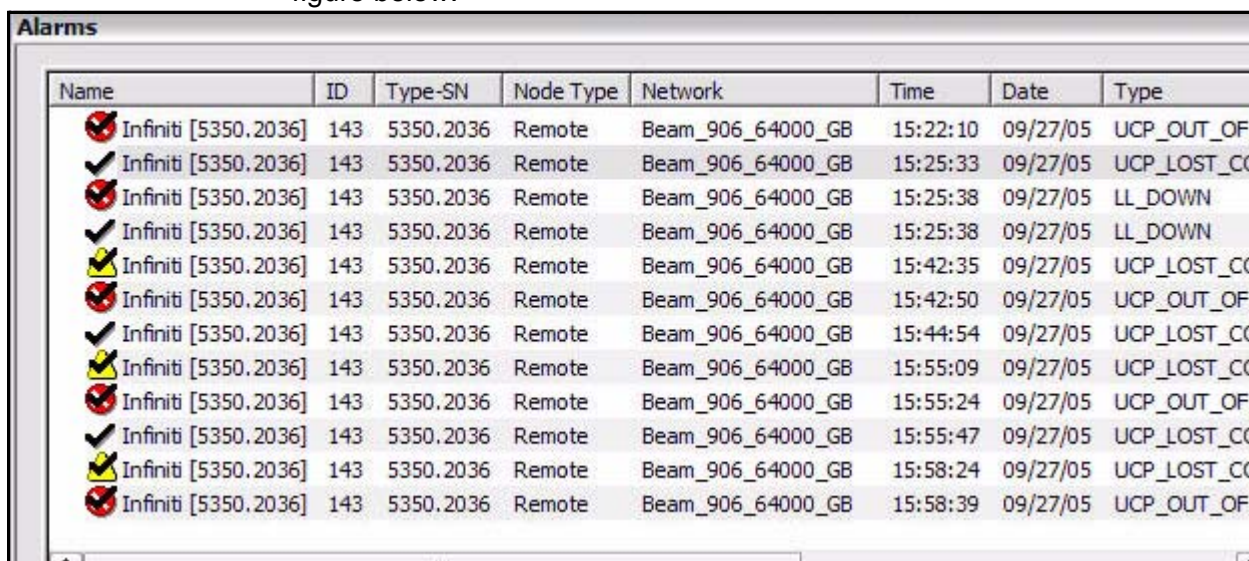


Acknowledging Conditions

You can also use iMonitor to acknowledge all conditions. If audio notification is in effect, acknowledging conditions prevents continuous audio notification, even if the condition that raised the audio notification has not cleared. Once you've acknowledged conditions, audio notification will stop until a new condition is raised. When you acknowledge conditions in iMonitor, *all* outstanding conditions are acknowledged. You cannot acknowledge individual conditions.

To acknowledge conditions:

- Step 1 If not already visible, open the **Conditions** pane by clicking the **Toggle Conditions** icon on the main toolbar.
- Step 2 On the **Conditions** pane, select the **Condition Log** tab.
- Step 3 Click the **Acknowledgement** icon on the main toolbar. On the Condition Log tab, a check is displayed for all acknowledged conditions as shown in the figure below.



The screenshot shows the 'Alarms' window with a table of conditions. Each row represents a condition with columns for Name, ID, Type-SN, Node Type, Network, Time, Date, and Type. A checkmark icon in the first column indicates that the condition has been acknowledged.

Name	ID	Type-SN	Node Type	Network	Time	Date	Type
✓ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:22:10	09/27/05	UCP_OUT_OF
✓ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:25:33	09/27/05	UCP_LOST_CO
✗ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:25:38	09/27/05	LL_DOWN
✓ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:25:38	09/27/05	LL_DOWN
✗ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:42:35	09/27/05	UCP_LOST_CO
✗ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:42:50	09/27/05	UCP_OUT_OF
✓ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:44:54	09/27/05	UCP_LOST_CO
✗ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:55:09	09/27/05	UCP_LOST_CO
✗ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:55:24	09/27/05	UCP_OUT_OF
✓ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:55:47	09/27/05	UCP_LOST_CO
✗ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:58:24	09/27/05	UCP_LOST_CO
✗ Infiniti [5350.2036]	143	5350.2036	Remote	Beam_906_64000_GB	15:58:39	09/27/05	UCP_OUT_OF

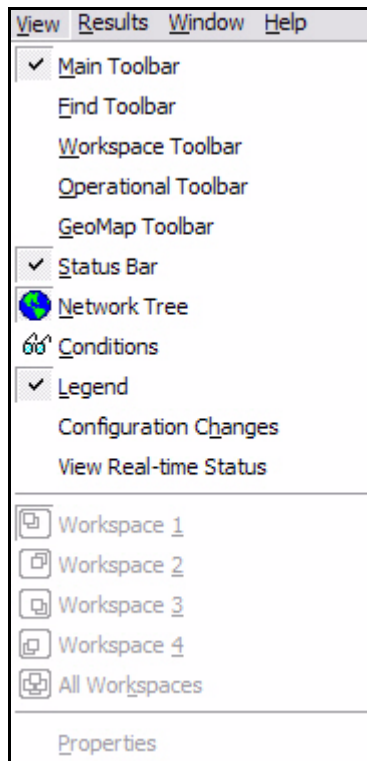


NOTE

When an operator acknowledges a condition, only that operator's view is affected. No changes are made on the NMS server or to other operator accounts.

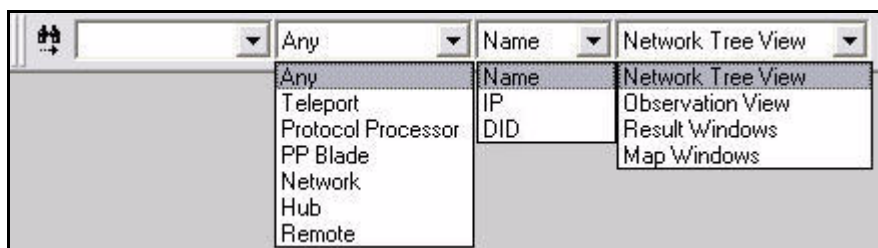
View Menu

The **View** menu on the main menu toolbar allows you to display or hide the following toolbars and panes. You can also right-click your *context menu* button (typically the right mouse button) to see the same options as those in the **View** menu.

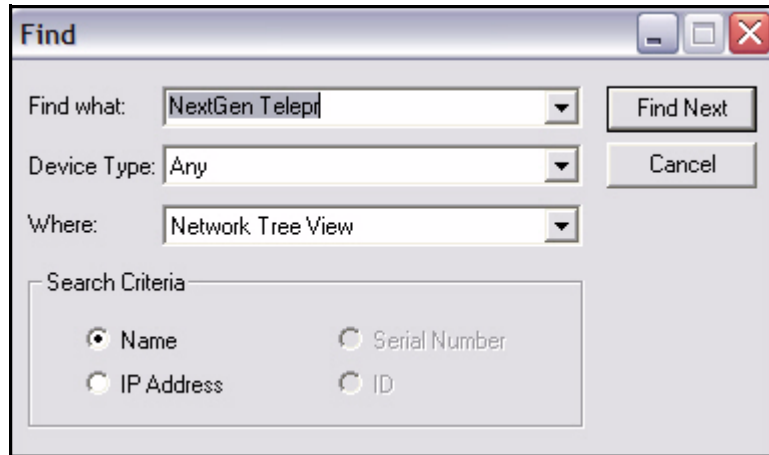


Find Toolbar

The **Find** toolbar provides users the option to search the NMS for a given element and display the results in either the **Network Tree View** or the **Results Window**. This becomes increasingly important as the network grows larger. You can search by selecting a specific element name in the first drop-down list (note that only elements you have created will be in the list); by type of element in the second drop-down list; or by **Name**, **IP address** or **ID number** in the third drop-down list. The figure below shows all of the various options within each category; however, you can actually only click one drop-down list at time. To display the Find toolbar, select **View → Find Toolbar** from the main menu.



You can also click the **Find** button on the toolbar to open a dialog box that gives you the same options.

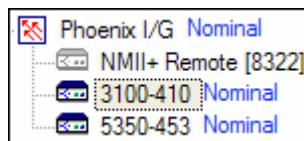


To perform a search, follow the steps below:

- Step 1 Select **View → Find Toolbar**, or click the **Find** button on the toolbar. Either the **Find** toolbar appears to the right of the main toolbar, or the **Find** dialog box appears in the Results pane.
- Step 2 Click the arrow on each drop-down list and click the criteria you want to use in your search.
- Step 3 To execute the search, you can do one of three things:
 - Press **Enter** on the keyboard if you are searching from the **Find** toolbar
 - Click the **Binoculars** icon to the left of the toolbar if you are searching from the **Find** toolbar
 - Click the **Find Next** button if you are searching from the **Find** dialog box
- Step 4 In the example below, the user chose to look for a **Remote** by the **Name** of **3100-410** and display it in the **Network Tree View**.



That remote is highlighted in the Tree when the user clicks on the binoculars icon.



Workspace Toolbar

The Workspace capability solves one of the biggest problems with real-time monitoring systems: window real estate. As you launch more and more displays, you may find that you're quickly running out of space in the results pane and you wish you had a bigger display. The Workspace Toolbar provides a convenient way for you to organize multiple displays into a series of "virtual workspaces". The four workspaces on this toolbar effectively give you four times the window real estate without having to add another display.

To launch the Workspace toolbar, select **View → Workspace** from iMonitor's main menu. You will see four small windows appear on the right-side of iMonitor's main tool bar. Each of these windows represents a virtual workspace where you can launch different displays. When you click one of the workspace windows, displays you launched on another workspace are hidden and a new, blank workspace appears. For convenience, each workspace is highlighted in yellow whenever a display is present on that workspace.

The figure below shows the **Workspace** toolbar in action. In this example, workspace one contains one or more displays and the other workspaces are empty. The fifth workspace pane, when clicked, shows all panes in all workspaces.



Figure 2-8: The Workspace Toolbar in Action

Saving and Reloading Workspaces

In addition to using workspaces in real-time, you may also save the contents of a workspace to be reloaded at a later time. The workspace file stores the following information about displays:

- The window pane size and position within the workspace.
- The request parameters originally specified in the requests.



NOTE

Only real-time and Get Past requests are saved in workspace files.

To save the contents of a workspace, select **File → Save Workspace As** from the main menu. This operation will save all the displays currently active in the workspace. You may also adjust the contents of any workspace and re-save it by selecting **File → Open Workspace** from the main menu.

To reload a previously-saved workspace, select **File → Open Workspace** from the main menu. When you reload a workspace the saved requests will be automatically resubmitted to the appropriate servers.

This feature works best when you have the iMonitor application maximized on your PC screen, but will also function properly if the application is not maximized.

Operational Toolbar




The **Operational Toolbar**, shown below, contains context-sensitive buttons, allowing you to perform a variety of operations on a currently-selected element without using its context menu. Their functions are described in [Table 2-2](#).



Table 2-2: Operational Toolbar Icons and Functions

Toolbar Icon	Functionality
	Request a Network Condition Snapshot.
	Request a Network Data Snapshot.
	Request a SAT Traffic Graph.
	Request an IP Stats Graph.
	Request a Mesh Traffic Graph.
	Request a Timeplan Slot Assignment Graph.
	Request latency results.
	Request a SATCOM Graph.
	Request a Remote Status/UCP report.
	Request modem events.
	Request conditions.
	Request a SAT Long Term Bandwidth Usage report.

Table 2-2: Operational Toolbar Icons and Functions (Continued)

Toolbar Icon	Functionality
	Request a Long Term Bandwidth Usage report.
	Put an element under observation.
	Open a terminal session.

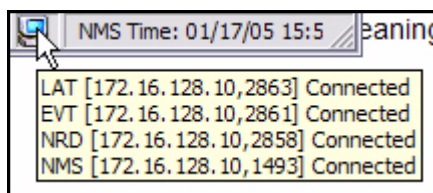
Status Bar

The **Status** bar is located at the bottom of the iMonitor window and displays the user name of the person who is currently logged in and what their server connection status is. On the toolbar shown below, the connection status is “Ready.”
















Connection Details on Status Bar Icon

When your mouse hovers over the **PC** icon next to the user name on the **Status** bar, the IP address of the NMS servers that you are currently connected to is displayed.



Conditions Pane

















The **Conditions** switch on the **View** menu opens the **Conditions** pane. See [Chapter 3, Monitoring Conditions and Events](#) for complete information on the tabs in this pane. Select **View → Conditions** on the main menu to open the pane.

Name	ID	Type	SN	DID	Nod...	Network	Time
 Tim G TxRx card M1D	2	M1D...	41433	123...	Hub ...	Tim G MESH/T...	8/ 5/2008 5:55:49 AM
 Tim G Rx card 2 M1D1	3	M1D...	7298	123...	Hub ...	Tim G MESH/T...	8/ 5/2008 1:55:43 AM
 Tim G Rx card 3 M1D1	18	M1D...	41118	123...	Hub ...	Tim G MESH/T...	8/ 5/2008 8:41:03 AM
 Tim G 8.3 Remote 73!	4	7350	41435	633...	Rem...	Tim G MESH/T...	8/ 1/2008 6:24:48 PM
 Tim G 8.3 Remote 73!	6	7350	41380	633...	Rem...	Tim G MESH/T...	8/ 3/2008 11:18:18 AM
 Tim G 8.3 Remote 73!	7	7350	4595	629...	Rem...	Tim G MESH/T...	8/ 4/2008 0:51:59 AM
 Tim G 8.3 Remote 73!	8	7350	41304	633...	Rem...	Tim G MESH/T...	8/ 1/2008 6:24:49 PM
 Tim G 8.3 Remote 73!	12	7350	48730	634...	Rem...	Tim G MESH/T...	8/ 1/2008 6:24:49 PM
 Tim G 8.3 Remote 73!	13	7350	48494	633...	Rem...	Tim G MESH/T...	8/ 1/2008 6:24:49 PM
 Tim G 8.3 PP Controlle	1				Prot...		8/ 1/2008 4:25:22 PM
 Tim G 8.3 PP Blade #:	1-1				PP Bl...		8/ 5/2008 8:41:03 AM
 Tim G 8.3 PP Controlle	1				Prot...		8/ 5/2008 8:49:05 AM
 Tim G 8.3 PP Blade #:	1-1				PP Bl...		8/ 5/2008 8:49:05 AM

Active Conditions Observation View Disabled Conditions **Condition Log**

Legend Pane

The **Legend** view displays the **Configuration State** icons and their meanings. They are organized by type of element as shown below:

CATEGORY	DESCRIPTION
CONFIGURATION STATE	
	Modem Incomplete Configuration not completely specified
	Modem Deactivated o... Not active in the network or configuration not yet applied
	Hub Incomplete Configuration not completely specified
	Hub Never Applied Configuration not yet applied
	Network Never Applied Configuration not yet applied
	Chassis Never Applied Configuration not yet applied
	Inroute Group Incom... Inroute Group not completely specified
CONDITION STATE	
	OK No alarms or warnings active
	Elsewhere Roaming remote in another network
	Sleep Sleeping remote
	Offline Remote Offline
	Alarm Alarms active
	Mesh Alarm Mesh Alarms active
	Warning Warnings active
	Unknown Unknown condition state
	Disabled Disabled state

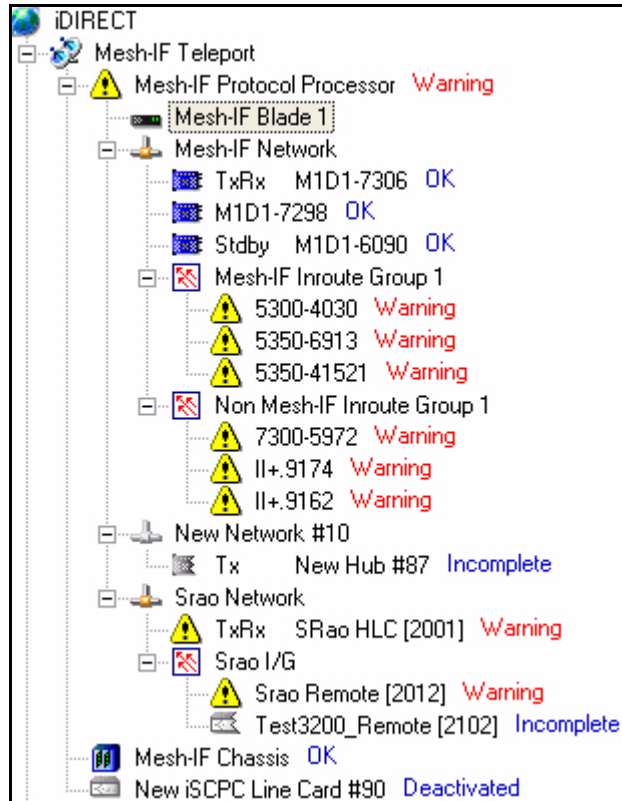
Legend

Configuration Changes Pane

Whenever there are changes made to the database by another user, they can be displayed on your screen in the **Configuration Changes** pane.

Viewing Real-Time Status

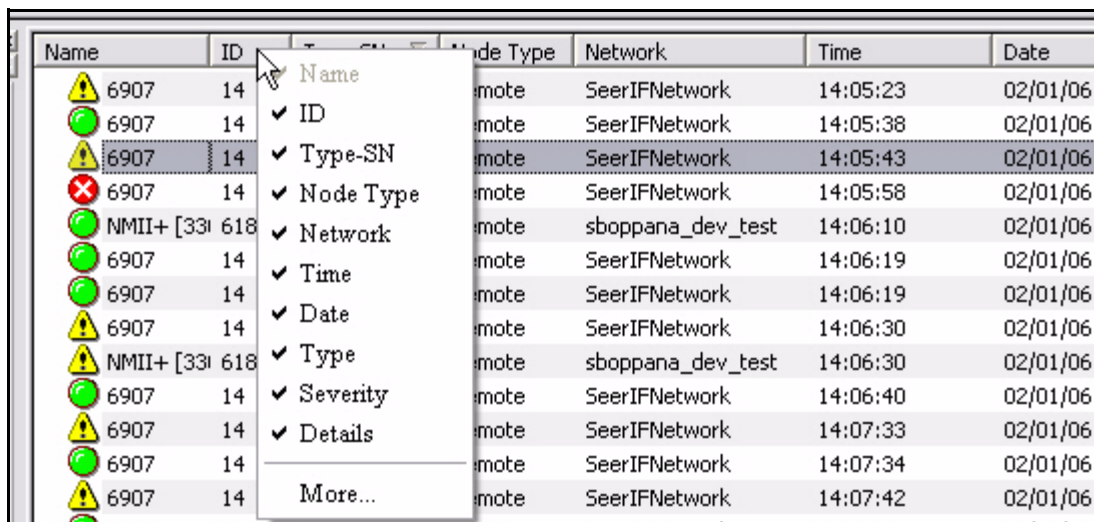
You can view the real time status of network elements in the Tree View by selecting **View Real-Time Status** from the **View** menu. The status of the various elements is displayed to the right of the element name in the tree.



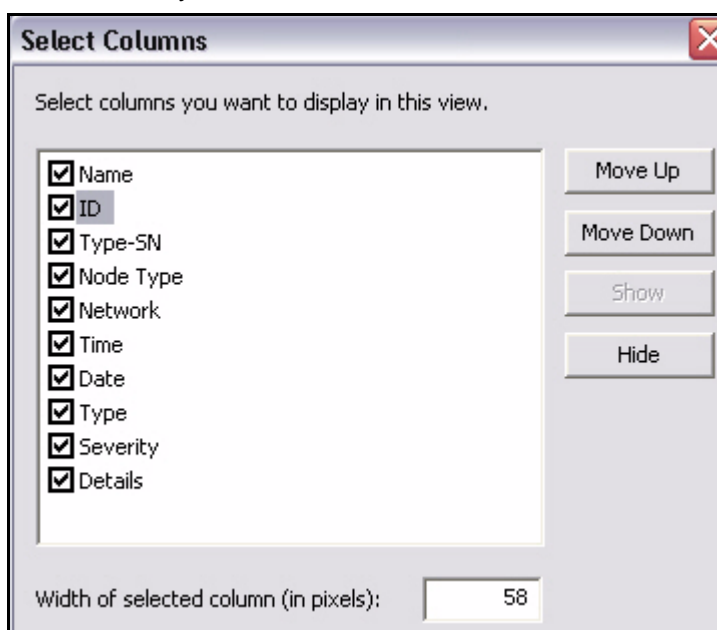
2.7.5 Selecting Columns for Viewing

In any iMonitor pane with columns, an operator can select the set of columns that will be displayed whenever that operator views the pane. Once changed, the modified display will persist for that operator even after log off. To select which columns to display, follow these steps:

- Step 1 Right-click anywhere in the column headings to display the column selection context menu.



- Step 2 You can use the menu to select or clear individual columns for display one at a time, or you can select **More** to view the **Select Columns** dialog box.



- Step 3 In the **Select Columns** dialog box, click the check boxes to select or clear the corresponding columns for display. (You can also select and clear a check box by first selecting the column name in the list, and then clicking

the **Show** or **Hide** button.) Only selected columns will be displayed in the pane.

- Step 4 To change the order in which columns appear in the pane:
- Click a column name to select it.
 - Click the **Move Up** button to move the selection one place up in the list. This will move the column to the left in the pane.
 - Click the **Move Down** button to move the selection down in the list. This will move the column to the right in the pane.
- Step 5 To change the width of a specific column, first select the column name. Then enter the new width in **Width of selected column**.

2.7.6 Monitoring iSCPC Links

With few exceptions, you can monitor iSCPC links using the same tools provided for Star or Star/Mesh networks. In some cases, particular monitoring screens for Star/Mesh networks are either different or not applicable to iSCPC links. One example is the graphical timeplan display for TDMA receive line cards — there is no equivalent display for iSCPC line cards because the upstream channel for these links does not have a timeplan.

The following table compares iSCPC and Star network monitoring capabilities available in iMonitor.

Table 2-3: Star Network vs. iSCPC Link Monitoring

Function	Star and Star / Mesh	iSCPC
Bandwidth Monitoring	SAT and IP stats	IP stats
Timeslot Monitoring	Timeplan display	N/A
Detailed remote debugging	Probe display Trace Route	Trace Route

Table 2-3: Star Network vs. iSCPC Link Monitoring (Continued)

Function	Star and Star / Mesh	iSCPC
Control Panel Tabs	General Events/Conditions SATCOM graph SAT traffic, IP traffic Probe Remote Status UCP Latency QoS	General, Events/Conditions IP traffic Remote Status Latency QoS
Built-in Reports	SAT and IP Usage Remote Availability Latency Remote Status and UCP Events/Conditions QoS Statistics	IP Usage Remote Availability Latency RemoteStatus Events/Conditions

3 Monitoring Conditions and Events

You can view **Conditions** on every element in the **Tree**, and you can view **Events** on every element except the Chassis. On the Protocol Processor and the Blades, you can further view Blade Information. Below is a table that identifies the types of information iMonitor provides for each element.

Table 3-1: Elements and Types of Information Provided

Elements	Type of Incident Information Provided
Teleport	Conditions
Protocol Processor	Events/Conditions/Blade Info
Blades	Events/Conditions/Blade Info
Network	Events/Conditions
Line Card	Events/Conditions
Inroute Group	Events/Conditions
Remotes	Events/Conditions
Chassis	Conditions

3.1 Conditions

Conditions in iMonitor are made up of Alarms and Warnings, which are collectively called “conditions.” Alarms alert you to an interruption in service, whereas Warnings indicate a condition that *could* result in an interruption of service if not handled in a timely fashion.

3.1.1 Representing State of Element via Icons

iMonitor automatically displays the current state of all network elements in the network tree view. Icons are used to indicate **OK**, **Warning**, **Alarm**, and **Offline** states.

Table 3-2: Real-Time States and Icons
















State	Icon	Meaning
OK		The element is functioning properly. Shown in order from left to right are a properly functioning PP, blade, line card, remote, chassis, external device and SkyMonitor.
OK		This icon is seen in the Conditions Log and indicates that the element is functioning properly.

Table 3-2: Real-Time States and Icons (Continued)

State	Icon	Meaning
Warning		One or more Warning conditions is active for the element.
Alarm		One or more Alarm conditions are active for the element (layer 2/3 alarm, unit not responding, etc.). Warnings may also be active in the Alarm state.
Mesh Alarm		One or more Mesh Alarm conditions are active for the element (layer 2/3 alarm, unit not responding, etc.). Warnings may also be active in the Alarm state.
Offline		The remote has been sent offline.
Elsewhere		Indicates that a roaming remote is acquired in a different network.
Sleep Mode		The remote has entered sleep mode.
Unknown Condition		Condition state unknown
Disabled		Disabled condition

3.1.2 Conditions Pane

In addition to representing the state of an element via an icon in the Tree view, you can click **View→Conditions** to open a dockable pane at the bottom of iMonitor's main window.

Name	ID	Type	SN	DID	Nod...	Network	Time
 Tim G TxRx card M1D	2	M1D...	41433	123...	Hub ...	Tim G MESH/T...	8/ 5/2008 5:55:49 AM
 Tim G Rx card 2 M1D1	3	M1D...	7298	123...	Hub ...	Tim G MESH/T...	8/ 5/2008 1:55:43 AM
 Tim G Rx card 3 M1D1	18	M1D...	41118	123...	Hub ...	Tim G MESH/T...	8/ 5/2008 8:41:03 AM
 Tim G 8.3 Remote 73!	4	7350	41435	633...	Rem...	Tim G MESH/T...	8/ 1/2008 6:24:48 PM
 Tim G 8.3 Remote 73!	6	7350	41380	633...	Rem...	Tim G MESH/T...	8/ 3/2008 11:18:18 AM

Active Conditions

Observation View

Disabled Conditions

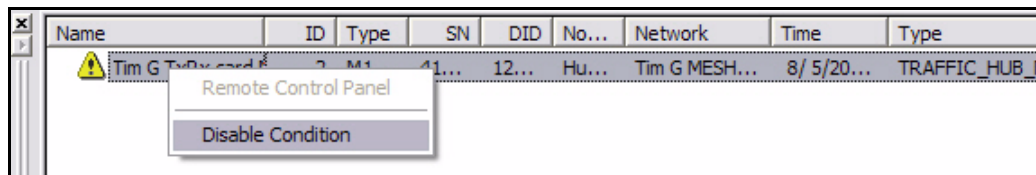
Condition Log

The **Conditions** pane has tabs that enable you to view conditions using different criteria, as follows:

- **Active Conditions** – This tab shows all outstanding conditions that have not been cleared. Any current alarms or warnings are displayed on this tab.
- **Observation View** – This tab shows all conditions for specific elements you have put “Under Observation”. You put a Protocol Processor, Blade, Line Card or Remote under

observation by clicking the element and selecting **Under Observation**. You may cancel the observation view by clicking the element in the tree and switching the **Under Observation** control off, or by right-clicking on a specific condition in the **Under Observation** tab and selecting **Cancel Observation**.

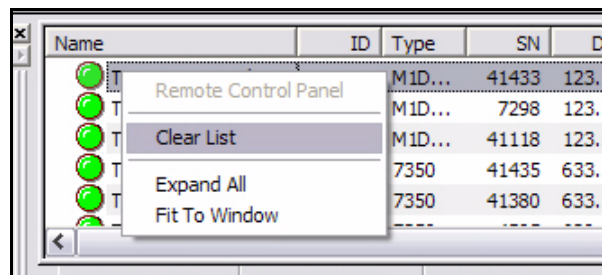
- **Disabled Conditions** – This tab shows any conditions that have been disabled. You can disable an active condition by right-clicking the condition and selecting **Disable Condition**.



- **Condition Log** – This tab shows the 500 most recent condition changes; older changes are dropped from the display. All conditions shown on the **Condition Log** tab are sorted by the time that the condition change occurred. iMonitor no longer groups condition changes.

You can clear the contents of the **Condition Log** tab as follows:

- Step 1 With the **Condition Log** tab selected, right-click anywhere in the Conditions Pane.
- Step 2 Select **Clear List** from the menu.



3.1.3 Elements with Multiple Conditions

It is possible for multiple conditions to exist simultaneously on a given network element. In fact, this is quite likely when a remote drops out of the network for some reason. In these cases, the element's overall state reflects the highest severity of any one condition, according to the following rules:

- No conditions: overall state is **"OK"**
- One or more Warnings: overall state is **"Warning"**
- One or more Warnings and one or more Alarms: overall state is **"Alarm"**
- Remote has been sent Offline: overall state is **"Offline"**

3.1.4 Offline State

The offline state is a special condition that overrides all other warnings and alarms. This state applies only to remotes. The offline state can be initiated by a remote user just before turning the remote off, to indicate to the network operator that no problem investigation is necessary.

When a remote is sent offline by the remote user, iMonitor and the back-end event server will ignore all subsequent alarms. If a unit is turned off without sending it offline first, the remote will go into the Alarm state at the hub.

The offline state clears automatically when the remote is turned back on and acquires into the network.

3.1.5 Alarms and Warnings on Elements

[Table 3-3](#) and [Table 3-4](#) list all of the alarm and warning conditions that can be raised for the various elements.

Table 3-3: Explanation of Alarms by Element

Element	Alarm Condition	Explanation
Chassis	Chassis Down	iMonitor cannot communicate with the EDAS
Protocol Processor	Protocol Processor Down	The heartbeat has not been received from the Protocol Processor
Hub Line Card	Line Card Down	iMonitor cannot communicate with the Hub Line Card
	Rx SCPC Loopback C/N	Line card SCPC loopback exceeds clear sky C/N.
	TDM Lock	Hub line card is no longer locked to the SCPC loopback
	10 MHz Clock Alarm	Board does not support 10 MHz clock
Remote	Mesh Mode Changed	Mesh remote is no longer in mesh mode
	Mesh Tx TDMA C/N	Mesh remote transmit TDMA exceeds clear sky C/N

Table 3-4: Explanation of Warnings by Element

Element	Warning Condition	Explanation
Chassis	Power Supply "n"	Failed
	Fan "n"	Failed
	RCM (Ref Clock Module) "n"	Failed
Four-Slot Chassis	Four Slot Chassis Over Temperature	Chassis exceeds temperature limit
	Four Slot RCM A Not Present	RCM A has not been installed in the Chassis
	Four Slot RCM A Fault	RCM A of the chassis has failed
	Four Slot RCM B Not Present	RCM B has not been installed in the chassis
	Four Slot RCM B Fault	RCM B of the chassis has failed
	Four Slot Power Alarm A Bad	Chassis power supply A has failed
	Four Slot Power Alarm A Over Temperature	Chassis power supply A exceeds temperature limit
	Four Slot Power Alarm B Bad	Chassis power supply B has failed
	Four Slot Power Alarm B Over Temperature	Chassis power supply B exceeds temperature limit
	Four Slot FSM Not Present	FSM has not been installed on the chassis
	Four Slot FSM Fault	FSM has failed on the chassis
	Four Slot FSM Fan Fault	FSM fan has failed on the chassis
	Four Slot IFM Not Present	IFM has not been installed on the chassis
	Four Slot IFM Fault	IFM has failed on the chassis
	Four Slot Alarm Disabled	Audible alarms are disabled for the chassis
	Four Slot OPM A Fault	OPM A has failed on the chassis
	Four Slot OPM B Fault	OPM B has failed on the chassis
Hub Line Card	Rx Overflow of frames	Downstream Packets per sec. overdrive
	Back plane lost 10 MHz Clock	The 10 MHz reference timing signal is absent from the chassis backplane
Protocol Processor	Blade CPU high	Blade CPU usage is above the defined limit

Table 3-4: Explanation of Warnings by Element (Continued)

Element	Warning Condition	Explanation
Remote	Upstream C/N, low 7 high 25	The perceived signal at the hub is above or below limits
	Downstream C/N, low 7 high 25	Perceived signal (at remote) is above or below limits
	Local LAN Disconnect	LAN port on remote is disconnected
	Lost Contact	PP has temporarily lost contact with remote
	Latency	Measured latency, hub to remote is more than 2 sec.
	Symbol Offset	PP has detected a symbol offset that exceeds +/- 1/2 the acquisition aperture.
	Remote Off-line State	The remote has been sent off-line.
	Calibrated Transmit Power	Transmit power below -35 dbm
	GPS Signal Lost	Don't reset remote warning
	Remote Temperature	Temperature on board is higher than 75 C and lower than 15 C
	AGC Out of Range	Remote Automatic Gain Control outside limits.
	Rx SCPC C/N	Remote receive SCPC exceeds clear sky C/N. Value will be -1 or -100.
	Mesh Rx TDMA Loopback C/N	Mesh remote receive TDMA loopback exceeds clear sky C/N
	Maximum Tx Power	Remote transmit power is within 0.5 dB of the maximum



NOTE

See the Maintenance section of the *iDirect Hub Chassis Installation and User's Guide* for information on replacing failed fan and power supply components.



NOTE

SCPC conditions that apply to either network line cards or TDMA remotes also apply to both iSCPC line cards and iSCPC remotes.

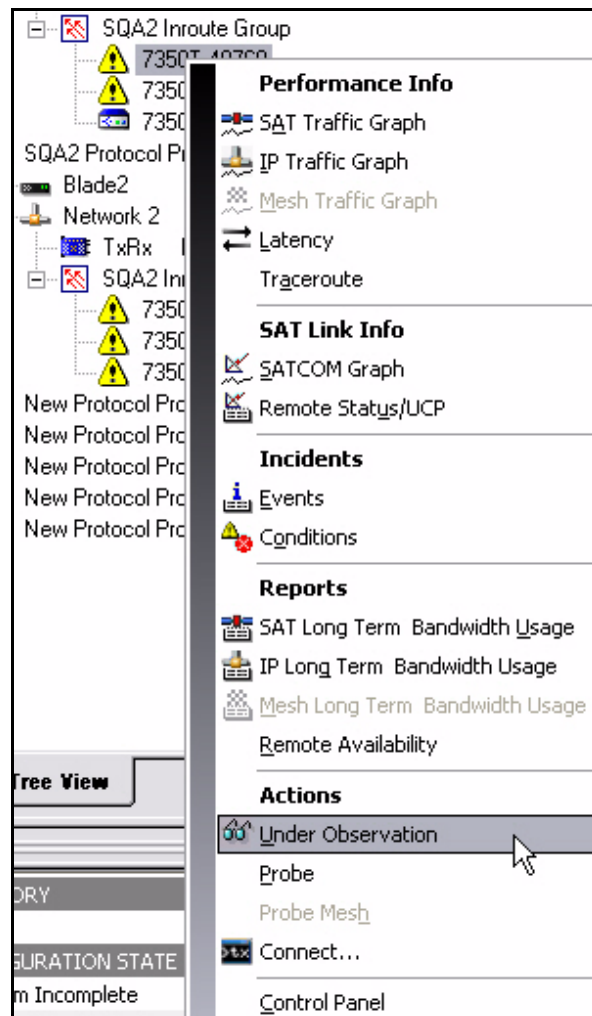
3.2 Putting an Element under Observation for Conditions

You can put an element “under observation” for the purpose of monitoring it for any conditions that arise on that element. Only the following elements can be put under observation for viewing conditions (alarms and warnings):

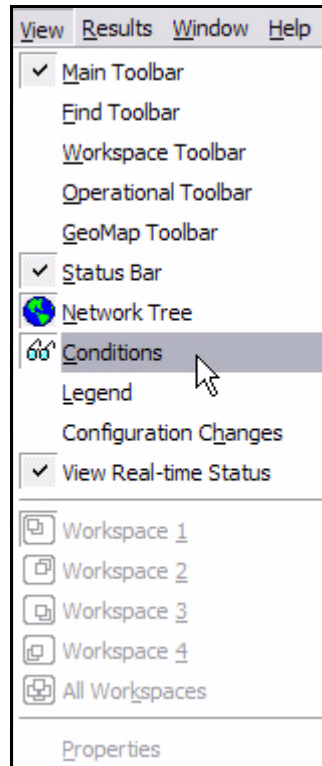
- Protocol Processor
- Blade
- Line Card
- Remote
- Chassis

To use the **Under Observation** feature, follow the directions below.

- Step 1 Right-click an element, for which you want to view alarms and warnings:
- Step 2 Click **Under Observation**.



- Step 3 Select **View → Conditions** from the main menu or click the **Conditions** icon on the main toolbar.

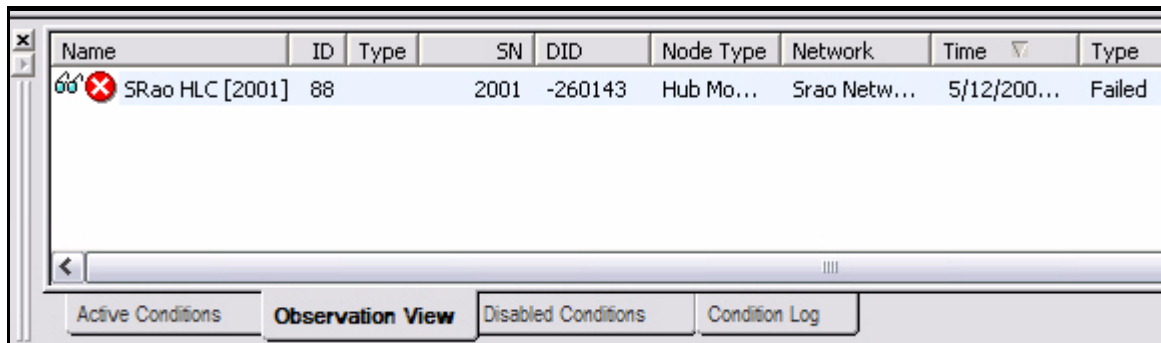


- Step 4 Click the **Observation View** tab. The **Observation View** pane appears in the iMonitor window, displaying only the conditions (alarms and warnings) for the element you chose.

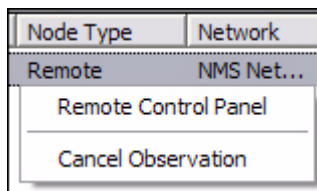


NOTE

If you have previously put another element under observation, without canceling that observation view, the previous element's information will still be visible in the pane. To omit the unwanted information, right-click on the unwanted element and select **Cancel Observation**.



- Step 5 Right-click on the element you selected to observe. You are provided the option to either view the element's control panel or cancel the observation. Click the desired option.



- Step 6 If you click **Cancel Observation**, the data in the **Observation** pane disappears.
- Step 7 If you click **Control Panel**, a pane appears providing more information for you to view. Following is an example of the types of information you may view on a given element (in this case, a remote) if you select **Control Panel**. (See [Section 4.8.4 "Control Panel" on page 96](#).)
- Step 8 Follow the directions in [Section 3.2.1 "Viewing Conditions or Events" on page 42](#).

General		Events/Conditions	SATCOM	SAT Traffic	IP Traffic	Probe	Remote Status	UCP Info	Latency	QoS
Information Name: Infiniti Test [5350.2036] ID: 222 Type-SN: 5350.2036 Derived ID: 6817780 LAN IP Address: 172.18.117.17 LAN Subnet Mask: 255.255.255.248 LAN Gateway: Mgmt IP Address: 172.19.117.3 Mgmt Subnet Mask: 255.255.0.0 Max Power: Initial Power: Max Downstream Infor...						Link Configuration ▶ Spacecraft: Beam_605_174000_GA ▶ Downstream Transponder: CBMS Transponder ▶ Downstream Bandwidth: Network1 Bandwidth ▶ Downstream Carrier: Network1 Downstream [2M] ▶ Upstream Transponder: CBMS Transponder ▶ Upstream Bandwidth: Network1 Bandwidth ▶ Upstream Carriers:				
Real-Time Summary Avg Downstream C/N: 9.90 dB Avg Upstream C/N: 11.42 dB Avg Tx Pwr: -26.00 dBm Avg Temp: 55.74 °C TDM Lost: 0 Rx Input Power: -51.81 dB Digital Rx Power: 21.45 dB FLL DAC: 0x607 Rx COF: -24 Up Time: 20 hours 03 min 28 sec ▶ Lan Port: Connected ▶ Connections:						VSAT Information Approx. Cable Length: 0.000000 ▶ BUC: CBMS BUC ▶ LNB: CBMS LNB ▶ Reflector: AL-7104 ▶ Reflector Mount: CBMS Reflector Mount ▶ IFL: CBMS IFL				

3.2.1 Viewing Conditions or Events

To view conditions or events, you must specify certain criteria on the **Select Items** dialog box.

Viewing Conditions

If you want to view conditions, you may want to put an element under observation first. For information on this, see [Section 3.2 “Putting an Element under Observation for Conditions” on page 39](#).

Viewing Events

If you are viewing events, you may want to filter the results. Often it's useful to retrieve certain events over an extended time period for one or more remotes. Although you can retrieve all events and sort the results to find the ones you're looking for, iMonitor also allows you to specify a text filter when retrieving historical events. When you specify a text filter, iMonitor shows you only those events that match the filter.

The text filter is available at the bottom of the historical time range parameters dialog box ([Figure 3-2](#) on [page 45](#)), either prior to retrieving events or from the **Time Range** button on an existing events display. The filter values are applied only to the **Event Description** section of the event message. The simplest filter string is simply a substring of the event description, such as “server”. Any event message that contains your specified substring will be returned from the server and displayed in the pane. The text field also supports full Linux regular expression matching, allowing you to apply an arbitrarily complex expression to the event description text. For more information on regular expressions, see any of the commercially-available Linux reference books.

To retrieve and view conditions or events, follow the directions below.

- Step 1 Right-click the element in the tree for which you want to view conditions or events.
- Step 2 Click on either **Conditions** or **Events**. The **Select Items** dialog box appears.

Select Items

☐ Historical None (Real-time)

☐ Save to Cnd_16_01_33.txt

Protocol Processors

Protocol Processor	Blade Name
<input checked="" type="checkbox"/> Nextgen II PP	<input checked="" type="checkbox"/> Blade II
	<input checked="" type="checkbox"/> Blade 1

External Devices

Device	Host Name
--------	-----------

Line Cards

Name	Type-SN	Network
<input checked="" type="checkbox"/> M1D1-13...	M1D1.135...	
<input checked="" type="checkbox"/> M0D1.21...	M0D1.2187	
<input checked="" type="checkbox"/> NM2+.37...	II+.3789	
<input checked="" type="checkbox"/> M1D1 [4...	M1D1.4113	
<input checked="" type="checkbox"/> New Hub	II.0	
<input checked="" type="checkbox"/> New Hu...	II+.0	

Remotes

☐ Devices

Name	Type-SN	Network
<input checked="" type="checkbox"/> 7350-5902	7350.5902	Nextgen II...
<input checked="" type="checkbox"/> NMII+_4...	II+.4584	Nextgen II...
<input checked="" type="checkbox"/> 7300-3974	7300.3974	Nextgen II...
<input checked="" type="checkbox"/> 5150_47...	5150.4748	Nextgen II...
<input checked="" type="checkbox"/> 3100_59...	3100.59904	Nextgen II...
<input checked="" type="checkbox"/> NMII+_32...	II+.3230	Nextgen II...
<input checked="" type="checkbox"/> New Re...	II.0	Nextgen II...
<input checked="" type="checkbox"/> Xiaoping ...	II.2	Nextgen II...
<input checked="" type="checkbox"/> New Re...	II.0	New Netw...

- Step 3 Make your selections on the **Select Items** dialog box, as follows:
- Step 4 Click either **Historical** or **Get Past**. If you are viewing Events, you can filter the results, or simply press OK to begin retrieving events in real-time. If you enter a **Text Filter** in the **Get Past** time range dialog box ([Figure 3-2](#)), the filter values are applied *only* to the **Event Description** field of the event message.
- a If you click **Historical**, click **Time Range**. The **Select Time Range** dialog box appears (see [Figure 3-1](#) for Conditions and [Figure 3-2](#) for Events). If desired, click the ellipses next to the Start and End times to set the time via the graphical clock display. If you selected **Get Past**, see [Step b](#).

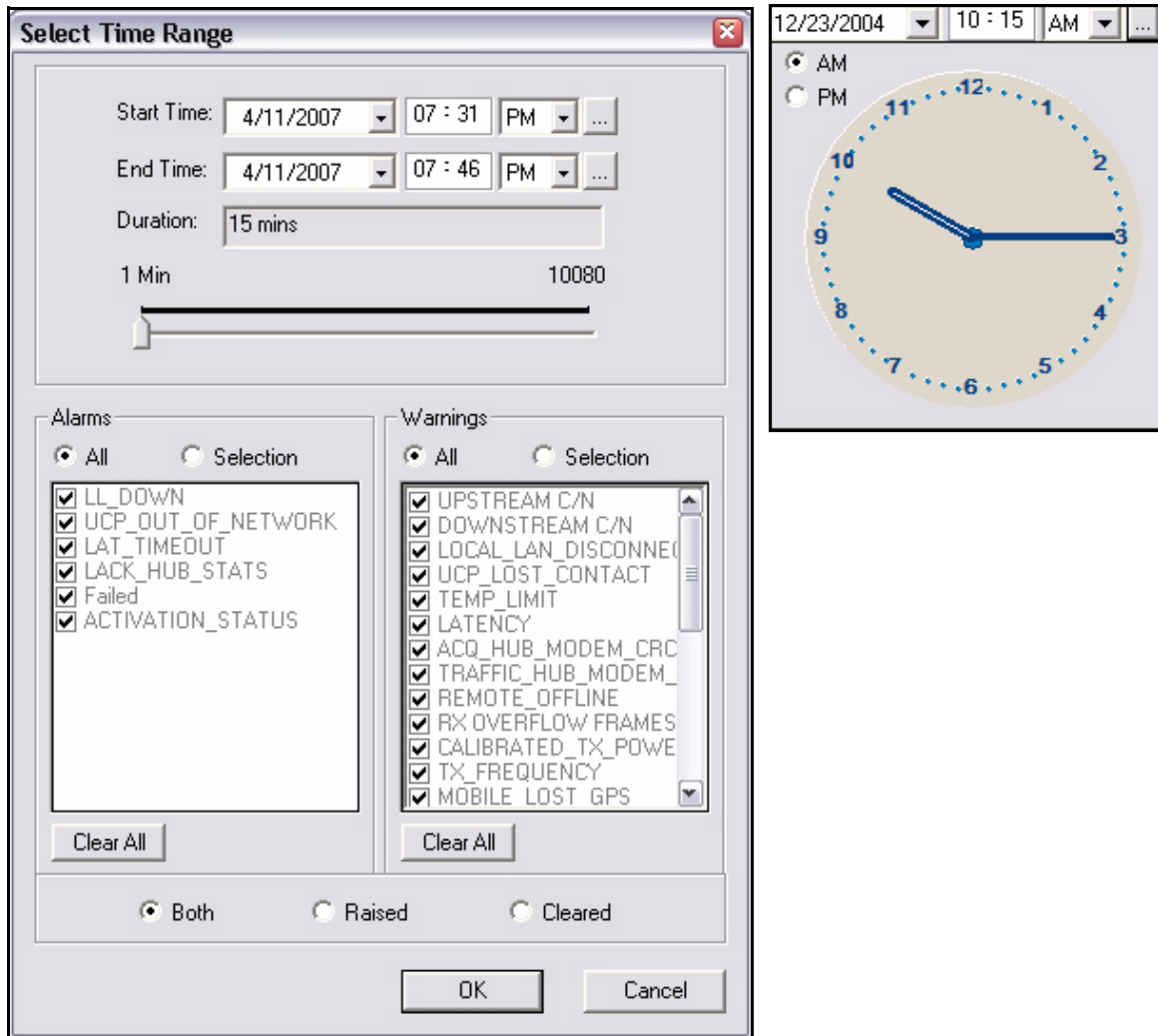


Figure 3-1: Conditions Time Range

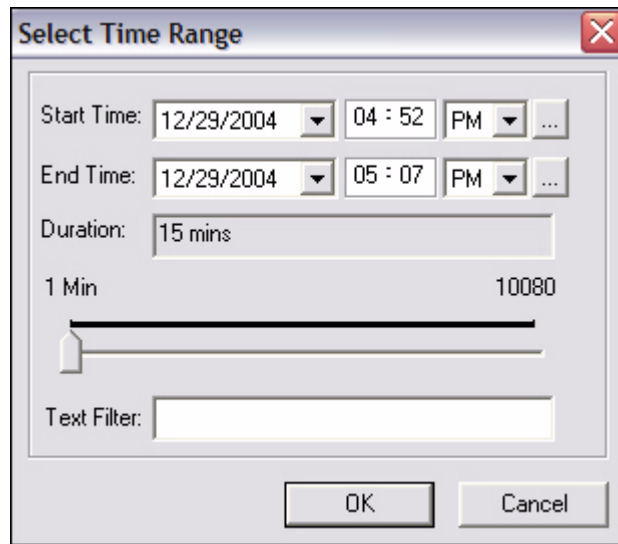
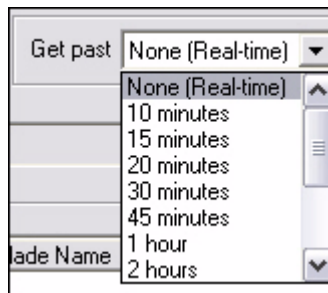


Figure 3-2: Events Time Range with Text Filter

- b If you click **Get Past**, the **Get Past** drop-down list appears.



- Step 5 Select the elements for which you want to view conditions or events.

Depending on what level in the system you chose to obtain information, the options in the **Select Items** dialog box will differ in what is available and unavailable for selection.

- Step 6 When you have made your selections, click **OK**.

Depending on whether you chose to view conditions or events, either the **Conditions/Time Line** pane appears or the **Events** pane appears. Follow the directions in [Step 7](#) for **Conditions** or [Step 10](#) for **Events** below.

- Step 7 **Conditions.** If you are retrieving data on conditions, the **Conditions/Time Line** pane appears, displaying the conditions logged for the specified period. This data is displayed in a multicolumn format. See [Figure 3-3](#) for an example of data displayed on the **Conditions** tab.

On the **Conditions** tab, notice that many remotes have an arrow next to them. If you click on the arrow so that it is pointing down, the conditions for that remote are revealed.

To view conditions in a graphical format, click the **Time Line** tab. See [Figure 3-4](#) for an example of data displayed on the **Time Line** tab.

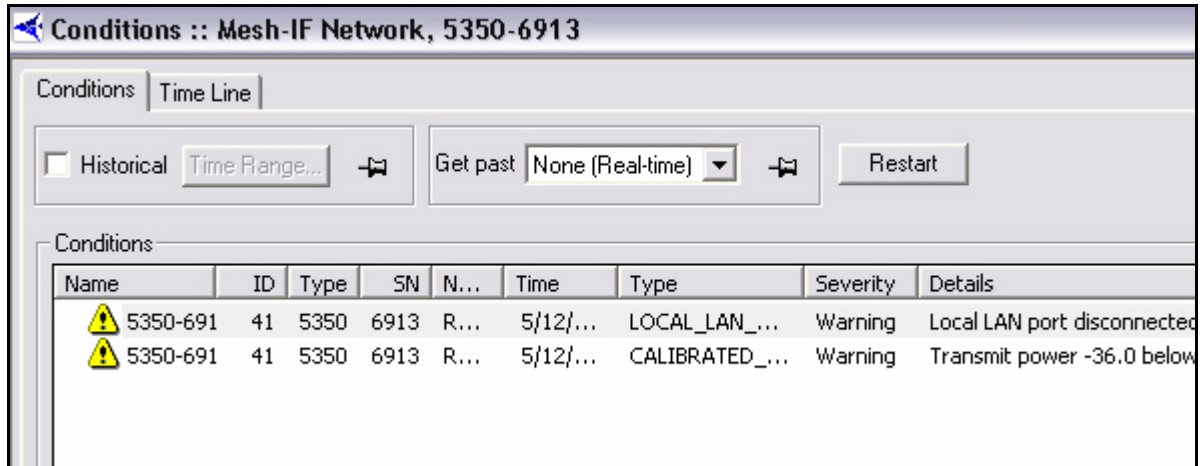


Figure 3-3: Conditions Results in Multicolumn Format

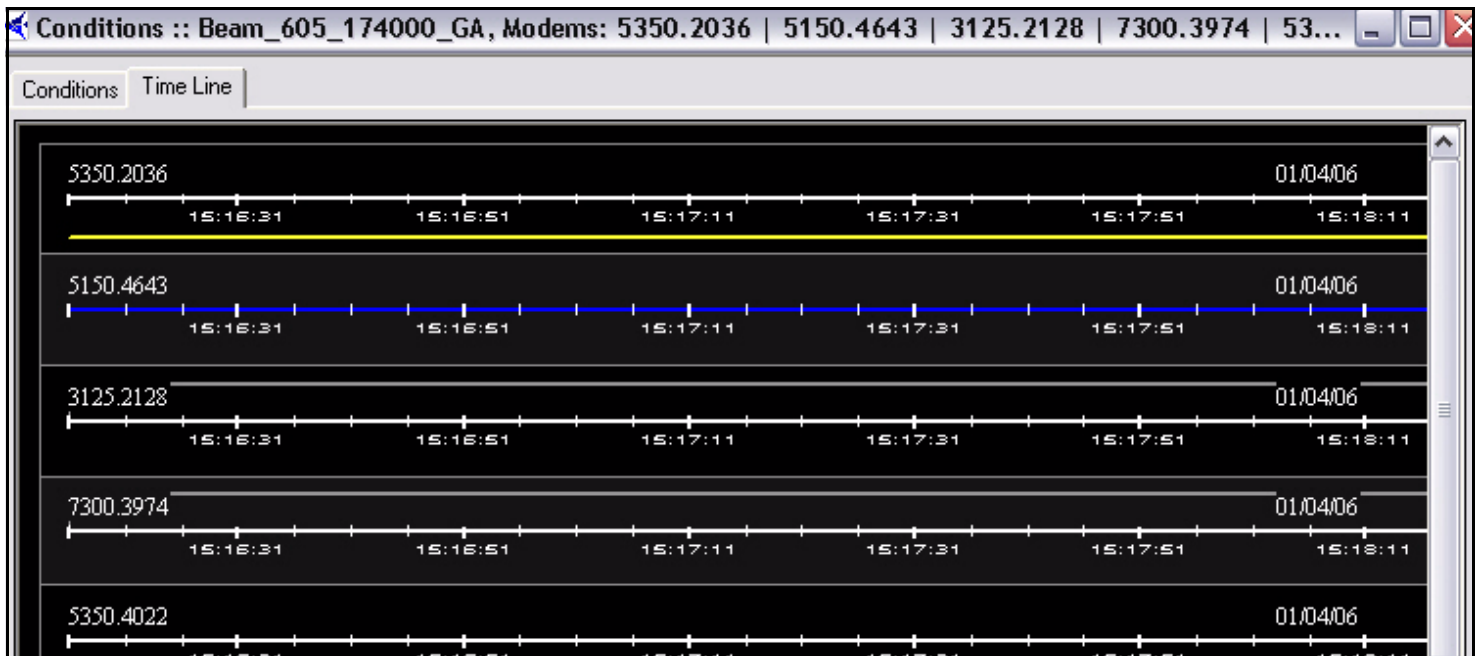
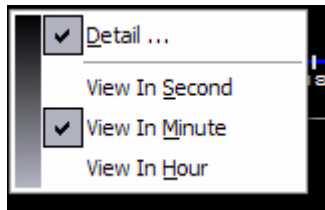


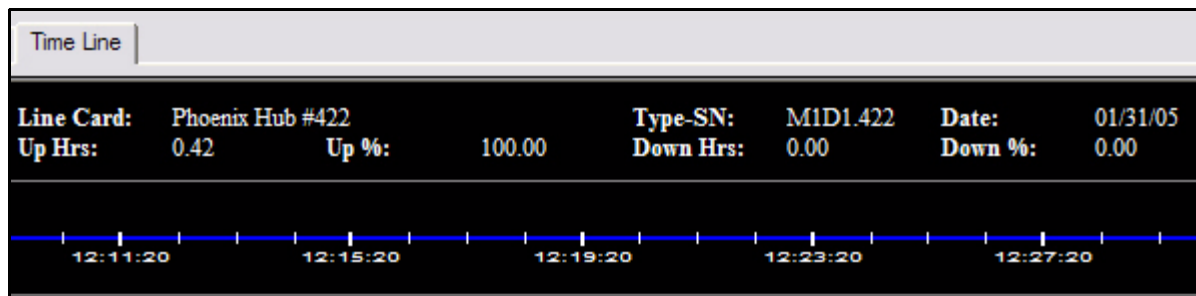
Figure 3-4: Conditions Time Line Results in Graphical Format

- Step 8 On the **Time Line** display, you can right-click to elect to view the results in Seconds, Minutes, or Hours.



- Step 9 You can also elect to view Details from this menu, which displays a heading line at the top of the display showing the following information:

- Name of Network Element
- Type and Serial Number of a Remote or Line Card
- Current Date
- Number of hours it has been up
- Number of hours it has been down
- Percentage of time it has been up (Up %)
- Percentage of time it has been down (Down %)



- Step 10 **Events.** If you are retrieving data on events, the **Events** pane appears, displaying the events logged for the specified period. This data is displayed in a multicolumn format only. It cannot be viewed in graphical format. See [Figure 3-3](#) for an example of data displayed on the **Events** tab.

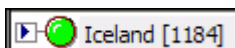
Time	Name	Type-SN	Type	Network	Eve...	Event Description
8/19/2008 11:41:42 AM	Tim G 8.3 Remote 735...	7350.48...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+8), P...
8/19/2008 11:42:02 AM	Tim G 8.3 Remote 735...	7350.48...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-1), FO(+1), P...
8/19/2008 11:39:43 AM	Tim G 8.3 Remote 735...	7350.4595	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+7), P...
8/19/2008 11:40:03 AM	Tim G 8.3 Remote 735...	7350.4595	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+12), P...
8/19/2008 11:40:23 AM	Tim G 8.3 Remote 735...	7350.4595	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+6), P...
8/19/2008 11:40:43 AM	Tim G 8.3 Remote 735...	7350.4595	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(-17), P...
8/19/2008 11:41:03 AM	Tim G 8.3 Remote 735...	7350.4595	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(-14), P...
8/19/2008 11:41:23 AM	Tim G 8.3 Remote 735...	7350.4595	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+3), P...
8/19/2008 11:41:43 AM	Tim G 8.3 Remote 735...	7350.4595	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(-5), P...
8/19/2008 11:42:02 AM	Tim G 8.3 Remote 735...	7350.4595	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+13), P...
8/19/2008 11:39:42 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-1), FO(+0), P...
8/19/2008 11:40:02 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-1), FO(-12), P...
8/19/2008 11:40:22 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+5), P...
8/19/2008 11:40:43 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-1), FO(-6), P...
8/19/2008 11:41:03 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-1), FO(+4), P...
8/19/2008 11:41:23 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+1), P...
8/19/2008 11:41:43 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-1), FO(+9), P...
8/19/2008 11:42:02 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-1), FO(+7), P...
8/19/2008 11:39:42 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-1), FO(-3), P...
8/19/2008 11:40:02 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+8), P...
8/19/2008 11:40:22 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+8), P...
8/19/2008 11:40:42 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(+7), P...
8/19/2008 11:41:02 AM	Tim G 8.3 Remote 735...	7350.41...	Rem...	Tim G MESH/TRANSEC...	Info	UCPI: SO(-2), FO(-3), P...

Figure 3-5: Event Results

3.2.2 Interpreting Conditions Results

By default, conditions are sorted in ascending order based on the timestamp. You may re-sort at any time by clicking on the desired column heading.

Each line in the conditions display shows a particular “state change” for the unit in question at the timestamp indicated. A state change occurs whenever a condition is raised or cleared. If the entry contains the arrow icon, shown below, in the first column, it means that additional conditions were active for this unit at the time of the state change. These conditions, along with the time they first occurred, are shown when you click the arrow icon.



Arrow

Below is an example illustrating the conditions output, including multiple simultaneous conditions.

Conditions :: UAT-RF Network, Venice [3126] Top [04/26/04 14:48:00 - 04/26/04 15:03:00]									
Time range: 04/26/04 14:48:00 - 04/26/04 15:03:00									
<input checked="" type="checkbox"/> Historical Time Range... Get past None [Real-time] Restart									
Name	ID	SN	Node...	Network	Time	Date	Type	Severity	Details
Venice [3126] Top	125	3126	Remote	UAT-RF Network	14:20:11	04/26/04	DOWNSTREAM_SNR	Cleared	Downstream SNR 7.21 above low limit (7.00)
Venice [3126] Top	125	3126	Remote	UAT-RF Network	15:00:12	04/26/04	UCP_LOST_CONTACT	Warning	PP lost contact with 3126
Venice [3126] Top	125	3126	Remote	UAT-RF Network	15:00:25	04/26/04	LAT_TIMEOUT	Alarm	Stopped receiving echo reply from 3126
Condition					15:00:12	04/26/04	UCP_LOST_CONTACT	Warning	PP lost contact with 3126
Venice [3126] Top	125	3126	Remote	UAT-RF Network	15:00:27	04/26/04	UCP_OUT_OF_NETWORK	Alarm	UCP timeout: 3126 out of network
Condition					15:00:25	04/26/04	LAT_TIMEOUT	Alarm	Stopped receiving echo reply from 3126
Condition					15:00:12	04/26/04	UCP_LOST_CONTACT	Warning	PP lost contact with 3126
Venice [3126] Top	125	3126	Remote	UAT-RF Network	15:01:04	04/26/04	UCP_LOST_CONTACT	Cleared	PP re-gained contact with 3126
Condition					15:01:04	04/26/04	UCP_OUT_OF_NETWORK	Cleared	UCP timeout: 3126 out of network
Condition					15:00:25	04/26/04	LAT_TIMEOUT	Alarm	Stopped receiving echo reply from 3126
Venice [3126] Top	125	3126	Remote	UAT-RF Network	15:01:10	04/26/04	LAT_TIMEOUT	Cleared	Stopped receiving echo reply from 3126
Venice [3126] Top	125	3126	Remote	UAT-RF Network	15:01:14	04/26/04	UPSTREAM_SNR	Warning	Upstream SNR 5.74 below low limit (7.00)
Venice [3126] Top	125	3126	Remote	UAT-RF Network	15:01:34	04/26/04	UPSTREAM_SNR	Cleared	Upstream SNR 10.28 above low limit (7.00)

This example takes us through a remote reset, and illustrates the following conditions:

1. The first entry shows the remote's state at the start of the specified time range: the remote is OK, and the last condition that cleared was DOWNSTREAM_SNR.
2. The next entry shows that the PP lost contact with the remote (this happens soon after the reset was sent from iBuilder).
3. The next entry shows two conditions: the LOST_CONTACT warning is still active, and has been joined by the layer 3 alarm LAT_TIMEOUT.
4. Finally, the Protocol Processor declares the remote OUT_OF_NETWORK, and this condition is added to the list, giving us a total of three simultaneous conditions.
5. The next line shows us that two of the three conditions cleared: The remote is back in the network and the Protocol Processor has re-gained contact with it. The layer 3 alarm at this point is still active.
6. The next line shows that the last condition, LAT_TIMEOUT, cleared.
7. The last two lines show a separate condition that was raised and cleared in a 15-second time span.

When multiple conditions are shown in this display, the icon in the left column does not represent the current state of the remote. Rather, it shows the type of condition that occurred at that time. For example, in number 5 above, the state of this remote is still ALARM, since the layer 3 alarm is still active. However, this particular entry represents the clearing of two conditions, and the green icon indicates that to the user.

3.3 Interpreting System Events

System events consist of a log of activity that occurs on elements in real-time and activity that is stored in the historical archive. See [Figure 3-5](#). Examples of system events include:

- Terminal connection set up or torn down
- Uplink control message from the Protocol Processor to remotes
- SWEEP messages during remote acquisition
- Multicast package processed or rejected
- Firmware image or options file written to flash

By default events are displayed in real-time and are sorted in ascending order by timestamp. You may re-sort the display in ascending or descending order by clicking on the appropriate column heading. You may also select historical events up to one week prior to the current date.

3.4 Snapshots

Snapshots can be selected from:

- Teleports
- Networks
- Inroute groups
- Remotes

3.4.1 Network Condition Snapshot

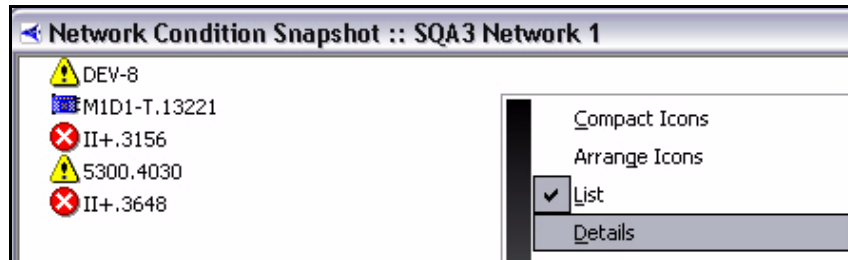
The **Network Condition Snapshot** shows all elements in a teleport, network, inroute group, or remote in a multicolumn list, allowing you to view their current states more compactly than is possible from the Tree view.

To view a snapshot of the network condition, follow these steps:

- Step 1 Right-click the teleport, network or inroute group for which you want to view a snapshot of the conditions.
- Step 2 Select **Network Condition Snapshot** or **Teleport Condition Snapshot**. The **Network Condition Snapshot** (or **Teleport Condition Snapshot**) pane appears. [Figure 3-6](#) shows an example of a **Network Condition Snapshot** at the network level. (Both the List and Detail views are shown. You can toggle between these views by right-clicking in the window and selecting List or Details from the menu.)
 - a If you selected **Teleport Condition Snapshot** at the teleport level, all protocol processors, protocol processor blades, chassis, inroute group, remotes

configured under the teleport, and external teleport devices are displayed in the **Network Condition Snapshot** box.

- b If you selected **Network Condition Snapshot** at the network level, every inroute group, remote, and remote external device in that network is displayed in the **Network Condition Snapshot** box.
- c If you selected **Network Condition Snapshot** on a particular inroute group, only the line cards, remotes, and remote external devices in that inroute group are displayed in the **Network Condition Snapshot** box.



Type-SN	Type	Name	Network	Condition	Details
DEV-8	Device	mutli-device host (32)		Warning	Device 'mutli-device host (32)' is in warning state.
M1D1-T.13221	Line card	M1D1 [13221]	SQA3 Network 1	OK	Line card is OK.
II+.3156	Line card	II+ [3156]	SQA3 Network 1	Alarm	Failed
5300.4030	Remote	5300 [4030] [DC on LNB]	SQA3 Network 1	Warning	CALIBRATED_TX_POWER;LOCAL_LAN_DISCONNECT
II+.3648	Remote	II+ [3648]	SQA3 Network 1	Alarm	UCP_OUT_OF_NETWORK

Figure 3-6: List and Details View of Network Condition Snapshot



NOTE

If all hosts of an external device configured at a remote or teleport are down, the device will be in Alarm state. If at least one host is up and at least one host is down, the device will be in Warning state.

- Step 3 You can view different data depending on your selections when you right-click a network element in the **Network Condition Snapshot** pane. Below is an example of a remote's submenu when right-clicked from this pane.

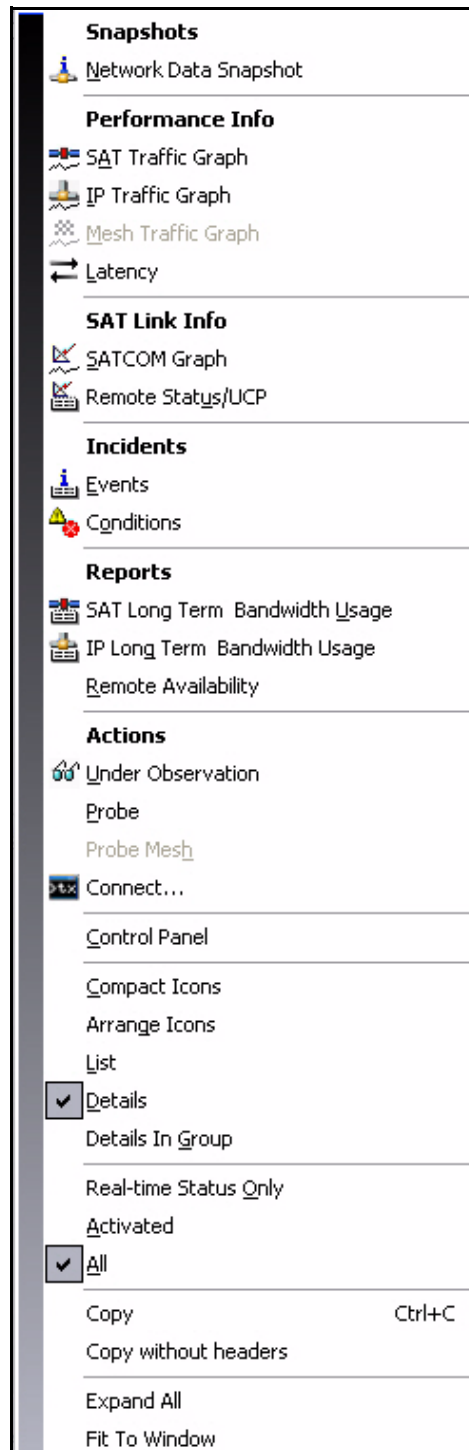

















Figure 3-7: Remote Submenu in Condition Snapshot

Step 4 In the lower half of the submenu are several options that allow you to tailor the **Network Condition Snapshot** view:

- Compact Icons
- Arrange Icons
- List
- Details
- Details in Group
- Real-time Status Only
- Activated

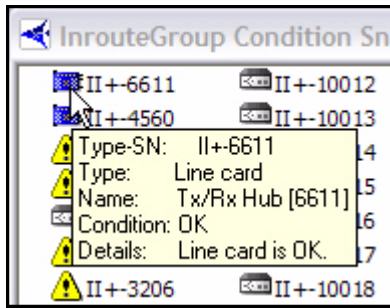
Step 5 The example below is a result of right-clicking **Details**.

InrouteGroup Condition Snapshot :: IG_1_UAT-RF [6611][4560]				
Type-SN	Type	Name	Condition	Details
 II+-3157	Remote	Copenhagen [3157]	Alarm	LOCAL_LAN_DISCONNECT
 II+-3196	Remote	Amsterdam [3196]	Deactivated	Remote is not activated.
 II+-3182	Remote	Oslo [3182]	Warning	LOCAL_LAN_DISCONNECT
 II+-3206	Remote	Belfast [3206]	Warning	LOCAL_LAN_DISCONNECT
 II-665	Remote	Tokyo [665]	Deactivated	Remote is not activated.
 II-1184	Remote	Iceland [1184]	Warning	LOCAL_LAN_DISCONNECT
 II+-4699	Remote	Argentina [4699]	Deactivated	Remote is not activated.
 II+-3201	Remote	Prague [3201]	Warning	LOCAL_LAN_DISCONNECT
 II+-10006	Remote	R10006	Deactivated	Remote is not activated.
 II+-10007	Remote	R10007	Deactivated	Remote is not activated.
 II+-10008	Remote	R10008	Deactivated	Remote is not activated.
 II+-10009	Remote	R10009	Deactivated	Remote is not activated.
 II+-10010	Remote	R10010	Deactivated	Remote is not activated.
 II+-10011	Remote	R10011	Deactivated	Remote is not activated.
 II+-10012	Remote	R10012	Deactivated	Remote is not activated.

Step 6 If you hover the pointer (mouse arrow) over an element in the snapshot, a box of information about that element is displayed. Below is an example of the pointer hovering over a line card in a network.

If you are ever in doubt as to what you are pointing at, look at the **Type: line**. In this case, you can see that the type of element for which the box is providing information is “**Line card**.” The box also provides the following information on this element:

- Type of Unit and Serial Number
- Type of element
- Name of element
- Current Condition of element
- Other Details about the element



- Step 7 You can further double-click on a Remote in the snapshot view to see the remote's Control Panel. See [Section 4.8.4 "Control Panel" on page 96](#) for information about the control panel.

Multiple Selection Options in Condition Snapshot View

You may also use Windows' multiple-select keys to select any number of remotes from the **Network Condition Snapshot** display. The elements you select are used to populate the parameters dialog windows for the following iMonitor displays:

- SAT/IP Traffic Stats
- Latency
- Events
- Conditions
- Network Data Snapshot
- SAT/IP Long Term Bandwidth Reports
- Remote Availability Report

The following figure illustrates the use of multiple-select to populate a parameters dialog.

- Step 1 In the **Network Condition Snapshot** results view, with **Details** selected as shown in [Figure 3-7](#), select the remotes whose data you want to automatically be filled in on one of the above parameters dialog boxes, such as Remote Availability Report. Below is a figure showing five remotes selected.

InrouteGroup Condition Snapshot :: IG_1_UAT-RF [6611][4560]				
Type-SN	Type	Name	Condition	Details
II+-3157	Remote	Copenhagen [3157]	Alarm	LOCAL_LAN_DISCONNECT
II+-3196	Remote	Amsterdam [3196]	Deactivated	Remote is not activated.
II+-3182	Remote	Oslo [3182]	Warning	LOCAL_LAN_DISCONNECT
II+-3206	Remote	Belfast [3206]	Warning	LOCAL_LAN_DISCONNECT
II-665	Remote	Tokyo [665]	Deactivated	Remote is not activated.
II-1184	Remote	Iceland [1184]	Warning	LOCAL_LAN_DISCONNECT
II+-4699	Remote	Argentina [4699]	Deactivated	Remote is not activated.
II+-3201	Remote	Prague [3201]	Warning	LOCAL_LAN_DISCONNECT
II+-10006	Remote	R10006	Deactivated	Remote is not activated.
II+-10007	Remote	R10007	Deactivated	Remote is not activated.
II+-10008	Remote	R10008	Deactivated	Remote is not activated.
II+-10009	Remote	R10009	Deactivated	Remote is not activated.
II+-10010	Remote	R10010	Deactivated	Remote is not activated.
II+-10011	Remote	R10011	Deactivated	Remote is not activated.
II+-10012	Remote	R10012	Deactivated	Remote is not activated.

- Step 2 With your mouse pointer located within the region of the highlighted elements, right-click and select a report from those available. In this example, **Remote Availability** is selected. Notice that the resulting **Select Remote Devices** parameters dialog box shows only the remotes that are highlighted above. If you had selected this same report (**Remote Availability**) from the Tree, even with these remotes highlighted, the resulting dialog box would have listed *all* of the remotes—not just the ones you highlighted. Thus, it is important to ensure that your mouse pointer is actually over the highlighted elements when you right-click.

Select Remote Devices

Network: 3
Historical
Get past

Remote Devices
All
Clear
Active

Name	Type-SN
<input checked="" type="checkbox"/> R10006	II+.10006
<input checked="" type="checkbox"/> R10007	II+.10007
<input checked="" type="checkbox"/> R10008	II+.10008
<input checked="" type="checkbox"/> R10009	II+.10009
<input checked="" type="checkbox"/> R10010	II+.10010

Time Range

Start Time: 1/24/2005 02:18 PM
End Time: 1/31/2005 02:18 PM
Duration: 1 week

1 Hour
1488

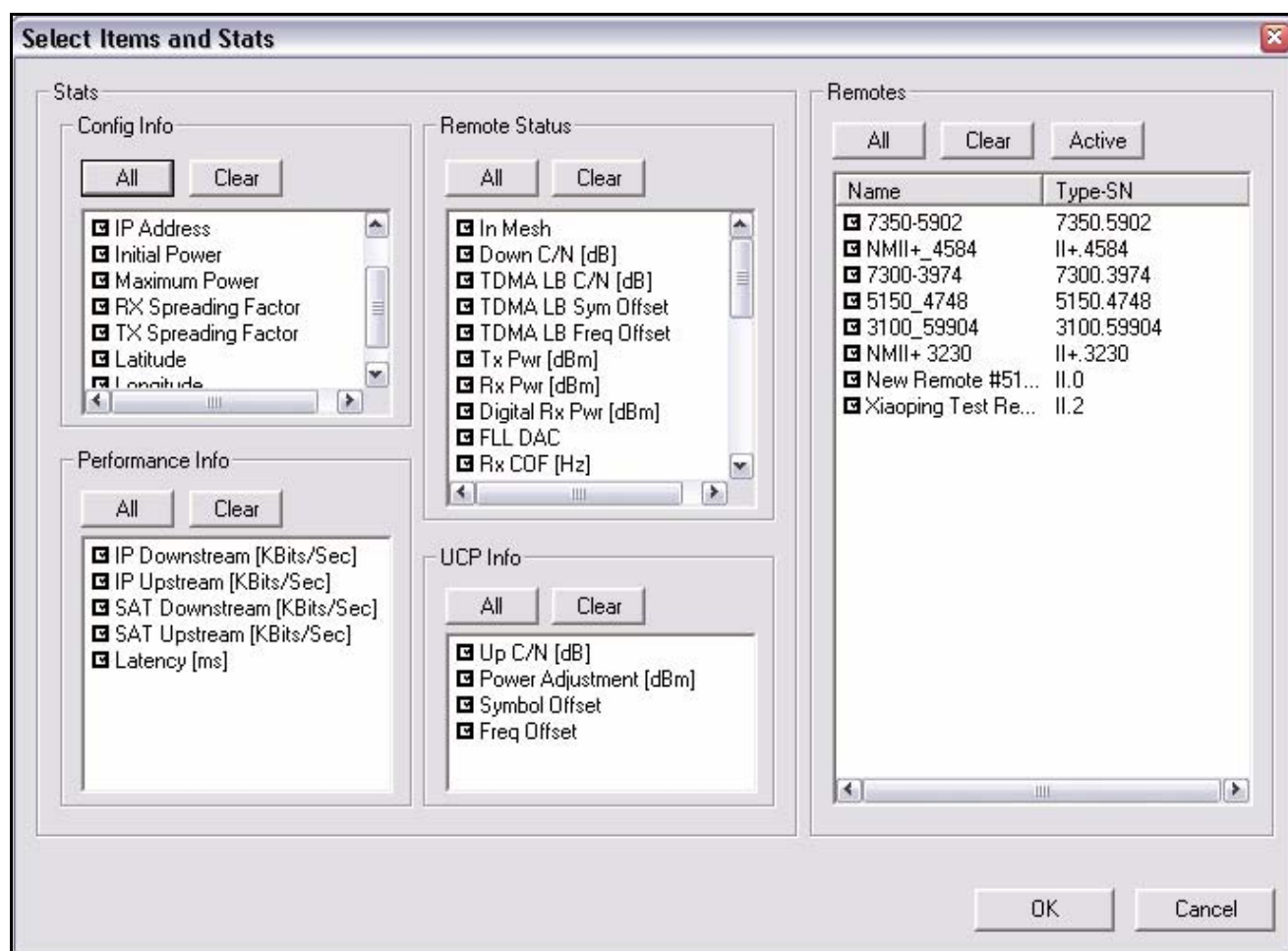
OK
Cancel

3.4.2 Network Data Snapshot

The **Network Data Snapshot** display allows you to select multiple real-time parameters for a group of remotes and display the data in a spreadsheet-like format. This display is very useful when you want to monitor a variety of real-time data points for multiple remotes simultaneously.

To view a snapshot of network data, follow the directions below:

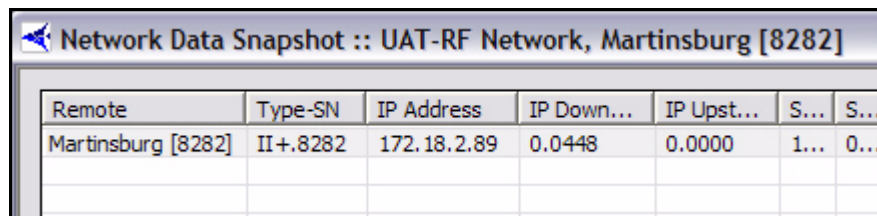
- Step 1 Right-click the element for which you want to view a snapshot of data for a network or specific inroute group.
- Step 2 Select **Network Data Snapshot**. The **Select Items and Stats** dialog box appears.



- Step 3 Select the items and statistics you want to display in your results view, as follows:

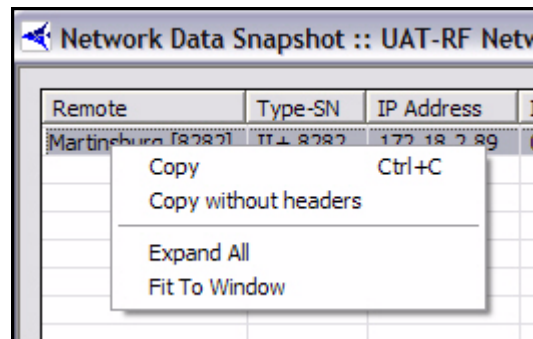
- Config Info
- Performance Info (IP/SAT stats and latency)
- Remote Status (runtime parameters from the remotes)

- UCP (uplink control messages to remotes from the PP)
- Step 4 By default all remotes are displayed in the **Remotes** section. To select only Activated remotes, select **Active**. To clear all remotes, select **Clear**. In this example, **Clear** was selected, and then only the Martinsburg remote was selected for the snapshot.
- Step 5 Click **OK**.
- Step 6 Real-time data is displayed in the results pane. Limit-checked parameters, such as downstream C/N, change to yellow if the values go outside the defined limits. Remotes that are out-of-network are displayed in red. Below is an example.



Remote	Type-SN	IP Address	IP Down...	IP Upst...	S...	S...
Martinsburg [8282]	II+,8282	172.18.2.89	0.0448	0.0000	1...	0...

- Step 7 You can right-click anywhere that data appears in the pane in order to take advantage of a set of options, as shown below.



- Step 8 From this set of options, you can do any of the following:
- copy this data to the clipboard for pasting into other applications
 - copy it without the headers to the clipboard for pasting into other applications
 - expand the headers to view the complete data within each column
 - fit the columns to the size of the window you have open for viewing
 - As with any Windows-based application, you can resize the viewing window or drag the edges of a column to expand or contract its width.

4 Obtaining Performance and Status Information

You can obtain many types of performance information on the elements in your network. The following sections describe how to obtain and interpret this information:

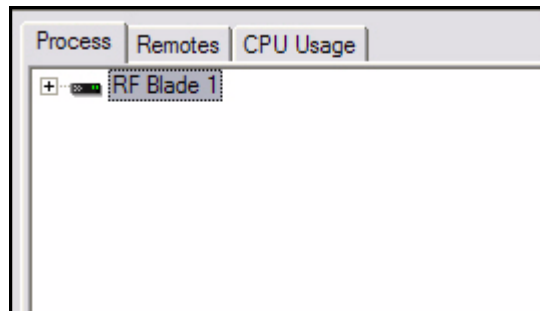
- [“Monitoring Blades in iMonitor” on page 59](#)
- [“Using the Remote Probe” on page 61](#)
- [“CPU Usage \(Blades Only\)” on page 66](#)
- [“Timeplan” on page 68](#)
- [“Inroute Distribution” on page 71](#)
- [“Latency” on page 74](#)
- [“Retrieving Information on Remotes using Probe Mesh” on page 77](#)
- [“Satellite Link Information” on page 79](#)
- [“Connecting to Network Elements” on page 98](#)
- [“Monitoring Your Bandwidth with SkyMonitor” on page 100](#)

4.1 Monitoring Blades in iMonitor

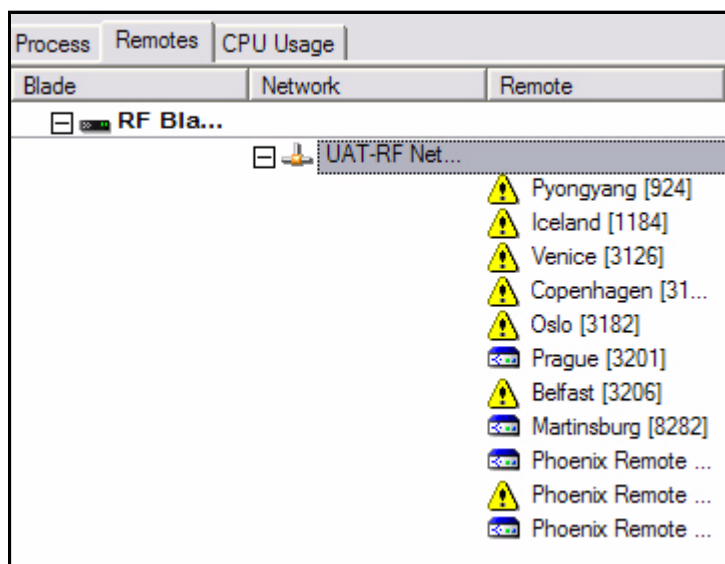
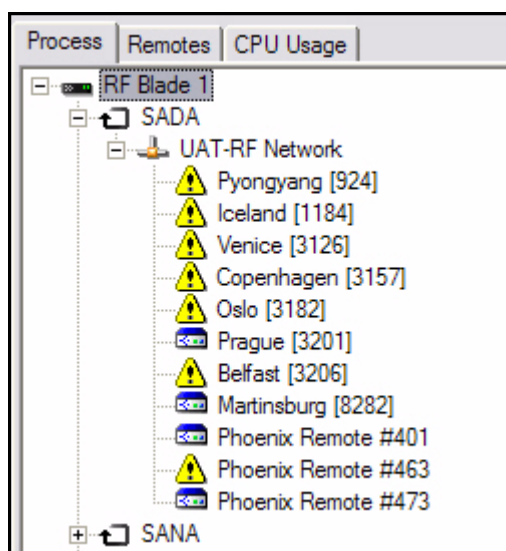
iMonitor provides a rich suite of monitoring tools to allow you to monitor blade activity and configuration. Various displays allow you to determine the processes running on each blade, the remotes assigned to each blade, and the CPU utilization of each blade. Additionally, the CPU usage is archived for historical retrieval (NOTE: archiving is implemented in release 6.0.0).

To view blade information, follow the directions below:

- Step 1 Right-click a protocol processor or a blade in the Tree.
- Step 2 Click **Blade Info**. The **Blade Info** pane appears.



- Step 3 Click on any of three tabs to view different types of information. See the following three images for examples of all three tabs' information.



The screenshot shows a window titled 'Blade Info :: NMS Blade 1'. It has three tabs: 'Process', 'Remotes', and 'CPU Usage'. The 'CPU Usage' tab is selected. Below the tabs is a table with three columns: 'Blade', 'Category', and 'Percentage'. The first row of the table is 'NMS Blade 1'. Below this, there are five rows of CPU usage statistics:

Blade	Category	Percentage
NMS Blade 1	User Time	0.40
	System Time	0.20
	Nice Time	0.00
	IO Wait Time	0.00
	Idle Time	99.30

- Step 4 You can also right-click on the blade in any of these displays and click **CPU Usage**. This option allows you to view historical information about CPU usage on blades. See [Section 4.3 “CPU Usage \(Blades Only\)” on page 66](#) for instructions on how to obtain and use this information.

4.2 Using the Remote Probe

The **Probe** pane is available from the individual Remote nodes in the network tree view. It allows you to perform specific tasks on a single remote, and provides a mechanism for retrieving protocol layer statistics from the Protocol Processor controlling the remote.

Specifically, the probe allows you to perform any of the following operations from a single dialog box:

- Change a remote's transmit power
- Connect to a remote or protocol processor blade
- Reset a remote
- Transmit a modulated or unmodulated carrier from a remote
- Retrieve data from and perform other functions on a remote's protocol processor
- Perform LL Bounce and Acq Bounce on all protocol layers

Because the information in the display is specific to an individual remote, when you select multiple remotes from an intermediate tree node iMonitor launches a separate pane for each remote.

The **Probe** pane is organized into the following sections:

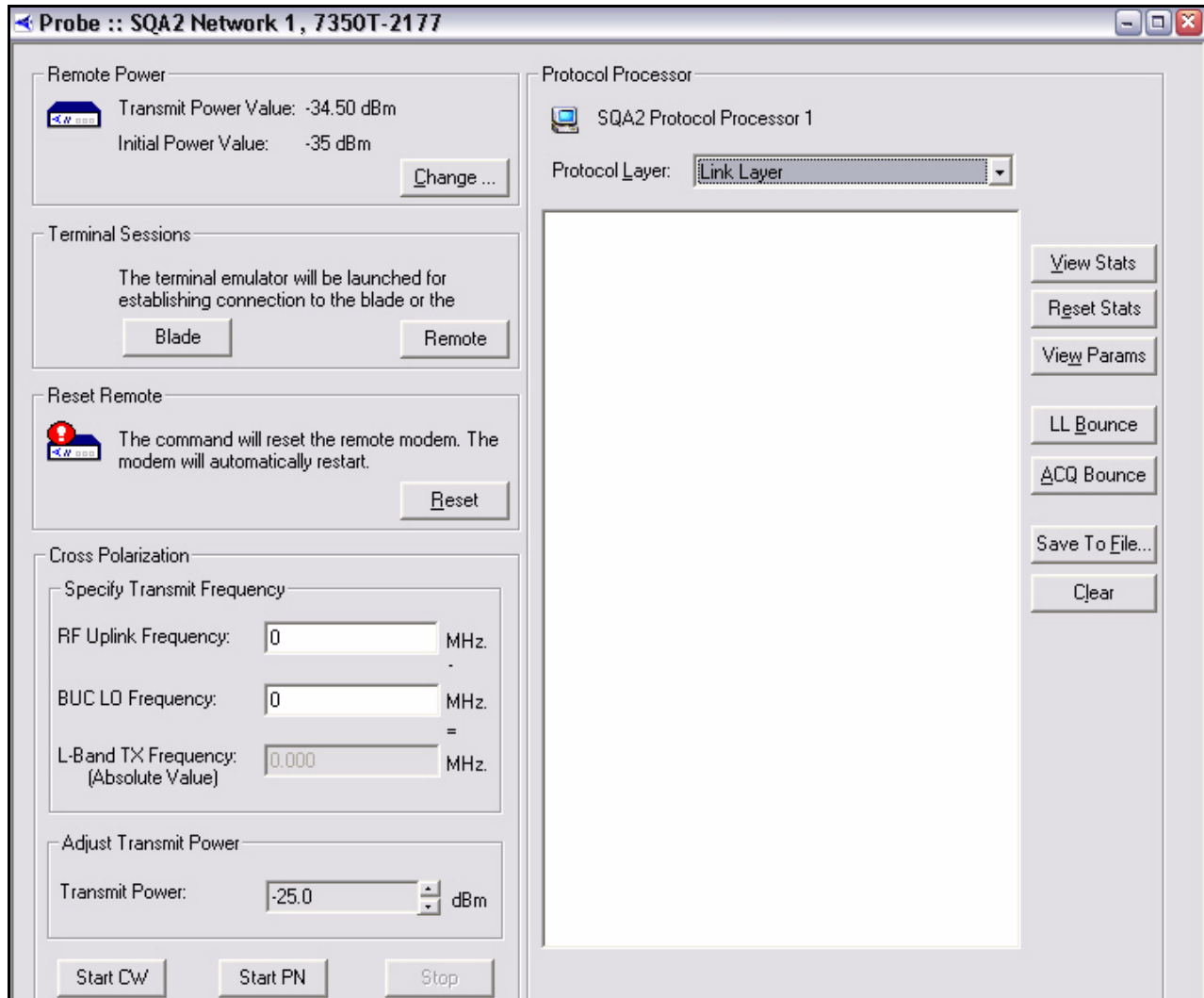
- **Remote Power** – allows you to dynamically change the remote's transmit power using a MAC-level message from the Protocol Processor. The remote does not have to be in the network to receive this message, but it must be locked onto the downstream carrier.
- **Terminal Sessions** – allows you to launch a terminal window to this remote or to the remote's protocol processor blade. The remote must be in the network and your PC must be able to “ping” the remote for the remote terminal function to work.

- **Reset Remote** – allows you to reset the remote using a MAC-level message from the Protocol Processor. The remote does not have to be in the network to receive this message, but it must be locked onto the downstream carrier.
- **Cross Polarization** – allows you to transmit an unmodulated or modulated carrier on a specified frequency from a remote.
- **Protocol Processor** – allows you to view statistics, reset statistics, view parameters, “bounce” the link layer, or perform an ACQ Bounce.

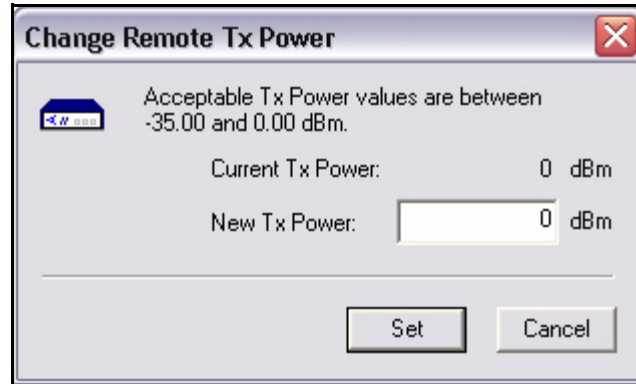
The **Protocol Processor** section of the Probe pane allows you to “bounce” the link layer, which causes it to go through its initialization handshake sequence and perform the “ACQ Bounce” function on this remote. ACQ Bounce is discussed in [“Performing ACQ Bounce” on page 73](#). Inroute Distribution is discussed in [Section 4.5 “Inroute Distribution” on page 71](#).

Step 1 Right-click a remote.

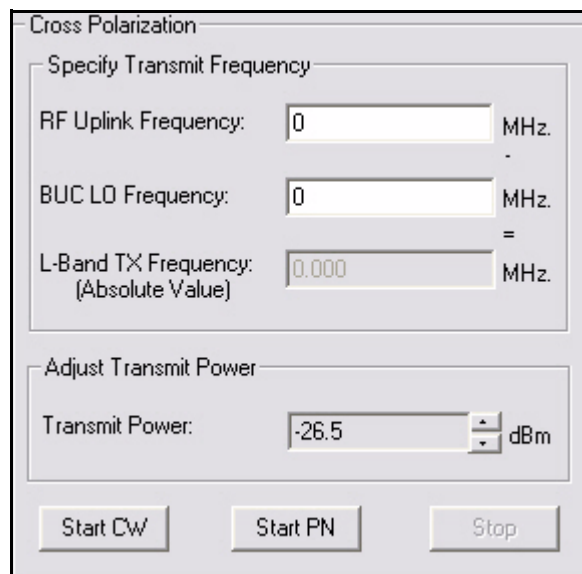
Step 2 Select **Probe** from the menu. The **Probe** dialog box appears.



- Step 3 To alter the **Transmit Power Value**, click **Change** in the **Remote Power** section to display the **Change Remote Tx Power** dialog box. Type the desired **New Tx Power** and click **Set**. Note that you cannot set the power outside of the Min/Max range defined for this remote in iBuilder.



- Step 4 To connect directly to the remote or protocol processor blade, click **Remote** or **Blade** in the **Terminal Sessions** box.
- Step 5 To reset the modem, click the **Reset** button.
- Step 6 To transmit an unmodulated (CW) or modulated (PN) carrier:
- Specify an unused **RF Uplink Frequency** for transmission. This is the center frequency of the satellite carrier you want to transmit.
 - Specify the **BUC LO Frequency** translation for the remote's BUC.
 - Click **Start CW** to begin transmitting an unmodulated carrier, or click **Start PN** to begin transmitting a modulated carrier.



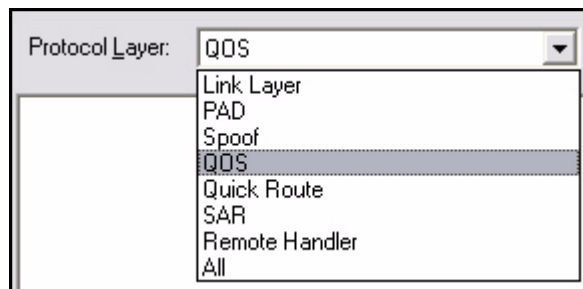
- d To dynamically change the transmit power once the carrier is active, select the up and down arrows in the **Transmit Power** section of the screen. Each time you click an arrow, the transmit power will change by .5 dBm.
- e To change to a different frequency, click the **Stop** button to bring down the existing carrier; specify a new **RF Uplink Frequency**; then click the appropriate start button to retransmit the carrier.
- f When you have finished, reset the remote to return the remote to normal functionality. You can use the **Reset** button on the probe, or you can reset the remote from iBuilder.



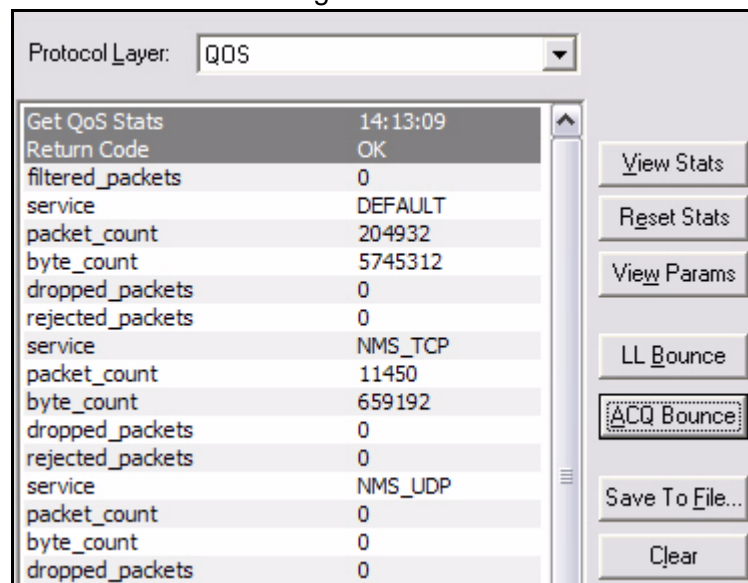
NOTE

A carrier launched from this screen will automatically stop transmitting five minutes after the carrier was started or the power was last adjusted. You can configure a custom key on the remote to change this timeout. See [“Modifying the Timeout Duration for a CW or PN Carrier” on page 65](#) for details.

- Step 7 To view statistics, reset statistics or perform “bounce” functions, select a layer in the **Protocol Layer** drop-down list.



- Step 8 Select the button to the right that will provide the desired data, reset the statistics or perform the desired bounce function. You can save data you retrieve to a file using the **Save To File** button.



Modifying the Timeout Duration for a CW or PN Carrier

A carrier launched from the **Cross Polarization** section of the Probe will automatically stop transmitting five minutes after the carrier was started or the power was last adjusted. You can modify this timeout duration in iBuilder by configuring a custom key on the remote, as follows:

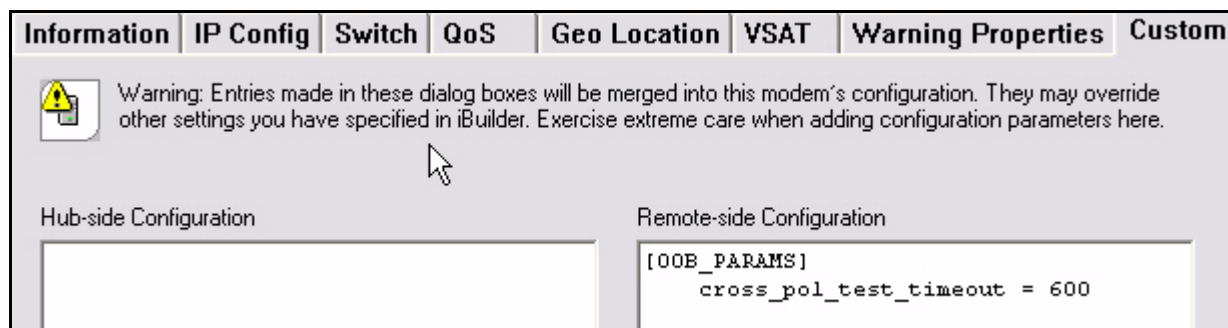
- Step 1 Right-click the remote in the iBuilder network tree and select **Modify→Item**.
- Step 2 Click the **Custom** tab.
- Step 3 In the **Remote-side Configuration** section of the **Custom** tab, define the following custom key:

```
[OOB_PARAMS]
```

```
cross_pol_test_timeout = <Seconds>
```

where <Seconds> is the carrier timeout in seconds.

The following example sets the timeout to 600 seconds (10 minutes).

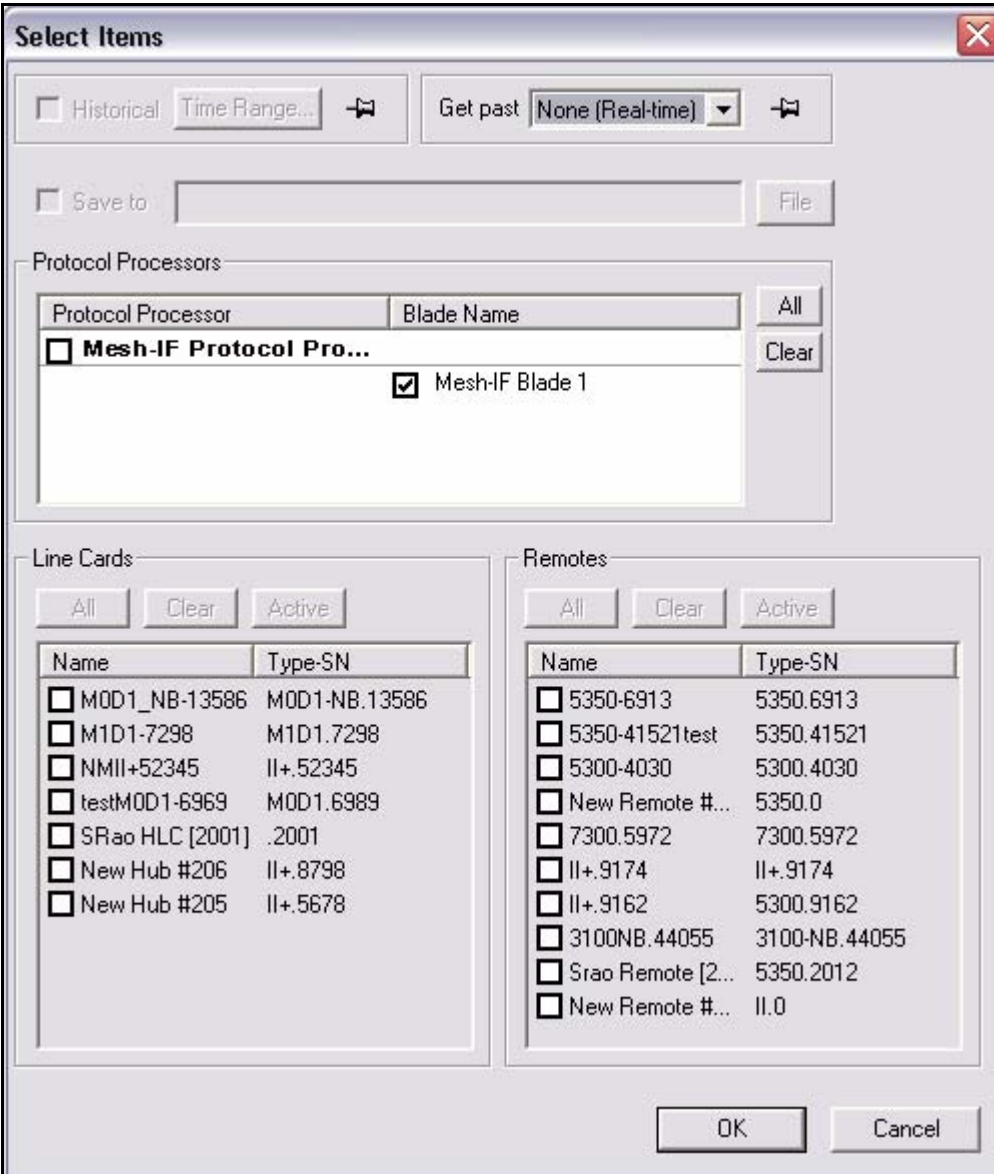


- Step 4 Click **OK** to save the remote configuration.
- Step 5 Right-click the remote in the iBuilder network tree and select **Apply Configuration→Reliable Remote-Side (TCP)**.
- Step 6 When the confirmation dialog box appears, click **Yes** to send the changes to the remote.
- Step 7 When the new dialog box appears, click **Reset Now** for the updated timer to take effect on the remote.



4.3 CPU Usage (Blades Only)

The CPU Usage display can be selected from blades. To view CPU usage, follow the directions below.

- Step 1 Right-click a blade and select **CPU Usage**. The **Select Items** dialog box appears. (Note that only **Real-time** will be available in the **Get Past** menu.)



The **Select Items** dialog box is used to configure data collection. It includes options for historical data, time range, and data source (Protocol Processors, Line Cards, or Remotes).

Historical: ☐ **Time Range...**  **Get past:** **None (Real-time)** 

Save to: **File**

Protocol Processors

Protocol Processor	Blade Name
<input type="checkbox"/> Mesh-IF Protocol Pro...	<input checked="" type="checkbox"/> Mesh-IF Blade 1

Line Cards

All **Clear** **Active**

Name	Type-SN
<input type="checkbox"/> MOD1_NB-13586	MOD1-NB.13586
<input type="checkbox"/> M1D1-7298	M1D1.7298
<input type="checkbox"/> NMII+52345	II+.52345
<input type="checkbox"/> testMOD1-6969	MOD1.6989
<input type="checkbox"/> SRao HLC [2001]	.2001
<input type="checkbox"/> New Hub #206	II+.8798
<input type="checkbox"/> New Hub #205	II+.5678

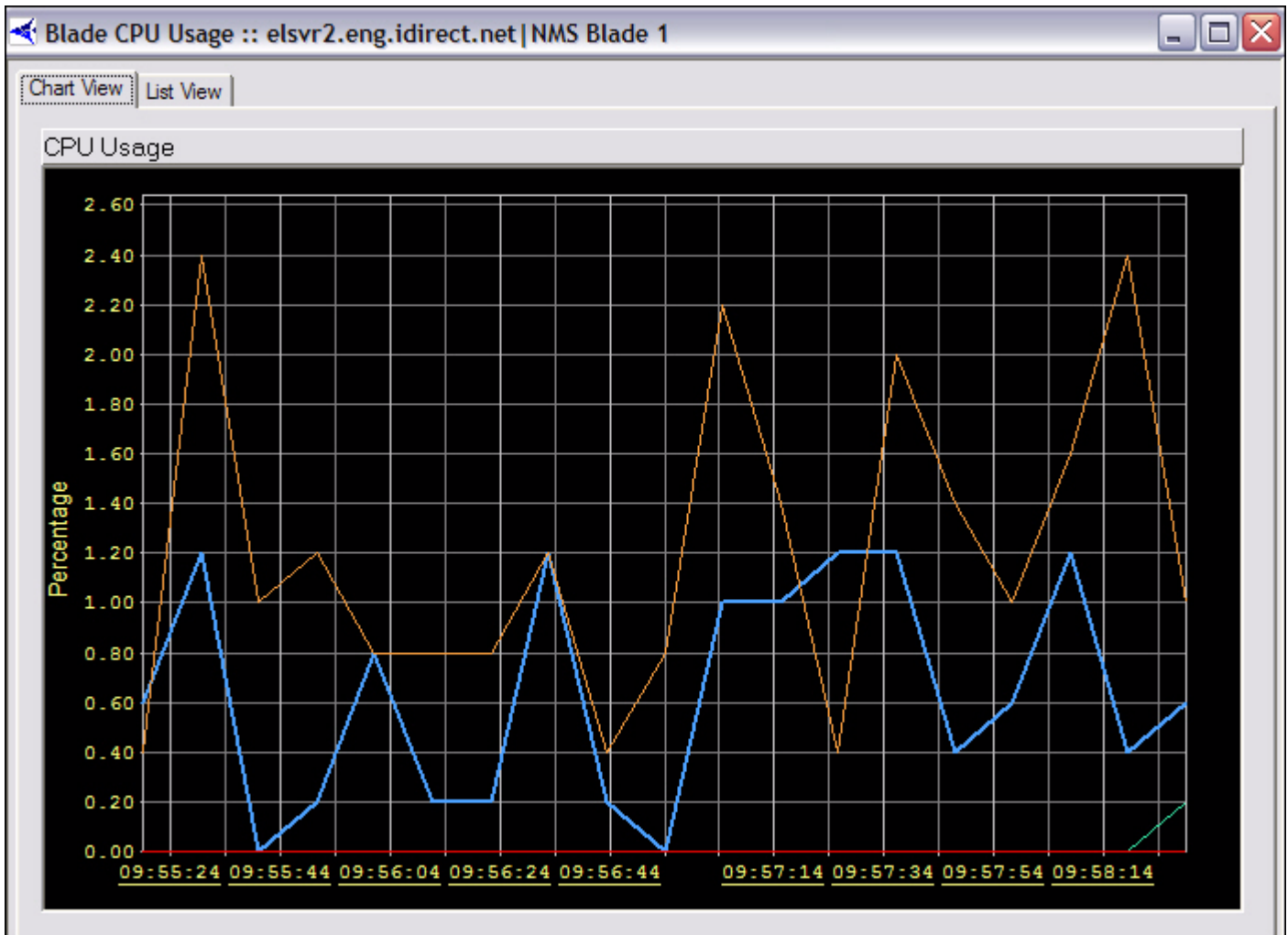
Remotes

All **Clear** **Active**

Name	Type-SN
<input type="checkbox"/> 5350-6913	5350.6913
<input type="checkbox"/> 5350-41521test	5350.41521
<input type="checkbox"/> 5300-4030	5300.4030
<input type="checkbox"/> New Remote #...	5350.0
<input type="checkbox"/> 7300.5972	7300.5972
<input type="checkbox"/> II+.9174	II+.9174
<input type="checkbox"/> II+.9162	5300.9162
<input type="checkbox"/> 3100NB.44055	3100-NB.44055
<input type="checkbox"/> Srao Remote [2...	5350.2012
<input type="checkbox"/> New Remote #...	II.0

OK **Cancel**

- Step 2 Select the blade for which you want to view information. Notice that the Line Cards and Remotes sections are unavailable for selection.



- Step 3 Click **List View** to view the data in multicolumn format.

The screenshot shows a window titled "Blade CPU Usage :: elsvr2.eng.idirect.net | NMS Blade 1". It has two tabs: "Chart View" and "List View", with "List View" selected. The window displays a table of CPU usage data with the following columns: Time, Date, User Time, System Time, IO Wait Time, Nice Time, and Total. The data is as follows:

Time	Date	User Time	System Time	IO Wait Time	Nice Time	Total
16:08:04	12/27/04	0.400	0.800	0.000	0.000	1.200
16:08:04	12/27/04	0.400	0.800	0.000	0.000	1.200
16:08:14	12/27/04	0.600	1.800	0.000	0.000	2.400
16:08:14	12/27/04	0.600	1.800	0.000	0.000	2.400
16:08:24	12/27/04	0.400	0.600	0.000	0.000	1.000
16:08:24	12/27/04	0.400	0.600	0.000	0.000	1.000
16:08:34	12/27/04	0.000	0.400	0.000	0.000	0.400
16:08:34	12/27/04	0.000	0.400	0.000	0.000	0.400
16:08:44	12/27/04	0.800	0.600	0.000	0.000	1.400
16:08:44	12/27/04	0.800	0.600	0.000	0.000	1.400
16:08:54	12/27/04	1.000	0.400	0.000	0.000	1.400
16:08:54	12/27/04	1.000	0.400	0.000	0.000	1.400
16:08:54	12/27/04	1.000	0.400	0.000	0.000	1.400
16:09:04	12/27/04	0.400	0.600	0.000	0.000	1.000
16:09:04	12/27/04	0.400	0.600	0.000	0.000	1.000
16:09:04	12/27/04	0.400	0.600	0.000	0.000	1.000
16:09:14	12/27/04	1.200	1.200	0.000	0.000	2.400
16:09:14	12/27/04	1.200	1.200	0.000	0.000	2.400
16:09:14	12/27/04	1.200	1.200	0.000	0.000	2.400
16:09:24	12/27/04	1.400	0.600	0.000	0.000	2.000
16:09:24	12/27/04	1.400	0.600	0.000	0.000	2.000
16:09:24	12/27/04	1.400	0.600	0.000	0.000	2.000
16:09:34	12/27/04	0.600	1.000	0.000	0.000	1.600
16:09:34	12/27/04	0.600	1.000	0.000	0.000	1.600
16:09:34	12/27/04	0.600	1.000	0.000	0.000	1.600
16:09:44	12/27/04	0.600	0.800	0.000	0.000	1.400
16:09:44	12/27/04	0.600	0.800	0.000	0.000	1.400
16:09:44	12/27/04	0.600	0.800	0.000	0.000	1.400

Step 4 You can also view limited CPU Usage information in list format on the **CPU Usage** tab by following the directions in [Section 4.1 "Monitoring Blades in iMonitor" on page 59](#).

4.4 Timeplan

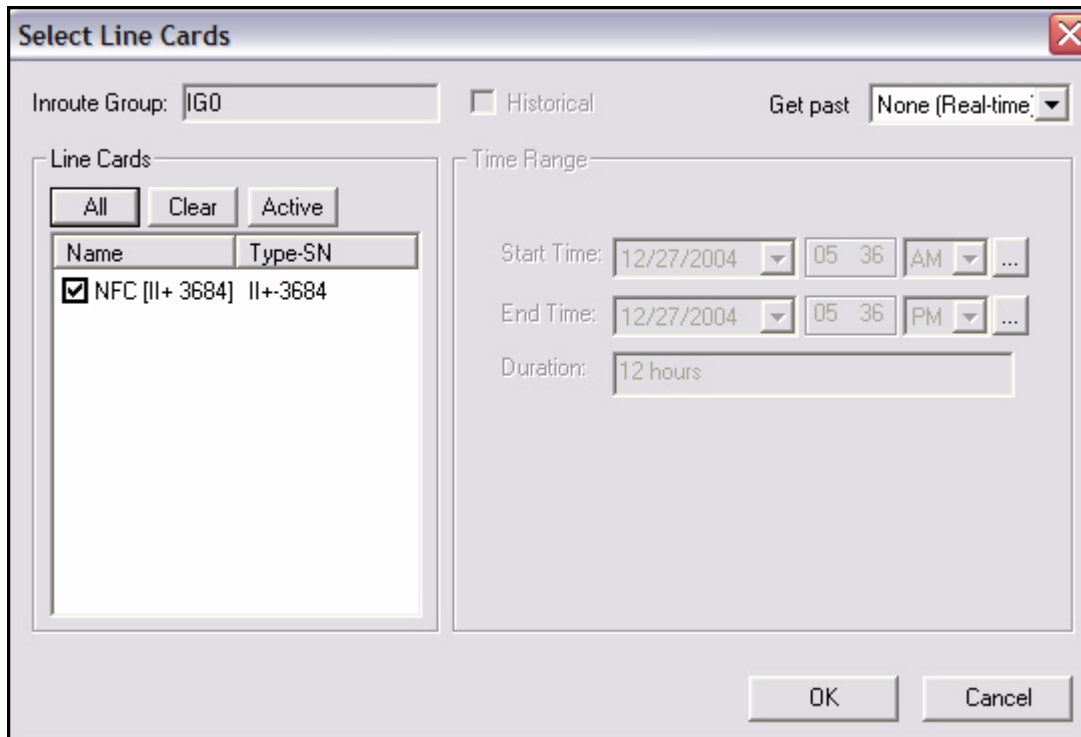
The Timeplan graph shows you the number of TDMA time slots allocated to each remote on an inroute, averaged over a one-second time period. This display provides an excellent glance at the relative "busy-ness" of the inroute and the remotes that are getting the most time slots. This display shows real-time data only; the NMS back-end does not archive Timeplan slot allocations.

The Timeplan display can be selected from:

- receive line cards
- inroute groups

To view Timeplan information, follow the directions below:

- Step 1 Right-click a receive line card or an inroute group.
- Step 2 Select **Time Plan** from the menu. If you selected an inroute group from the tree, the **Timeplan** graph will appear immediately. However, if you selected a receive line card from the tree, the **Select Line Cards** dialog box appears.



The "Select Line Cards" dialog box is shown. It has a title bar with a close button. Inside, there is a section for "Inroute Group:" with a text field containing "IG0". To the right of this is a checkbox labeled "Historical" which is unchecked. Further right is a "Get past" dropdown menu set to "None (Real-time)". Below the "Inroute Group:" section is a "Line Cards" section containing three buttons: "All", "Clear", and "Active". Below these buttons is a table with two columns: "Name" and "Type-SN". The table contains one row with a checked checkbox, the name "NFC [II+ 3684]", and the type "II+3684". To the right of the "Line Cards" section is a "Time Range" section. It contains three rows: "Start Time:" with a date dropdown set to "12/27/2004", a time dropdown set to "05 36", and an AM/PM dropdown set to "AM"; "End Time:" with a date dropdown set to "12/27/2004", a time dropdown set to "05 36", and an AM/PM dropdown set to "PM"; and "Duration:" with a text field containing "12 hours". At the bottom right of the dialog are "OK" and "Cancel" buttons.

- Step 3 Select the receive line cards or inroute groups for which you wish to view data. You can also select:
 - **All** to select all elements in the list
 - **Clear** to clear all elements in the list
 - **Active** to select only the active elements in the list.
- Step 4 Click **OK**.
- Step 5 The **Timeplan** graph appears.

Because the information in the display is specific to an individual inroute (i.e. line card), when you select multiple line cards from the inroute group level iMonitor launches a separate pane for each line card.

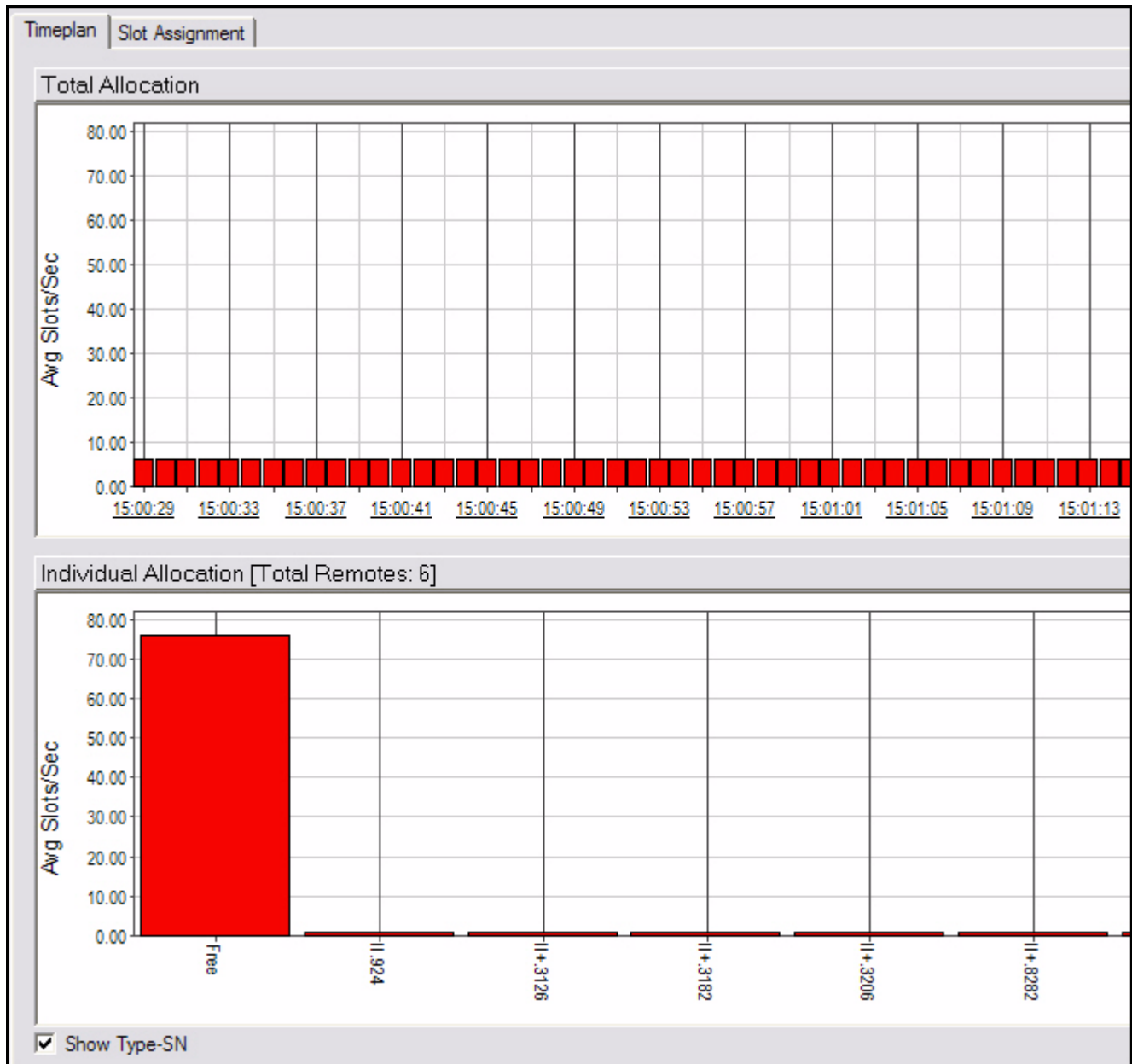
The graph is organized into two sections. The top section of the graph shows the total number of slots allocated across all remotes in the inroute. The Y-axis of this display is scaled to the total number of time slots available on this inroute. For each entry written to the top graph, the bottom

graph shows the slot allocation to each remote, along with the total number of unallocated (i.e. free) slots. Check the “Show Serial Numbers” box to toggle the display of remote name vs. serial number in the bottom graph.



NOTE



The graph does not show slots handed out via free-slot allocation; it only shows slots allocated based on remote demand.



Step 6 Click **Slot Assignment**.

- Step 7 The **Slot Assignment** multicolumn list appears. A second tab, labeled **Slot Assignment**, shows each raw timeplan message as it is sent to the remotes.

Pausing the Timeplan Graph and Highlighting Individual Entries

For convenience, and to study a particular section of the graph for an extended period of time, iMonitor allows you to pause the output of the Timeplan graph. On iMonitor's main tool bar, press the **Pause**  button to temporarily stop output. You may now click a particular entry in the top graph; the lower graph changes to reflect the allocation across remotes for that particular entry in the graph. Press the **Forward**  button to resume the display (no data is shown for the time period during which you were paused).

Timeplan		Slot Assignment		
Time	Total Slots	Allocated Slots	Free Slots	Slots Per Remote
15:03:34	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:34	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:34	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:34	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:34	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:34	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:34	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:34	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:35	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:35	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:35	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:35	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:35	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...
15:03:35	82.00	6.00	76.00	[463] : 1, [924] : 1, [3126] : 1, [3182] : 1, [3206...

4.5 Inroute Distribution

The Inroute Distribution display also shows timeplan slot allocation averaged over a 1-second interval, but in this case it is displayed in table format for *all* inroutes in an inroute group. This display is useful for displaying how slots are allocated across all inroutes in a group that is using Frequency Hopping. The display show data in real-time only; the NMS back-end does not archive timeplan slot allocations.

The Inroute distribution display can be selected from:

- networks
- inroute groups

Because the information in the display is specific to an individual inroute group, when you select multiple line cards from the network level iMonitor launches a separate pane for each inroute group in the network.

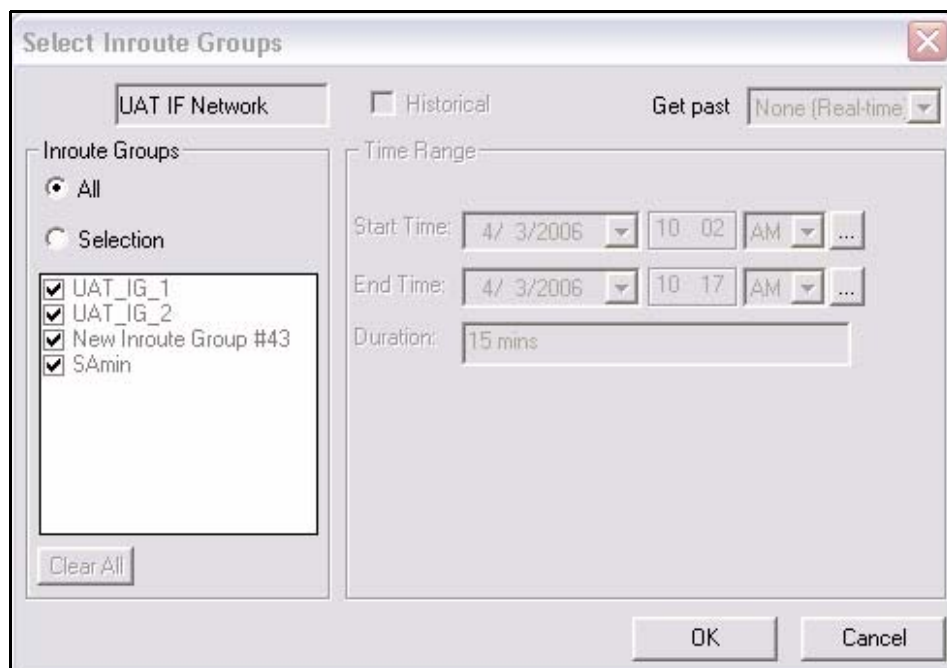
This display is organized into the following columns:

- Remote name and serial number
- Total slots allocated to this remote across ALL inroutes
 - The totals at the bottom show the total slots allocated to all remotes across all inroutes, the percentage of the total bandwidth this represents, and the total number of slots in all timeplans
 - For each inroute, the total number of slots allocated to each remote in the inroute
 - The totals at the bottom show the total slots allocated to all remotes in this inroute, the percentage of this inroute's bandwidth this represents, and the total number of slots in this timeplan

To view the inroute distribution, follow the directions below. The procedure is slightly different depending on whether you start by clicking on a network or directly on an inroute group:

Networks

- Step 1 Right-click a network in the Tree.
- Step 2 Click **Inroute Distribution**. The **Select Inroute Groups** dialog box appears. In the example below, this network has only one inroute group. However, a network may have many inroute groups listed.



- Step 3 Select the inroute groups for which you want to view data.
- Step 4 Click **OK**. The **Inroute Distribution** pane appears.

Remote Name	Type-SN	Total	Slots/frame	UAT IF [II+.6625] (I...)
Tysons Corner [4774] 5	II+.4774	1.00	1.00	1.00
Towson [4943] 2	II+.4943	1.00	1.00	1.00
iConnex [7064] 2	iConnex-R.7064	1.00	1.00	1.00
Leesburg [8406] 5	II+.8406	1.00	1.00	1.00
Lynchburg [8971]	II+.8971	1.00	1.00	1.00
Waldorf [8989] 4	II+.8989	1.00	1.00	1.00
Laurel [9177] 3	II+.9177	1.00	1.00	1.00
Total Allocated (%)		25.00 (96.15%)		25.00 (96.15%)
Maximum		26		26

Inroute Groups

- Step 1 Right-click an inroute group.
- Step 2 Click **Inroute Distribution**. The **Inroute Distribution** pane appears, as shown above.

Performing ACQ Bounce

The Inroute Distribution display allows you to perform the “ACQ Bounce” function for all remotes or selected remotes in the inroute group. This function is most useful if the inroute group is in Carrier Grooming mode, and due to a hub reset remotes are no longer evenly-distributed across the inroutes in the group. ACQ Bounce causes remotes to go through the acquisition process from scratch without resetting. It takes only a few seconds, and the Protocol Processor will re-distribute the remotes evenly across all inroutes.

To perform the ACQ Bounce function, select the remotes you want to bounce, launch the context menu with your right-mouse button, and select the ACQ Bounce option.

Remote Name	Type-SN	Total
Tysons Corner [4774] 5	II+.4774	1.00
Towson [4943] 2	II+.4943	1.00
iConnex [7064] 2	iConnex-R.7064	1.00
Leesburg [8406] 5	II+.8406	1.00
Lynchburg [8971]	II+.8971	1.00
Waldorf [8989] 4	II+.8989	1.00
Laurel [9177] 3	II+.9177	1.00
Total Allocated (%)		25.00 (96.15%)
Maximum		26

4.6 Latency

The NMS measures the round-trip time from the hub to each remote and back every five seconds. All values are available from iMonitor in real-time. Latency responses exceeding 800 msec. are available from the historical archive and are saved for one week by default. The Latency display can be selected from:

- networks
- inroute groups
- remotes

To view latency, follow the directions below:

Step 1 Right-click a network, inroute group, or remote in the Tree.

Step 2 Click **Latency**. The **Select Items** dialog box appears.

Select Items

☐ Historical **Time Range...** Get past **None (Real-time)**

☐ Save to **Lat_15_00_17.txt** **File**

Protocol Processors

Protocol Processor	Blade Name
<input type="checkbox"/> elsvr2.eng.idirect.net	<input type="checkbox"/> NMS Blade 1

Line Cards

All **Clear** **Active**

Name	Type-SN
<input type="checkbox"/> AFL [II+ 6656]	II+-6656
<input type="checkbox"/> AFC [II+ 3658]	II+-3658
<input type="checkbox"/> NFC [II+ 3684]	M1D1-3684

Remotes

All **Clear** **Active**

Name	Type-SN
<input checked="" type="checkbox"/> Buffalo [II+ 3224]	II+-3224
<input checked="" type="checkbox"/> Baltimore [II+ 3491]	II+-3491
<input checked="" type="checkbox"/> Tampa Bay [II 613]	II-613

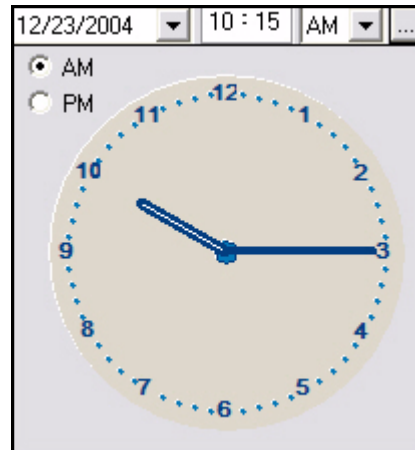
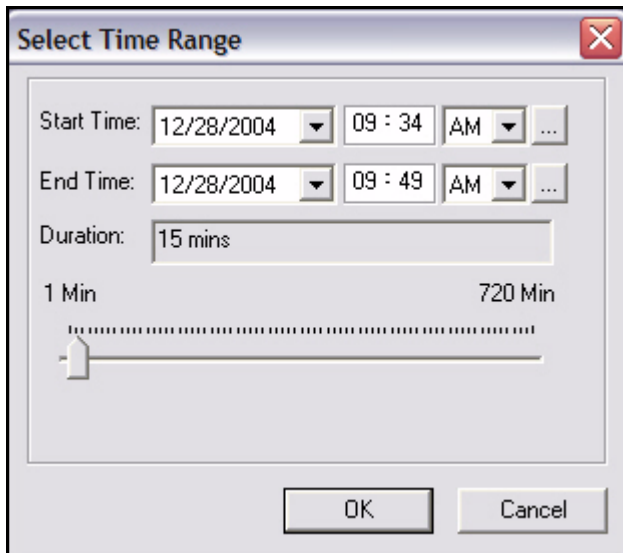
OK **Cancel**

Step 3 Select the remotes for which you want to view information. Notice that all but the Remotes section are unavailable for selection.

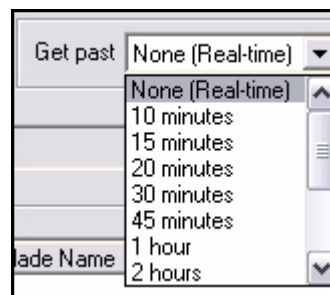
Step 4 Select either the **Historical** or the **Get Past check box**, or press **OK** to begin viewing latency in real-time.

- a If you select **Historical**, click **Time Range**. The **Select Time Range** dialog box appears (see below). If desired, click the ellipses next to the Start and End times to set the time via the graphical clock display. If you selected **Get Past**, see [Step b](#). (Note that historical latency reports will show only data for

latency timeouts. They will not show measurements that are below the threshold.)

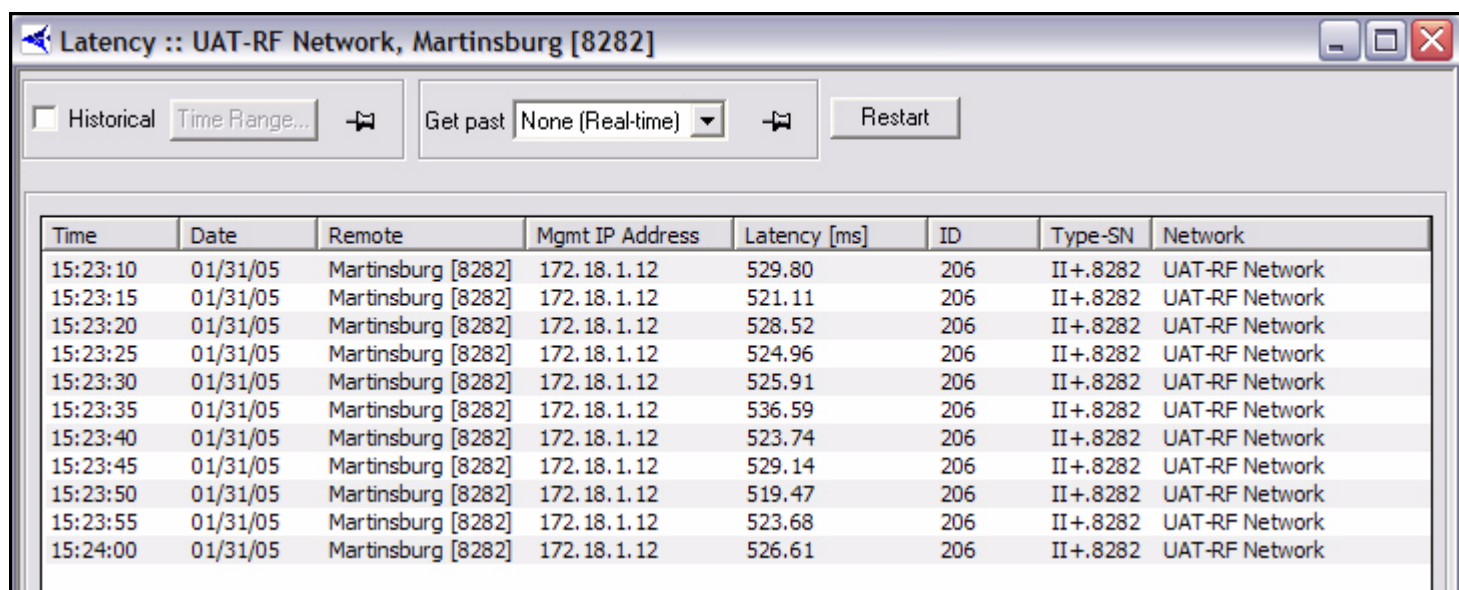


- b If you selected **Get Past**, the **Get Past** drop-down list appears. Select an interval of time.



Step 5 Click **OK**.

Step 6 The **Latency** pane appears, as shown below.



Time	Date	Remote	Mgmt IP Address	Latency [ms]	ID	Type-SN	Network
15:23:10	01/31/05	Martinsburg [8282]	172.18.1.12	529.80	206	II+.8282	UAT-RF Network
15:23:15	01/31/05	Martinsburg [8282]	172.18.1.12	521.11	206	II+.8282	UAT-RF Network
15:23:20	01/31/05	Martinsburg [8282]	172.18.1.12	528.52	206	II+.8282	UAT-RF Network
15:23:25	01/31/05	Martinsburg [8282]	172.18.1.12	524.96	206	II+.8282	UAT-RF Network
15:23:30	01/31/05	Martinsburg [8282]	172.18.1.12	525.91	206	II+.8282	UAT-RF Network
15:23:35	01/31/05	Martinsburg [8282]	172.18.1.12	536.59	206	II+.8282	UAT-RF Network
15:23:40	01/31/05	Martinsburg [8282]	172.18.1.12	523.74	206	II+.8282	UAT-RF Network
15:23:45	01/31/05	Martinsburg [8282]	172.18.1.12	529.14	206	II+.8282	UAT-RF Network
15:23:50	01/31/05	Martinsburg [8282]	172.18.1.12	519.47	206	II+.8282	UAT-RF Network
15:23:55	01/31/05	Martinsburg [8282]	172.18.1.12	523.68	206	II+.8282	UAT-RF Network
15:24:00	01/31/05	Martinsburg [8282]	172.18.1.12	526.61	206	II+.8282	UAT-RF Network

The NMS measures latency by sending an empty ICMP echo request and measuring the elapsed time until it receives a corresponding ICMP echo response from the remote. The round-trip time (RTT) is limit-checked by default; if the RTT is greater than two seconds, iMonitor will raise a Warning for this remote. Additionally, the receipt of the ICMP echo response is used to generate the layer 3 LATENCY Alarm, which indicates a potential IP problem. The NMS back-end generates this alarm if it misses three consecutive ICMP echo responses.



NOTE

Latency is measured from the NMS server; the latency results do not represent latency values from the remotes to arbitrary IP addresses on the public Internet.

As with all multicolumn lists, you may copy/paste multiple rows from the latency display into another Windows application such as Excel for further analysis.

4.7 Retrieving Information on Remotes using Probe Mesh

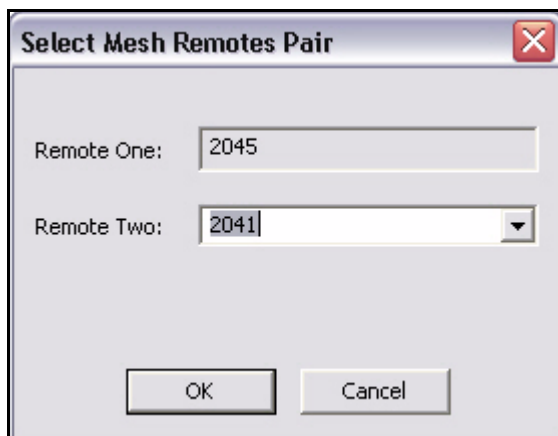
The **Probe Mesh** pane is available from the individual mesh remote nodes in the network tree view. It allows you to examine statistics on mesh communications between pairs of mesh remotes.

Specifically, **Probe Mesh** allows you select a pair of remotes and observe the following data for each:

- The number of attempts to transmit to the peer remote
- The number of bursts successfully transmitted to the peer remote
- The number of bursts received from the peer remote
- The number of bursts received from the peer remote that were dropped

To display the **Probe Mesh** pane:

- Step 1 Right-click on a mesh remote and click **Probe Mesh** to display the **Select Mesh Remotes Pair** dialog box.



The dialog box titled "Select Mesh Remotes Pair" has a close button (X) in the top right corner. It contains two input fields: "Remote One:" with the value "2045" and "Remote Two:" with a dropdown menu showing "2041". At the bottom are "OK" and "Cancel" buttons.

- Step 2 Select the peer remote from the **Remote Two** list and click **OK**. The **Probe Mesh** pane is displayed showing the information described above.

Mesh Info						Mesh Info					
From:		2045				From:		2041			
To:		2041				To:		2045			
Time	Date	Tx Attempts	Tx Bursts	Rx Bursts	Rx Dropped	Time	Date	Tx Attempts	Tx Bursts	Rx Burs	
14:42:31	01/19/06	0	0	0	0	14:42:16	01/19/06	0	0	0	
14:42:51	01/19/06	0	0	0	0	14:42:36	01/19/06	0	0	0	
14:43:11	01/19/06	0	0	0	0	14:42:56	01/19/06	0	0	0	
14:43:31	01/19/06	0	0	0	0	14:43:16	01/19/06	0	0	0	
14:43:51	01/19/06	0	0	0	0	14:43:36	01/19/06	0	0	0	
14:44:11	01/19/06	0	0	0	0	14:43:56	01/19/06	0	0	0	



NOTE

Probe Mesh is primarily intended for debugging. When **Probe Mesh** is enabled, the remotes send debug information to iMonitor. This increases the processing on the remotes and uses upstream bandwidth that could otherwise be used to send traffic.

4.8 Satellite Link Information

Satellite link information can be selected from:

- networks—Line Card Stats
- line cards—Line Card Stats
- remotes—SATCOM Graph and Remote Status/UCP

4.8.1 Line Card Statistics

The NMS collects hub line card statistics on a regular basis and saves them in the historical archive. iMonitor can display these stats either in real-time or from the archive. By default, the NMS saves line card statistics for one week.

The line cards statistics are available from the following nodes in the network tree view:

- Network
- Line Cards

Because the information in the display is specific to an individual line card, when you select multiple line cards from the network level, iMonitor launches a separate pane for each line card.

The line card statistics contain the following information for each line card. Note that some information will be blank depending on the role of the line card (Tx, Tx/Rx, Rx):

- Date/time the measurement was taken
- Name and serial number of the line card
- Attempted transmits during the time period
- Transmitted bytes during the time period
- Transmit errors
- Acquisition and Traffic CRC errors
- TDMA Bursts detected
- Received bytes
- Receive power in dBm
- Number of DMA resets (receive buffer overflow)
- PP line card tunnel receive errors
- PP line card tunnel transmit errors
- Receive digital gain
- FLL DAC
- SCPC loopback clear sky C/N
- SCPC loopback symbol offset
- SCPC loopback frequency offset

- TDM lock (locked or not locked)
- Number of times TDM lock was lost

To view line card statistics on networks and line cards, follow the directions below:

- Step 1 Right-click the network or line card for which you want to view line card status.
- If you selected **Line Card Stats** at the Network level, every line card in that network is displayed in the **Line Cards** box.
 - If you selected **Line Card Stats** on a particular line card, only that line card is displayed in the **Line Cards** box.
- Step 2 Click **Line Card Stats**. The **Select Items** dialog box appears.

Select Items

☐ Historical

☐ Save to

Protocol Processors

Protocol Processor	Blade Name	
<input checked="" type="checkbox"/> elsvr2.eng.indirect.net		<input type="button" value="All"/>
	<input type="checkbox"/> NMS Blade 1	<input type="button" value="Clear"/>

Line Cards

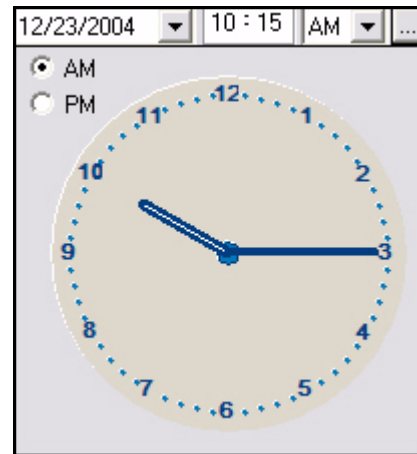
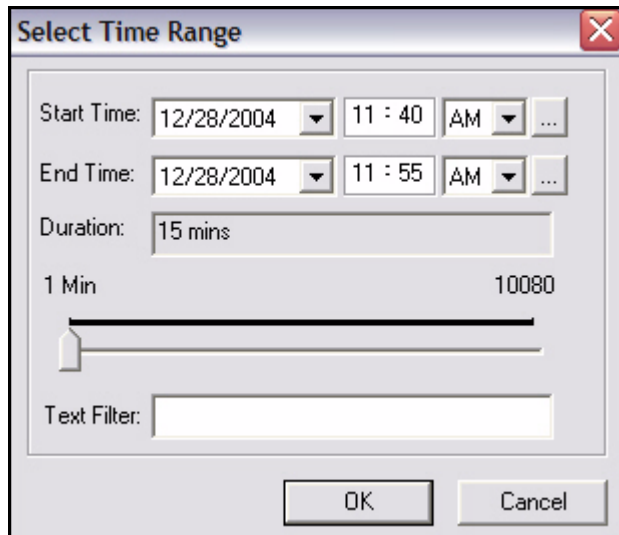
Name	Type-SN
<input checked="" type="checkbox"/> AFL [II+ 6656]	II+-6656
<input checked="" type="checkbox"/> AFC [II+ 3658]	II+-3658
<input checked="" type="checkbox"/> NFC [II+ 3684]	II+-3684

Remotes

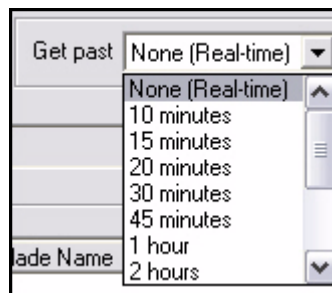
Name	Type-SN
<input type="checkbox"/> Buffalo [II+ 3224]	II+-3224
<input type="checkbox"/> Baltimore [II+ 3491]	II+-3491
<input type="checkbox"/> Tampa Bay [II 613]	II-613

Step 3 Click either **Historical** or **Get Past**, or click **OK** for real-time.

- a If you select **Historical**, click **Time Range**. The **Select Time Range** dialog box appears (see below). If desired, click the ellipses next to the Start and End times to set the time via the graphical clock display. If you selected **Get Past**, see [Step b](#).



- b If you click **Get Past**, the **Get Past** drop-down list appears.



Step 4 Select the line cards for which you want to view statistics, and click **OK**. The **Hub Stats** results pane appears.

Time	Date	Name	Type-SN	T.	T.	T.	A.	T.	Bursts	Rx Bytes	Rx Power [dBm]
15:20:20	12/29/04	Rx3 Hub [3097]	II+-3097	0	0	0	0	0	136	11152	-42.11
15:20:35	12/29/04	Rx3 Hub [3097]	II+-3097	0	0	0	0	0	135	11070	-42.11
15:20:50	12/29/04	Rx3 Hub [3097]	II+-3097	0	0	0	0	0	122	10004	-42.11
15:21:05	12/29/04	Rx3 Hub [3097]	II+-3097	0	0	0	0	0	130	10660	-42.11
15:21:20	12/29/04	Rx3 Hub [3097]	II+-3097	0	0	0	0	0	130	10660	-42.11
15:21:35	12/29/04	Rx3 Hub [3097]	II+-3097	0	0	0	0	0	113	9266	-42.11
15:21:50	12/29/04	Rx3 Hub [3097]	II+-3097	0	0	0	0	0	111	9102	-42.11

Identifying Remotes Causing Rx CRC Errors on iNFINITI Line Cards

Transmit problems on one or more remotes may cause CRC errors on the hub line card that is receiving the upstream carrier. CRC errors could be caused by any of a number of problems: a remote transmitting above the saturation point, a bad cable, interference, etc.

If the upstream carrier is being received by an iNFINITI line card, you can use the iDirect Rx CRC Correlation feature to identify which remote or remotes are causing the receive packet errors (Rx CRC errors) on the card.

See [Appendix D, Rx CRC Error Correlation](#) on [page 203](#) for details.

4.8.2 SATCOM Graph

The SATCOM display shows satellite link characteristics for an individual remote on the upstream and downstream channels, either in real-time or from the historical archive. This display is most useful for showing the relationships between hub-side uplink power control and remote transmit power. It also graphs the frequency and symbol offset calculations applied to the remote from the Protocol Processor.

The SATCOM display is available only from remotes. Because the information in the display is specific to an individual remote, when you select multiple remotes from an intermediate node, iMonitor launches a separate pane for each remote.

Remote Status and UCP Info

Remote Status messages come from the remote itself, while UCP messages come from the Protocol Processor during uplink control processing. Sometimes it is useful to see the actual raw data that is used to generate the graph. The remote status message contains a number of other pieces of information not shown in the graph. As with any multicolumn list, you may copy/paste multiple rows from these tabs into another Windows application, such as Excel, for further

processing. These real-time/historical displays show raw UCP and Remote Status information. This display allows you to request up to one week of UCP and Remote Status messages.

Display

You may adjust the default color settings on this display by selecting the **Properties** option from the context menu. Right-click anywhere inside the display to launch the menu.

Procedure for Viewing SATCOM Graph, Remote Status and UCP Info

To view the **SATCOM Graph**, **Remote Status**, or **UCP Info** on remotes, follow the directions below:

- Step 1 Right-click the remote for which you want to view information. Select **SATCOM Graph** or **Remote Status/UCP Info**. The **Select Items** dialog box appears. (You can also view this information on the remote Control Panel. See [Section 4.8.4 “Control Panel” on page 96.](#))

The 'Select Items' dialog box is shown with the following details:

- Historical:** ☐ **Time Range...** (button)
- Get past:** **None (Real-time)** (dropdown menu)
- Save to:** (text field) **File** (button)
- Protocol Processors:**

Protocol Processor	Blade Name
<input type="checkbox"/> UAT-RF Protocol Pro...	<input type="checkbox"/> RF Blade 1
- Line Cards:**

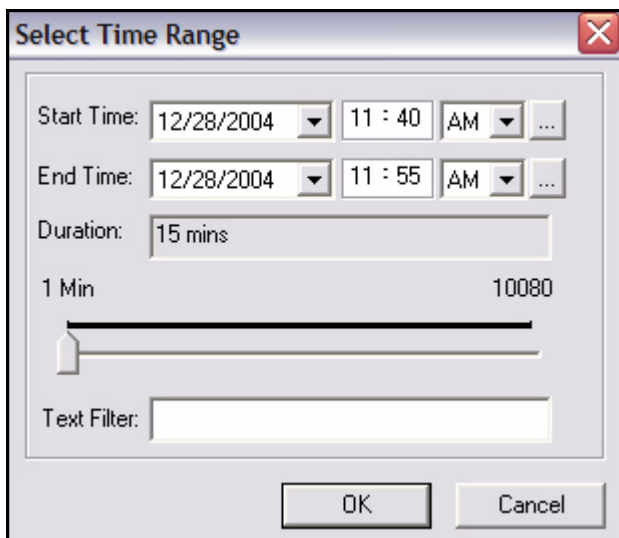
Name	Type-SN
<input type="checkbox"/> Phoenix Hub #...	M1D1.435
- Remotes:**

Name	Type-SN
<input checked="" type="checkbox"/> Martinsburg [82...	II+ 8282

OK **Cancel**

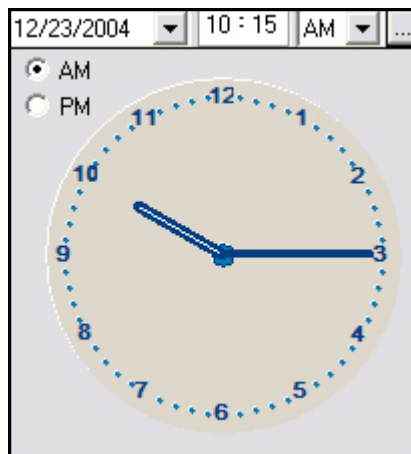
- Step 2 Click either **Historical** or **Get Past**, or **OK** for real-time.
- a If you select **Historical**, click **Time Range**. The **Select Time Range** dialog box appears (see below). If desired, click the ellipses next to the Start and End

times to set the time via the graphical clock display. If you selected **Get Past**, see [Step b](#).

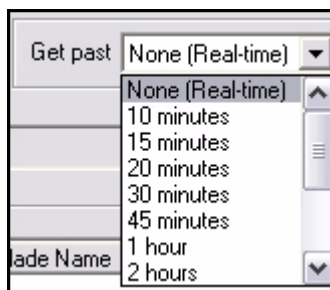


The 'Select Time Range' dialog box contains the following fields and controls:

- Start Time:** 12/28/2004, 11 : 40, AM, ...
- End Time:** 12/28/2004, 11 : 55, AM, ...
- Duration:** 15 mins
- 1 Min:** 10080
- Text Filter:** (empty text box)
- Buttons:** OK, Cancel



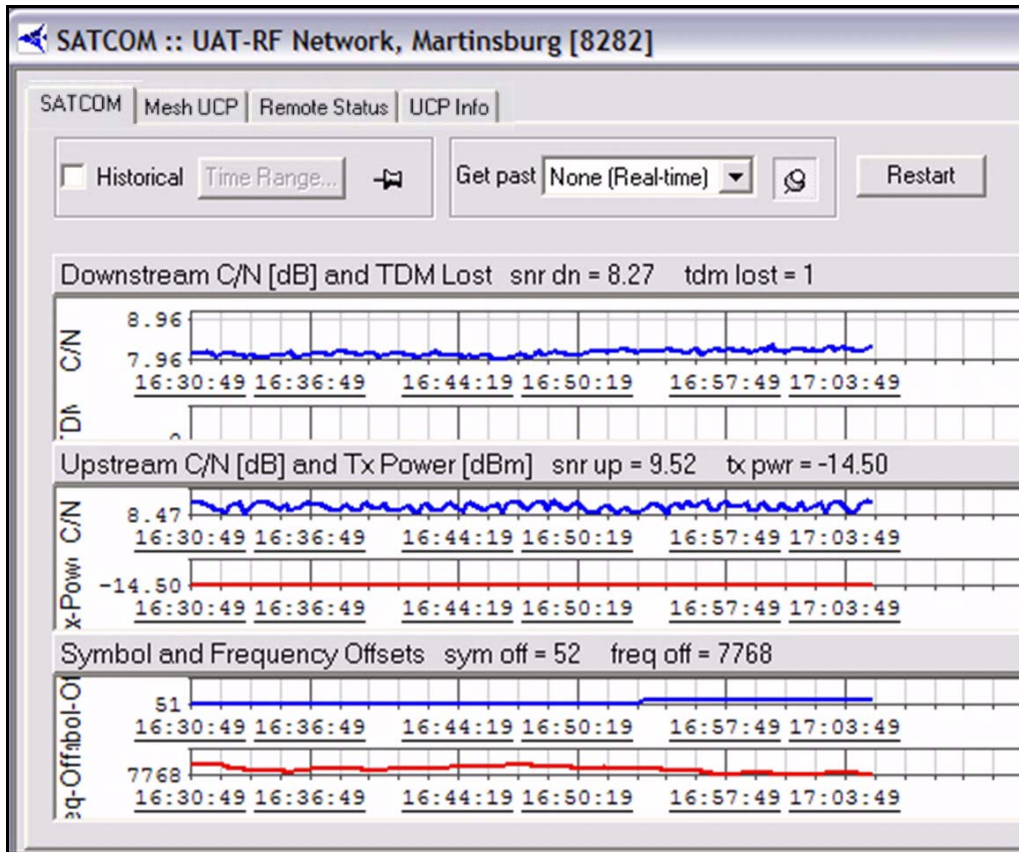
- b If you click **Get Past**, the **Get Past** drop-down list appears.



The 'Get Past' drop-down list shows the following options:

- None (Real-time)
- None (Real-time)
- 10 minutes
- 15 minutes
- 20 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 2 hours

The **SATCOM Graph** pane appears with four tabs. The Remote Status and UCP Info tabs contain the raw data used to draw the SATCOM graph. The **Mesh UCP** tab can be used to graph various Uplink Control parameters for a remote.



The figure above is an example of the SATCOM display. This example shows the most recent twenty minutes of data using the “Get Past” option of the parameters dialog box. The window is organized into three separate graphs. The displays show the following information:

- **Graph 1** – The downstream signal-to-noise ratio as perceived at the remote, superimposed on top of the number of times the remote has lost lock on the downstream carrier (TDM lost). The TDM lost value is cumulative since the remote was last powered-up, but this graph shows only deltas from message to message.
- **Graph 2** – The upstream signal-to-noise ratio as perceived at the hub, superimposed on top of the remote’s transmit power.
- **Graph 3** – The symbol and frequency offset values applied to the remote from the Protocol Processor as part of uplink control processing.

Each graph contains heading text that shows the last value received (either real-time or from the archive depending on the type of request). You may close any of the displays by clicking on the “X” in the upper-right corner of the graph.



NOTE

The maximum time range you may display in this pane is one hour. This limit includes both historical and real-time information.

Mesh UCP Tab

You can use the **Mesh UCP** tab to display graphs of hub-side and remote-side UCP information for a remote. There are three graphs in the Mesh UCP pane: **View 1**, **View 2** and **Tx Power**.

To view the **Mesh UCP** pane and select the parameters to view in each graph:

Step 1 Select the **Mesh UCP** tab to display the graphs.

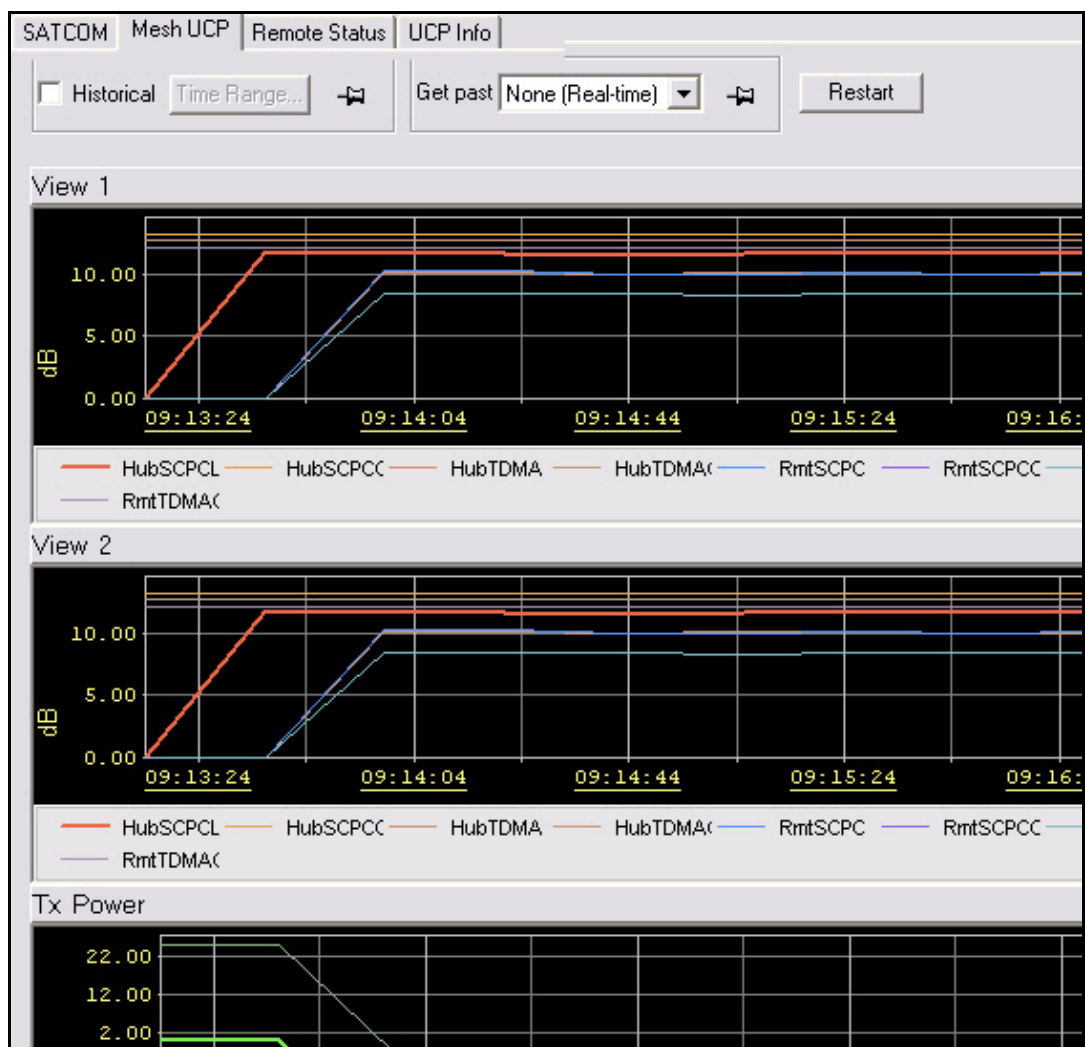
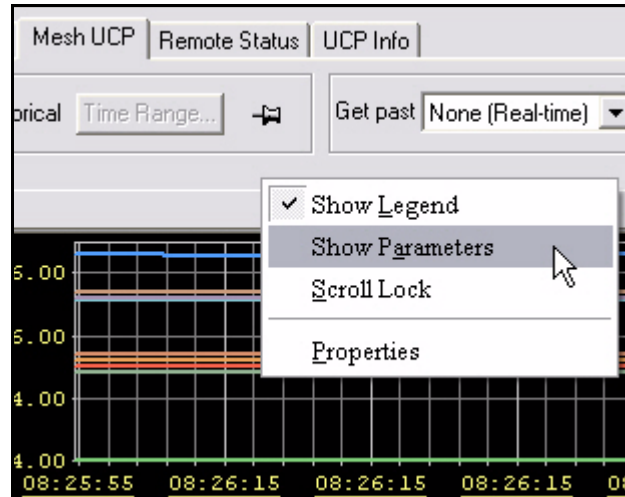


Figure 4-1: Mesh UCP Graph

- Step 2 Display the Parameters section of the screen by right-clicking anywhere in the **Mesh UCP** pane and selecting **Show Parameters** from the menu.



- Step 3 In the Parameters section, select the parameters you want to display in the three graphs. (Parameter selection and parameter definitions are discussed in detail in the next two sections.)

Interval <input checked="" type="radio"/> Seconds <input type="radio"/> Minutes <input type="radio"/> Hours	Hub-Side Information <input checked="" type="checkbox"/> SCPC C/N (Loopback) <input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> SCPC Clear Sky C/N <input type="checkbox"/> None <input checked="" type="checkbox"/> TDMA C/N <input checked="" type="checkbox"/> TDMA Clear Sky C/N	Remote-Side Information <input checked="" type="checkbox"/> SCPC C/N <input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> SCPC Clear Sky C/N <input type="checkbox"/> None <input checked="" type="checkbox"/> TDMA C/N (Loopback) <input checked="" type="checkbox"/> TDMA Clear Sky C/N	Show <input checked="" type="checkbox"/> All (View 1 and View 2) <input type="checkbox"/> None (View 1 and View 2) <input checked="" type="checkbox"/> SCPC <input checked="" type="checkbox"/> TDMA	Tx Power <input checked="" type="checkbox"/> Tx Power <input checked="" type="checkbox"/> Init Tx Power <input checked="" type="checkbox"/> Tx Power <input type="checkbox"/> Init Tx Power
---	--	---	---	--

Selecting Parameters in the Mesh UCP Tab

The following rules apply when you select or clear the various parameter check boxes:

- For parameters with two check boxes:
 - Selecting the first check box causes the parameter to be displayed in **View 1**.
 - Selecting the second check box causes the parameter to be displayed in **View 2**.
- For Hub-Side and Remote-Side Information, you can select individual parameters, or you can select the parameter group using the **All** or **None** check boxes.
- The **Show** area of the pane allows you to select or clear groups of parameters in both views as follows:
 - Selecting **All (View 1 and 2)** causes all parameters to be displayed in both views.
 - Selecting **None (View 1 and 2)** causes all parameters to be cleared from both views.
 - Selecting or clearing the two **SCPC** check boxes controls the display of all SCPC parameters in **View 1** and **View 2** as a group.
 - Selecting or clearing the two **TDMA** check boxes controls the display of all TDMA parameters in **View 1** and **View 2** as a group.

- The **Tx Power** area of the pane allows you to select which of the transmit power parameters are displayed in the **Tx Power** graph.

Mesh UCP Parameter Definitions

In the **View 1** and **View 2** graphs, you can view UCP parameters for both the downstream SCPC carrier and for the remote's TDMA mesh carrier.

The first two parameters under **Hub Side Information** show the hub's values for the SCPC carrier:

- **SCPC C/N (Loopback)** is the current C/N value for the downstream SCPC carrier as measured by the hub line card.
- **SCPC Clear Sky C/N** is the C/N of the loopback SCPC carrier set during hub commissioning.

The second two parameters under **Hub Side Information** show the hub's values for the TDMA mesh carrier used by this remote:

- **TDMA C/N** is the current C/N value for the remote's TDMA mesh carrier as measured by the hub line card.
- **TDMA Clear Sky C/N** is the C/N of the remote's TDMA mesh carrier set during hub commissioning.

The first two parameters under **Remote Side Information** show the remote's values for the SCPC carrier:

- **SCPC C/N** is the current C/N value for the downstream SCPC carrier as measured by the remote modem.
- **SCPC Clear Sky C/N** is the C/N of the downstream SCPC carrier set during remote commissioning.

The second two parameters under **Remote Side Information** show the remote's values for the TDMA mesh carrier:

- **TDMA C/N** is the current C/N value for the remote's TDMA mesh carrier as measured by the remote modem.
- **TDMA Clear Sky C/N** is the C/N of the loopback TDMA mesh carrier set during remote commissioning.

In the **Tx Power** graph you can view the following transmit power parameters for the remote:

- **Tx Power** is the current transmit power setting for the remote.
- **Init Tx Power** is the initial transmit power for the remote set during remote commissioning.
- **Tx Power – Init Tx Power** shows the difference between the first two parameters

Remote Status and UCP Info Tabs

The **Remote Status** data and **UCP Info** are displayed in the two figures below.

SATCOM :: NMS Network, Baltimore [II+ 3491] [12/28/04 12:20:47]

Time range: 12/28/04 12:20:47

SATCOM | Mesh UCP | Remote Status | UCP Info

Time	Date	Dow...	Tx P...	Rx P...	Digit...	FL...	Rx...	Te...	TD...	SC...
12:...	12...	10.28	-25.00	-28.95	17.30	0x...	-40	66...	4	0
12:...	12...	10.36	-25.00	-28.95	17.30	0x...	-331	66...	4	0
12:...	12...	10.42	-25.00	-28.95	17.48	0x...	711	66...	4	0
12:...	12...	10.35	-25.00	-28.95	17.68	0x...	845	66...	4	0
12:...	12...	10.31	-25.00	-28.95	17.12	0x...	-452	66...	4	0
12:...	12...	10.35	-25.00	-28.95	17.12	0x...	-278	66...	4	0
12:...	12...	10.34	-25.00	-28.95	17.30	0x...	-292	66...	4	0

Figure 4-2: Remote Status Raw Data

SATCOM :: NMS Network, Baltimore [II+ 3491] [12/28/04 12:20:47]

Time range: 12/28/04 12:20:44

SATCOM | Mesh UCP | Remote Status | UCP Info

Time	Date	Up C/N [dB]	Power Adjustment [d...	Symbol Offset	Freq Offset [Hz]
12:36:10	12/28/04	9.59	0.0	8	943
12:36:25	12/28/04	9.58	0.0	8	968
12:36:40	12/28/04	9.58	0.0	8	968
12:36:55	12/28/04	9.60	0.0	8	960
12:37:10	12/28/04	9.59	0.0	8	955
12:37:25	12/28/04	9.59	0.0	8	942
12:37:40	12/28/04	9.59	0.0	8	942
12:37:55	12/28/04	9.60	0.0	8	974
12:38:10	12/28/04	9.55	0.0	8	960
12:38:25	12/28/04	9.57	0.0	8	943
12:38:40	12/28/04	9.57	0.0	8	943
12:38:55	12/28/04	9.55	0.0	8	963
12:39:10	12/28/04	9.54	0.0	8	956

Figure 4-3: UCP Info Raw Data

4.8.3 Group QoS Statistics

You can view the following real-time or historical Group QoS Statistics in iMonitor:

- Upstream QoS statistics for QoS groups and subgroups for any Inroute Group
- Upstream QoS statistics for individual remotes or for specific applications running on individual remotes
- Downstream QoS statistics for QoS groups and subgroups for any Network



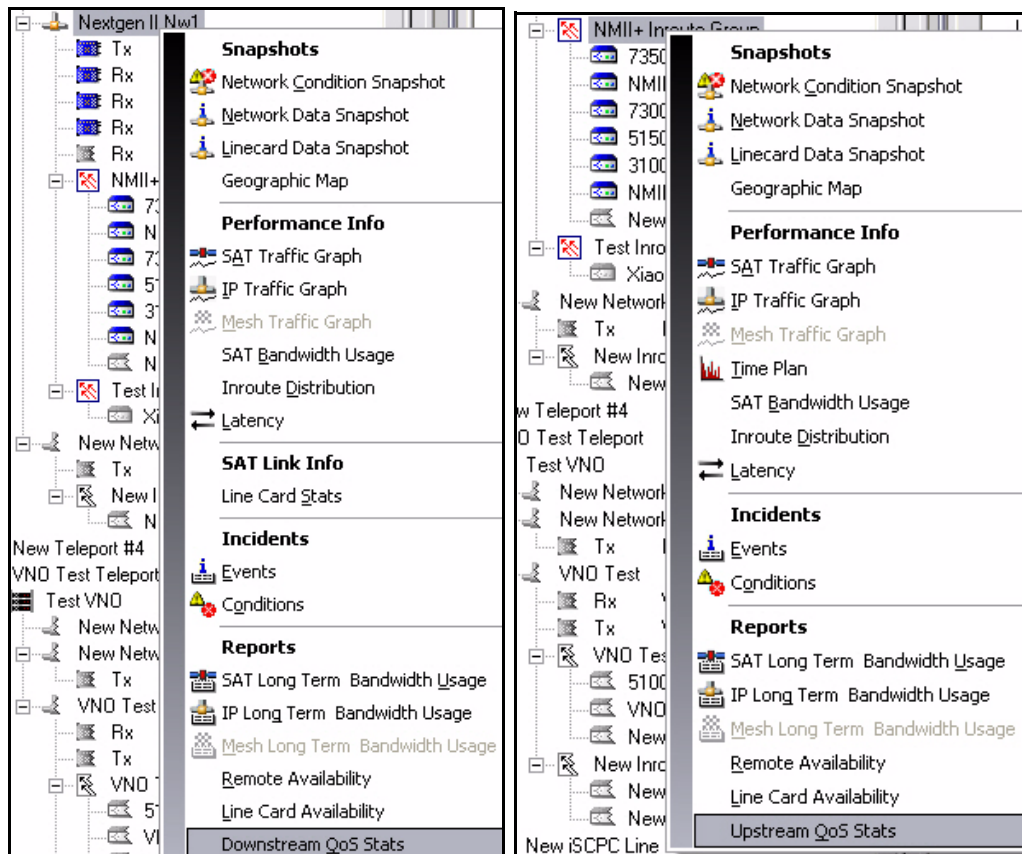
NOTE

If the GQoS configuration has changed, then historical GQoS statistics that were logged under the previous configuration will not be displayed.

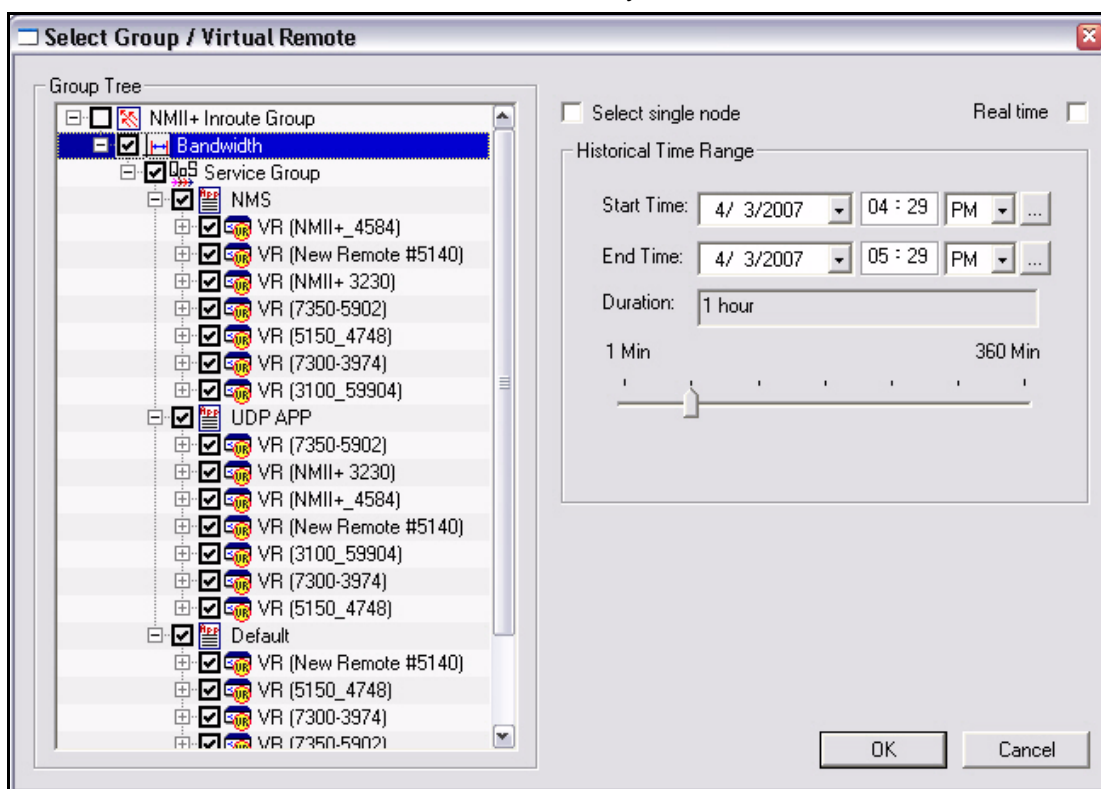
Viewing QoS Statistics

Step 1 To view QoS statistics, do one of the following:

- Right-click your Network in the iMonitor tree and select **Downstream QoS Stats** from the menu, or
- Right-click an Inroute Group or Remote in the iMonitor tree and select **Upstream QoS Stats** from the menu.

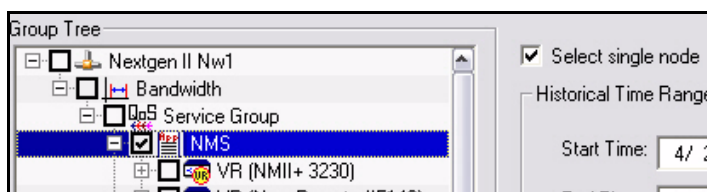


- Step 2 In the **Group Tree** pane of the **Select Group** dialog box, select an element in the tree over which you want to aggregate the Group QoS statistics. Sub-elements will be automatically selected.

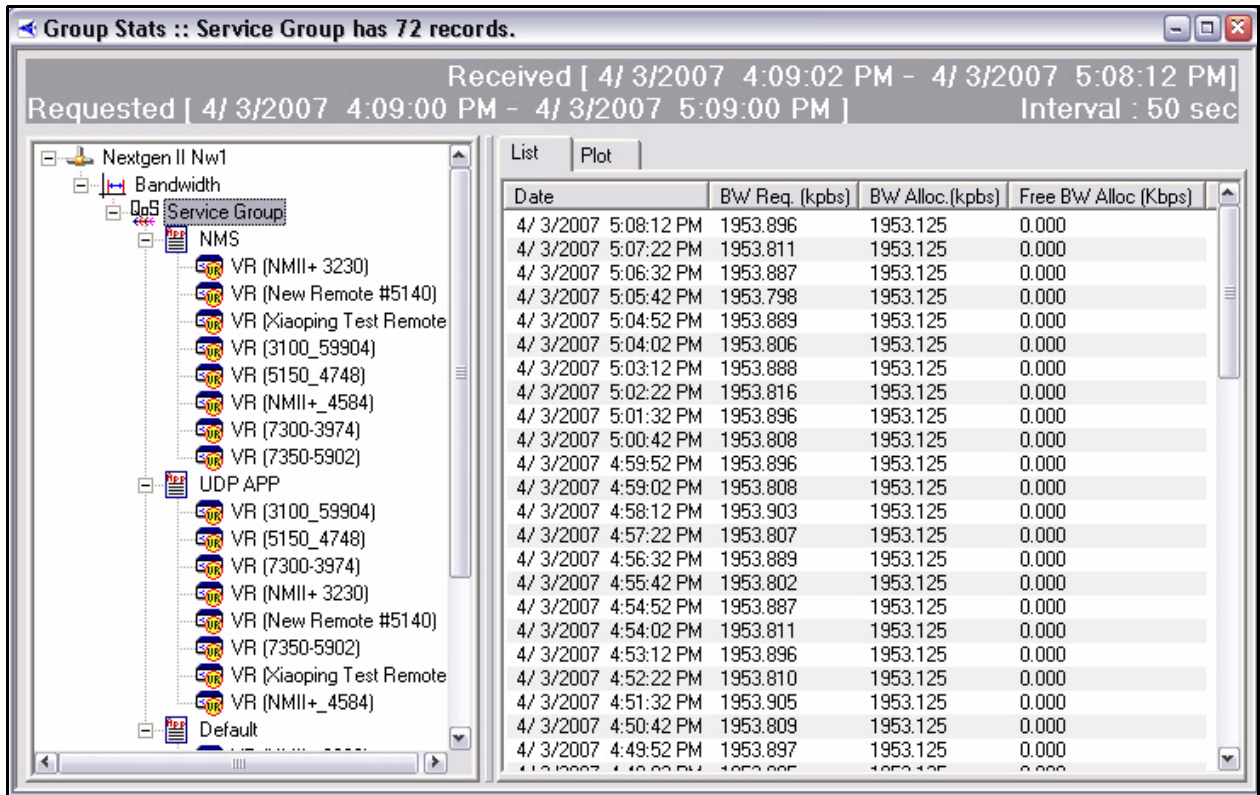


NOTE

Checking **Select single node** allows you to select an individual element in the **Group Tree** pane. This is illustrated below.



Step 3 Select **Real time**, or enter a **Start Time**, **End Time** and **Duration**. Then click **OK** to view the **Group Stats** display.



Step 4 By selecting elements at different levels of the tree in the left-hand pane, you can control the aggregation of the statistics displayed in the **List** and **Plot** tabs of the right-hand pane. The example above shows the total statistics aggregated over the selected **Service Group**.

The following statistics are displayed in the **List** tab in the right-hand pane of the **Group Stats** display:

- **BW Req** shows the total bandwidth requested by the selected subgroup
- **BW Alloc** shows the total bandwidth allocated by the selected subgroup
- **Free BW Alloc** shows the number of slots allocated to the remote in excess of the requested bandwidth.



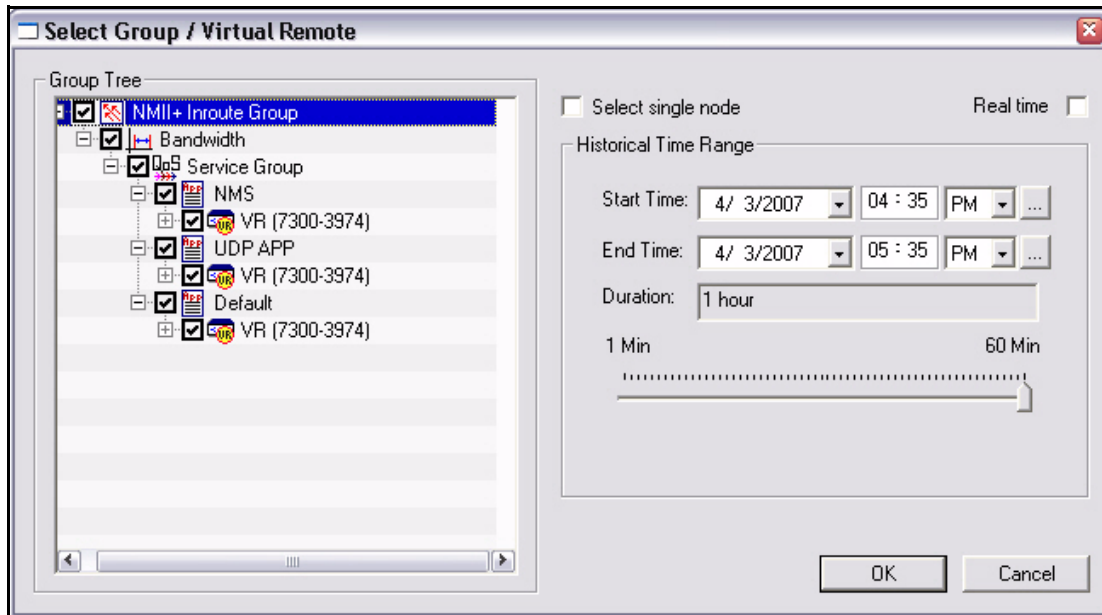
NOTE

The **BW Req** column only displays correct data when congestion is not present.

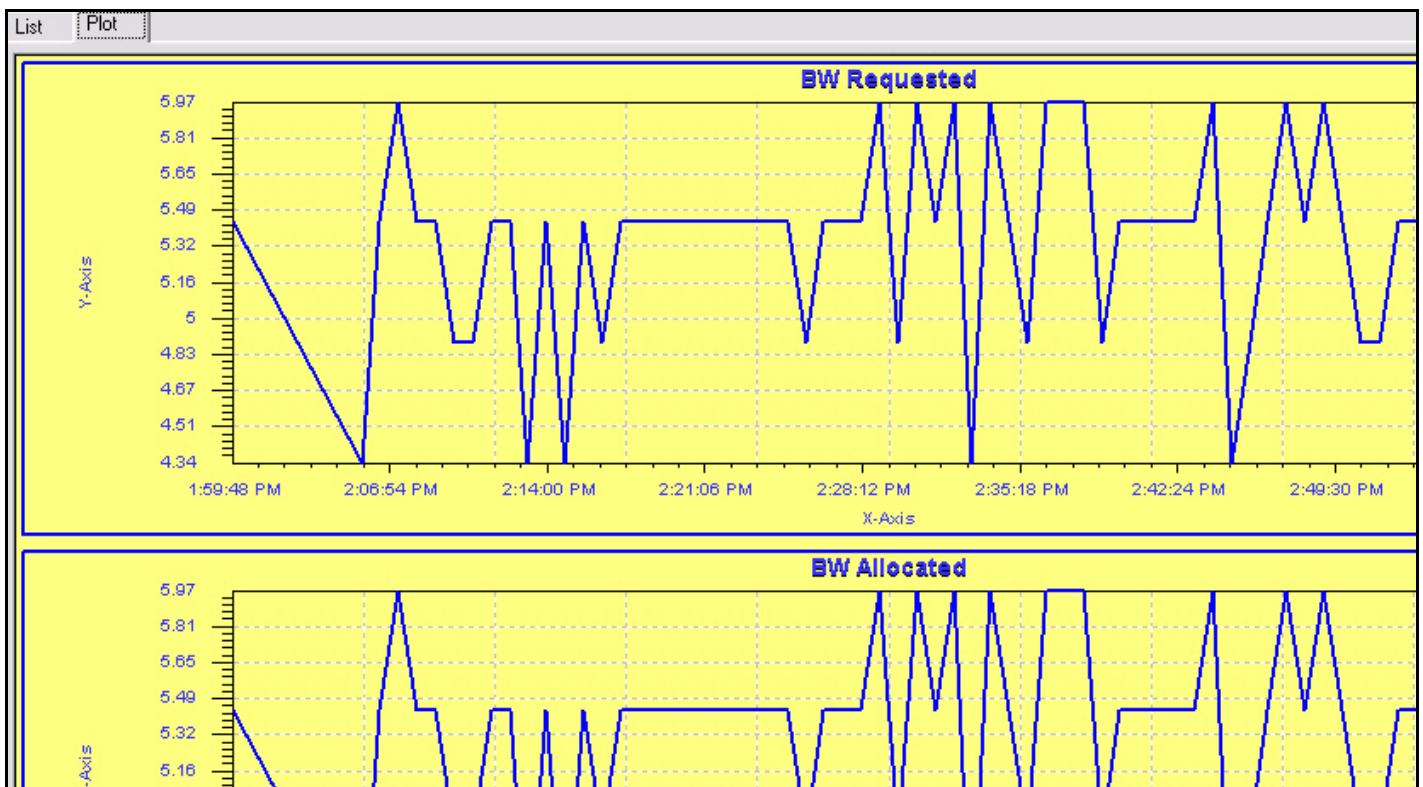


NOTE

When you right-click on a remote and select **Upstream QoS Stats** from the menu, you can view all the QoS statistics for a single remote. The **Select Group** dialog box for a single remote is shown below.



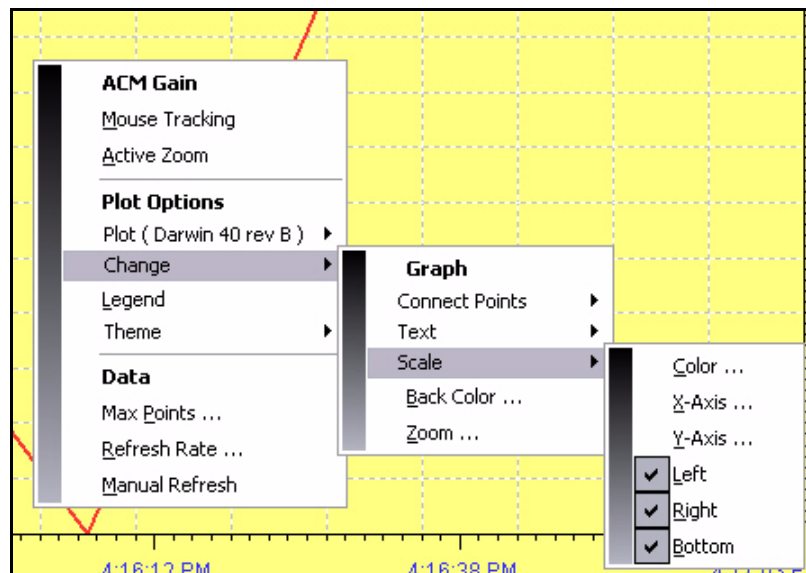
Step 5 Click the **Plot** tab to view a graphical representation of the data on the **List** tab. By default, three graphs appear: BW Requested, BW Allocated and BW Free.



- Step 6 You can right-click anywhere in the plot area and highlight **Select Graph** to view or hide any of the three graphs.



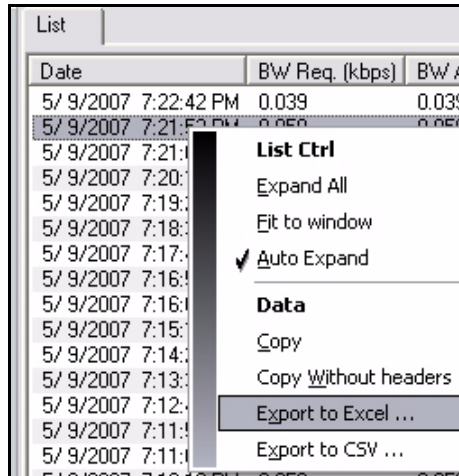
You can also use the right-click menu to change the display. For example, you can select **Change→Scale** to modify the scales of the X axis or Y axis; select **Legend** to display or hide the legend; or **Change** the background (**Back Color**) or **Text** color. If you select **Mouse Tracking**, you can click and drag along the plot line to view the value of each data point.



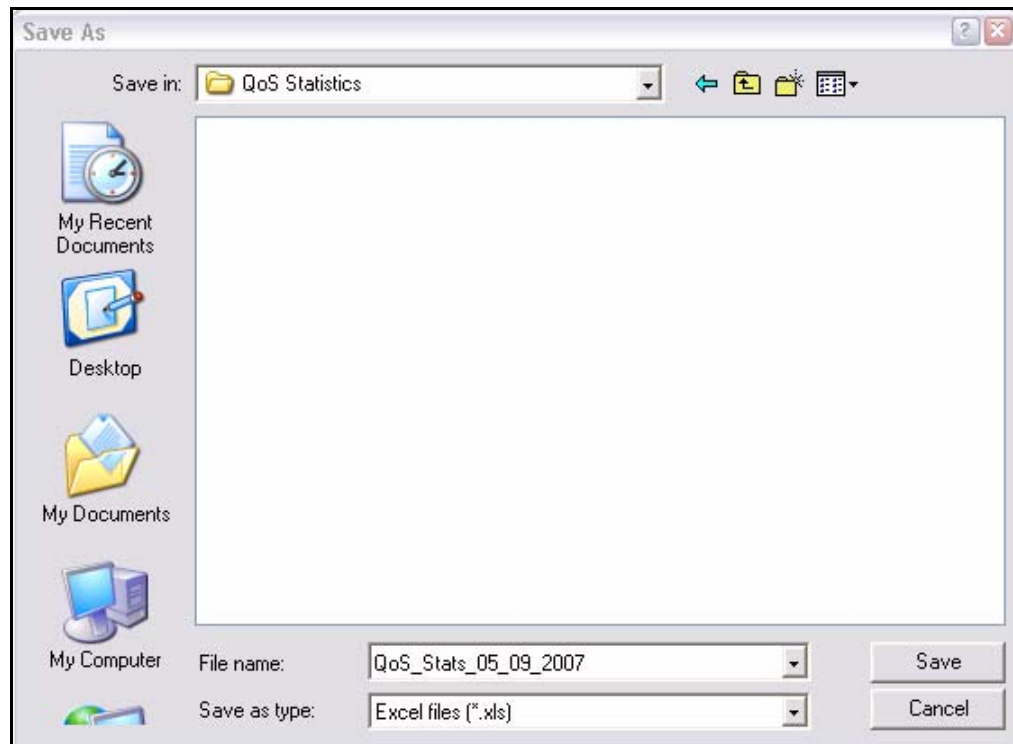
Saving QoS Statistics to an Excel Spreadsheet or to a CSV Formatted File

You can export the Group QoS statistics from the **Group Stats List** tab to an Excel spreadsheet or to Comma Separated Variable (CSV) formatted file by following these steps:

- Step 1 Right-click in the display area of the **List** tab and select **Export to Excel** or **Export to CSV** from the menu.



- Step 2 In the **Save As** dialog box, browse to the folder in which you want to save the statistics. Then enter a **File Name** and click **Save**.



4.8.4 Control Panel

The Control Panel is available only on remotes. It provides “everything you ever wanted to know about a remote” in a single, multi-tabbed display. You can view configuration information, SATCOM information, IP and satellite traffic statistics, Probe, QoS settings, latency, and events/conditions simply by clicking from tab to tab in this single pane.

The Control Panel is available only from individual remotes in the network tree view. Additionally, you may have only four Control Panel panes launched at the same time.

When you launch the Control Panel it automatically requests real-time data for each tab in the pane; you may also request historical data for any tab in the pane using the Historical or Get Past tools at the top of each tab.

The **Control Panel** is organized into the following tabs:

- **General** – contains configuration information organized into functional areas, and a real-time summary in the lower-left corner that updates in real-time as long as you keep the pane open.
- **Events/Conditions** – shows events and conditions in real-time or for the specified time period. When you re-submit requests, you may select only events or only conditions by selecting the appropriate entry in the “List” drop-down box.
- **SATCOM** – Identical to the individual SATCOM pane, except this pane shows only the graph, not the raw data behind it.
- **Mesh UCP** – Identical to the **Mesh UCP** tab on the SATCOM graph. (See [“Mesh UCP Tab” on page 86.](#))
- **IP Traffic** – shows IP statistics on the downstream and/or upstream for this remote.
- **SAT Traffic** – shows satellite traffic statistics on the down/up for this remote.
- **Probe** – a Probe pane for this remote.
- **Remote Status** and **UCP Info** – these two tabs are not tied to the Control Panel’s SATCOM display. They provide a means for retrieving these messages over a longer period of time than can be shown in the SATCOM graph. A real-time/historical display shows raw UCP and Remote Status information. This display allows you to request up to one week of UCP and Remote Status messages.
- **Latency** – a latency pane for this remote.
- **QoS** – displays the current QoS profile settings for this remote.

Below are two examples of the many tabs of information accessible from a remote’s control panel.

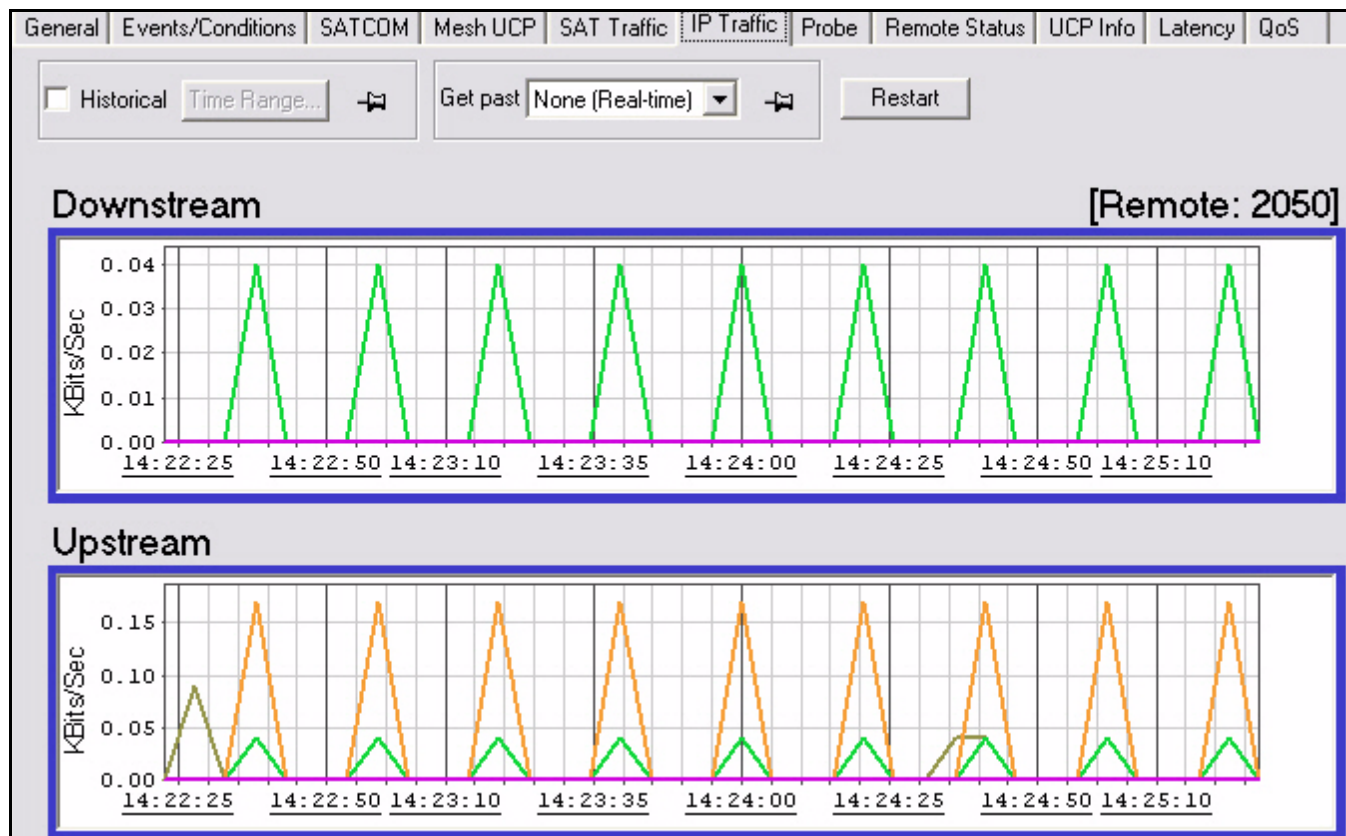
General Events/Conditions SATCOM Mesh UCP SAT Traffic IP Traffic Probe Remote Status UCP Info Latency QoS

Information	
Name	2045
ID	691
Type-SN	5350.2045
Derived ID	6817789
LAN IP Address	172.25.34.9
LAN Subnet Mask	255.255.255.0
LAN Gateway	
Mgmt IP Address	172.25.33.9
Mgmt Subnet Mask	255.255.255.248
Max Power	
Initial Power	
Max Downstream T	

Link Configuration	
Spacecraft	mvinjamuri
Downstream Transponder	mvinjamuri
Downstream Bandwidth	mvinjamuri
Downstream Carrier	1400 Down Stream Car...
Upstream Transponder	mvinjamuri
Upstream Bandwidth	mvinjamuri
Upstream Carriers	

Real-Time Summary	
Avg Downstream C/N	
Avg Upstream C/N	
Avg Tx Pwr	
Avg Temp	
TDM Lost	

VSAT Information	
Approx. Cable Length	0.000000
BUC	Bench Test BUC (I/F)
LNB	Bench Test LNB (I/F)
Reflector	
Reflector Mount	



4.9 Connecting to Network Elements

You can access the **Connect** option from the **Action** section of any of the following elements' menus:

- Protocol Processor
- Blade
- Line Card
- Remote (also accessible from a remote's **Probe** dialog box)

The Connect command opens a PuTTY telnet session to the selected element for detailed anomaly investigation. Please contact iDirect's Technical Assistance Center for further information on using system consoles.

Examining IP Routing and HDLC Information on Remotes

You can view the following IP Routing and HDLC information after connecting to a remote:

- The IP routing table currently loaded on the remote
- MAC and IP addresses for all remotes in the remote's inroute group.

To examine this data on a remote, follow these steps:

- Step 1 Right-click the remote in the iMonitor network tree and select **Connect** from the context menu.
- Step 2 When the **PuTTY** window appears, log in with **Username: admin**.
- Step 3 You can enter the following commands to view the IP and HDLC information:
 - **ip table** displays the IP routing table on the remote. In the **Flags** column for any remote IP address:
 - An **S+** indicates star routing (i.e., all transmissions pass through the hub).
 - An **M+** indicates that mesh routing is in effect between this remote and other mesh remotes in the inroute group.
 - **rmtarp** displays the MAC and IP addresses for all remotes in this remote's inroute group. This does not include the remote you are connected to.
 - **11 hdlc** shows the HDLC address of this remote.

These commands are illustrated in the example below.

```
Telnet 172.18.144.1
Username: admin
Password: *****

[RMt:6913] admin@telnet:10.0.50.61;1781
>

[RMt:6913] admin@telnet:10.0.50.61;1781
> ip table
VLAN Network          Netmask          NextHop          Interface Cost  TTL  Flags
1 0.0.0.0              0.0.0.0          0.0.0.0          sat0      2   N/A  (S+)
1 172.18.49.0          255.255.255.0    172.18.144.6     sat0      2   77   (M+)
1 172.18.51.0          255.255.255.0    172.18.144.3     sat0      2   77   (M+)
1 172.18.144.0         255.255.255.0    0.0.0.0          sat0      2   N/A  (A+)
1 172.18.144.1         255.255.255.255  172.18.144.1     int1      2   N/A  (A+)
1 172.18.144.3         255.255.255.255  172.18.144.3     sat0      2   77   (M+)
1 172.18.144.6         255.255.255.255  172.18.144.6     sat0      2   77   (M+)
1 172.18.145.0         255.255.255.248  0.0.0.0          ixp1      2   N/A  (A+)
1 172.18.145.1         255.255.255.255  172.18.145.1     int0      2   N/A  (A+)
1 172.18.145.16        255.255.255.248  172.18.144.3     sat0      2   77   (M+)
1 172.18.145.40        255.255.255.248  172.18.144.6     sat0      2   77   (M+)

[RMt:6913] admin@telnet:10.0.50.61;1781
> rmtarp
      HDLC      VLAN      IP Address      TTL
      1002      1       172.18.144.3     3
      1004      1       172.18.144.6     3

[RMt:6913] admin@telnet:10.0.50.61;1781
> ll hdlc
HDLC Address: 0x03EB  (1003)

[RMt:6913] admin@telnet:10.0.50.61;1781
>
```

4.10 Monitoring Your Bandwidth with SkyMonitor

SkyMonitor is an iDirect digital spectrum analyzer that is fully integrated with the NMS. You can use a SkyMonitor unit to view your iDirect carriers, or to view other carriers present at your hub. Each SkyMonitor unit has eight RF ports, each of which can be configured in iBuilder to monitor one or more L-band carriers or a specific area of the spectrum.

You can connect one or more SkyMonitor spectrum analyzers to your hub LAN using standard Ethernet connections. In addition, a single iDirect Global NMS can connect to multiple SkyMonitor units at multiple hub locations. Each unit can operate using either an internal reference clock or an external 10 MHz reference signal. For details on SkyMonitor installation, see the *iDirect SkyMonitor 1880 Spectrum Analyzer Installation and Safety Manual*.



NOTE

SkyMonitor is a licensed feature. If you plan to add SkyMonitor units to your networks, please contact the iDirect Technical Assistance Center (TAC).

You can launch SkyMonitor from the iMonitor network tree either by right-clicking the SkyMonitor unit itself, or by selecting a line card carrier that you have associated with a SkyMonitor port in iBuilder. If in iBuilder you configured a port for a specific iDirect carrier, then when you right-click the line card for that carrier and launch SkyMonitor, SkyMonitor will automatically display the bandwidth defined for that carrier. If you launch SkyMonitor by right-clicking the SkyMonitor unit, the ports will be automatically tuned to the center frequency that you configured for each port. For details on configuring SkyMonitor units in iBuilder, see the *iBuilder User Guide*.

4.10.1 Viewing the Spectrum with SkyMonitor

Follow these steps to view the iDirect carriers or SkyMonitor ports as configured in iBuilder.

- Step 1 To view an iDirect carrier, right-click the line card that is transmitting or receiving the carrier; then select **Spectrum Monitor–Tx** or **Spectrum Monitor–Rx** from the menu. This will launch SkyMonitor and automatically select the RF port associated with the carrier.

As an alternative, you can right-click the SkyMonitor unit in the tree and select **Spectrum Monitor**. This will launch SkyMonitor and select RF port 1 by default.

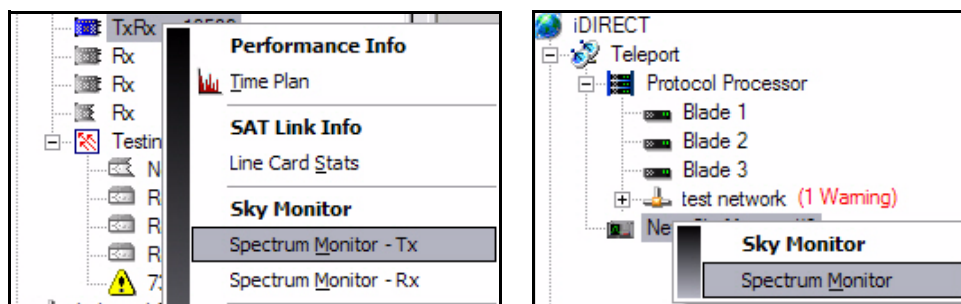


Figure 4-4 shows the initial SkyMonitor view. The current settings (**Center Freq.**, **Span**, etc.) are displayed in the monitor pane on the left.

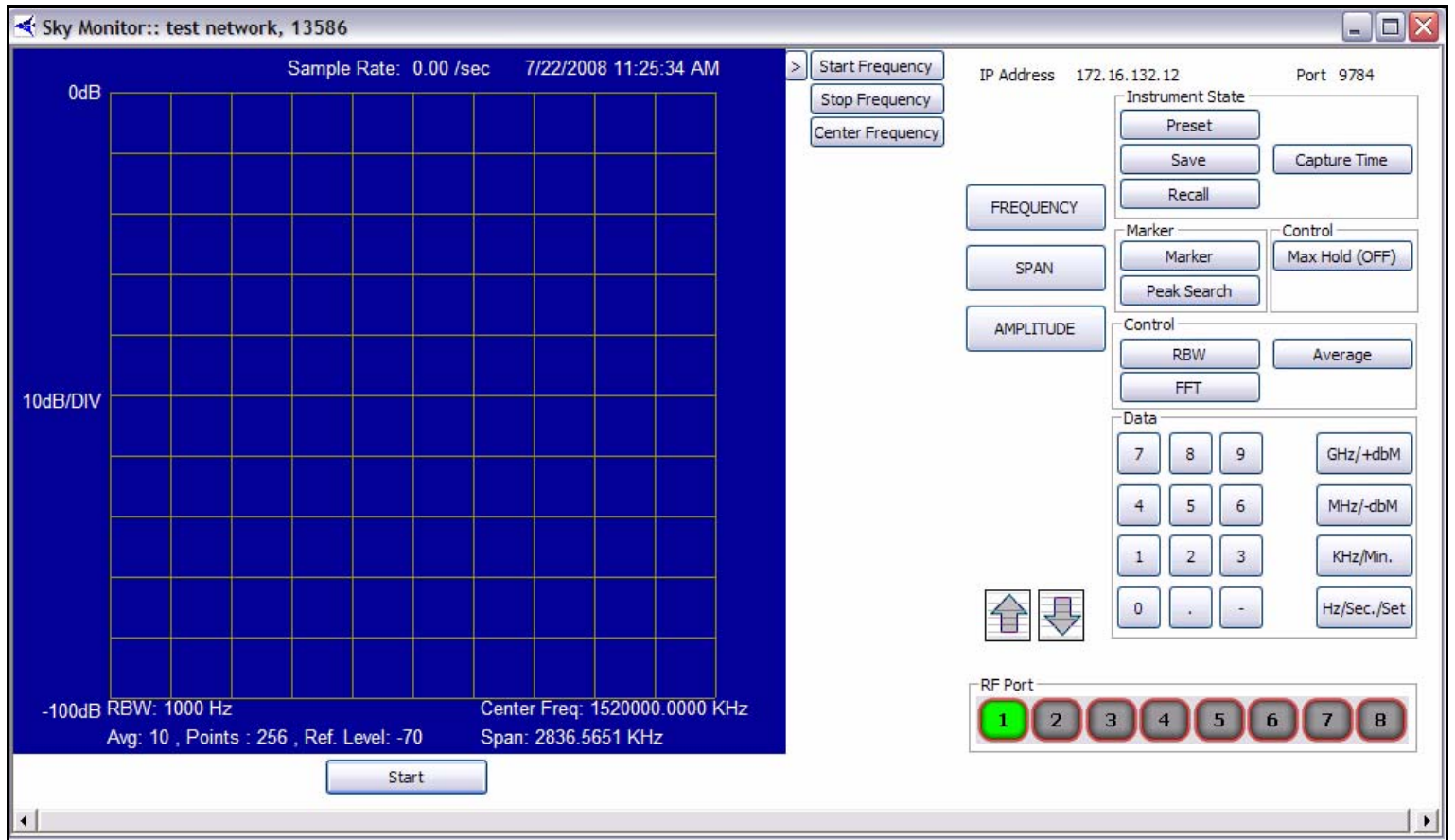


Figure 4-4: SkyMonitor Initial View

- Step 2 The keypad on the right allows you to temporarily change the RF port settings, capture data, recall captures, and save screen images. These functions are discussed in detail later in this section.
- Step 3 You can select a new SkyMonitor port by clicking a port number in the **RF Port** section of the keypad. (If you launched SkyMonitor from a line card, the RF port configured for the carrier is automatically selected.)
- Step 4 Click the **Start** button to begin monitoring your preconfigured carrier or RF port. [Figure 4-5](#) shows an iDirect carrier being monitored by a SkyMonitor spectrum analyzer.
- Step 5 Click the **Stop** button if you want to stop monitoring the bandwidth and clear the display.

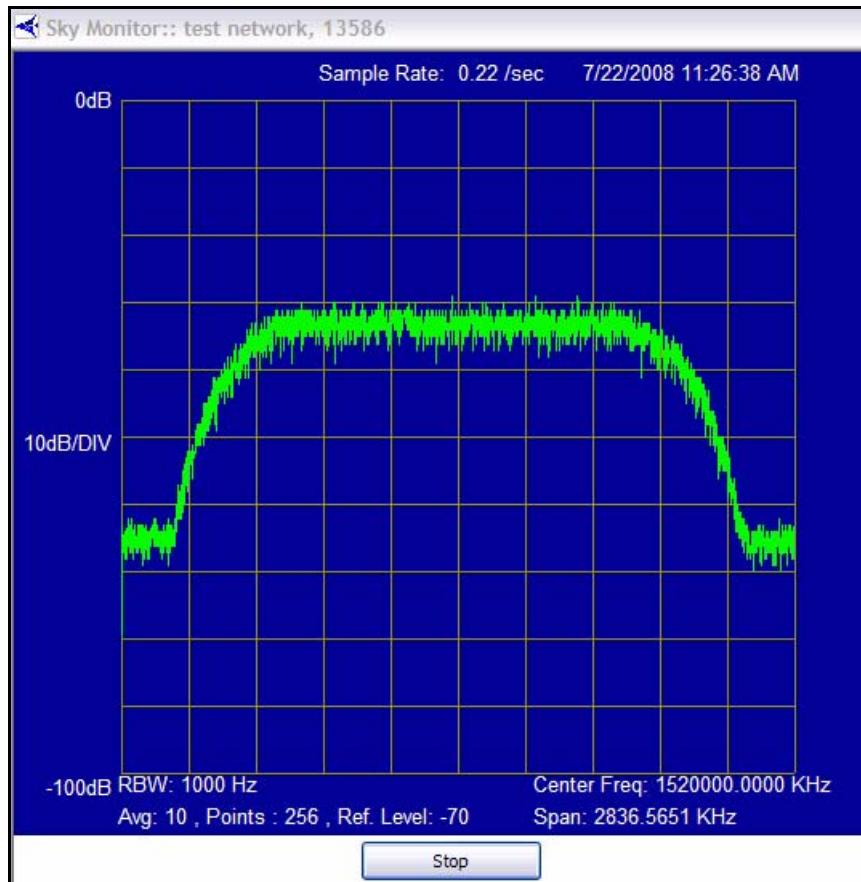
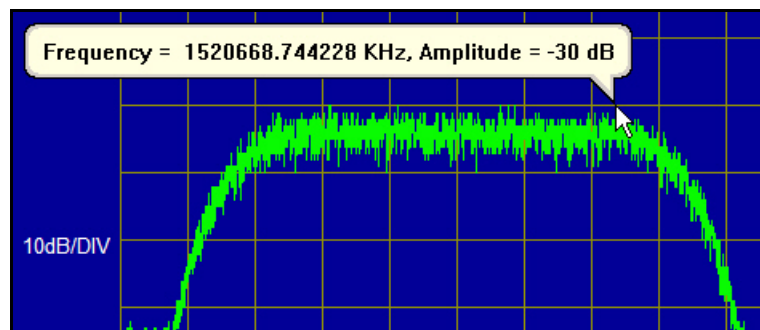


Figure 4-5: Monitoring a Carrier with SkyMonitor



NOTE

You can view the exact frequency and amplitude of any point on the monitor by positioning your cursor over that point on the screen.



4.10.2 Changing the SkyMonitor Settings

SkyMonitor displays the iBuilder configuration for the carrier or RF port by default. However, you can use the spectrum analyzer keypad to temporarily change these settings during your SkyMonitor session. However, you must make any permanent configuration changes in iBuilder. The **Frequency**, **Span**, and **Amplitude** buttons all have associated sub-function buttons. The sub-function buttons appear in the upper-left portion of the keypad when you click one of these main buttons. The results of clicking **Frequency**, **Span**, and **Amplitude** are shown in [Figure 4-6](#).

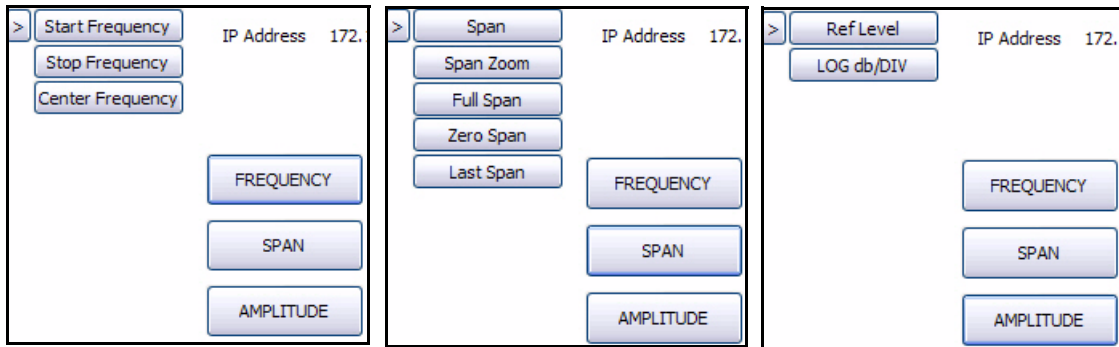
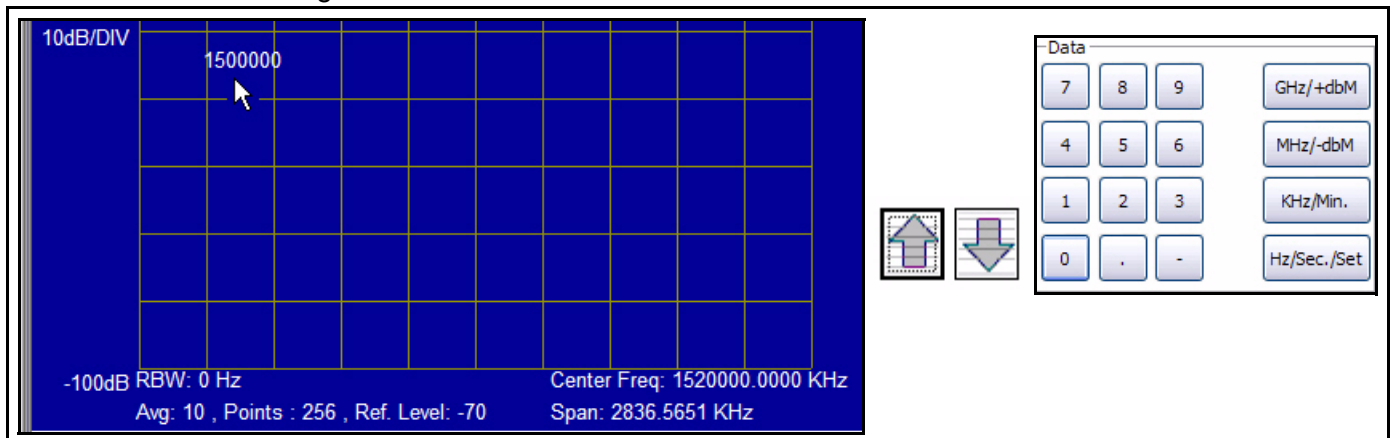


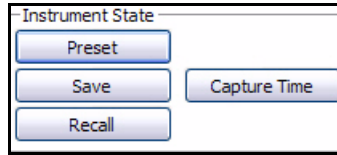
Figure 4-6: SkyMonitor Function Buttons

Operate the keypad buttons as you would the buttons on a typical spectrum analyzer. As an example, if you want to temporarily change the **Center Frequency** to be different from the iBuilder configuration, follow these steps:

- Step 1 Click the **Frequency** button to view the sub-function buttons. (See [Figure 4-6](#).)
- Step 2 Click the **Center Frequency** button.
- Step 3 Using the **Data** section of the keypad, click the number buttons to enter the value of the new center frequency. As you enter the data, it is displayed in the monitor pane on the left side of the window. You can click the up and down arrow buttons to increment or decrement the last digit you entered. You can also click the minus sign button (-) to clear the previously-entered digit.



- Step 4 Click the appropriate button for the units you are entering (**GHz**, **MHz**, **KHz** or **Hz**). Once you select the units, the value displayed at the bottom of the screen will change to the new center frequency, converted to KHz.
- Step 5 If you want to restore the iBuilder configuration, click the **Preset** button in the **Instrument State** section of the keypad.



4.10.3 Capturing and Recalling SkyMonitor Data

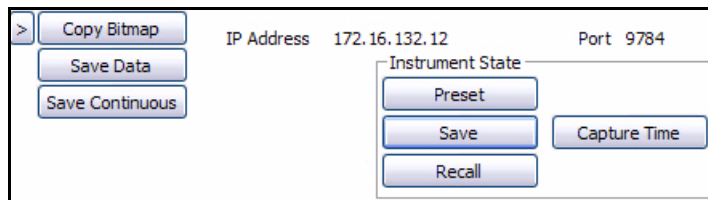
SkyMonitor allows you to:

- Save the current spectrum analyzer data to a file on the NMS server
- Periodically save the spectrum analyzer data to a file at five minute intervals
- Recall saved data files for viewing in SkyMonitor
- Copy a bitmap image of the monitor pane to your computer clipboard for pasting into an application such as MS Word.

Saving SkyMonitor Data

To save the current SkyMonitor data, or to initiate a background task to capture data at intervals over a set period, follow these steps.

- Step 1 Click the **Save** button in the **Instrument State** area of the SkyMonitor keypad. This allows you to view the **Copy Bitmap**, **Save Data**, and **Save Continuous** buttons.



- Step 2 If you want to save the current data, click the **Save Data** button. This will write the spectrum analyzer data to a file on your NMS server.
- Step 3 To capture data at five minute intervals over a set time period:
- a Click the **Capture Time** button.

- b In the **Data** area of the keypad, enter the time period over which you want to collect data and click the **Min** or **Sec** button.

The image shows a keypad titled "Data". It contains a numeric keypad with buttons for digits 0-9, a decimal point, and a minus sign. To the right of the numeric keypad are four buttons for unit selection: "GHz/+dbM", "MHz/-dbM", "KHz/Min.", and "Hz/Sec./Set".

- c Click the **Save Continuous** button. Data will be saved to a single capture file on the NMS server every five minutes for the specified time period.

Recalling and Viewing SkyMonitor Data

Follow these steps to recall and view saved SkyMonitor data files:

- Step 1 If you are currently monitoring the spectrum, click the **Stop** button below the monitor pane. (See [Figure 4-5](#) on [page 102](#).)
- Step 2 In the **Instrument State** area of the SkyMonitor keypad, click the **Recall** button to display the **Select Time Range** dialog box.

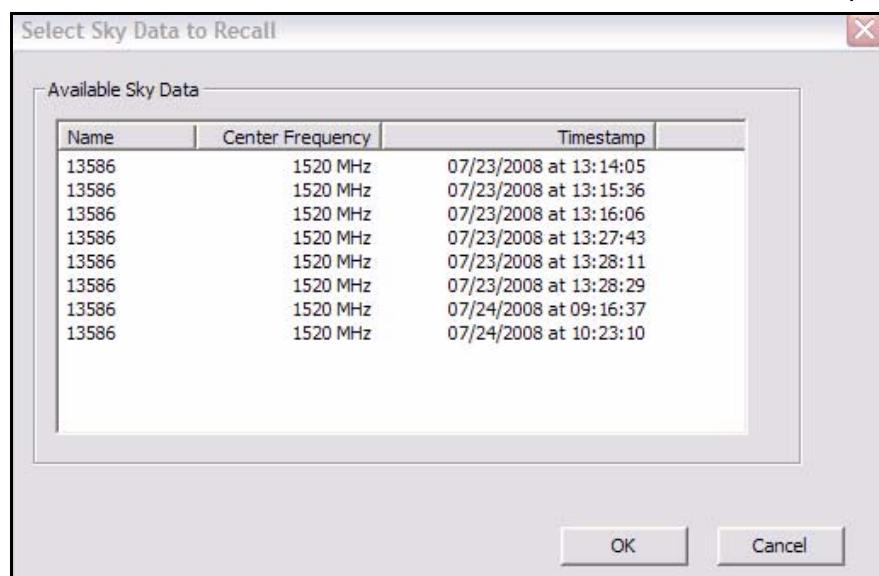
The image shows a keypad titled "Instrument State". It contains four buttons: "Preset", "Save", "Recall", and "Capture Time".

The image shows a dialog box titled "Select Time Range". It has a close button (X) in the top right corner. The dialog contains the following fields and controls:

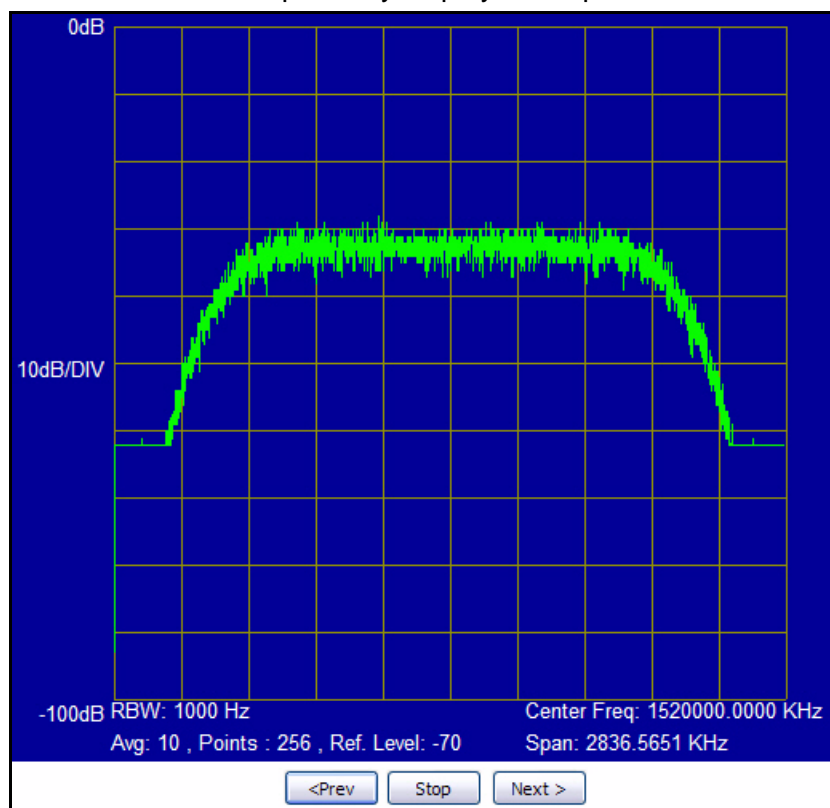
- Start Time: 7/23/2008 09:48 PM
- End Time: 7/24/2008 09:48 AM
- Duration: 12 hours
- A slider bar below the duration field, with "1 Min" on the left and "10080" on the right.
- OK and Cancel buttons at the bottom.

- Step 3 Select a time range within which to search for data files by entering a **Start Time** and **End Time** or by adjusting the slider. Then click **OK** to view the **Select Sky Data to Recall** dialog box. (The maximum time range you can enter is one week.)

- Step 4 In the **Select Sky Data to Recall** dialog box, select the data you want to recall and click **OK**. The dialog box shows the **Center Frequency** and **Timestamp** of each data file. For iDirect carriers, the line card **Name** is also displayed.



- Step 5 If the file you selected contains a continuous capture, you can click the **Prev** and **Next** buttons to sequentially display the captured data.

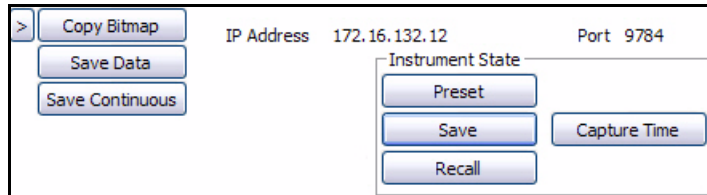


- Step 6 Click the **Stop** button when you want to stop viewing the data file.

Capturing an Image of the SkyMonitor Display

Follow these steps to copy a bitmap image in SkyMonitor's monitor pane to your computer clipboard and paste into an application such as MS Word.

- Step 1 Click the **Save** button in the **Instrument State** area of the SkyMonitor keypad. This allows you to view the **Copy Bitmap**, **Save Data**, and **Save Continuous** buttons.



- Step 2 Click the **Copy Bitmap** button. This copies the image on the monitor pane to the computer's clipboard.
- Step 3 Open the application into which you want to past the image.
- Step 4 Select the paste function of the application, or type Ctrl + V to paste the image into the application.

5 IP, SAT and Mesh Traffic Graphs

This section discusses the IP, Satellite, and Mesh Traffic graphs. It also describes the statistics on which the various graphs are based.

5.1 IP Statistics

iMonitor's IP statistics display shows you IP traffic in both downstream and upstream directions for any number of remotes in your networks. When you select multiple remotes, by choosing IP Stats from an intermediate network node, iMonitor displays the aggregate total of all the remotes you selected.

The IP Stats display is available from the following nodes in the network tree view:

- Network
- Inroute Group
- Individual Remotes

5.2 SAT Statistics

The SAT Stats display can be launched from the same locations as the IP Stats display, but displays statistics differently. The following fields represent SAT bytes:

- Reliable bytes sent to and received from remotes (e.g. TCP traffic)
- Unreliable bytes sent to and received from remotes (e.g. UDP traffic)
- Overhead bytes sent to and received from remotes (e.g. TDMA protocol header bytes)
- On the downstream only, multicast and broadcast bytes sent to remotes.

The SAT stats display also resolves a limitation with the previous IP Stats-only display: SAT traffic now accurately represents compressed RTP (CRTP) voice traffic.

5.3 IP Statistics vs. SAT Statistics

Bandwidth usage statistics are divided into two different displays in iMonitor, each representing different classes of usage: over-the-air bytes and upstream LAN bytes.

To understand why this is necessary, let's first review the TCP acceleration process. When the PP accelerates TCP traffic on the downstream, it sends acknowledgements to the sending server at the same time it queues the traffic for transmission to the remote. When the receiving client actually receives the data and acknowledges it, the remote no longer needs to send the acknowledgement; it has already been sent by the protocol processor.

This technique allows TCP traffic to flow at line rate across the satellite, and it minimizes the number of TCP ACKs that are transmitted over the air. Because of this, the amount of traffic flowing upstream from the protocol processor (eth0 to the Internet) differs from the amount of traffic flowing across the satellite. A large TCP download, for example, can cause significant traffic

to flow out of the upstream interface of the protocol processor, even though little of that traffic is transmitted across the satellite.

The IP Stats display shows the traffic on the upstream side of protocol processor while SAT Stats display shows the traffic on the tunnel side of the protocol processor. This is illustrated in [Figure 5-1](#).



NOTE

Due to the different collection points for IP and SAT statistics, the IP Stats display may show more upstream traffic than is actually possible; i.e., greater than the channel rate or configured rate limit. This is normal and not a cause for concern.

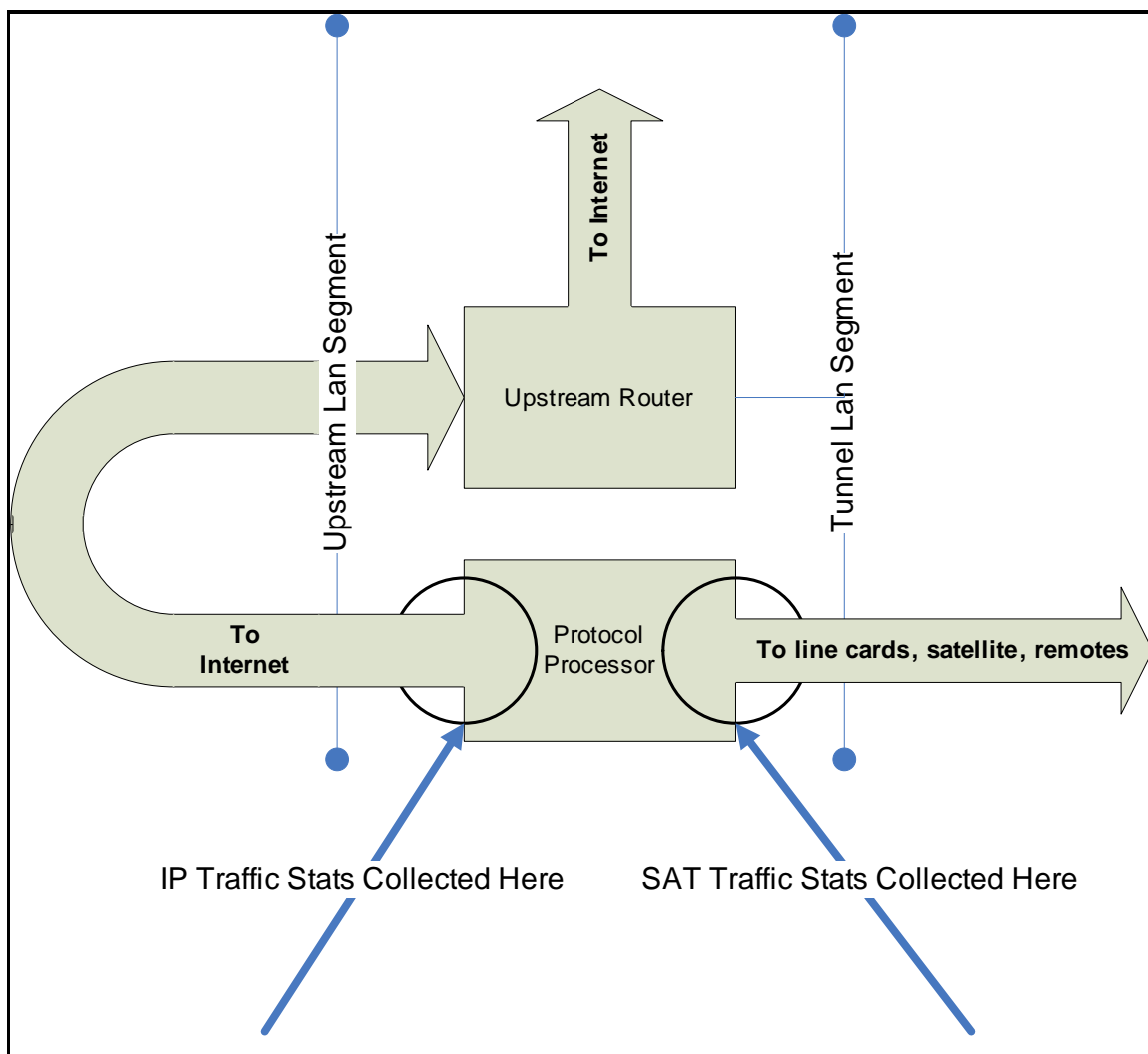


Figure 5-1: Collection Points for IP Usage Statistics

5.4 SAT Traffic Graph

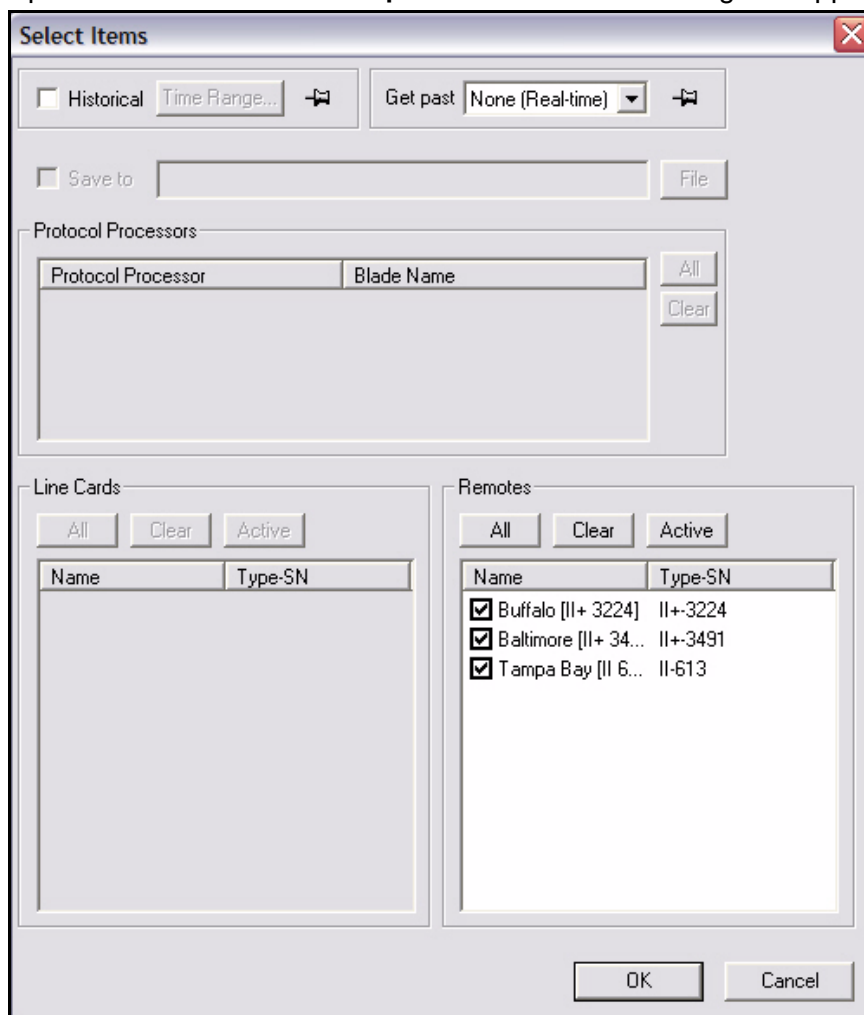
SAT (satellite) traffic information can be selected from:

- networks
- inroute groups
- remotes

To view the satellite traffic graph, follow the directions below:

Step 1 Right-click a network, an inroute group or a remote.

Step 2 Click **SAT Traffic Graph**. The **Select Items** dialog box appears.



The **Select Items** dialog box is shown. It has a title bar with a close button (X). The dialog contains several sections:

- Historical**: A checkbox and a **Time Range...** button.
- Get past**: A dropdown menu set to **None (Real-time)** and a button.
- Save to**: A checkbox and a text field with a **File** button.
- Protocol Processors**: A table with columns **Protocol Processor** and **Blade Name**, and buttons **All** and **Clear**.
- Line Cards**: Buttons **All**, **Clear**, and **Active**, and a table with columns **Name** and **Type-SN**.
- Remotes**: Buttons **All**, **Clear**, and **Active**, and a table with columns **Name** and **Type-SN**. The table contains three rows, all of which are checked:

Name	Type-SN
Buffalo [II+ 3224]	II+-3224
Baltimore [II+ 34...	II+-3491
Tampa Bay [II 6...	II-613

At the bottom of the dialog are **OK** and **Cancel** buttons.

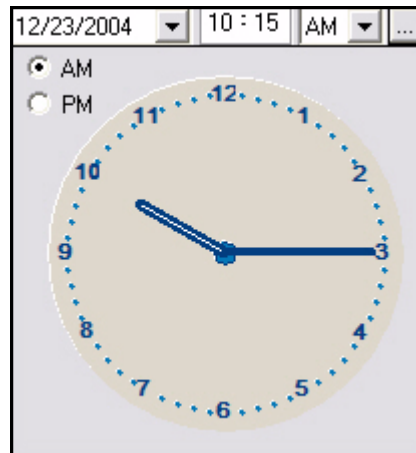
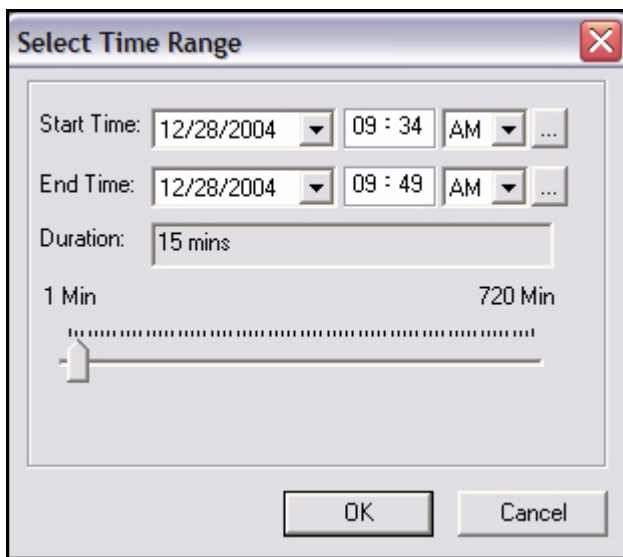
Step 3 Select the remote for which you want to view information. Notice that all but the Remotes section are unavailable for selection.

Step 4 Click either **Historical** or **Get Past**, or **OK** to view real-time.

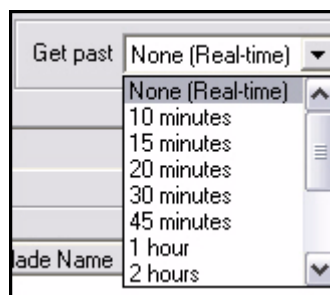
You may specify a historical time range or Get Past value from the parameters dialog. The maximum interval you can select is 12 hours. The farther you go back in time, less granularity will be available from the database due to archive consolidation.

If you retrieve more than 30 minutes of data, the display will be easier to read if you select the Minutes or Hours interval from the context menu.

- a If you select **Historical**, click **Time Range**. The **Select Time Range** dialog box appears (see below). If desired, click the ellipses next to the Start and End times to set the time via the graphical clock display. If you selected **Get Past**, see [Step b](#).

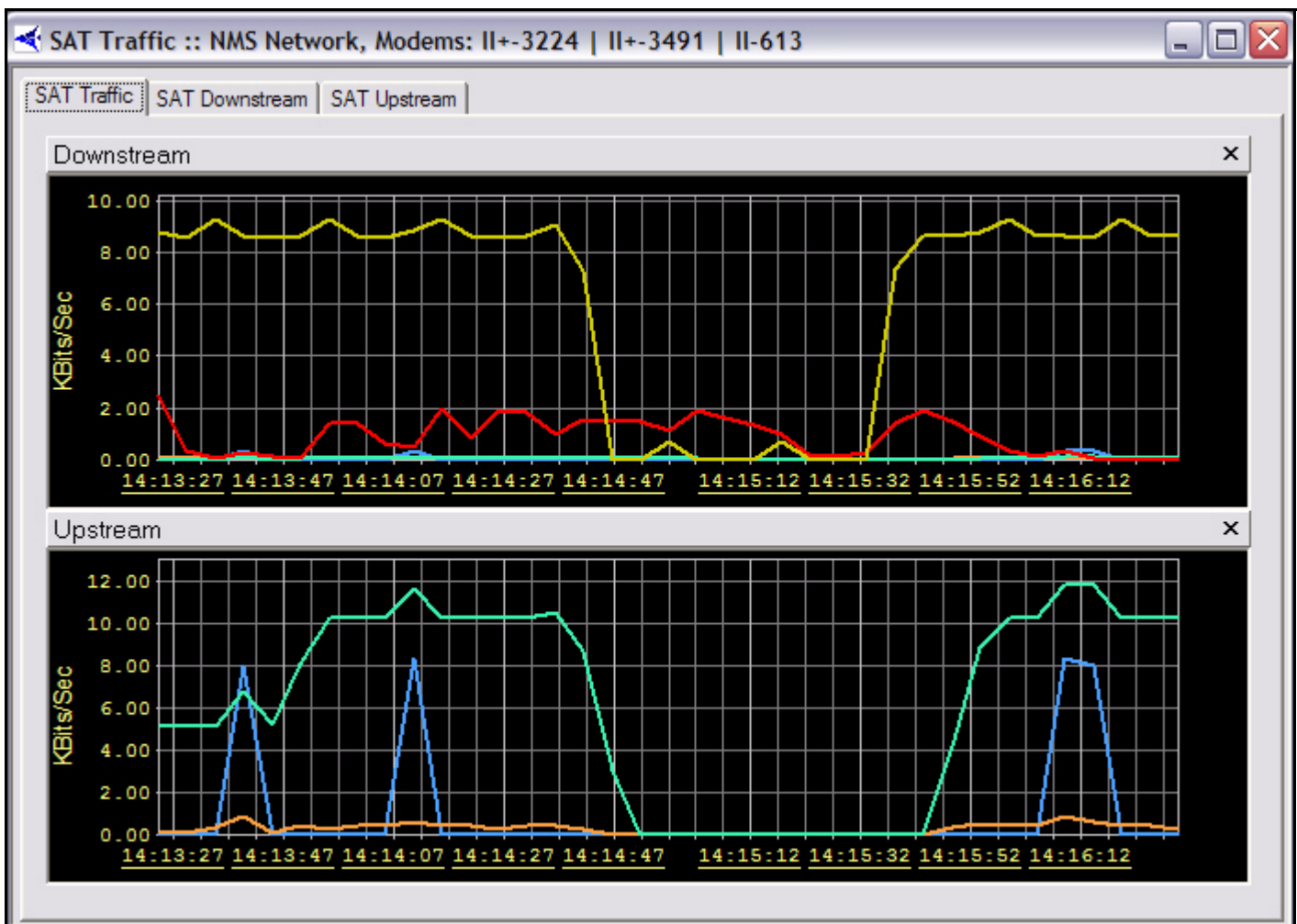


- b If you selected **Get Past**, the **Get Past** drop-down list appears. Select an interval of time.



Step 5 Click **OK**.

Step 6 The **SAT Traffic** pane appears with three tabs. Below are examples of the **SAT Traffic** tab and the **SAT Downstream** tab. The **SAT Upstream** tab has the same format as the downstream, but displays data regarding the upstream path.



SAT Traffic :: NMS Network, Modems: II+-3224 II+-3491 II-613							
SAT Traffic SAT Downstream SAT Upstream							
Time	Date	Reliable [K...	UnReliable ...	Overhead [...	Multicast [K...	Broadcast [...	Total [KBits]
14:15:02	12/28/04	0.000	0.416	0.176	9.472	0.000	10.064
14:15:07	12/28/04	0.000	0.000	0.048	8.288	0.000	8.336
14:15:12	12/28/04	0.000	0.000	0.048	6.848	0.000	6.896
14:15:17	12/28/04	0.000	0.000	0.048	4.992	3.408	8.448
14:15:22	12/28/04	0.000	0.000	0.096	0.576	0.000	0.672
14:15:27	12/28/04	0.000	0.000	0.048	0.864	0.000	0.912
14:15:32	12/28/04	0.000	0.000	0.048	1.440	0.000	1.488
14:15:37	12/28/04	0.000	0.000	0.048	7.072	36.640	43.760
14:15:42	12/28/04	0.000	0.000	0.048	9.376	42.976	52.400
14:15:47	12/28/04	0.000	0.208	0.112	7.424	42.976	50.720
14:15:52	12/28/04	0.000	0.416	0.176	4.640	43.952	49.184
14:15:57	12/28/04	0.000	0.416	0.176	1.728	46.288	48.608
14:16:02	12/28/04	0.000	0.416	0.176	0.608	42.976	44.176
14:16:07	12/28/04	1.776	0.416	0.592	1.760	42.976	47.520
14:16:12	12/28/04	1.776	0.416	0.592	0.320	42.880	45.984
14:16:17	12/28/04	0.000	0.416	0.176	0.000	46.288	46.880
14:16:22	12/28/04	0.000	0.416	0.176	0.000	42.976	43.568
14:16:27	12/28/04	0.000	0.416	0.176	0.000	42.976	43.568
14:16:32	12/28/04	0.000	0.416	0.224	5.120	42.880	48.640
14:16:37	12/28/04	0.000	0.416	0.176	9.696	47.360	57.648
14:16:42	12/28/04	0.000	0.416	0.176	5.920	42.976	49.488
14:16:47	12/28/04	0.000	0.416	0.176	3.456	42.976	47.024
14:16:52	12/28/04	0.000	0.416	0.176	0.288	42.880	43.760
14:16:57	12/28/04	0.000	0.416	0.176	1.152	46.288	48.032
14:17:02	12/28/04	0.000	0.416	0.176	3.168	42.976	46.736
14:17:07	12/28/04	0.000	0.416	0.176	2.016	42.976	45.584
14:17:12	12/28/04	0.000	0.416	0.176	2.592	42.880	46.064
14:17:17	12/28/04	0.000	0.416	0.176	4.608	46.288	51.488

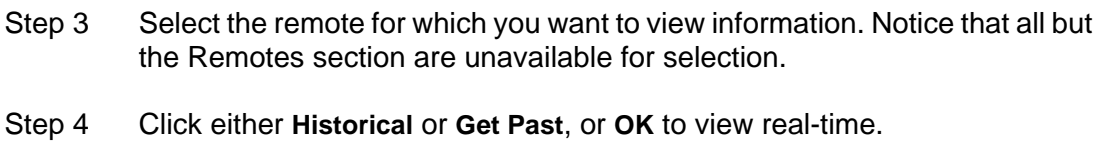
5.5 IP Traffic Graph

IP traffic information can be selected from:

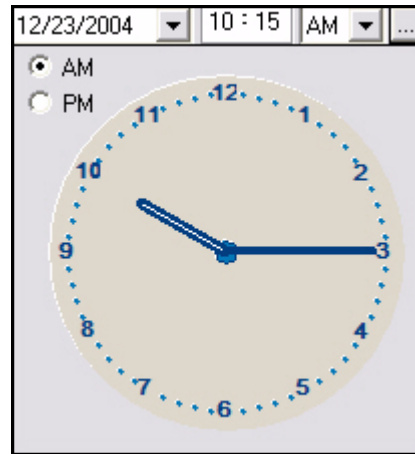
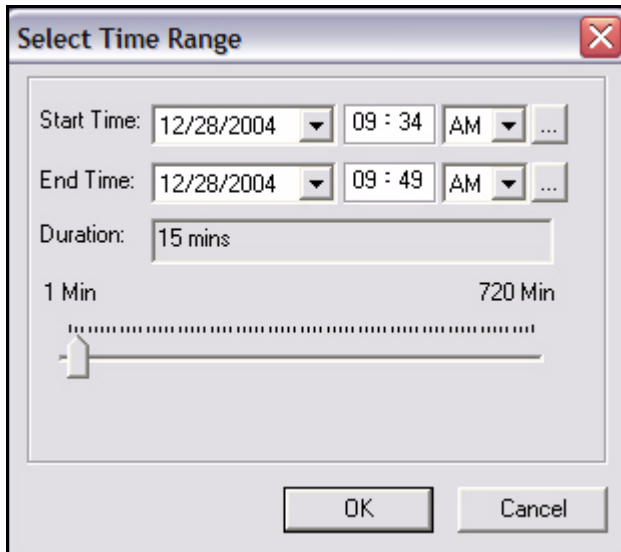
- networks
- inroute groups
- remotes

To view the IP traffic graph, follow the directions below:

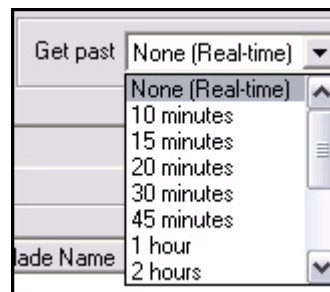
- Step 1 Right-click a network, inroute group, or remote.
- Step 2 Click **IP Traffic Graph**. The **Select Items** dialog box appears.



- a If you select **Historical**, click **Time Range**. The **Select Time Range** dialog box appears (see below). If desired, click the ellipses next to the Start and End times to set the time via the graphical clock display. If you selected **Get Past**, see [Step b](#).

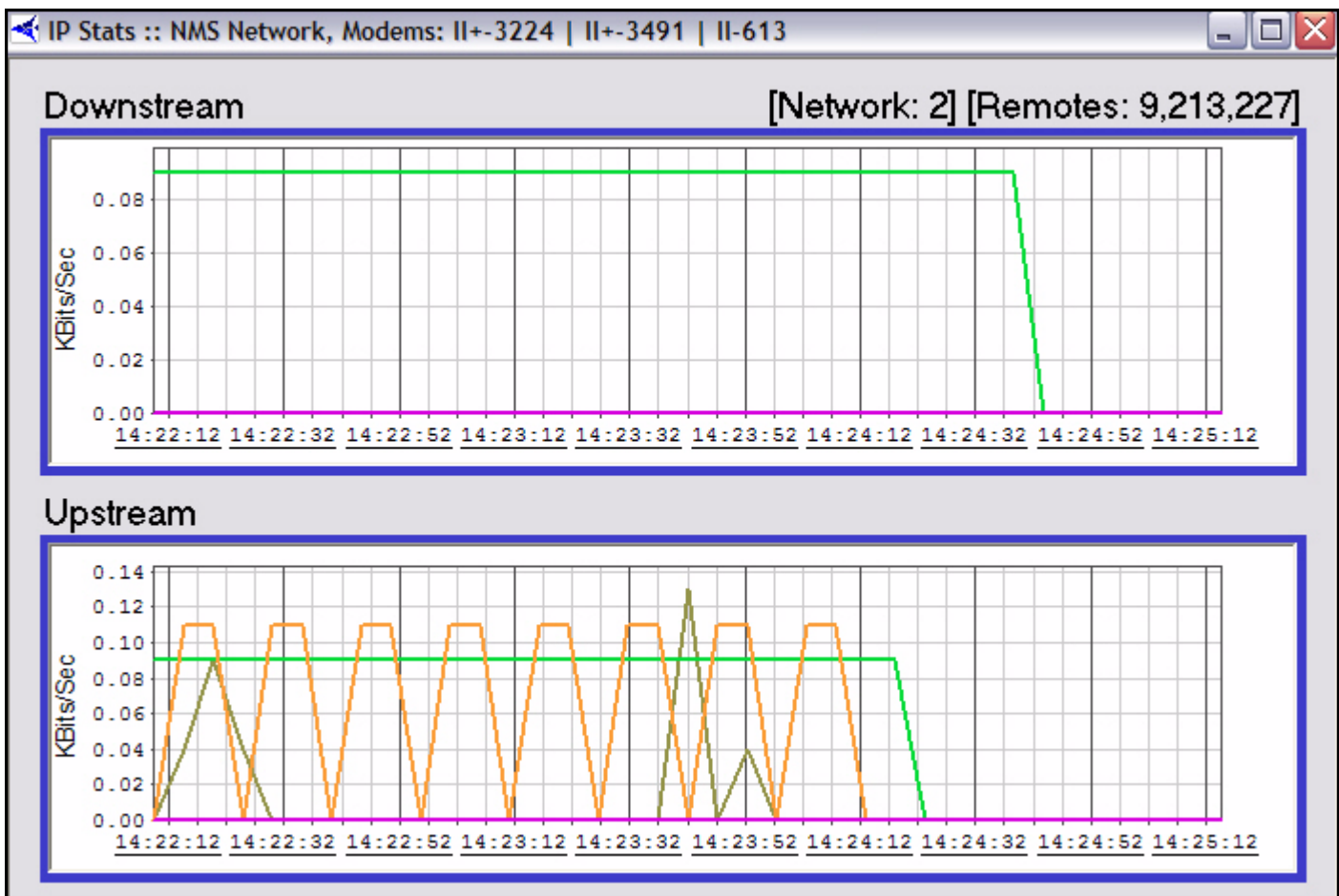


- b If you selected **Get Past**, the **Get Past** drop-down list appears. Select an interval of time.



Step 5 Click **OK**.

Step 6 The **IP Traffic Stats** pane appears, as shown below. Refer to the [Archive Database Tables, discussed on page 151](#) for information on these results.



5.6 Viewing Options

To choose among various display options on the graph, click **IP Stats** or **SAT Stats** from the main menu or right-click inside the window to view the menu below.

Show Legend	
Show Parameters	
Scroll Lock	
Direction	►
Units	►
Interval	►
Activity	►
Rate Limits	►
Copy	Ctrl+C
Properties	

The menu options are described below:

- **Show Legend** – displays a color-coded legend of the graph contents
- **Show Parameters** – shows a static options section at the top of the pane
- **Scroll Lock** – locks the upstream and downstream scroll bars together after a historical query
- **Direction** – allows you to view upstream traffic, downstream traffic, or both
- **Units** – switches between kilobits per second and kilobytes per second
- **Interval** – switches between the following:
 - Seconds (3 minutes total)
 - Minutes (1 hour total, averaged over 1 minute)
 - Hours (12 hours total, averaged over 10 minutes)
- **Activity** – allows you to selectively choose which IP types to display, or to show the total IP traffic as a single graph line
- **Rate Limits** – displays configured upstream and downstream rate limits. This selection only exists for Satellite Traffic statistics; it does not exist in the IP Traffic statistics menu.
- **Copy** – copies the current graph display to your PC's clipboard
- **Properties** – allows to you modify the default color settings

5.7 Bandwidth Usage

This display is useful as an at-a-glance display of the total kbps traffic in both directions for a selected group of remotes. The information is shown in real-time only in a multi-column list. You can sort each column in ascending or descending order.

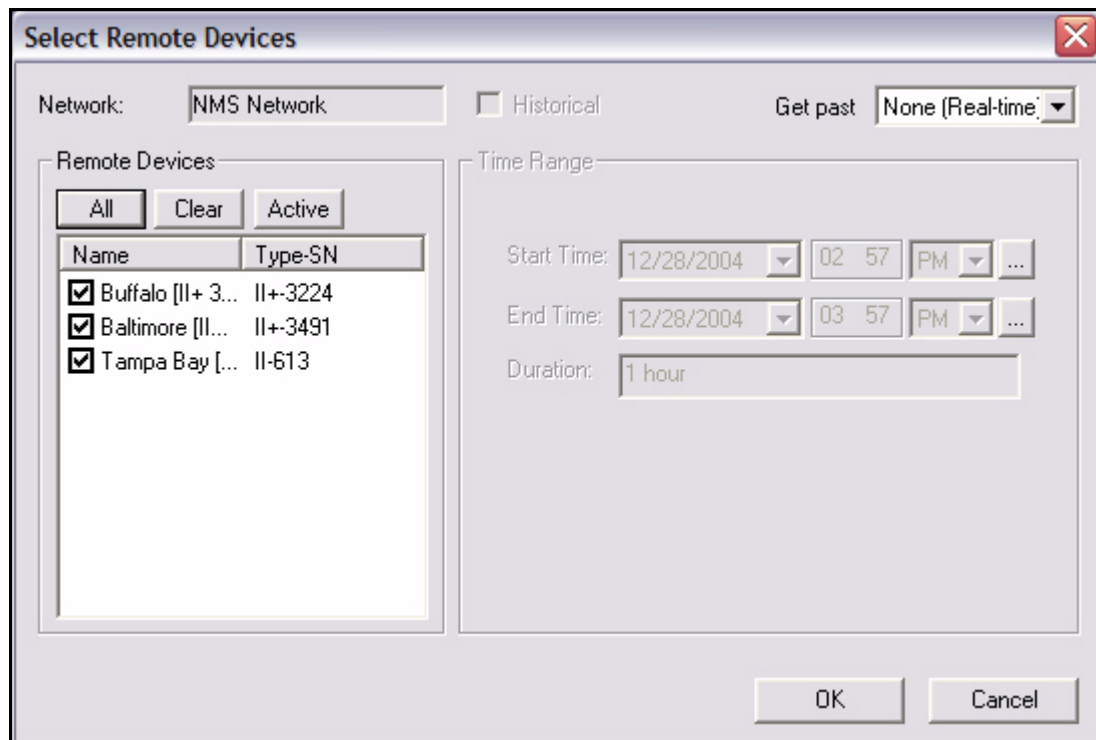
The Bandwidth Usage display can be selected from:

- Networks
- Inroute Groups

To view the bandwidth usage, follow the directions below:

Step 1 Right-click a network or inroute group.

Step 2 Click **Bandwidth Usage**. The **Select Remote Devices** dialog box appears



Step 3 Make the appropriate selections, and click **OK**. The **Bandwidth Usage** results pane appears, as shown below.

Remote	ID	Ty...	Downstream [KBits/Sec]	Upstream [KBits/Sec]
NYK Atlas	228	51...	0.01	0.00
Infiniti Test [5350.2036]	222	53...	0.00	0.00
Infiniti 5350.4022	248	53...	0.00	0.00
Multicast			7.20	
Broadcast			6.05	
Total			13.26	0.00

Figure 5-2: Real-Time Bandwidth Usage Display

5.8 Mesh Statistics

The NMS collects mesh traffic statistics to and from remotes, saves it in the data archive, and provides it to iMonitor for real-time and historical displays. You can view the following mesh traffic statistics:

- Reliable bytes sent to and received from remotes on mesh inroutes (e.g. TCP traffic)
- Unreliable bytes sent to and received from remotes on mesh inroutes (e.g. UDP traffic)
- Overhead bytes sent to and received from remotes on mesh inroutes (e.g. TDMA protocol header bytes)

Mesh statistics refer only to single-hop traffic between mesh remotes. In a typical network configuration, TCP traffic between remotes will be routed through the hub. In that case, the reliable byte count will be zero. However, if TCP acceleration is turned off for a mesh inroute group, then both reliable (TCP) and unreliable (UDP) traffic between mesh remotes will be single hop traffic and will be counted in these statistics.

When viewing stats for mesh-enabled remotes, it's important to keep the following facts in mind:

- Remote-to-remote traffic traverses the satellite on the TDMA inroute.
- When viewing the SAT traffic graph, the upstream graph *includes* any remote-to-remote mesh traffic.
- The Mesh traffic graph includes any remote-to-remote mesh traffic and remote-to-hub traffic. The displays for transmitted and received traffic *do not include* non-mesh traffic. That is, traffic from remotes destined for an upstream host is not included on the display.
- Mesh traffic is never displayed on the IP traffic graph, since this display represents traffic upstream from the protocol processor.

You may use the Mesh IP statistics to determine if there is mesh traffic loss on the link. In order to do this, you must select *all* mesh remotes for the display. When you do this, the transmitted kbps and received kbps should be identical. If they are not identical, it is likely there is packet loss across the mesh link.

[Figure 5-3](#) shows the various collection points for Mesh, SAT, and IP statistics.

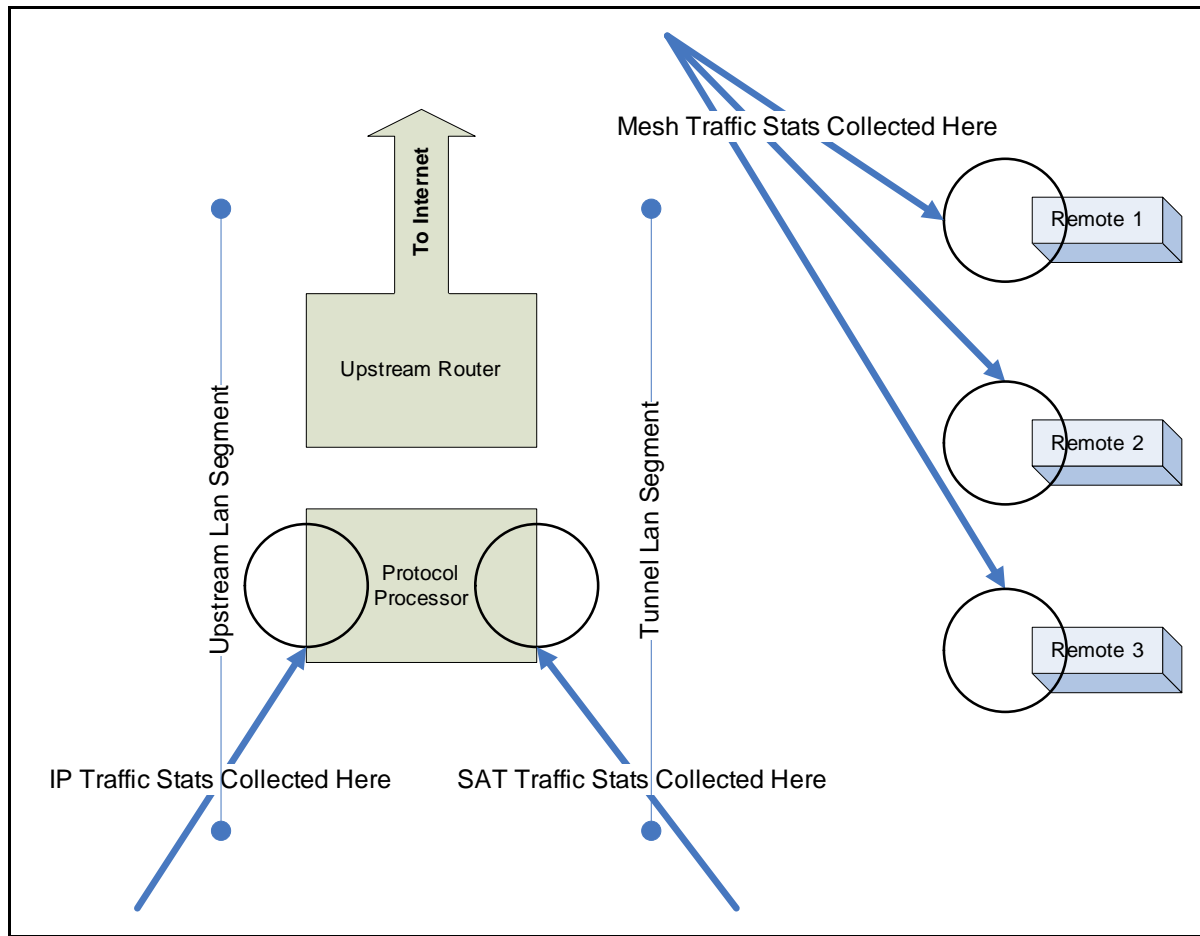


Figure 5-3: Collection Points for Mesh, SAT, and IP Statistics

5.8.1 Mesh Traffic Graph

Mesh traffic information can be selected for the following network elements:

- networks
- inroute groups
- remotes

To view the mesh traffic graph, follow the directions below:

Step 1 Right-click a network, an inroute group or a remote.

Step 2 Click **Mesh Traffic Graph**. The **Select Items** dialog box appears.

Select Items

☐ Historical **Time Range...**

Get past **None (Real-time)**

☐ Save to **File**

Protocol Processors

Protocol Processor	Blade Name
--------------------	------------

All **Clear**

Line Cards

All **Clear** **Active**

Name	Type-SN
------	---------

Remotes

All **Clear** **Active**

Name	Type-SN
<input checked="" type="checkbox"/> 2045	5350.2045
<input checked="" type="checkbox"/> 2041	5350.2041
<input checked="" type="checkbox"/> 2050	5350.2050

OK **Cancel**

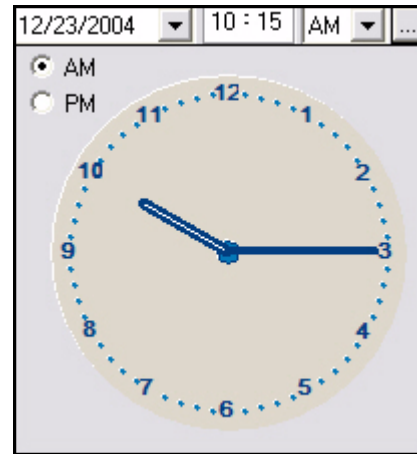
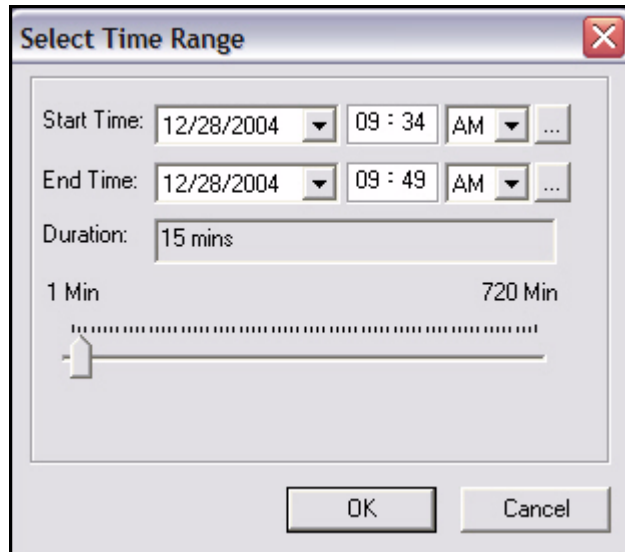
Step 3 Select the remote or remotes for which you want to view information. Notice that all but the **Remotes** section of the dialog box are unavailable for selection.

Step 4 Click either **Historical** or **Get Past**; or click **OK** to view real-time statistics.

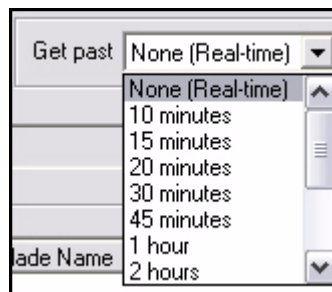
You may specify a historical time range or Get Past value from the parameters dialog. The maximum interval you can select is 12 hours. The farther you go back in time, less granularity will be available from the database due to archive consolidation.

If you retrieve more than 30 minutes of data, the display will be easier to read if you select the Minutes or Hours interval from the context menu.

- a If you select **Historical**, click **Time Range**. The **Select Time Range** dialog box appears (see below). If desired, click the ellipses next to the Start and End times to set the time via the graphical clock display. If you selected **Get Past**, see [Step b](#).



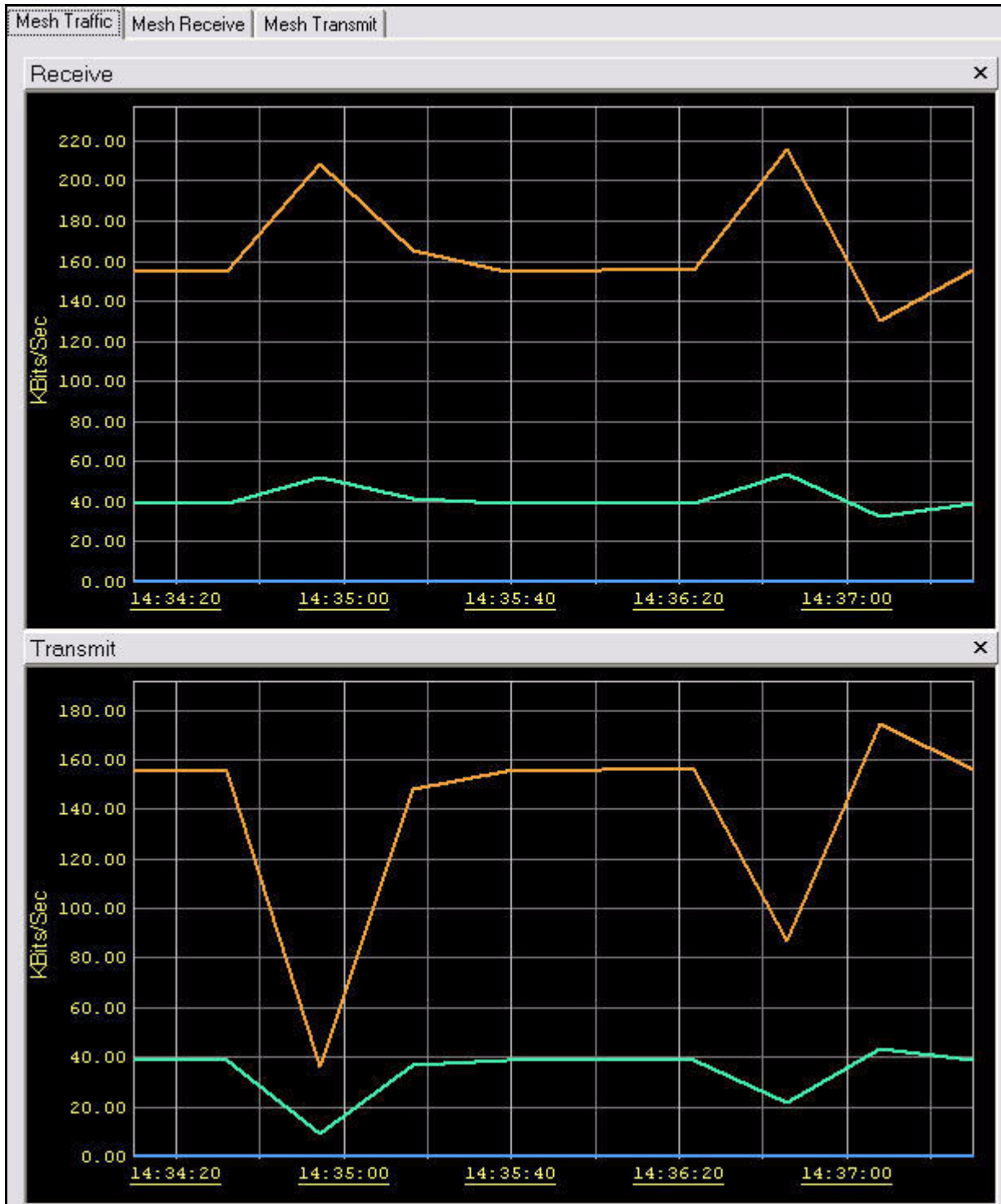
- b If you selected **Get Past**, the **Get Past** drop-down list appears. Select an interval of time.



Step 5 Click **OK**.

Step 6 The **Mesh Traffic** pane appears with three tabs. Below are examples of the **Mesh Traffic** tab and the **Mesh Receive** tab. The **Mesh Transmit** tab has the

same format as the **Mesh Receive** tab but displays data regarding the transmitted traffic.



Step 7 If you right-click inside the frame and click **Show Parameters** from the context menu, you can select what you want to see in the graph from the options shown below.

Direction <input type="radio"/> Downstream <input type="radio"/> Upstream <input checked="" type="radio"/> Both	Units <input checked="" type="radio"/> Bits <input type="radio"/> Bytes	Interval <input checked="" type="radio"/> Seconds <input type="radio"/> Minutes <input type="radio"/> Hours	Traffic Type <input type="checkbox"/> Reliable <input type="checkbox"/> Unreliable <input type="checkbox"/> Overhead <input type="checkbox"/> All <input checked="" type="checkbox"/> None <input type="checkbox"/> Total	Rate Limits <input type="checkbox"/> Downstream Max <input type="checkbox"/> Upstream Max
---	--	---	---	--

Note that the **Rate Limits (Downstream Max and Upstream Max)** are only selectable if you have configured rate limits on the QoS tab of the selected remotes.

Mesh Traffic					
Mesh Receive		Mesh Transmit			
Time		Reliable [KBits]	UnReliable [KBits]	Overhead [KBits]	Total [KBits]
6/15/2006 1:08:55 PM		0.064	7.104	30.352	37.760
6/15/2006 1:09:00 PM		0.000	5.056	30.288	35.344
6/15/2006 1:09:05 PM		0.000	7.232	33.488	40.720
6/15/2006 1:09:10 PM		0.000	12.576	30.288	42.864
6/15/2006 1:09:15 PM		0.064	8.384	30.352	39.040
6/15/2006 1:09:20 PM		0.000	1.632	30.288	31.920
6/15/2006 1:09:25 PM		0.000	1.280	33.488	34.768
6/15/2006 1:09:30 PM		0.000	4.480	30.080	34.560
6/15/2006 1:09:35 PM		0.064	4.192	30.560	35.056
6/15/2006 1:09:40 PM		0.000	5.120	30.080	35.200
6/15/2006 1:09:45 PM		0.000	9.952	33.696	43.648
6/15/2006 1:09:50 PM		0.000	3.200	30.080	33.280
6/15/2006 1:09:55 PM		0.064	3.904	30.560	34.768
6/15/2006 1:10:00 PM		0.000	1.632	30.080	31.712
6/15/2006 1:10:05 PM		0.000	0.992	33.696	34.688

6 Reporting on Networks

iMonitor provides four built-in reports that allow you to generate long-term reports from the statistics archive. Each is discussed in detail below.

6.1 Reports

Reports can be generated from:

- networks
- inroute groups
- remotes
- TDMA line cards
- iSCPC line cards

On each of these elements, you can generate all of the following reports:

- SAT Long Term Bandwidth Usage
- IP Long Term Bandwidth Usage
- Mesh Long Term Bandwidth Usage
- Remote Availability
- Line Card Availability

6.1.1 Long-Term Bandwidth Usage Report

Long-term bandwidth usage reports can be generated in iMonitor, providing you with a fast and flexible way to show bandwidth utilization. On the Average Tab of the SAT or Mesh Long Term Bandwidth Usage report, a *percent-of-max-capacity* figure is also calculated, which you can use to quantify unused bandwidth margin on both the upstream and downstream channels. At each level of the Tree, you can report on all remotes below the element you have selected.

6.1.2 IP, SAT and Mesh Long Term Bandwidth Usage Reports

To generate, view, save, or print the SAT Long Term Bandwidth Usage report, follow the directions below:

- Step 1 Right-click a network, inroute group, or remote.
- Step 2 Select **IP Long Term Bandwidth Usage**, **SAT Long Term Bandwidth Usage** or **Mesh Long Term Bandwidth Usage**. The **Long Term Bandwidth Usage Parameters** dialog box appears.

Long Term Bandwidth Usage Parameters

Network:

☒ Total all remotes

Remote Devices

Name	Type-SN
<input checked="" type="checkbox"/> Infiniti Test [5...	5350.2036
<input checked="" type="checkbox"/> NYK Atlas	5150.4643
<input checked="" type="checkbox"/> Infiniti [3125....	3125.2128
<input checked="" type="checkbox"/> Infiniti [7300....	7300.3974
<input checked="" type="checkbox"/> Infiniti 5350.4...	5350.4022
<input checked="" type="checkbox"/> Copy of Infinit...	3100.0
<input checked="" type="checkbox"/> New Remote ...	3100.0

Direction

☐ Downstream
☐ Upstream
☒ Both

IP Type

☐ None ☒ All

☒ IGMP ☒ UDP ☒ HTTP
☒ ICMP ☒ TCP ☒ OTHER

☒ Total IP Traffic

Time Range

Start Time: 12/28/2005 07 : 46 PM ...

End Time: 1/ 4/2006 07 : 46 PM ...

Duration: 1 week

1 Hour 8784

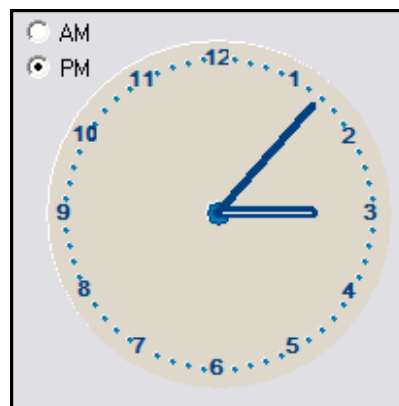
Interval 1 Min Sort By Timestamp Ascending

☐ Save to IP_LTBW_14_54_11

- Step 3 Make the appropriate selections, as described below:
- Step 4 In **Remote Devices**, select the check boxes of the remote devices for which you want to generate reports.
- Step 5 When the **Total All Remotes** box is selected, iMonitor will add all the values together for all of the selected remotes. If clear, iMonitor reports on each remote individually.

- Step 6 In **Direction**, select **Downstream**, **Upstream**, or **Both** to tell iMonitor whether to report on downstream usage, upstream usage, or usage in both directions.
- Step 7 In **IP Type**, **SAT Type** or **Mesh Type**, select one or more protocol types that you would like in your report, or select **None** to report only on total traffic, not broken down by protocol. Selecting the **All** check box selects all of the protocol type boxes and results in a complete listing of the individual values for each protocol type. Select **Total Traffic** to sum the columns of IP traffic in a Grand Total.
- Step 8 In **Time Range** select the time period for your report. By default, you can select up to six months in the past; values older than this are not saved by the back-end server. If you wish to save IP statistics for longer than six months, please contact iDirect's Technical Assistance Center (TAC).

In **Time Range**, enter the start date by selecting a day, month, and year from the calendar drop-down box. You can enter time values using the text boxes, or by clicking the **Details** button to display the clock tool.



To specify an hour value, click the hour hand, and then click the hour. To select a minute value, use the same technique, but click the minute hand instead. You can also double-click anywhere on the dial to move both hands to that location.



NOTE

This method for specifying time is available from all historical query parameters panes.

- Step 9 The **Interval** box allows you to specify the time period represented by each message returned from the server. This feature allows you to show more or less granularity in the results depending on the type of report you want.

In general, raw data is less informative for long-term reporting than data consolidated to represent larger time periods.

The minimum interval available will vary depending on the Start Time you specify for your report. As usage data ages, the NMS server automatically consolidates records for disk space, so the higher-granularity intervals may not be available if your Start Time value is far in the past. iMonitor automatically chooses the highest-granularity interval for you. For more information on how the NMS server consolidates usage records see [Appendix A “Accessing the NMS Statistics Archive” on page 147](#).

- Step 10 In the **Sort By** list, specify a sort to initially sort the values for the report. Once the report is generated you can re-sort at any time by clicking on the appropriate column heading.
- Step 11 When you have finished specifying your desired run-time parameters, click **OK** to run the report. After the server has retrieved the data, consolidated it into your chosen interval, and delivered it to your client, a separate pane appears showing the results of the report.

Results

The report is organized into **Totals** and **Averages** tabs. The **Totals** tab shows total kilobytes for each message returned from the server in the interval that you selected. There is a total value at the end of each row, and a grand total at the bottom of each column. The **Averages** tab shows the calculated kilobits per second value for each message.

Totals Tab

[Figure 6-1](#) shows an example of the **Totals** tab of the **Sat Long-Term Bandwidth Report**. In this example, the user chose to total all remotes, and to not break out the report by IP protocol type. If the user had chosen to report individual IP protocols, each supported protocol would have appeared in its own column.

Averages Tab

[Figure 6-2](#) shows the same report as [Figure 6-1](#), but with the **Averages** tab selected. As with the **Totals** tab, only the averages for the total IP traffic are calculated, since the user chose to not break out the data by individual IP protocol type.

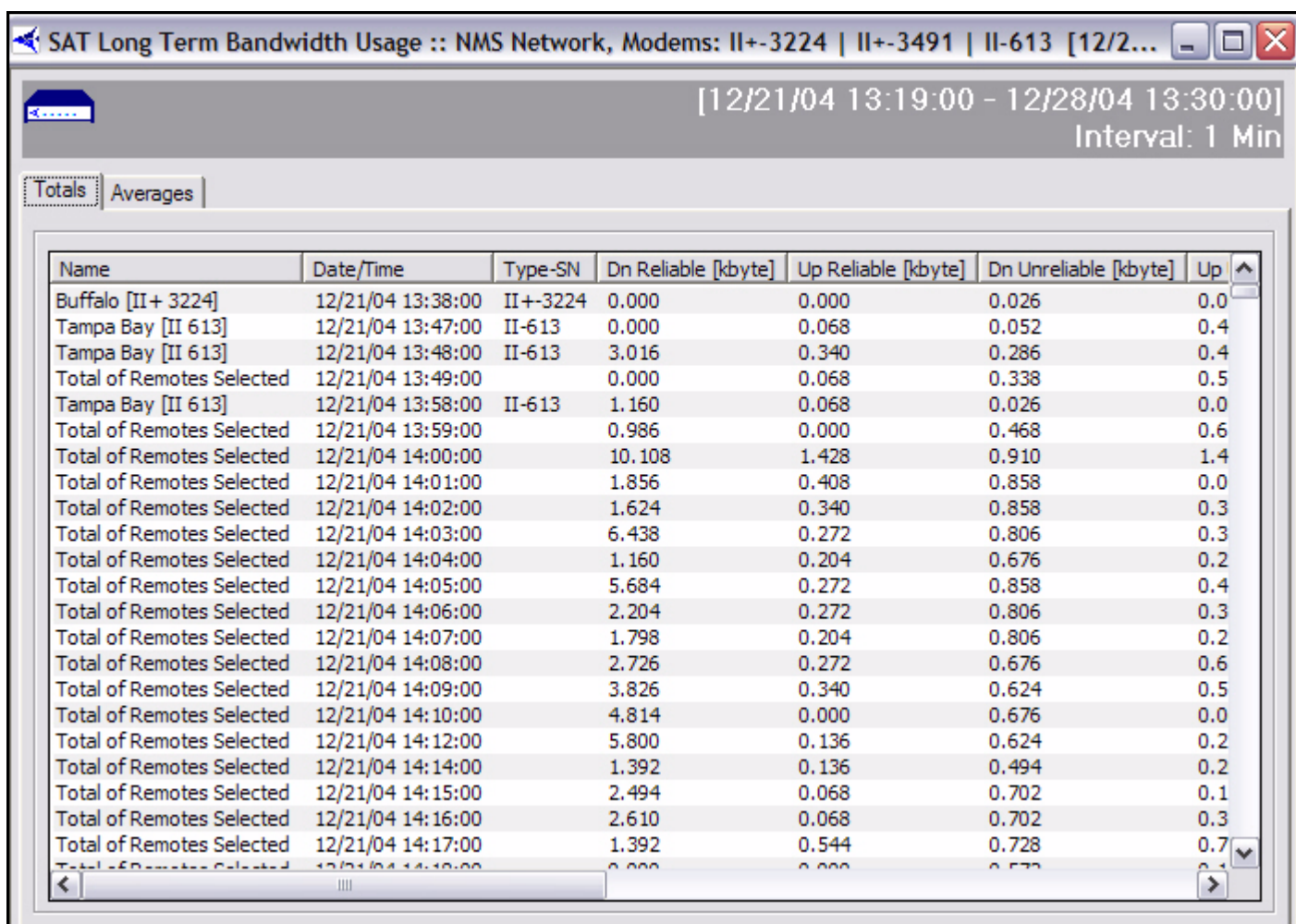


Figure 6-1: SAT Long Term Bandwidth Usage Report

- Step 12 Click **Averages** to view the average values for each parameter for the period of time the report covers.

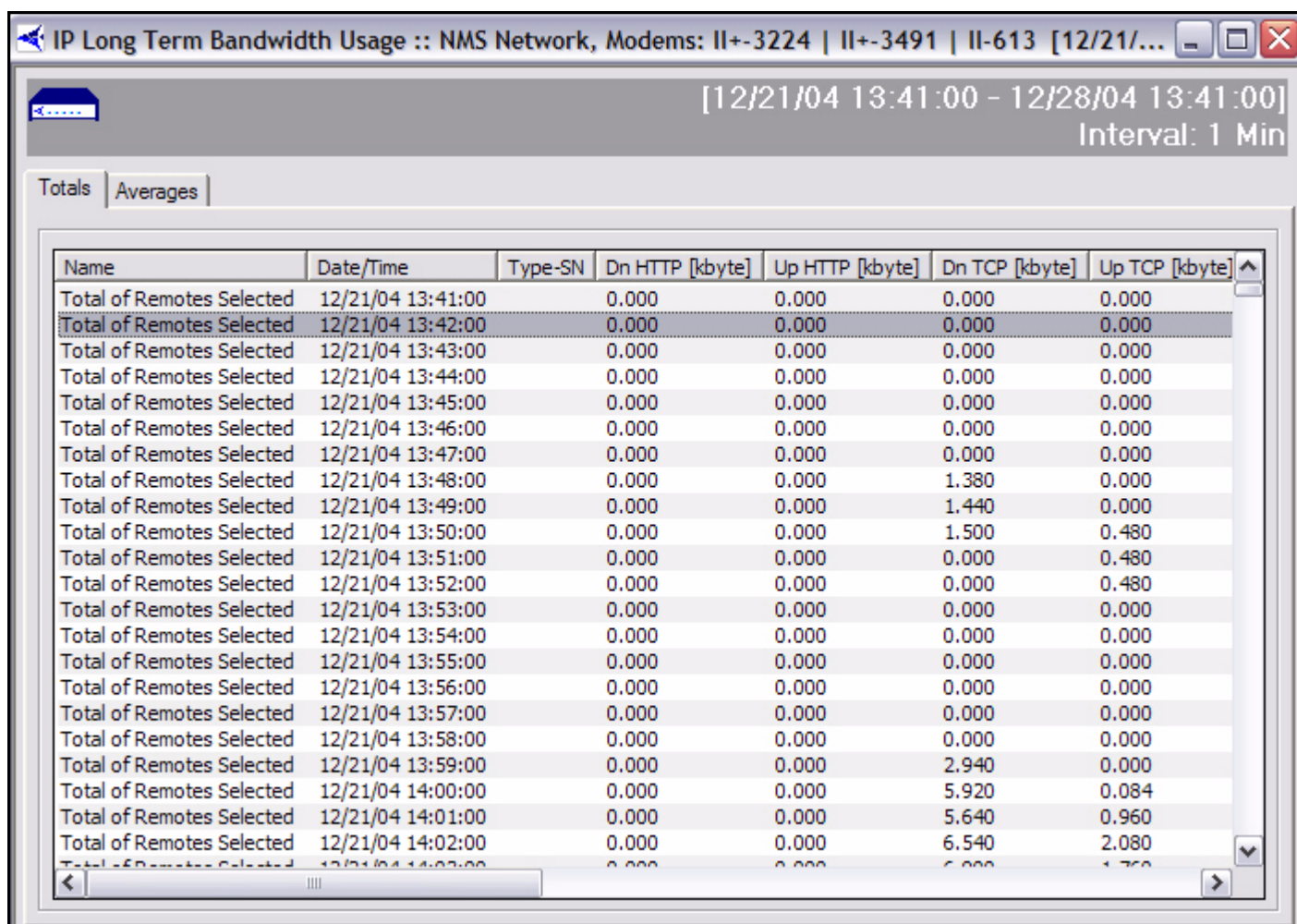


Figure 6-2: IP Long Term Bandwidth Usage Report

6.1.2.1 Interpreting the Report

Percentage of Channel Capacity

In addition to the kbps value, the averages tab contains the percentage of the maximum channel capacity on your upstream and/or downstream channels for the interval chosen. The values in these two columns will give you a general idea of the bandwidth margin you have on your upstream and downstream. The values are estimates only; the actual channel capacities may be slightly higher or lower depending on a number of factors, such as the number of remotes in the network, whether or not the Download Distributer is turned on, etc. However, the values are accurate enough to tell you when you should consider adding additional bandwidth to a particular channel.

For the downstream, we take 2.5% off the top for overhead. Overhead includes HDLC framing, timeplans, UCP commands, etc. The theoretical maximum for a downstream with a 2 Mbps information rate would be $2 * .975 = 1.95$ Mbps. For the upstream, we use the following calculation to determine the theoretical maximum in bits per second:

$$(\text{bytes per slot}) * (8 \text{ bits per byte}) * (\text{slots per frame}) * (1000 / \text{frame_len})$$

In the first clause, the byte count per slot does **NOT** include our internal overhead. Additionally, this calculation removes unique word and guard band overhead. In a typical network configuration with small FEC blocks, a 658 kbps information rate, a 125 ms frame, and 109 traffic slots, the theoretical maximum would be as follows:

$$(70 \text{ bytes per slot}) * 8 * (109 \text{ slots}) * (1000 / 125) = 488320 \text{ bps} = 488.320 \text{ kbps}$$

The upstream theoretical maximum is an estimate only; the actual maximum will vary depending on a number of factors, such as the number of remotes in the network, the minimum data rate for each remote, and IP packet sizes.

Keep in mind that the larger your interval, the lower the percentage will probably be. This is due to the fact that kbps values are averaged over the entire period of the interval, so spikes in activity will tend to be hidden in the average value.

6.2 Remote and Line Card Availability Reports

The Remote Availability report and Line Card Availability report allow you to report on the amount of time a remote or group of remotes was active in the network and able to pass IP traffic. The availability reports also includes a count of the number of times a remote or line card was out-of-network during the reporting period.

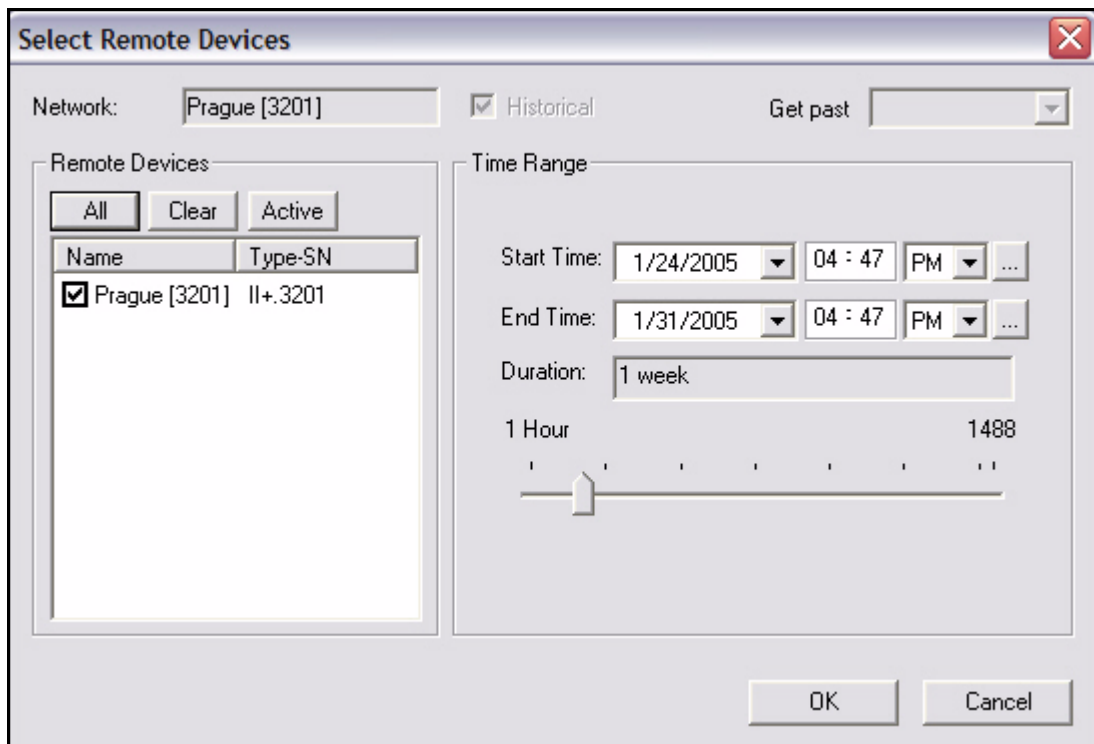
This report is available from the following levels of the network tree view:

- Network
- Inroute Groups
- Individual Remotes
- Individual Line Cards

This example explains how to view the Remote Availability report. You can perform similar steps to view the Line Card Availability report.

To generate, view, save, or print the Remote Availability report, follow the directions below:

- Step 1 Right-click a network, inroute group, or remote.
- Step 2 Select **Remote Availability**. The **Select Remote Devices** dialog box appears



Step 3 Make the appropriate selections, and click **OK**. The **Remote Availability** report appears, as shown below.

Specify the devices on which you want to report and the time period, and click **OK**.

The default time period is one week, but you can specify any arbitrary time period. By default, you can specify a time period up to two months in the past.

An example report is shown below. For each remote you selected, the report displays the percentage of the time period the device was up and down, and the total number of hours during the time period the device was up and down. “Up” refers to the time the remote was able to pass traffic, and “Down” refers to the time the remote was unable to pass traffic due to either a Layer 2 or Layer 3 Alarm being active (or both). The last line of the report shows the average up/down hours and percent of all the devices for which you generated the report.

Remote Availability :: UAT-RF Network, Prague [3201] [01/30/05 16:4...						
Time range: 01/30/05 16:45:00 - 01/31/05 16:45:00 Interval: 1 Day(s)						
Remote Name	Type...	Up [hrs]	Up [%]	Down ...	Down ...	Outag...
Prague [3201]	II+....	23.93	99.71	0.07	0.29	5
Average		23.93	99.71	0.07	0.29	5.00

7 Monitoring Remotes Using the Geographic Map

You can view your teleport and all remotes in your networks on iMonitor's Geographic Map. These elements are positioned on the map according to their current geographic locations. A remote is represented by a green, yellow, or red icon, depending on its real-time state. You can interact with the map to zoom, pan, select remotes for further operations, toggle labels and elevation, and perform other useful functions.



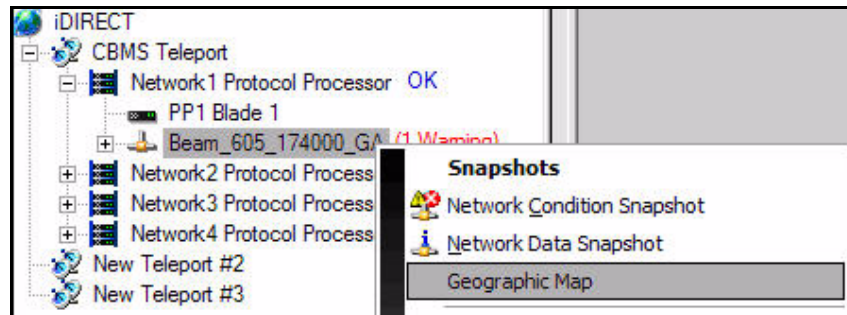
NOTE

You must be logged on as a Super User to use the Geographic Map in iMonitor. See the [iBuilder User Guide](#) for information on configuring user account privileges.

7.1 Launching the Geographic Map

To launch the geographic map:

- Step 1 Right-click a **Teleport**, a **Network** or an **Inroute Group** in the Network Tree and select **Geographic Map** to display the **Select Remotes** dialog box.



- Step 2 In the **Remotes** area of the **Select Remotes** dialog box, select the remotes you want to view on the map. You can use the buttons to select **All** remotes, to **Clear** all remotes, or to select only **Active** remotes. If you select **Historical** and enter a **Time Range**, the map will be displayed with remote tracking

over the selected time. (See [section 7.3 “Tracking and Locating Mobile Remotes”](#) on page 140 for details.)

Select Remotes

Teleport: ☒ Historical Get past:

Remotes

Name	Type-SN	Network
<input checked="" type="checkbox"/> 7350.5907	7350.5907	Beam_605_174000...
<input checked="" type="checkbox"/> 7350.5949	7350.5949	Beam_605_174000...
<input checked="" type="checkbox"/> II+.9177	II+.9177	Test Network
<input checked="" type="checkbox"/> 7350.5949	7350.5949	Beam_906_64000...
<input checked="" type="checkbox"/> 7350.12491	7350.12491	Beam_906_64000...
<input checked="" type="checkbox"/> 7350.5907	7350.5907	Beam_906_64000...
<input checked="" type="checkbox"/> 7350.5907	7350.5907	Beam_603_340000...
<input checked="" type="checkbox"/> 7350.5949	7350.5949	Beam_603_340000...
<input checked="" type="checkbox"/> 7350.12542	7350.12542	Beam_707_307000...
<input checked="" type="checkbox"/> 7350.5949	7350.5949	Beam_707_307000...
<input checked="" type="checkbox"/> 7350.5907	7350.5907	Beam_707_307000...

Time Range

Start Time: ...

End Time: ...

Duration:

1 Min 720 Min

- Step 3 As an alternative to selecting **Historical** and a **Time Range**, you can select a duration from the **Get Past** drop down menu to display tracking for that time period up to the present.

Get past:

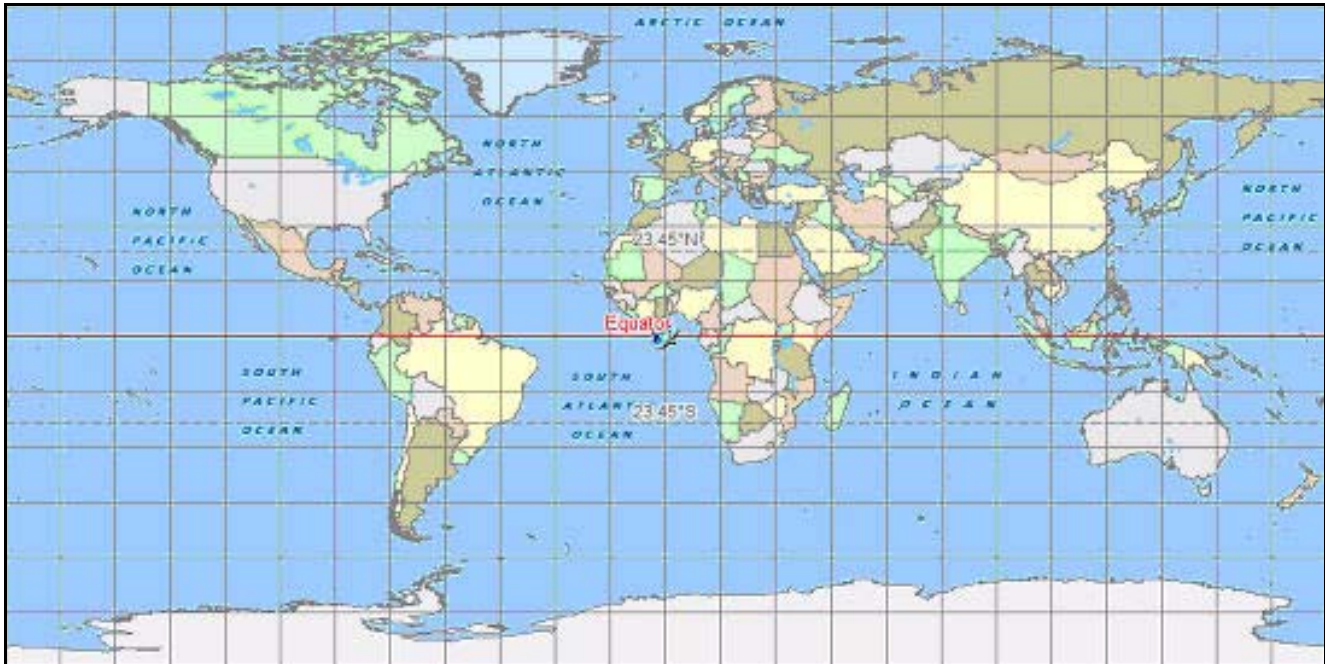
- None (Real-time)
- 10 minutes
- 15 minutes**
- 20 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 2 hours

5/ 9/2007 05

5/ 9/2007 05

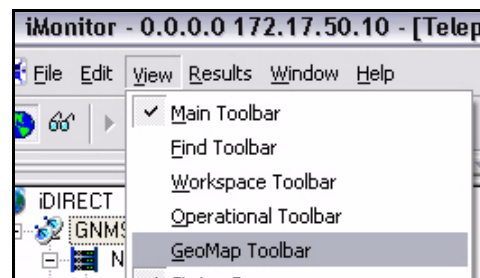
5 mins

Step 4 When you have finished making your selections, click **Ok** to view the Geographic Map in the main pane of the iMonitor display.



7.2 The Map Toolbar

The Map Toolbar allows you to interact with the map in various ways. To display the toolbar, select **GeoMap Toolbar** from the iMonitor **View** menu.



The toolbar is shown below. It is highlighted whenever one or more Geographic Maps is active.



The table below describes the functionality of all buttons on the Map Toolbar. Icon names used in this document are in bold typeface.

Table 7-1: Geographic Map Toolbar Icons and Functions






















Toolbar Icon	Functionality
	Allows you to Zoom In through successive map levels, centered on the current mid-point of the map.
	Allows you to Zoom Out through successive map levels, centered on the current mid-point of the map.
	Allows you to Pan to a new region of the map within the current zoom level by using the hand cursor to drag the map in any direction. If the entire map is visible, this function does nothing.
	Jumps directly to the Highest Zoom Level from the current zoom level. (The highest zoom level shows the entire map.)
	Allows you to Group Select a number of geographically-adjacent remotes by dragging a box around a group of remote icons. You can then right-click to launch the Network Tree menu for operations on multiple remotes. As with other group-select modes, the parameters dialog box for the selected display is pre-populated with your selected remotes.
	Allows you to click your mouse on a remote icon to determine Details of that remote. When you click a remote icon, the remote's name, exact location, and any current conditions are displayed.
	Enables and disables Mobile Remote Tracking . When enabled, mobile remotes that move within the network leave a trail on the map indicating where they have been.
	The Clear Track button clears the trails of mobile remotes from the map that result when Mobile Remote Tracking is enabled. This button does not disable Mobile Tracking.
	The Toggle Elevations button turns on or off elevation measurements and contours on the map display. Elevations are available only on lower zoom levels.
	The Map Labels button turns on or off the name display for map features such as cities, towns, rivers, ports, and highway route numbers. The labels displayed vary with zoom level.
	This button causes remotes to be displayed as Small Icons on the map.
	This button causes remotes to be displayed as Medium Icons on the map.
	This button causes remotes to be displayed as Large Icons on the map.

Table 7-1: Geographic Map Toolbar Icons and Functions (Continued)

Toolbar Icon	Functionality
	When enabled, the Circle Remote Images button causes the map to display a shadow or outline around each remote icon. This function is useful when remotes are clustered, or when elevation or label data obscures the remote icons.
	When enabled, the Flash Remote Images button causes all remote icons to flash continuously. This feature allows you to quickly identify all remotes in a specific network or inroute group. It is especially useful at higher zoom levels.
	When the Filter on Alarms button is selected, remotes with alarm status are visible on the map.
	When the Filter on Warnings button is selected, remotes with warning status are visible on the map.
	When the Filter on Mesh Alarms button is selected, remotes with mesh alarm status are visible on the map.
	When the Filter on OK button is selected, remotes with OK status are visible on the map.
	When the Filter on Elsewhere button is selected, roaming remotes with elsewhere status for the network being monitored are visible on the map.
	When the Filter on Offline button is selected, remotes with offline status are visible on the map.

7.3 Tracking and Locating Mobile Remotes

Stationary remotes are placed on the map during initialization when their geographic locations are stored in the NMS database. Mobile remotes, however, cannot be placed correctly until they report their locations to iMonitor.

By default, the map shows all mobile remotes in the same location: 0 degrees latitude and 0 longitude. To show your mobile remotes in the current, correct location, select the **Mobile Remote Tracking** button on the Map Toolbar. As the remotes transmit their geographic coordinates to the NMS, iMonitor places the remotes on the map in their reported locations.

Mobile remote tracking also traces the location history of each mobile remote in real time by leaving a grey ghost image of the remote whenever its reported location changes. In the figure below, the green icon just off the coast of Russia is the current location of the remote. The grey trail traces its movement over time.



NOTE

It is not possible to track Secure Mobile Remotes. By design, these units do not report their geographic locations to the hub.

Enabling Remote Tracking and Clearing Remote Tracks

To turn on Remote Tracking, select the **Mobile Remote Tracking** button on the Geographic Map Toolbar. iMonitor will update the map with your remotes' new locations each time they report their positions to the NMS. Past positions will be indicated by trails of grey icons on the map. To clear the trails for your remotes from the map, select the **Clear Tracks** button on the toolbar.

Determining a Remote's Current Location and State

When tracking your remotes, you can determine a remote's current location and state as follows:

- Step 1 Select the **Details** button on the Geographic Map toolbar.
- Step 2 Click the icon representing the remote on the map. An Information Message will display the remote's name, it's current position, and any conditions associated with the remote.



Determining a Remote's Past Locations at Specific Times

You can also determine the past locations of a remote at exact times.

- Step 1 Select the **Details** button on the Geographic Map toolbar.

- Step 2 Click any of the grey icons in the trail of a remote. An Information Message will display the name of the remote along with its position and the time of day when its location corresponded to the grey icon you selected.



7.4 Using the Map to Select from the Network Tree Menu

You can use the Geographic Map to display the remote Network Tree submenu and make menu selections for one or more remotes.

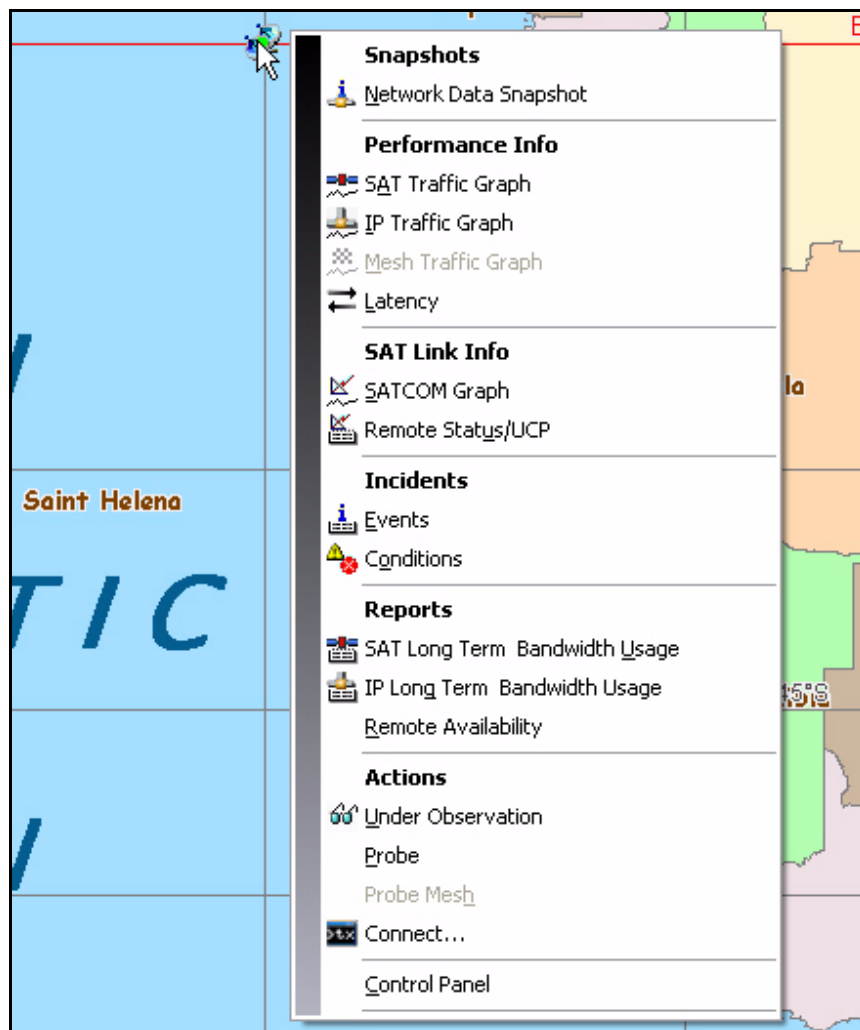
Selecting from the Remote Submenu for a Single Remote

If you hold the mouse pointer over a remote icon and right-click, the Tree submenu for remotes is displayed. You can then select an iMonitor operation from the remote menu. The remote you are pointing to will be pre-selected for the operation. This is identical to right-clicking the remote in the Network Tree View.

To use the Geographic Map to display the Network Tree menu for a single remote:

- Step 1 Select the **Details** button on the Geographic Map toolbar.
- Step 2 Place the cursor over the icon representing the remote on the map. (Do not click the remote.)

- Step 3 Right-click to display the remote submenu. When you select an operation from the menu, iMonitor will display the results with the remote pre-selected.



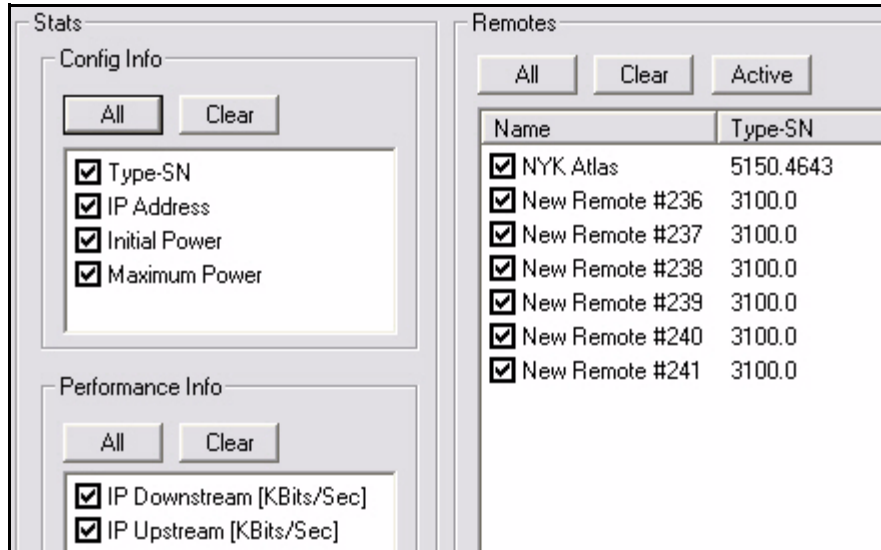
Selecting from the Remote Submenu for Multiple Remotes

If you right-click after selecting a group of geographically-adjacent remotes on the map, then all of those remotes will be pre-selected when the parameters dialog box is displayed.

To use the Geographic Map to select an operation for multiple remotes:

- Step 1 Select the **Group Select** button on the Geographic Map toolbar.
- Step 2 On the map, drag a box around the group of remotes you want to select.
- Step 3 Right click with the cursor over the selected group of remotes and select from the remote submenu. iMonitor will display the parameters dialog box with the all remotes in the group pre-selected. The figure below shows the

results of selecting seven remotes on the map, and then selecting **Network Data Snapshot** from the menu.



Name	Type-SN
<input checked="" type="checkbox"/> NYK Atlas	5150.4643
<input checked="" type="checkbox"/> New Remote #236	3100.0
<input checked="" type="checkbox"/> New Remote #237	3100.0
<input checked="" type="checkbox"/> New Remote #238	3100.0
<input checked="" type="checkbox"/> New Remote #239	3100.0
<input checked="" type="checkbox"/> New Remote #240	3100.0
<input checked="" type="checkbox"/> New Remote #241	3100.0

7.5 Geographic Map Filtering Based on Remote Status

By default, all remotes are visible on the geographic map. However, you can set filters to view or hide remotes on the map based on the real-time status of the remotes in the network. When a remote filter is selected, all remotes with that status are displayed. When a filter is not selected, remotes with that status become invisible.



NOTE

If the status of a remote changes so that the remote status no longer matches a selected filter, the remote will disappear from the map. Similarly, if a remote that was not visible due to filtering changes to a visible status, the remote will appear on the map.

The following criteria can be applied when filtering Remotes on the geographic map:

- Show all remotes (no filtering)
- Show or hide remotes with Alarm status
- Show or hide remotes with Warning status
- Show or hide remotes with Mesh Alarm status
- Show or hide remotes with OK status
- Show or hide remotes with Elsewhere status (See note below.)
- Show or hide remotes with Offline status
- Hide all remotes



NOTE

Remotes with Elsewhere status are roaming remotes that are configured in the network being monitored, but that have moved to another network. An icon for a remote with Elsewhere status reflects the last position in which that remote was displayed on the geographic map prior to leaving the network.

Filters can be set either by selecting icons on the geographic map toolbar, or by right-clicking in the map pane and using the filter menu. The following two sections describe these options.

Applying Filters Using the Geographic Map Toolbar

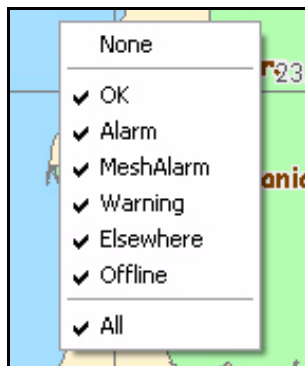
Clicking a filter icon on the map toolbar toggles the associated remote status between visible and invisible. When a filter icon is selected, remotes with that status are visible on the map. When a filter icon is cleared, remotes with that status are not displayed. By default, all filter icons are selected, making all remotes visible on the map. With the settings shown in the figure below, only remotes with Alarm status or Warning status are displayed on the map. (See [Section 7.2 “The Map Toolbar” on page 137](#) for filter icon definitions.)



Applying Filters Using the Filter Menu

To filter on remote status using the geographic map filter menu:

- Step 1 Right-click anywhere in the geographic map pane where no remotes are present to display the menu. By default, all remotes are visible, regardless of status.



- Step 2 Select or clear the check marks in the menu to choose the remotes you want to view on the map. You can select any combination of status filters.

With the settings shown in the figure below, only remotes with **Alarm** or **Warning** status are visible on the map.



NOTE

Selecting **All** from the filter menu selects all menu items. Selecting **None** clears all selections. These are quick methods for toggling all geographic map filtering on or off.

Appendix A Accessing the NMS Statistics Archive

Many of our customers have requested specific reports on various aspects of their network behavior, ranging from IP traffic activity to system uptime to satellite link behavior. iMonitor allows users to retrieve historical data and populate a number of raw and graphical displays on both firmware versions and per-remote uptime via web-based tools. iMonitor also provides an easier way of retrieving long-term bandwidth usage statistics for network usage profiling.

iDirect also provides limited support for read-only direct archive access. This section discusses how this is done and provides information about specific tables in the archive database.



NOTE

The intended audience for this appendix is a technical person who has experience developing relational database applications, preferably using ODBC.

A.1 Optimization of the Statistics Archive

The NMS employs the techniques described in this section in order to store the archive data efficiently and to minimize data retrieval time.

A.1.1 Optimized NMS Statistics Archive Storage

In order to efficiently store the data, the statistics archive eliminates or consolidates certain records according to the following rules:

- All-zero IP Stats and SAT Stats are not logged to the archive. This happens for remotes that are out-of-network. The long-term bandwidth reports and usage displays handle missing messages automatically. *Note: if you access the stats archive using ODBC, you may have to modify your reporting software to handle gaps in the data.*
- Latency measurements below a default threshold of 800 msec are not logged to the archive; only measurement times above this value are logged.
- Consecutive latency time-outs are written to a single entry in the database along with a count. For example, 10 consecutive latency time-outs are written as a single database record with a count of -10.
- Consecutive SWEEP messages are written to a single entry in the database along with a count. For example, 10 consecutive SWEEPs are written as a single database record with a count of 10.

All of these settings can be overridden or modified if necessary. Please contact iDirect's Technical Assistance Center for help changing the default archive behavior.

A.1.2 Optimized NMS Statistics Archive Lookup

Large historical requests are broken into multiple segments that are processed separately. This results in better memory utilization on the server and improved response time in the GUI.

A.1.3 Archive Consolidation

To prevent filling up the NMS server's hard disk, a consolidation process runs every night at approximately midnight by default. Using rules defined in the config database, it runs through all tables in the archive database and either deletes old records or collects multiple records together into a single record.

Consolidation rules govern how long data is saved, and are given default values when your configuration database is created. These defaults are designed to allow your networks to grow quite large (many hundreds of remotes) without you having to worry about disk space problems. If you want to modify the default values, please contact iDirect's Technical Assistance Center (TAC) at (703) 648-8151 for assistance. The default consolidation values for each table are listed in [Table A-1](#) on [page 151](#).

A.2 NMS Database Overview

Connecting to the NMS Archive Database with ODBC

All statistical archive information is contained in a MySQL relational database on the primary NMS server machine. MySQL is an open source database server that is widely praised in the Linux community for its reliability, speed, and ease-of-use. There are many different books available on MySQL, and there is a wealth of information online at www.mysql.com.

Obtaining the ODBC Connection Library

MySQL supports access via the Microsoft standard called ODBC (for Open DataBase Connectivity). The installation of MySQL on your NMS server already contains support for ODBC connections, so there's nothing you have to download to from the Internet to enable ODBC access on the server-side. However, you must download the appropriate ODBC client library from the MySQL web site. Full details, including an installation and usage manual, are available from www.mysql.com.

Setting up a Simple ODBC Access Account

As the name implies, access with ODBC is open, i.e. not secure, so we require setting up a specific read-only MySQL account to restrict access to just the information you need to generate reports. The details of this user account are typically specific to each customer installation. However, we have provided instructions here for setting up a generic read-only account.

Step 1 Log in to the NMS server as "root".

Step 2 Enter the mysql database utility:

```
mysql
```

Step 3 At the mysql prompt, type the following command:

```
mysql> grant SELECT on *.* to <user>@'%' identified by  
"password";
```

Replace the string <user> with the user name you want for the account, and replace the string "password" with the password you want. Note that the

double quotes around password and single quotes around the percent sign are required.

Step 4 Activate the account:

```
mysql> flush privileges;
```

Step 5 Exit the mysql utility:

```
mysql> quit;
```

The user you just created has the following privileges:

- Can connect from any host.
- Can see all databases.
- Can only read information.

You can further restrict the access privileges on this account, e.g. you can specify connection only from a specific remote host. If you wish to tailor this account to provide additional security, you should contact iDirect's TAC at (703) 648-8151.

Once you have set up the read-only access account, you must connect to the database named "nrd_archive". Other connection details are your responsibility. There are a number of database clients that support ODBC connections, each with their own specific requirements. Unfortunately, we are unable to provide support for all the different ODBC clients in the marketplace.

A.3 Basic Archive Database Information

Types of NMS Databases and Supported Access

The NMS stores its information in two separate databases. One database, typically called the "config database", contains all the configuration information that you define in iBuilder: remotes, hub line cards, carriers, etc. The other database, called the "archive database", contains all the real-time statistical information generated by your networks: IP stats, remote status, conditions, etc.

iDirect supports read-only access to the archive database only. The configuration database contains a number of intricate relationships between tables that require a detailed knowledge of the structure to interpret. This structure usually changes from one release to another to allow configuration of new data path features, which would further complicate customer access.

Structure Changes between Releases

The structure of the archive database tables has remained relatively static over recent releases. While we anticipate this to be the case in the future as well, iDirect reserves the right to change this structure from one release to another to improve the product and to enhance statistical information about real-time operation. These changes may impact your custom reports, and if so will require ongoing maintenance by someone on your staff. We will document all changes and additions to the archive database, but iDirect cannot take responsibility for customer reports that break due to database structure changes.

Accessing Remote and Network Names from Configuration Database

There are two exceptions to the restriction on accessing the config database: retrieval of remote names and network names. Entries in the archive database are keyed to individual remotes by a unique database ID, and do not contain the name assigned to the remote in iBuilder. To retrieve the remote's name, you must reference the appropriate table in the config database with the unique ID.



NOTE

Retrieving information based on serial number is not recommended – you will lose access to historical data if the hardware is swapped in the field.

In the archive database, remote unique ids in all tables are stored in the column named "unique_id". In the config database, this same ID is stored in a table named "NetModem" in the column "NetModemId". The remote name is in the column named "NetModemName".

A sample SQL query that grabs the remote's name from a known remote ID might be:

```
select NetModemName from nms.NetModem where NetModemId = 15;
```

The config database name is "nms", and that name must be in your query to tell the MySQL server which database to look in.

In the archive database, network ids in all tables are stored in the column named "network_id". In the config database, this same ID is stored in a table named "Network" in the column named "NetworkId". The network name is in the column named "NetworkName".

A sample SQL query that grabs a remote's network name from a known network ID might be:

```
select NetworkName from nms.Network where NetworkId = 1;
```

Timestamps

All raw data received from network elements is time stamped at the NMS prior to being written to the database. All timestamp fields in the archive database are Linux time_t values, which represent the number of seconds since January 1, 1970.

Overview of the Archive Database Tables

The following table contains a list of all the archive database tables, what information each one contains, and how long the data is saved. Each table is discussed in greater detail later in this appendix.



NOTE

For efficiency, archive data is divided into multiple tables for each data type. Names of tables that contain data are derived from the base table names shown in [Table A-1](#). For details, see [Section A.5 "NMS Statistics Archive Database Restructuring" on page 167](#). When referring to "tables" in this section, the base table name is used.

Table A-1: Archive Database Tables

Base Table Name	Contains	Data Saved For
raw_ip_stats	IP stats sent from the protocol processor	24 hours
ip_minute_stats	raw IP stats consolidated to one record per minute	30 days
ip_hour_stats	IP minute stats consolidated to one record per hour	6 months
lat_stats	latency measurement	1 week
nms_hub_stats	hub line card statistics	1 week
nms_remote_status	remote information	1 week
nms_ucp_info	uplink control adjustments	1 week
event_msg	events sent from protocol processors, hub line cards, and remotes	1 week
state_change_log	hub line card and remote state changes (conditions raised and lowered)	30 days
pp_state_change_log	protocol processor state changes	30 days
chassis_state_change_log	chassis state changes	30 days
raw_ota_stats	Over-the-air stats sent from the protocol processor	24 hours
ota_minute_stats	raw ota stats consolidated to one record per minute	30 days
ota_hour_stats	ota minute stats consolidated to one record per hour	6 months
raw_otacast_stats	Over-the-air multicast stats sent from the protocol processor	24 hours
otacast_minute_stats	raw otacast stats consolidated to one record per minute	30 days
otacast_hour_stats	otacast minute stats consolidated to one record per hour	6 months
raw_mesh_stats	Mesh stats sent from the remote	24 hours
mesh_minute_stats	raw mesh stats consolidated to one record per minute	30 days
mesh_hour_stats	mesh minute stats consolidated to one record per hour	6 months

A.4 Database Table Details

The following sections describe each of the archive tables in some detail. For further information, please contact iDirect's Technical Assistance Center (TAC) at (703) 648-8151.

A.4.1 IP Stats Tables

As shown in [Table A-1](#), there are three separate base table types for IP stats, each one containing records that cover a particular period of time. The `ip_minute_stats` and `ip_hour_stats` tables have all the fields contained in the `raw_ip_stats` plus additional fields containing maximum and standard deviation calculations for all IP types. These fields are discussed in more detail later in this section.

IP statistics for all active remotes are calculated on the protocol processor and sent to the NMS every 5 seconds. After sending a stats message, the protocol processor zeros its counts, so that every database record contains the delta in activity from the previous record. The protocol processor continues to send messages to the NMS even if a remote is out-of-network; the counts for these records contain all zeros.



NOTE

For convenience, HTTP traffic is broken out separately from TCP traffic, but the TCP counts include HTTP as well. If you want a total count of traffic, do not include the HTTP values in your addition.

Table A-2: IP Stats Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the message arrived at the NMS server
t_interval	int(10) unsigned	interval in seconds that the data covers
network_id	smallint(5) unsigned	identifies the network
unique_id	int(10) unsigned	uniquely identifies the remote
modem_sn	smallint(5) unsigned	remote's serial number
rx_tcp_kbyte	double	kilobytes of TCP data received from the remote (upstream)
tx_tcp_kbyte	double	kilobytes of TCP data sent to the remote (downstream)
rx_udp_byte	double	kilobytes of UDP data received from the remote
tx_udp_kbyte	double	kilobytes of UDP data sent to the remote
rx_icmp_kbyte	double	kilobytes of ICMP data received from the remote
tx_icmp_kbyte	double	kilobytes of ICMP data sent to the remote
rx_igmp_kbyte	double	kilobytes of IGMP data received from the remote
tx_igmp_kbyte	double	kilobytes of IGMP data sent to the remote
rx_http_kbyte	double	kilobytes of HTTP data received from the remote.
tx_http_kbyte	double	kilobytes of HTTP data sent to the remote
rx_other_kbyte	double	kilobytes of data from other protocol types received from the remote.
tx_other_kbyte	double	kilobytes of data from other protocol types sent to the remote

Consolidated IP Stats Tables

The two consolidated tables, ip_minute_stats and ip_hour_stats, contain all the fields in the raw_ip_stats table plus the additional fields that hold maximum and standard deviation values for each IP type. Each maximum column indicates the maximum individual measurement of all records consolidated into this record. Each standard deviation value, calculated using a common formula, tells you how clustered the consolidated measurements were around the average of all consolidated data records.

Table A-3: Additional Consolidated IP Stats Table Fields

Column Name	Data Type	Meaning
rx_tcp_max	double	The maximum rx_tcp_kbyte value of the records consolidated into this record.
tx_tcp_max	double	As above, for tx_tcp_kbyte
rx_udp_max	double	As above, for rx_udp_kbyte
tx_udp_max	double	As above, for tx_udp_kbyte
rx_icmp_max	double	As above, for rx_icmp_kbyte
tx_icmp_max	double	As above, for tx_icmp_kbyte
rx_igmp_max	double	As above, for rx_igmp_kbyte
tx_igmp_max	double	As above, for tx_igmp_kbyte
rx_http_max	double	As above, for rx_http_kbyte
tx_http_max	double	As above, for tx_http_kbyte
rx_other_max	double	As above, for rx_other_kbyte.
tx_other_max	double	As above, for tx_other_kbyte.
rx_tcp_stddev	float(10,5)	The standard deviation of all consolidated rx_tcp_kbyte records.
tx_tcp_stddev	float(10,5)	As above, for tx_tcp_kbyte
rx_udp_stddev	float(10,5)	As above, for rx_udp_kbyte.
tx_udp_stddev	float(10,5)	As above, for tx_udp_kbyte.
rx_icmp_stddev	float(10,5)	As above, for rx_icmp_kbyte
tx_icmp_stddev	float(10,5)	As above, for tx_icmp_kbyte
rx_igmp_stddev	float(10,5)	As above, for rx_igmp_kbyte
tx_igmp_stddev	float(10,5)	As above, for tx_igmp_kbyte
rx_http_stddev	float(10,5)	As above, for rx_http_kbyte
tx_http_stddev	float(10,5)	As above, for tx_http_kbyte
rx_other_stddev	float(10,5)	As above, for rx_other_kbyte
tx_other_stddev	float(10,5)	As above, for tx_other_kbyte

Statistics Consolidation Process

Four types of statistics are consolidated by the NMS:

- IP statistics
- Over-the-air statistics
- Over-the-air multicast statistics
- Mesh statistics

The statistics consolidation process is more complicated than for data in other tables. It's a multi-step process designed to keep very old data without losing information, and at the same time optimize disk space usage. As the stats data gets older, multiple individual records are combined together to form a single record. Using this method, the count of total traffic sent through the system is maintained as the data ages; all that's lost is the granularity between shorter periods of time.

The consolidation process works as follows. Every day, using consolidation parameters from the config database, the consolidator process performs the following tasks on the each of the four raw stats tables (default values are used here):

- Step 1 Delete all records from the hour stats table older than 4464 hours.
- Step 2 Consolidate all records from the minute stats table older than 744 hours into one record per hour and write that record to the ip_hour_table.
- Step 3 Delete all records from the minute stats table older than 744 hours.
- Step 4 Consolidate all records from the raw stats table older than 24 hours into one record per minute and write that record to the minute stats table.
- Step 5 Delete all records from the raw stats table older than 24 hours.

A.4.2 Latency Measurements

The lat_stats table contains latency measurement results for all active remotes in the network. To generate latency information, the NMS latsvr process sends ICMP echo requests to all active remotes every 5 seconds and measures the round trip time. Queries for individual remotes are offset in time to prevent a burst of messages every 5 seconds. For remotes that are out-of-network, the round trip time is -1 or -100. [Table A-4](#) shows the contents of the lat_stats table.

Table A-4: lat_stats Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t the round trip time was calculated
network_id	smallint(5) unsigned	identifies the network
unique_id	int(10) unsigned	uniquely identifies the remote
modem_sn	int(10) unsigned	remote's serial number

Table A-4: lat_stats Record Format (Continued)

Column Name	Data Type	Meaning
rtt	double	the measured round trip time in milliseconds (-1 or -100 if remote is out-of-network)
ip_addr	varchar(20)	IP address that was queried (management IP address of the remote)

If remotes are not active in the network, i.e. they are deactivated or incomplete in iBuilder, the latency server will not attempt to measure their latency and no data will be written to this table in the database for them.

A.4.3 Hub Line Card Statistics

All hub line cards in steady state send a statistics message into the NMS every 15 seconds. This message serves two purposes: the absence of the message causes an alarm to be raised in iMonitor, and it contains useful information about the last 15 seconds of hub line card activity. The data values in each message represent deltas from the previous message. [Table A-5](#) shows the contents of the nms_hub_stats table.

Table A-5: nms_hub_stats Table Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the message arrived at the NMS server
network_id	smallint(5) unsigned	identifies the network
unique_id	int(10) unsigned	uniquely identifies the hub line card
modem_sn	int(10) unsigned	hub line card's serial number
scpc_num_tx_attempts	int(10) unsigned	number of SCPC transmit attempts
scpc_num_tx_bytes	int(10) unsigned	number of SCPC bytes transmitted
scpc_num_tx_errors	int(10) unsigned	number SCPC transmit errors
acq_crc_errors	int(10) unsigned	number of acquisition CRC errors
traffic_crc_errors	int(10) unsigned	number of traffic CRC errors
bursts_detected	int(10) unsigned	number of TDMA bursts detected at this hub
bytes_rxed	int(10) unsigned	number of TDMA bytes received at this hub
rx_overflow_frames	int(10) unsigned	number of times the DMA was reset due to an overflow condition
rx_composite_power	double	output of the receive power detector converted to dBm.
rx_tunnel_errors	int(10) unsigned	number of receive tunnel errors.
tx_tunnel_errors	int(10) unsigned	number of transmit tunnel errors.
rx_digital_gain	smallint(5) unsigned	receive digital gain at the hub

Table A-5: nms_hub_stats Table Format (Continued)

Column Name	Data Type	Meaning
scpc_snr_cal	double	calibrated SNR value of the loopback downstream carrier
scpc_sym_offset	int(11)	loopback SCPC symbol offset.
scpc_freq_offset	int(11)	loopback SCPC frequency offset.
scpc_frame_lock_status	tinyint(4)	SCPC loopback lock status (locked, unlocked)
lostlock_count	int(10) unsigned	number of times SCPC frame lock was lost
flr_dac	int(10) unsigned	current value of the frequency locked loop digital to analog converter; normal range is 0x200 to 0xE00

Transmit (tx) values are always zero for receive-only line cards, and receive (rx) values are always 0 for transmit-only line cards. While traffic CRCs almost always indicate an anomaly condition, acquisition CRC values well above zero are normal when remotes are coming into the network. In fact, by default iMonitor doesn't raise a warning condition on acquisition CRCs until they go above 200 in a 15 second period.

A.4.4 Remote Status

All remotes in steady state send a status message into the NMS every 15 seconds. This message is sent as a UDP datagram, so there's no guarantee that every message sent will be received. However, built-in QoS rules give it higher priority than other types of traffic, and our experience has shown that these messages are rarely dropped. The message contains a variety of information about the remote, including temperature, number of milliseconds since last boot-up, perceived SNR, etc. In the absence of other traffic from the remote, the `nms_remote_status` message fits into a single small-block TDMA burst. Its contents are shown in [Table A-6](#) below.

Table A-6: nms_remote_status Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the message arrived at the NMS server
network_id	smallint(5) unsigned	identifies the network
unique_id	int(10) unsigned	uniquely identifies the remote
modem_sn	int(10) unsigned	remote's serial number
time_tics	bigint(20) unsigned	number of milliseconds since last boot-up
snr_cal	double	calibrated SNR value of the downstream carrier
rx_power	double	output of the receive power detector converted to dBm
power_in_dbm	double	current transmit power in dBm
temperature_celcius	double	current temperature measured on the board (not ambient temp)

Table A-6: nms_remote_status Record Format (Continued)

Column Name	Data Type	Meaning
digital_rx_power	double	derived from the digital gain setting in the SCPC demod, converted to dBm
lostlock_count	int(10) unsigned	number of time since boot-up that the remote has lost lock on the downstream carrier
flr_dac	int(10) unsigned	current value of the frequency locked loop digital to analog converter; normal range is 0x200 to 0xE00
rmtflags	int(10) unsigned	boolean flag field; contact iDirect's TAC for latest definition
rx_cof	int(11)	carrier offset frequency; difference, in Hz, of the incoming frequency and the receiver's reference frequency
scpc_rx_errors	int(10) unsigned	number of SCPC receive errors since last boot-up
tdma_snr_cal	double	calibrated SNR value of the upstream carrier
tdma_sym_offset	smallint(6)	TDMA symbol offset
tdma_freq_offset	int(11)	TDMA frequency offset
tdma_crc_errors	int(10) unsigned	number of tdma crc errors during the last interval
rx_reliable_byte	int(10) unsigned	reliable (e.g. TCP) bytes received by the remote
tx_reliable_byte	int(10) unsigned	reliable (e.g. TCP) bytes sent by the remote
rx_unreliable_byte	int(10) unsigned	unreliable (e.g. UDP) bytes received by the remote
tx_unreliable_byte	int(10) unsigned	unreliable (e.g. UDP) bytes sent by the remote
rx_oob_byte	int(10) unsigned	out-of-band bytes received by the remote
tx_oob_byte	int(10) unsigned	out-of-band bytes sent by the remote

A.4.5 Uplink Control Adjustments

To maintain iDirect's industry-leading "always on" feature, the protocol processor sends a network adjustment message to each in-network remote every 20 seconds. The message is also sent into the NMS for archiving purposes. The timing of each message is offset to prevent a burst of traffic at 20-second boundaries, so timestamps will typically vary from remote to remote. This message contains adjustment values for power, frequency, and timing offset to account for a variety of conditions: satellite drift, weather conditions at the hub or remote, and remote transmit equipment inaccuracies. The format of the nms_ucp_info table is shown in [Table A-7](#).

Table A-7: nms_ucp_info Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the message arrived at the NMS server
network_id	smallint(5) unsigned	identifies the network
unique_id	int(10) unsigned	uniquely identifies the remote

Table A-7: nms_ucp_info Record Format (Continued)

Column Name	Data Type	Meaning
modem_sn	int(10) unsigned	remote's serial number
sym_offset	int(11)	timing offset in symbols; the remote applies this offset to its current frame start delay value
power_adjustment	int(11)	power offset in dBm; the remote adjusts its transmit power by this value
freq_offset	int(11)	frequency offset; the remote adjusts its current transmit frequency by this value
snr_cal	double	the current SNR of the remote's transmit signal as perceived at the hub
scpc_snr_cal	double	the current SNR of the hub loopback SCPC transmit signal as perceived at the hub

A.4.6 Event Messages

All protocol processors, hub line cards, and remotes send in event messages to record certain situations that arise during operations. Some events cause conditions to be raised in iMonitor and others are for informational purposes only. Event messages are not sent at regular time intervals, nor do they follow a specific text format. The format of the event_msg table is shown in [Table A-8](#).

Table A-8: event_msg Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the message arrived at the NMS server.
event_level	int(11)	a number signifying the severity level of the message. This field deprecated.
event_class	int(11)	a number signifying the portion of the system that generated the event. This field is deprecated.
unique_id	int(10) unsigned	uniquely identifies the remote or hub line card (0 for protocol processor events)
modem_sn	int(10) unsigned	the remote's or line card's serial number (0 for protocol processor events)
time_tics	bigint(20) unsigned	for remotes and line cards, the number of milliseconds since boot-up; for protocol processors, time_t in milliseconds of the machine
msg	varchar(255)	free-form event message text

A.4.7 Hub and Remote State Changes

During everyday system operation, situations occasionally arise that require operator attention, or at least operator notification. These situations are called “conditions”, and are associated with a change in the operational state of the network element in question. Examples of conditions include temperature warnings, SNR below limit warnings, and out-of-network alarms.

All conditions and changes of state are recorded in the archive database. For hub line cards and remote units, these conditions are recorded in the archive table `state_change_log`. The format of this table is shown in [Table A-9](#) below.

Table A-9: state_change_log Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the condition was raised or cleared
unique_id	int(10) unsigned	uniquely identifies the remote or hub line card
modem_sn	int(10) unsigned	remote's or line card's serial number
current_state	enum	current state of the modem after this condition is processed; values are: <ul style="list-style-type: none">• OK• WARNING• ALARM• UNKNOWN• OFFLINE• ELSEWHERE• MESHALARM• STATE_NONE NOTE: MySQL enumeration types are 1-based, not 0-based.
occurred_at	timestamp(14)	time_t of original condition in the case of multiple simultaneous conditions

Table A-9: state_change_log Record Format (Continued)

Column Name	Data Type	Meaning
error_type	smallint(6)	<p>translates to a condition type; current values are (in ascending numeric order):</p> <ul style="list-style-type: none"> • UPSTREAM_SNR = 0 • DOWNSTREAM_SNR • LOCAL_LAN_DISCONNECT • UCP_LOST_CONTACT, • TEMP_LIMIT • LL_DOWN • UCP_OUT_OF_NETWORK, • LATENCY • LAT_TIMEOUT • LACK_HUB_STATS • ACQ_HUB_MODEM_CRC • TRAFFIC_HUB_MODEM_CRC • SYMBOL_OFFSET • REMOTE_OFFLINE • RX_OVERFLOW_FRAMES • CALIBRATED_TX_POWER • TX_FREQUENCY • MOBILE_LOST_GPS • DOWNSTREAM_PPS_OVERDRIVE • BACKPLANE_LOST_10MHZ • FAILED • RESET • UNREADY • SCPC_RX_ERRORS • FLL_DAC_ERRORS • FLASH • ACTIVATION_STATUS • ELSEWHERE_ERROR • FANALARM • AGCOUTOFRANGE
error_severity	enum	<p>severity of the condition; values are:</p> <ul style="list-style-type: none"> • EVTWarning • EVTAlarm • EVTCleared • EVTOffline • EVTElsewhere • EVTMeshAlarm • EVTNone <p>NOTE: MySQL enumeration types are 1-based, not 0-based.</p>
reason	varchar(255)	text explanation of the condition

Interpreting the entries in the `state_change_log` table requires some understanding of how the NMS manages conditions and overall element state. First of all, it is possible for multiple conditions to be active for a single hub or remote at any given time. Consider the following scenario:

1. A remote is in steady state with no active conditions. The overall state of the unit is OK.
2. A rain storm blows into a remote's location, which causes the SNR of the downstream signal to drop below the defined low limit. This is condition 1, a warning. The overall state of the unit changes to WARNING.
3. The weather situation persists, and the protocol processor loses contact with the remote. This is condition 2, a warning. The overall state of the unit remains at WARNING.
4. The protocol processor is unable to re-gain contact with the remote, so it declares the unit out-of-network. This is condition 3, an alarm. The overall state of the unit changes to ALARM.
5. The NMS latency server stops hearing ICMP echo responses from the remote. This is condition 4, an alarm. The overall state of the unit remains at ALARM.

We now have four simultaneously active conditions, and the overall state of the remote is ALARM. Each time a new condition is raised for a remote, it is written to the database with the current time of the NMS server machine in the `timestamp` field. The `occurred_at` field is also given the same timestamp. All pre-existing conditions for that same element are re-written with the same timestamp in the `timestamp` field. However, their `occurred_at` fields remain unchanged, thus indicating the time those conditions were first raised. Using the `timestamp` field as a key, you can determine all active conditions for a remote at any given time.

When conditions clear, they are written once again to the `state_change_log` table, but this time with the `severity` field set to `EVT_CLEARED`. Not all conditions clear at the same time, but when all conditions have cleared the overall state of the unit returns to OK.

The only conditions with alarm severity are those that cause a service interruption. Currently there are three conditions that fall into this category: `LLDOWN` (layer 2), `UCP_OUT_OF_NETWORK` (layer 2), and `LAT_TIMEOUT` (layer 3). You can generate a remote up/down report for a given time period by correctly parsing the entries in this table and ignoring all warning conditions.

A.4.8 Protocol Processor State Changes

Protocol processor state changes are stored in their own table in MySQL, named the `pp_state_change_log`. Currently the event server generates no PP-specific warnings; its possible states are UNKNOWN, OK, and ALARM. The OK state is present whenever the event server is hearing a special PP heartbeat event, and ALARM when that event fails to arrive two successive timeout periods (6 seconds each). The UNKNOWN state is the default state of all PPs in the event server when it initially starts up, before it has heard from PPs in the network.

All changes of PP state are stored in the `pp_state_change_log` table. The format of this table is shown in [Table A-10](#) below.

Table A-10: pp_state_change_log Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that this condition was raised or cleared
pp_id	int(10) unsigned	uniquely identifies the protocol processor
blade_id	int(10) unsigned	identifies the protocol processor blade
current_state	enum	current state of the protocol processor after this condition is processed; values are: <ul style="list-style-type: none"> • OK • WARNING • ALARM • UNKNOWN • OFFLINE • STATE_NONE Currently, only OK, ALARM, and UNKNOWN are raised for protocol processors.
occurred_at	timestamp(14)	time_t the condition was first raised in case of multiple simultaneous conditions
error_severity	enum	severity of the condition; values are <ul style="list-style-type: none"> • EVTWarning • EVTAlarm • EVTCleared • EVTOffline • EVTNone
reason	varchar(255)	text explanation of the condition

Entries in this table can be processed in essentially the same way as hub line card and remote state changes. See that section for more details.

A.4.9 Hub Chassis State Changes

Hub chassis state changes are stored in their own table in MySQL, named the chassis_state_change_log. Chassis warnings are raised for power and fan alarms from the chassis. The event server and iMonitor treat these “alarms” as warnings, since service is not interrupted and immediate action is not absolutely necessary. The ALARM condition is raised only when the event server loses contact with the hub chassis. In this case, service may still not be interrupted, since the event server communicates with an independent component of the chassis known as the EDAS board.

Chassis state changes are stored in the chassis_state_change_log table. The format of this table is shown in [Table A-11](#) below.

Table A-11: chassis_state_change_log Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that this condition was raised or cleared
chassis_id	int(10) unsigned	uniquely identifies this chassis
current_state	enum	current state of the chassis after this condition is processed; values are: <ul style="list-style-type: none"> • OK • WARNING • ALARM • UNKNOWN • OFFLINE • STATE_NONE
occurred_at	timestamp(14)	time_t this condition was first raised in the case of multiple simultaneous conditions.
severity	enum	severity of this condition; values are: <ul style="list-style-type: none"> • EVTWarning • EVTAlarm • EVTCleared • EVTOffline • EVTNone
reason	varchar(255)	text explanation of this condition

A.4.10 Over-the-Air Statistics Tables

As shown in [Table A-1](#), there are three separate base table types for over-the-air statistics, each one containing records that cover a particular period of time. The ota_minute_stats and ota_hour_stats tables have all the fields contained in the raw_ota_stats plus additional fields containing maximum and standard deviation calculations for all fields of over-the-air data. These fields are discussed in more detail later in this section.

Over-the-air statistics for all active remotes are calculated by the protocol processor and sent to the NMS every five seconds. After sending a stats message, the protocol processor zeros its counts, so that every database record contains the delta in activity from the previous record. The protocol processor continues to send messages to the NMS even if a remote is out-of-network; the counts for these records contain all zeros.

Table A-12: OTA Stats Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the message arrived at the NMS server
t_interval	int(10) unsigned	interval in seconds that the data covers

Table A-12: OTA Stats Record Format

Column Name	Data Type	Meaning
network_id	smallint(5) unsigned	identifies the network
unique_id	int(10) unsigned	uniquely identifies the remote
modem_sn	int(10) unsigned	remote's serial number
rx_reliable_kbyte	double	kilobytes of reliable (e.g. TCP) data received
tx_reliable_kbyte	double	kilobytes of reliable (e.g. TCP) data sent to the remote
rx_unreliable_kbyte	double	kilobytes of unreliable (e.g. UDP) data received
tx_unreliable_kbyte	double	kilobytes of unreliable (e.g. UDP) data sent to the remote
rx_oob_kbyte	double	kilobytes of out-of-band bytes received
tx_oob_kbyte	double	kilobytes of out-of-band bytes sent to the remote

Consolidated Over-the-Air Statistics Tables

The two consolidated tables, ota_minute_stats and ota_hour_stats, contain all the fields in the raw_ota_stats table plus the additional fields that hold maximum and standard deviation values for each field of over-the-air data. Each maximum column indicates the maximum individual measurement of all records consolidated into this record. Each standard deviation value, calculated using a common formula, tells you how clustered the consolidated measurements were around the average of all consolidated data records.

Table A-13: Additional Consolidated OTA Stats Table Fields

Column Name	Data Type	Meaning
rx_reliable_max	double	The maximum rx_reliable_kbyte value of the records consolidated into this record
tx_reliable_max	double	As above, for tx_reliable_kbyte
rx_unreliable_max	double	As above, for rx_unreliable_kbyte
tx_unreliable_max	double	As above, for tx_unreliable_kbyte
rx_oob_max	double	As above, for rx_oob_kbyte
tx_oob_max	double	As above, for tx_oob_kbyte
rx_reliable_stddev	float(10,5)	The standard deviation of all consolidated rx_reliable_kbyte records
tx_reliable_stddev	float(10,5)	As above, for tx_reliable_kbyte
rx_unreliable_stddev	float(10,5)	As above, for rx_unreliable_kbyte
tx_unreliable_stddev	float(10,5)	As above, for tx_unreliable_kbyte
rx_oob_stddev	float(10,5)	As above, for rx_oob_kbyte
tx_oob_stddev	float(10,5)	As above, for tx_oob_kbyte

A.4.11 Over-the-Air Multicast Statistics Tables

As shown in [Table A-1](#), there are three separate base table types for over-the-air multicast statistics, each one containing records that cover a particular period of time. The otacast_minute_stats and otacast_hour_stats tables have all the fields contained in the raw_otacast_stats plus additional fields containing maximum and standard deviation calculations for all fields of over-the-air multicast data. These fields are discussed in more detail later in this section.

Over-the-air multicast statistics for all active remotes are calculated by protocol processor and sent to the NMS every five seconds. After sending a stats message, the protocol processor zeros its counts, so that every database record contains the delta in activity from the previous record. The protocol processor continues to send messages to the NMS even if a remote is out-of-network; the counts for these records contain all zeros.

Table A-14: OTACAST Stats Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the message arrived at the NMS server
t_interval	int(10) unsigned	interval in seconds that the data covers
network_id	smallint(5) unsigned	identifies the network
tx_bcast_kbyte	double	kilobytes of broadcast data transmitted
tx_mcast_kbyte	double	kilobytes of multicast data transmitted

Consolidated Over-the-Air Statistics Tables

The two consolidated tables, otacast_minute_stats and otacast_hour_stats, contain all the fields in the raw_otacast_stats table plus the additional fields that hold maximum and standard deviation values for each field of over-the-air data. Each maximum column indicates the maximum individual measurement of all records consolidated into this record. Each standard deviation value, calculated using a common formula, tells you how clustered the consolidated measurements were around the average of all consolidated data records.

Table A-15: Additional Consolidated OTACAST Stats Table Fields

Column Name	Data Type	Meaning
tx_bcast_max	double	The maximum tx_bcast_kbyte value of the records consolidated into this record
tx_mcast_max	double	As above, for tx_mcast_kbyte
tx_bcast_stddev	double	The standard deviation of all consolidated tx_bcast_kbyte records
tx_mcast_stddev	double	As above, for tx_mcast_kbyte

A.4.12 Mesh Stats Tables

As shown in [Table A-1](#), there are three separate base table types for mesh stats, each one containing records that cover a particular period of time. The mesh_minute_stats and mesh_hour_stats tables have all the fields contained in the raw_mesh_stats plus additional fields containing maximum and standard deviation calculations for all fields of mesh statistics. These fields are discussed in more detail later in this section.

Mesh statistics for all active remotes are calculated by the remote and sent to the NMS every 20 seconds. After sending a stats message, the remote zeros its counts, so that every database record contains the delta in activity from the previous record. The remote continues to send messages to the NMS even if a remote is out-of-network; the counts for these records contain all zeros.

Table A-16: Mesh Stats Record Format

Column Name	Data Type	Meaning
timestamp	timestamp(14)	time_t that the message arrived at the NMS server
t_interval	int(10) unsigned	interval in seconds that the data covers
network_id	smallint(5) unsigned	identifies the network
unique_id	int(10) unsigned	uniquely identifies the remote
modem_sn	smallint(5) unsigned	remote's serial number
rx_reliable_kbyte	double	kilobytes of reliable (e.g. TCP) mesh data received by the remote
tx_reliable_kbyte	double	kilobytes of reliable (e.g. TCP) mesh data sent by the remote
rx_unreliable_kbyte	double	kilobytes of unreliable (e.g. UDP) mesh data received by the remote
tx_unreliable_kbyte	double	kilobytes of unreliable (e.g. UDP) mesh data sent by the remote
rx_oob_kbyte	double	kilobytes of out-of-band mesh data received by the remote
tx_oob_kbyte	double	kilobytes of out-of-band mesh data sent by the remote

Consolidated Mesh Tables

The two consolidated tables, mesh_minute_stats and mesh_hour_stats, contain all the fields in the raw_mesh_stats table plus the additional fields that hold maximum and standard deviation values for each field of mesh data. Each maximum column indicates the maximum individual measurement of all records consolidated into this record. Each standard deviation value, calculated using a common formula, tells you how clustered the consolidated measurements were around the average of all consolidated data records.

Table A-17: Additional Consolidated Mesh Stats Table Fields

Column Name	Data Type	Meaning
rx_reliable_max	double	The maximum rx_reliable_kbyte value of the records consolidated into this record
tx_reliable_max	double	As above, for tx_reliable_kbyte
rx_unreliable_max	double	As above, for rx_unreliable_kbyte
tx_unreliable_max	double	As above, for tx_unreliable_kbyte
rx_oob_max	double	As above, for rx_oob_kbyte
tx_oob_max	double	As above, for tx_oob_kbyte
rx_reliable_stddev	float(10,5)	The standard deviation of all consolidated rx_reliable_kbyte records
tx_reliable_stddev	float(10,5)	As above, for tx_reliable_kbyte
rx_unreliable_stddev	float(10,5)	As above, for rx_unreliable_kbyte
tx_unreliable_stddev	float(10,5)	As above, for tx_unreliable_kbyte
rx_oob_stddev	float(10,5)	As above, for rx_oob_kbyte
tx_oob_stddev	float(10,5)	As above, for tx_oob_kbyte

A.5 NMS Statistics Archive Database Restructuring

iDS Release 6.1 and all later releases include a major overhaul to the statistics archive database. The primary goal of this restructuring is to improve overall performance of the NMS server machines as networks grow, and to improve historical query response times on large networks.

iMonitor users will see no difference in the way historical archive statistics are retrieved and displayed other than a noticeable improvement in performance. If you access the current archive directly, or if you're interested in the new structure, you should read this section. Otherwise you may safely skip ahead to [Section A.5.6 "Converting Data between Table Formats" on page 172](#).



WARNING

If you are currently accessing the statistics archive directly using ODBC, your software will not work on this new archive structure without modifications. See the following sections for detailed information.

A.5.1 Background

In older iDS releases, each archive data type was represented by a single MySQL database table. Using the **raw_ip_stats** table as an example, all IP statistics for all remotes were written directly to this table as they arrived at the NMS. Historical queries for IP statistics were performed on this table as well. In large networks, the table could grow to well over one gigabyte. This large size, combined with a large amount of read and write operations, caused a significant performance load on the NMS server's CPU and degraded response time in the iMonitor and iBuilder GUIs.

To alleviate this situation, the NMS now uses a multiple-table storage scheme in which each type of archived data is divided among multiple tables by time and groups of remotes. Dividing tables in this manner is known as *data striping*. The following sections discuss this implementation change in detail.

A.5.2 The New Archive Database Structure

Each type of statistical data that was formerly stored in a single database table is now stored in multiple tables. All the tables that together contain the records of a particular statistics type are called a *table set*. The table set for each type is sized on two dimensions: time and unique ID. The default values specify a *time dimension* of 6 x 360 and an *ID dimension* of 1. The time dimension consists of two parameters: the number of tables (which defaults to 6) and the time span of the data in each table (which defaults to 360 minutes). For a complete list of data types, see [Table A-19](#) on [page 170](#).

These two dimensions result in the table set shown in [Figure A-1](#) on [page 168](#). Data in this default table set is *striped* across the six tables in six-hour segments (hence the 6 x 360 time dimension). Day by day, the six tables in the set will have the data striped across them as shown in [Table A-18](#) on [page 168](#).

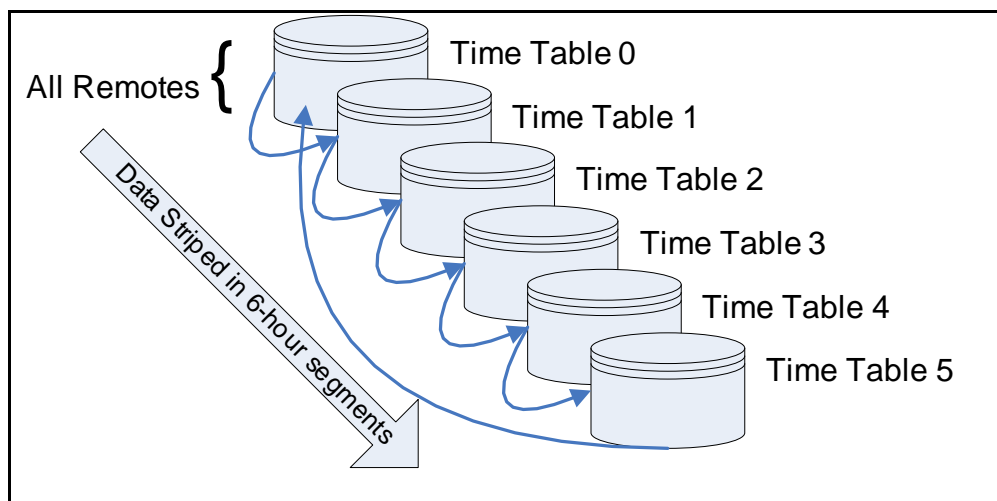


Figure A-1: Default Table Set

Table A-18: Default Data Striping

	Day 1	Day 2	Day 3	Day 4	Day 5
Table 0	00:00 – 06:00	12:00 – 18:00	...	00:00 – 06:00	12:00 – 18:00
Table 1	06:00 – 12:00	18:00 – 24:00	...	06:00 – 12:00	18:00 – 24:00
Table 2	12:00 – 18:00	...	00:00 – 06:00	12:00 – 18:00	...
Table 3	18:00 – 24:00	...	06:00 – 12:00	18:00 – 24:00	...

Table A-18: Default Data Striping

	Day 1	Day 2	Day 3	Day 4	Day 5
Table 4	...	00:00 – 06:00	12:00 – 18:00	...	00:00 – 06:00
Table 5	...	06:00 – 12:00	18:00 – 24:00	...	06:00 – 12:00

A.5.3 The New Archive Process

The following two diagrams illustrate how statistics archiving has changed in iDS 6.1 from previous releases.

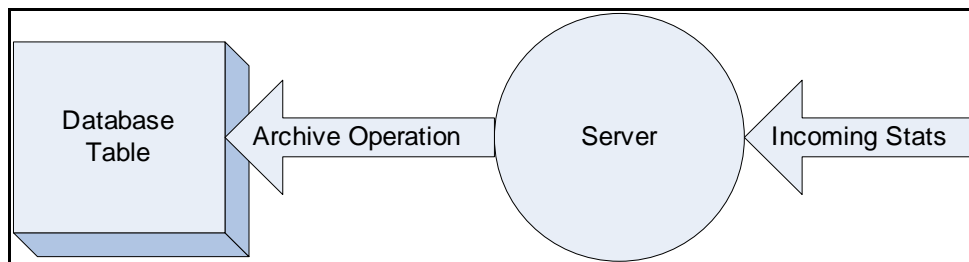


Figure A-2: Release 6.0 and Earlier Stats Archiving Process

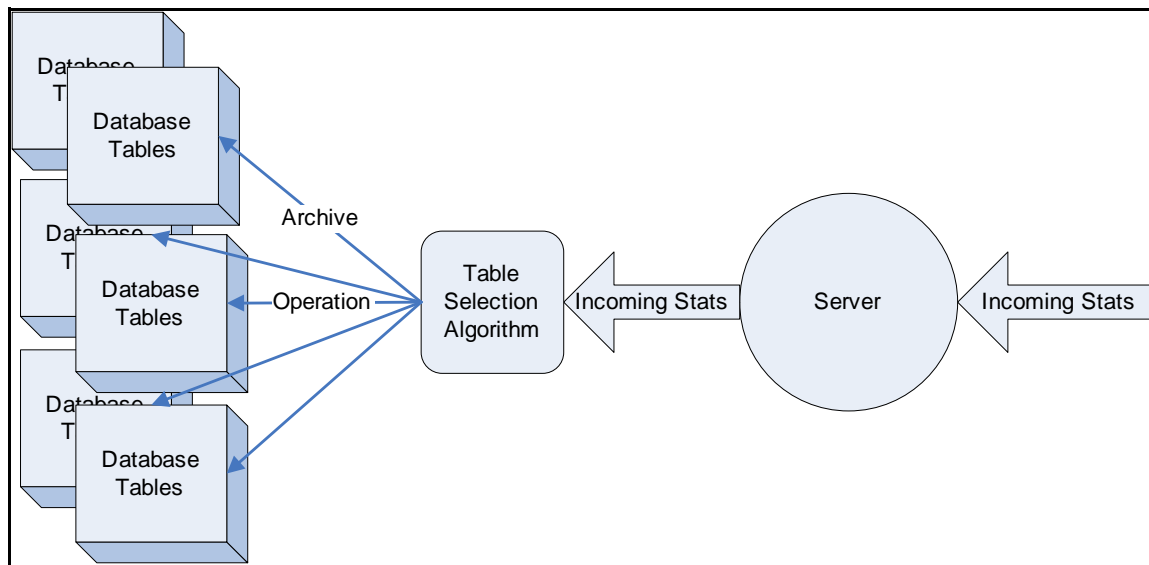


Figure A-3: Release 6.1 Stats Archiving Process

In iDS 6.1 as well as later releases, instead of writing all data to one table as it arrives at the NMS, the server first passes the data through a *table selection algorithm*. This process determines the correct database table for the data that has just arrived. A similar selection process also occurs when historical data is queried from iMonitor.

The selection rules are based on the following criteria:

- The type of data – IP statistics, events, condition changes, etc. As before, each type of data has its own table structure
- The remote's unique database ID
- The current timestamp

A.5.4 Table Division Rules

All table selection rules are stored in the NMS configuration database in a table called **TABLE_INFO**. This table has the following format and default values:

Table A-19: TABLE_INFO Format and Default Contents

table_type_id	time_table_number	second_dimension_table_number	time_interval	base_table_name	second_dimension_name
The type of statistics data	The number of time periods kept for this statistics type	The number of tables per time period kept for the second dimension data type ID	The time segment interval in each table, in minutes	The actual tables names, derived from the base table name. (These match the table names in prior releases)	The second dimension data type ID
0	6	1	360	chassis_state_change_log	chassis_id
1	6	1	360	event_msg	unique_id
2	6	1	360	lat_stats	unique_id
3	6	1	360	nms_hub_stats	unique_id
4	6	1	360	nms_remote_status	unique_id
5	6	1	360	nms_ucp_info	unique_id
6	6	1	360	pp_state_change_log	blade_id
7	6	1	360	raw_ip_stats	unique_id
8	6	1	360	raw_ota_stats	unique_id
9	6	1	360	raw_otacast_stats	network_id
10	6	1	360	state_change_log	unique_id
11	6	1	360	ip_minute_stats	unique_id
12	6	1	360	ip_hour_stats	unique_id
13	6	1	360	ota_minute_stats	unique_id
14	6	1	360	ota_hour_stats	unique_id

Table A-19: TABLE_INFO Format and Default Contents (Continued)

15	6	1	360	otacast_minute_stats	unique_id
16	6	1	360	otacast_hour_stats	network_id

A.5.5 Table Selection Process

Insertion, selection, and deletion operations all use table selection algorithms, based on current timestamp and current id, to determine which table to access.

The algorithm for calculating a table name for an operation has a number of steps, as shown below:

Constants:

```
base_time = 1072915201 (Linux time_t)
```

Database Values:

```
ttn = TABLE_INFO.time_table_number
tis = (TABLE_INFO.time_interval * 60) // convert to seconds
sdtn = TABLE_INFO.second_dimension_table_number
btn = TABLE_INFO.base_table_name
```

Variables:

```
t = <timestamp> (Linux time_t)
id = unique_id of element (e.g. remote)
```

Calculate the current Remote Index value

```
remote_index = id % sdtn
```

Calculate the current Time Index value

```
time_index = (t - base_time) / tis % ttn
```

Calculate the current Table Index value

```
table_index = (ttn * remote_index) + time_index
```

Derive the appropriate Table Name

```
table_name = btn <concat> "_" <concat> table_index
```

For example, table_name = event_msg_3



NOTE

When running a distributed NMS system, you must read TABLE_INFO from the master MySQL machine. This is typically the same machine as your Configuration Server.

A.5.6 Converting Data between Table Formats

After the Upgrade to Release 6.1

Your existing archive data is *not* converted to the new format during the NMS upgrade. Rather, the new table structure is created with empty tables, and all your existing data remains in the old tables. The following figure illustrates the database structure for raw_ip_stats statistics after you complete the upgrade of your NMS server machine to iDS 6.1.

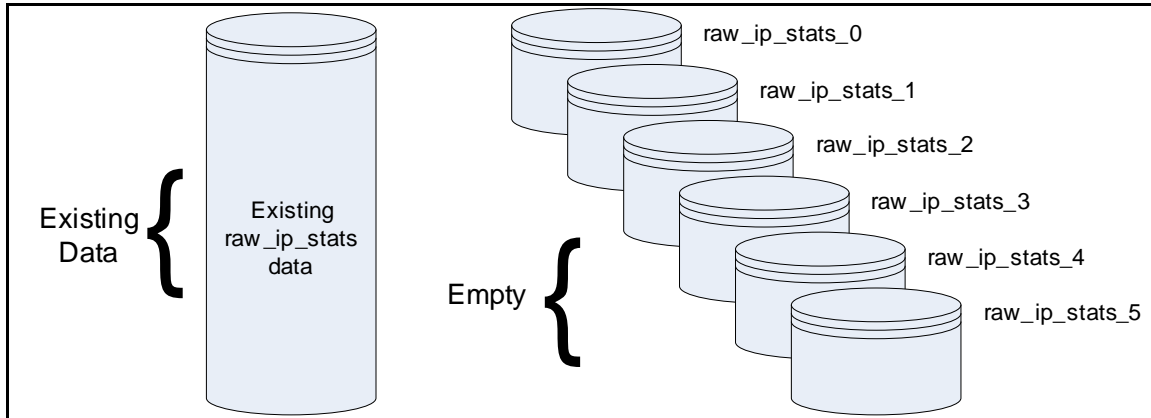


Figure A-4: Archive Database after Conversion to 6.1

When you restart the NMS servers, new data arriving at the NMS will be archived to the new tables. The old data will remain in the old tables until you delete it or convert it to the new format.

If you want to convert your existing archive data to the new format, follow these steps:

Step 1 Log onto the NMS server as **root**.

Step 2 At the command prompt, type:

```
cd /home/nms/utils/db_maint
```

Step 3 Convert your archive data by typing

```
./DB-Conversion.pl
```

Converts your archive data to the new table format

The **DB-Conversion.pl** command has the following format and output:

```
./DB-Conversion.pl -h
```

Usage:

```
DB-Conversion.pl [-cd=NAME] [-ad=NAME]
```

```
-cd      : Change config database from [nms]
```

```
-ad      : Change archive database from [nrd_archive]
```

Changing the 6.1 Table Structure

You can modify the TABLE_INFO settings show in [Table A-19](#) on [page 170](#). For example, you can change the number of time tables, the second dimension tables, or the time interval.



WARNING

If you choose to modify the default TABLE_INFO settings, and you are running a Distributed NMS, you must change the database on the master MySQL machine. This is typically the same machine as your Configuration Server.

Follow these steps to modify the TABLE_INFO settings:

Step 1 Log onto the NMS server as **root**.

Step 2 At the command prompt, type:

```
cd /home/nms/utils/db_maint
```

Step 3 Stop NMS Services by typing:

```
service idirect_nms stop
```



WARNING

You *must* stop NMS Services before changing the table structure, or run this process offline.

Step 4 Use the **./DB-Migration.pl** script to change the table structure. All forms of this script are shown below.

```
# ./DB-Migration.pl -h
```

```
DB-Migration.pl [-cd=NAME] [-ad=NAME] [-DD]
  -cd      : Change config database from [nms]
  -ad      : Change archive database from [nrd_archive]
  -DD      : Do not touch any data outside of the ip_stats
  -suffix  : Change suffix for existing tables for database
[nrd_archive], default is "old"
```

If you run the script with no arguments as shown below, it will rename the existing tables by adding the suffix "old." For example, "event_msg_1" becomes "event_msg_1_old." Once you have verified the data in the new format, you should remove these renamed tables.

```
./DB-Migration.pl <RET>
```

Converts existing 6.1 data into new table structure

A.5.7 Optimizing Archive Database Performance

The efficiency of archive database access is affected by the size and number of tables for each of the 17 statistics types in the archive. iDirect provides a database partitioning calculator to help you determine the optimal size of these tables based on the number of remotes in your network and the frequency with which the statistics are updated in the archive. Once you have used the calculator to determine the optimal settings, you can update the information in columns two through four of the TABLE_INFO table shown in [Table A-19](#) on [page 170](#) to match the results of your calculations.

Copying the Archive Database Partitioning Calculator to Your PC

The calculator is installed on your NMS server as part of the iDirect software release. Before using the calculator, you should copy it to your PC or laptop. The procedure in this section shows how to use Cygwin to retrieve the calculator.



NOTE

You must have access to the **root** account on the NMS server to retrieve the calculator.

Follow these steps to copy the archive database partitioning calculator to your PC or laptop using Cygwin:

Step 1 Create a folder on your PC or laptop where you want to store the calculator.

Step 2 Start Cygwin on your PC or laptop.

Step 3 In the Cygwin window, use the **cd** command to change your directory to the new folder. The command syntax is show here using the directory **db_calculator** at the top level of the **C:** drive.

```
cd /c/db_calculator
```

Step 4 In the Cygwin terminal window, type:

```
SCP root@<IP Address>:/home/nms/utills/db_maint/  
table_info-calculator.htm ./
```

where **<IP Address>** is the IP address of your NMS server.

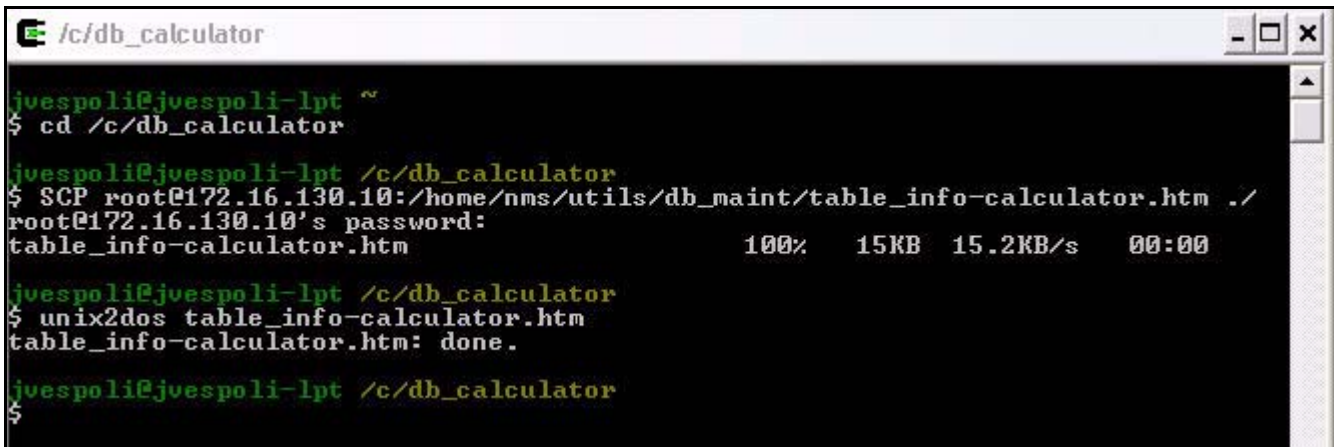
Step 5 Enter the **root** password when prompted and press ENTER. The calculator will be transferred to your PC.

Step 6 Execute the following command to reformat your copy of the file for the Windows environment.

```
unix2dos table_info-calculator.htm
```

Step 7 Close your Cygwin terminal window.

[Figure A-5](#) presents an example of these steps.



```

jvespoli@jvespoli-lpt ~
$ cd /c/db_calculator

jvespoli@jvespoli-lpt /c/db_calculator
$ SCP root@172.16.130.10:/home/nms/utills/db_maint/table_info-calculator.htm ./
root@172.16.130.10's password:
table_info-calculator.htm                               100%  15KB  15.2KB/s   00:00

jvespoli@jvespoli-lpt /c/db_calculator
$ unix2dos table_info-calculator.htm
table_info-calculator.htm: done.

jvespoli@jvespoli-lpt /c/db_calculator
$

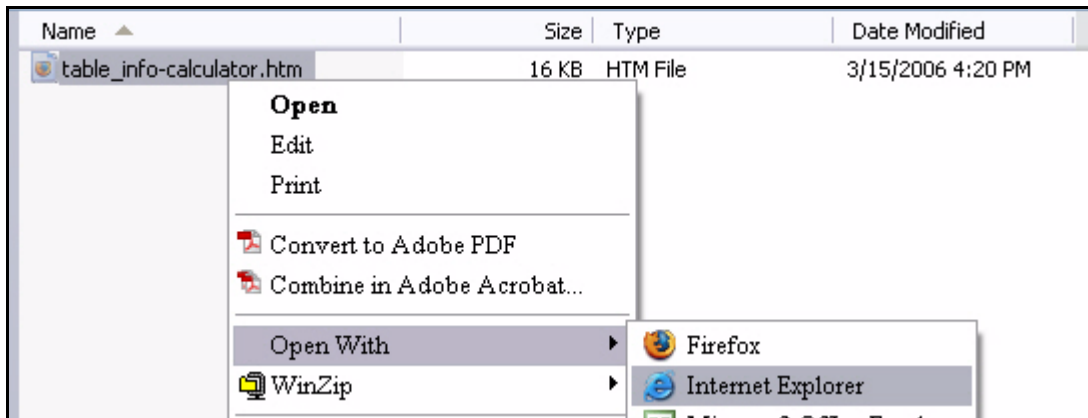
```

Figure A-5: Retrieving the Database Partitioning Calculator Using Cygwin

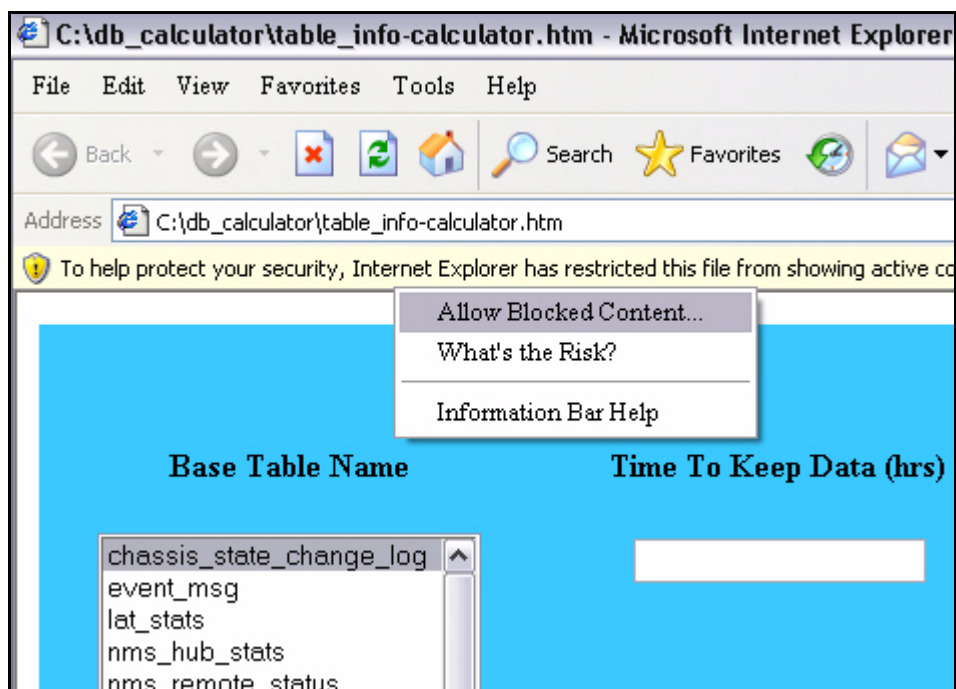
Using the Archive Database Partitioning Calculator

The archive database partitioning calculator is an HTML application that must be run in Microsoft's Internet Explorer (IE) web browser. To use the calculator:

- Step 1 On your PC or laptop, navigate to the folder into which you copied the calculator.
- Step 2 Right-click the calculator and select **Open With → Internet Explorer** to display the calculator in your browser window.



- Step 3 If you are running Windows XP with Service Pack 2, you must right-click the security message at the top of the calculator window and select **Allow Blocked Content**. Then click **Yes** in the warning dialog box.



- Step 4 Use the calculator to determine the optimal settings for your archive database partitions. The parameters and their usage is described below.

Base Table Name	Time To Keep Data (hrs)	Maximum Table Size (MB)
<div> chassis_state_change_log event_msg lat_stats nms_hub_stats nms_remote_status nms_ucp_info pp_state_change_log raw_ip_stats raw_ota_stats raw_otacast_stats state_change_log ip_minute_stats ip_hour_stats ota_minute_stats </div>	168	150
	Number of Second-Dimension Elements 750	Number of Records per Minute 4
		Record Size (in bytes) 152

Time Table Number	Second Dimension Name	Time Interval (hrs)
12	2	14

Calculate Table_Info data

Figure A-6: Archive Database Partitioning Calculator

[Figure A-6](#) shows the calculated results for the **nms_remote_status** table in a network with 750 remotes with a logging rate of four times per minute. The parameters are entered in the top portion of the screen. The results appear in the lower (yellow) portion of the screen when you click the **Calculate Table_Info data** button.

The following parameters can be entered in the calculator.

- The **Base Table Name** (identical to the **base_table_name** in the TABLE_INFO table on [page 170](#)) represents the table definition for the table set that contains all statistics of this type. Before calculating the results, you should select the **Base Table Name** of interest from this list.
- **Time to Keep Data (hrs)** represents the amount of time in hours to retain the data for this **Base Table Name** before it is overwritten. You can modify this parameter based on

your requirement to keep records of this type on the NMS server and your available disk space.

- **Maximum Table Size (MB)** is used to calculate the optimal number of tables that should be created for this **Base Table Name**. This parameter is not stored in the database. It is a limit used by the calculator to help compute the best results. In general, you should use the default setting.
- **Number of Records per Minute** is the rate per minute at which records of this type are being logged for each remote (or other device) in the table set. This is not a configurable parameter and it varies dynamically with network load. If you have measured a value for your network for which you want to optimize the table set, you can change this parameter to reflect that value. Otherwise, you should use the default setting.
- **Number of Second Dimension Elements** represents approximately the total number of devices (second dimension elements) associated with the **Base Table Name** in your network. Note that if the number of remotes in your network changes significantly, you should consider re-executing the calculator and reconfiguring the TABLE_INFO for tables that log remote statistics. You can vary the number of second dimension elements used by the calculator in increments of 250.
- **Record Size (in bytes)** is the size of the database record for this **Base Table Name**. In general, you should use the default setting.

After entering all parameters, click the **Calculate Table_Info data** button to calculate the following results:

- **Time Table Number** represents the optimal number of time segments recommended for this **Base Table Name** based on the parameters entered. This result corresponds to the **time_table_number** in the TABLE_INFO table shown in [Table A-19](#) on [page 170](#).
- **Second Dimension Name** represents the number of tables per time period recommended for this **Base Table Name** based on the parameters entered. This result corresponds to the **second_dimension_name** in the TABLE_INFO table.
- **Time Interval (hrs)** represents the length of time for each time segment recommended for this **Base Table Name** based on the parameters entered. This result corresponds to the **time_interval** in the TABLE_INFO table.

After you have calculated the optimal **time_table_number**, **second_dimension_name** and **time_interval** for all tables you want to optimize, you can log into the root directory of the NMS server and use MySQL to change the TABLE_INFO configuration in the NMS database to match the optimal values.

[Figure A-7](#) shows the table set that would be created for **nms_remote_status** if INFO_TABLE were modified in accordance with the values calculated in figure [Figure A-6](#) on [page 177](#).

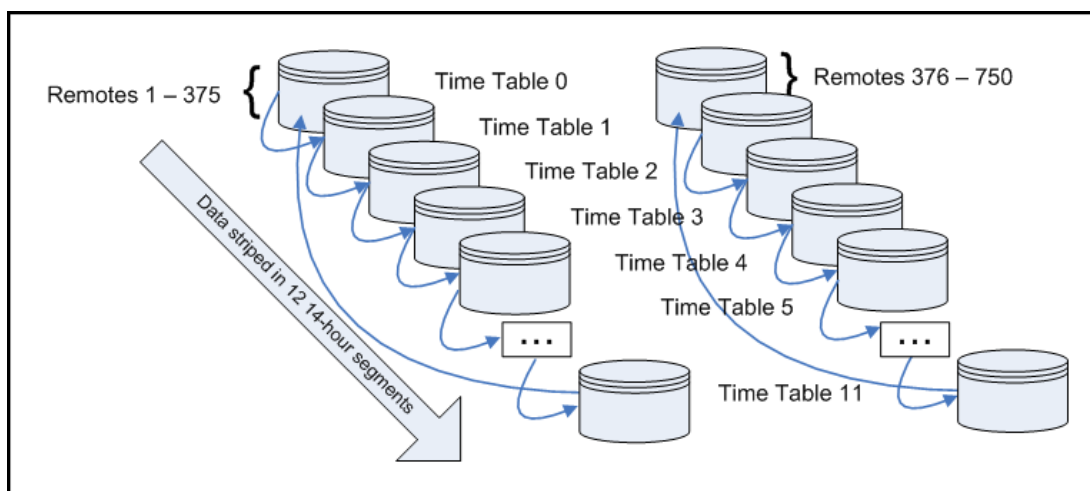


Figure A-7: Segmented `nms_remote_status` archive tables

A.5.8 Selecting from the Restructured Database

In the past, when selecting records from the statistics archive, you would use a single query against a single table to find your answer. For instance, to get all state_change_log records with time range of 2006-11-20 10:00 to 2006-11-20 14:00, you would issue the query:

```
SELECT * FROM state_change_log WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;
```

Because all records were in one table, state_change_log, a complete result set was returned.

A bit more work goes into getting the same answer from a “striped” database. The main thing to remember is that in the restructured database, a query on a sufficiently large time range (by default +6 hours) is guaranteed to span multiple tables. When a query’s time range reaches $ttn * tis$ hours ($6 * 6 = 36$ hours by default), the result takes stripes from every table in the table set. Up to the $ttn * tis$ time range limit, you must choose between efficiency and simplicity. When the goal is efficiency, a query must be pre-processed and split, so that only tables containing matching records are queried. When the goal is simplicity, queries are re-factored to cast a wide net, potentially querying tables that do not contribute to the result set.

Identifying the Location of the Result Set

When the result set is guaranteed to come from only one or two tables, it makes sense to avoid query overhead by applying the query selectively. To do so, first calculate the index for every table containing records in your query time range. Then, run one query per table index calculated.

Using the example above and default striping parameters:

Inputs:

```
Stripe base time (base) = 2004-01-01 00:00:01 = 1072915201
TABLE_INFO.time_table_number (ttn) = 6 tables
TABLE_INFO.time_interval (tis) = 6 hours = 21600 seconds
TABLE_INFO.second_dimension_table_number = 1, which allows us to ignore
this dimension. (Anything modulo 1 equals 0, so there is no second dimension
component to the table index)
Query start time (start) = 2006-11-20 10:00:00 = 1164016800
Query end time (end) = 2006-11-20 14:00:00 = 1164031200
```

Calculate all table indexes:

To get the range of table indexes, calculate the index of the query start and end times. Those two indexes, and everything in between, must be included in the queries.

The first table index is derived from start:

```
Idx_0 = ((start - base) / tis % ttn
        = ((1164016800 - 1072915201) / 21600) % 6
        = 5
```

The last table index derives from end:

```
Idx_N = ((end - base) / tis) % ttn
       = ((1164031200 - 1072915201) / 21600) % 6
       = 0
```

Divide the query among all indexes:

In this case, the first half of our records is in state_change_log_5:

```
SELECT * FROM state_change_log_5 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;
```

and the remaining records are in state_change_log_0:

```
SELECT * FROM state_change_log_0 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;
```

Concatenating the two result sets returns the same answer arrived at in the 1st example.

Larger query time range:

The procedure is exactly the same with a larger time ranges:

```
Query start time (start) = 2006-11-20 19:00:00 = 1164049200
Query end time (end) = 2006-11-21 07:00:00 = 1164092400
Idx_0 = ((1165059200 - 1072915201) / 21600) % 6
       = 1
Idx_N = ((1164092400 - 1072915201) / 21600) % 6
       = 3
```

The queries to run are:

```
SELECT * FROM state_change_log_1 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;
SELECT * FROM state_change_log_2 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;
SELECT * FROM state_change_log_3 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;
```

Ignoring the Location of the Result Set Part One:

When the goal is to write simpler scripts, or when query time ranges near the *tis* * *ttn* limit, skip query pre-processing and simply query all tables. There are two portable methods for doing this:

Multiple queries, external concatenation:

As in the second example, you could make multiple queries, and then concatenate and sort externally (in Perl, for instance):

```

SELECT * FROM state_change_log_0 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;

SELECT * FROM state_change_log_1 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;

SELECT * FROM state_change_log_2 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;

SELECT * FROM state_change_log_3 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;

SELECT * FROM state_change_log_4 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;

SELECT * FROM state_change_log_5 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000;

```

Unions

A slightly simpler method is to use UNIONS:

```

(SELECT * FROM state_change_log_0 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000)
UNION
(SELECT * FROM state_change_log_1 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000)
UNION
(SELECT * FROM state_change_log_2 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000)
UNION
(SELECT * FROM state_change_log_3 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000)
UNION
(SELECT * FROM state_change_log_4 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000)
UNION
(SELECT * FROM state_change_log_5 WHERE timestamp BETWEEN
20061120100000 AND 20061120140000)
ORDER BY timestamp;

```

With this method, MySQL concatenates and sorts the records for you. No external post-processing required.

Ignoring the Location of the Result Set Part Two:

MySQL has a feature that makes querying multiple tables even simpler. A MERGE table is a collection of identical tables that can be used as a single table. To create a MERGE table of state_change_log_X:

```

CREATE TABLE state_change_log_merged (
    `timestamp` timestamp(14) NOT NULL,
    `unique_id` int(10) unsigned NOT NULL default '0',
    `modem_sn` int(10) unsigned NOT NULL default '0',
    `current_state`
enum('OK','WARNING','ALARM','UNKNOWN','OFFLINE','ELSEWHERE','MESH
ALARM','SLEEP','STATE_NONE') default NULL,
    `occurred_at` timestamp(14) NOT NULL,
    `error_type` smallint(6) default NULL,
    `error_severity`
enum('EVTWarning','EVTAlarm','EVTcleared','EVToffline','EVTElsewh
ere','EVTMeshAlarm','EVTSleep','EVTNone') default 'EVTNone',
    `reason` varchar(255) default NULL,
    KEY `IDX_TIME_UQ` (`timestamp`,`unique_id`))
TYPE=MERGE
UNION=(state_change_log_0, state_change_log_1,
state_change_log_2, state_change_log_3, state_change_log_4,
state_change_log_5);

```

Most of the **CREATE** statement consists of a copy of state_change_log_X's **CREATE** statement (you can view it by issuing the query "**SHOW CREATE TABLE state_change_log_0**".) The differences are the name, of course; the **TYPE** or **ENGINE** clause, which tells MySQL what kind of table we're creating (normally MyISAM); and an additional **UNION** clause, which identifies the list of tables in the collection.

With a **MERGE** table interface to the restructured database, your old queries require only one change:

```

SELECT * FROM state_change_log_merged WHERE timestamp BETWEEN
20061120100000 AND 20061120140000 ORDER BY timestamp;

```

A query on a **MERGE** table behaves, internally, the same way as the **UNION** query. MySQL runs the query on every table in the collection then collates the results (as directed by the **ORDER BY** clause.) The sole benefit is shorter, cleaner queries.

Appendix B Alarms and Warnings

The iDirect NMS provides real-time notification of system anomalies, classified by severity. The iMonitor GUI provides complete visibility to the real-time status and operational characteristics of network elements. “Status” refers to the real-time state of network elements, i.e. OK, warning, and alarm.

Alarms indicate an interruption in service or remote sites that are out-of-network. Warnings display potential anomalous conditions and system values that are out of range.

B.1 Alarms

The following table lists alarms, their descriptions and recommended actions.

Table B-1: Alarms

Alarm	Description	Action, Troubleshooting
Chassis Down	The HUB Chassis controller interface has failed or become unavailable from the NMS	<ul style="list-style-type: none">• Check if the network path to the HUB Chassis is available from the NMS server (ping, tracer).• Check if the HUB Chassis is powered up.• Make sure the chassis controller card (EDAS) is connected to the upstream LAN, not the tunnel LAN.• <u>NOTE:</u> It is likely that the HUB line cards are still operating.
Line Card Down	Line Card is powered off or has failed.	<ul style="list-style-type: none">• Make sure the NMS server can reach the Line Cards across upstream router (ping, tracer).• Check chassis slot power via NMS.• In case of card failure, check status LED on Line Card front panel for cause. Solid Red status LED indicates that the Universal Line Card has detected a fault, or Application software or firmware cannot be loaded. Replace Line Card or reload firmware images.
PP Down	Protocol Processor is not responding	<ul style="list-style-type: none">• Check if the network path to Protocol Processor is available from the NMS server (ping, tracer).• Check if Protocol Processor is powered up and operational.

Table B-1: Alarms (Continued)

Alarm	Description	Action, Troubleshooting
Remote Layer 2	Remote is not in network (out of network or link layer down)	<ul style="list-style-type: none"> • Verify configuration in iBuilder. • Check stability of the RF link • Check history in iMonitor of Tx Power and Down C/N of remote. Higher Tx power and lower C/N indicate degradation. <ol style="list-style-type: none"> 1 Short-term possibly due to rain fade. 2 Long-term possibly due to degradation of installation. Check RF chain: BUC, LNB, cables, connectors for moisture. Dish positioning.
Remote Layer 3	Remote is not responding to ICMPs, i.e. has missed 3 ICMPs in a row.	<ul style="list-style-type: none"> • This can be due to high traffic load. (Remote may still be in network) • Check if network path to Remote is available from the NMS server (tracert, ping) or where the network path is broken.

B.2 Warnings

Warnings signal a condition that could possibly result in a future interruption in service if not handled in a timely fashion. The following table lists warnings, their descriptions and recommended actions.



NOTE

The following “alarms” are classified as warnings in the NMS: PowerAlarm(1/2/3), FanAlarm, RCM(A/B)Alarm.



NOTE

Warning limits can be configured using iBuilder. Any specific limits shown in [Table B.2](#) represent default values. For details on setting warning limits, see the [iBuilder User Guide](#).

Table B-2: Warnings

Device	Warning Condition	Description	Action, Troubleshooting
HUB Chassis	PowerAlarm1	HUB Chassis power supply 1 failed. If one of the three Power Supply Modules fails, the other two Power Supply Modules are capable of sourcing enough power to make up for the failed supply module.	Replace power supply 1
	PowerAlarm2	HUB Chassis power supply 2 failed	Replace power supply 2
	PowerAlarm3	Hub Chassis power supply 3 failed	Replace power supply 3
	FanAlarm	A Fan failure is reported if the any of the three Fan Modules propeller spins below a predetermined revolution-per-minute (RPM). A fully loaded iDirect HUB Chassis (20 Universal Line Cards) can remain in operation with two of the three Fan Modules still functioning.	<ul style="list-style-type: none"> Verify the Fan Alarm Status on the rear of the HUB chassis. A failed fan will be indicated by the red color LED. Replace failed cooling fan
	RCMAAlarm	HUB chassis reference clock module (RCM) A failed.	<ul style="list-style-type: none"> If RCM [A, B] is set to external clock mode, check for loss of 10 MHz clock source. Check RCM A for failure. Replace reference clock module A.
	RCMBAlarm	HUB chassis reference clock module (RCM) B failed.	<ul style="list-style-type: none"> If RCM [A, B] is set to external clock mode, check for loss of 10 MHz clock source. Check RCM B for failure. Replace reference clock module B.
HUB Line Card	RX_OVERFLOW_FRAMES	Received frames are lost. Total of received and transmitted frames exceed HUB line card's performance limits.	<ul style="list-style-type: none"> Add new HUB line card and dedicate one line card to transmission only.
	DOWNSTREAM_PPS_OVERDRIVE	Downstream packets-per-second count above fixed limit	

Table B-2: Warnings (Continued)

Device	Warning Condition	Description	Action, Troubleshooting
	BACKPLANE_LOST_10MHZ	Line card lost the chassis backplane 10 MHz timing signal	Make sure both RCMs are installed and functional. If they are, this could mean a possible chassis backplane failure; contact the TAC for further assistance.
Remote	UPSTREAM_SNR	Remote's C/N as perceived at HUB is below/above limits	<ul style="list-style-type: none"> Weak signal could be due to rain fade. Check transmit power levels in iBuilder and iMonitor to determine if the remote is transmitting at max power.
	DOWNSTREAM_SNR	Downstream C/N as perceived at remote is below/above limits	<ul style="list-style-type: none"> Weak signal could be due to rain fade. Check transmit power levels in iBuilder.
	LOCAL_LAN_DISCONNECT	LAN port on remote is disconnected	Call customer.
	UCP_LOST_CONTACT	Protocol Processor has temporarily lost contact with remote. Could be due to rain fade.	
	TEMP_LIMIT	Remote's on-board temperature is below/above defined limits	Call customer.
	LATENCY	Measured latency, hub to remote is more than 2000 ms.	Increased latency may be related to high traffic load.
	ACQ_HUB_MODEM_CRC	Line card's acquisition CRC count above defined limit of 200 within 15 seconds.	Normal during acquisition process.
	TRAFFIC_HUB_MODEM_CRC	Line card's traffic CRC count above defined limit of 10 within 15 seconds.	Check for timing problem, power problem, RF link.
	SYMBOL_OFFSET	Remote's timing offset below or above calculated limits	Verify exact geographic location of satellite, hub, and remote. Adjust in order to minimize offset.
	REMOTE_OFFLINE	(Typically a mobile) remote has been taken offline by local operator. Causes all alarms and warnings from this remote to be ignored.	<ul style="list-style-type: none"> This is not an alarm or warning. When remote comes in again, it clears.
	CALIBRATED_TX_POWER	Remote's transmit power below or above defined power limits	
	MOBILE_LOST_GPS	Mobile remote's GPS has stopped functioning	<ul style="list-style-type: none"> Don't reset remote! Contact customer.

B.3 Acronyms

C/N	Carrier to noise density
CRC	Cyclic Redundancy Check
RCM	Reference Clock Module
SNR	Signal to Noise Ratio
UCP	Uplink Control Processing

B.4 Default Warning Limit Thresholds

Table B-3: Warning Limit Thresholds

Warning Type	Limit Type	Limit Value
UpstreamSNR	High	25
UpstreamSNR	Low	7
DownstreamSNR	High	25
DownstreamSNR	Low	7
TempLimit	High	77
TempLimit	Low	15
AcqHubModemCRC	High	200
TrafficHubModemCRC	High	10
Latency	High	2000
RxOverflowFrames	High	1
CalibratedTxPower	High	7
CalibratedTxPower	Low	-35



NOTE

Each remote's symbol offset is also automatically checked, and if the value goes above or below the limit a warning is raised in iMonitor. The symbol offset limit ranges are automatically calculated for each remote based on the upstream information rate.

Appendix C SNMP Proxy Agent

Beginning with release 3.1, iDirect's NMS includes an SNMP proxy agent that provides real-time status, statistical information, and basic configuration information to any interested SNMP client.

C.1 How the Proxy Agent Works

The SNMP Proxy Agent is a client of the NMS Configuration Server, NMS Event Server, NRD Server and Latency Server. It gets a list of network elements from the Configuration Server; the real-time status of each element from the Event Server; Statistical information for all remotes and line cards from the NRD Server; and the Latency information from the Latency Server. The statistical information is provided beginning in Release 7.0. Figure 1 illustrates how the SNMP Proxy Agent fits into the overall NMS architecture.

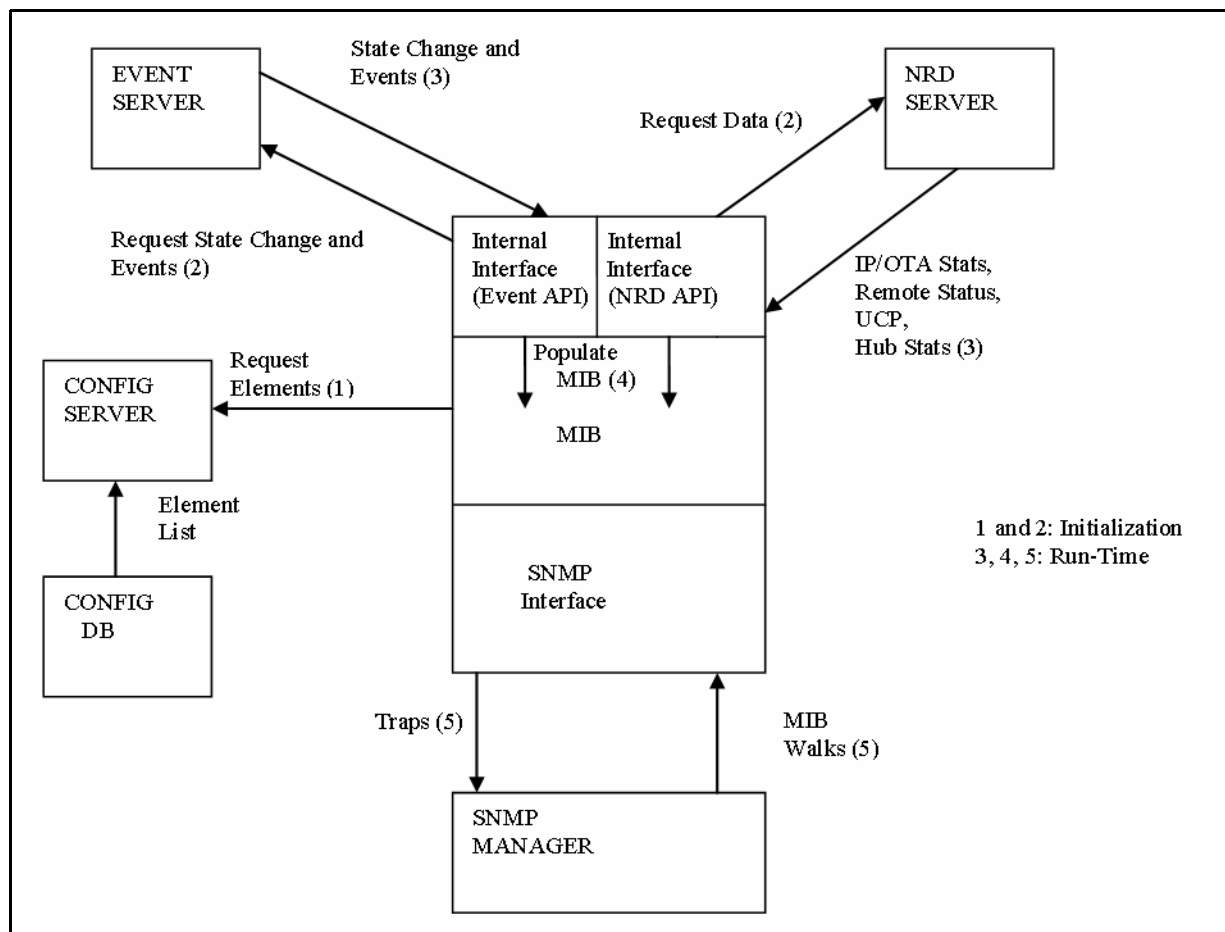


Figure C-1: SNMP Proxy Architecture

The SNMP Proxy Agent Management Information Base (MIB) supports both SNMP Get requests for polling and SNMP traps for asynchronous notification of status changes. The MIB is automatically updated to reflect changes in element status and/or configuration, including the

addition and deletion of network elements. It also collects statistical information regarding network elements.

The SNMP Proxy Agent is automatically installed on the NMS server as part of the iDirect software release and is included in the normal NMS server startup and shutdown procedure.

C.2 The iDirect Management Information Base (MIB)

The SNMP MIB supplies the following information for iDirect network elements.

Table C-1: iDirect MIB Contents

Element Type	Available Information
Protocol Processor	<ul style="list-style-type: none">• ID• Name• Teleport ID• Current State• List of Warnings• List of Alarms• Condition Raised (trap)• Condition Cleared (trap)
Chassis	<ul style="list-style-type: none">• ID• Name• Current State• List of Warnings• List of Alarms• Condition Raised (trap)• Condition Cleared (trap)
Remote Modem	<ul style="list-style-type: none">• ID• Serial Number• Name• Geographic Location Coordinates• Network ID• Protocol Processor ID• Teleport ID• Receive ID (identifies inroute)• IP Address• Type ID• Current State• List of Warnings• List of Alarms• Condition Raised (trap)• Condition Cleared (trap)

Beginning with iDirect Release 7.0, the SNMP MIB supplies the following statistical information for iDIRECT network elements.

Table C-2: iDirect MIB Statistical Information

Statistics Type	Available Information	Data Class
IP Statistics	Net Modem DID	Not Applicable
	Rx tcp Packets in bytes	Running Total
	Rx udp Packets in bytes	Running Total
	Rx icmp Packets in bytes	Running Total
	Rx igmp Packets in bytes	Running Total
	Rx http Packets in bytes	Running Total
	Rx other Packets in bytes	Running Total
	Tx tcp Packets in bytes	Running Total
	Tx udp Packets in bytes	Running Total
	Tx icmp Packets in bytes	Running Total
	Tx igmp Packets in bytes	Running Total
	Tx http Packets in bytes	Running Total
	Tx other Packets in bytes	Running Total
	Ip statistics last updated timestamp	
OTA Statistics	Net Modem DID	Not Applicable
	Downstream reliable in bytes	Running Total
	Downstream unreliable in bytes	Running Total
	Downstream overhead in bytes	Running Total
	Downstream multicast in bytes	Running Total
	Downstream broadcast in bytes	Running Total
	Downstream total in kilobytes	Running Total
	Upstream reliable in bytes	Running Total
	Upstream unreliable in bytes	Running Total
	Upstream overhead in bytes	Running Total
	Upstream total in kilobytes	Running Total
	OTA statistics last updated Timestamp	

Table C-2: iDirect MIB Statistical Information (Continued)

Statistics Type	Available Information	Data Class
Remote UCP	Net Modem DID	Not Applicable
	Upstream SNR in dB	Overwrite
	Power Adjustment in dBm	Overwrite
	Symbol Offset	Overwrite
	Frequency Offset in Hz	Overwrite
	Remote UCP statistics last updated Timestamp	
Latency	Net Modem DID	Not Applicable
	Net Modem Name	Not Applicable
	Net Modem SN	Not Applicable
	IP address	Overwrite
	Latency in seconds	Overwrite
	Network Name	Not Applicable
	Latency statistics last updated Timestamp	
Hub Statistics	Line Card DID	Not Applicable
	Type SN	Not Applicable
	Tx attempts	Running Total
	Tx bytes	Running Total
	Tx errors	Running Total
	Acq CRC errors	Running Total
	Traffic CRC errors	Running Total
	Bursts	Running Total
	Rx bytes	Running Total
	Rx power	Overwrite
	dma reset	Running Total
	tunnel rx errors	Running Total
	tunnel tx errors	Running Total
	Hub statistics last updated Timestamp	

Table C-2: iDirect MIB Statistical Information (Continued)

Statistics Type	Available Information	Data Class
Remote Status	Net Modem DID	Not Applicable
	Down SNR in dB	Overwrite
	Tx power in dBm	Overwrite
	Rx power in dBm	Overwrite
	Digital rx gain in dB	Overwrite
	Fll dac	Overwrite
	Rx cof	Overwrite
	Temperature	Overwrite
	TDM lost	Running Total
	SCPC errors	Running Total
	Time ticks	Overwrite
	LAN Port	Overwrite
	Ethernet mode	Overwrite
	Ethernet speed	Overwrite
	Ethernet auto-negotiate	Overwrite
	terminal session	Overwrite
	iSite session	Overwrite
	Remote Status last updated Timestamp	
Server Start Time	This Timestamp specifies the start time of the statistical Data	

C.2.1 Resetting Statistical Data

There are two classes of statistics contained in the MIB: cumulative statistics, such as IP statistics and CRC errors; and discrete snapshot measurements, such as temperature and frequency offset.

Each time statistics arrive from the network and the MIB is updated, new values for cumulative statistics are added to current values, creating running totals. In contrast, new values for discrete statistics overwrite the old values. These two types of statistics are distinguished in [Table C-2](#) by the “Data Class” column.

Cumulative statistics are useful in determining a total value since some previous time period. In order to reset the baseline time period for cumulative statistics, that is, to reset the counts to zero, a special object type is included in the MIB. When referenced, this object will reset all the statistics counters to zero.

The object is defined in the MIB as follows:

```
resetAllStatTables OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION " This field will reset all the statistical
                  tables under the idirectstats OID"
    ::= { idirectstats 7}
```

To reset the statistical data, follow these steps:

- Step 1 Log in to the NMS server machine as “root”.
- Step 2 Using the vi editor, edit the Net-SNMP daemon configuration file `snmpd.conf`:

```
# cd /etc/snmp
# vi snmpd.conf
```

- Step 3 Add the following line:

```
rwcommunity private
```



NOTE Add the above line only if `snmpd.conf` does not already contain it.

- Step 4 Restart the *snmpd* service:

```
Example: /etc/init.d/snmpd restart
```

- Step 5 Use the SNMP SET command to set the MIB Object `resetAllStatTables` to 1.

```
Usage: snmpset -v 2c -c private <NMS server Ipaddress>
resetAllStatTables.0 u 1
```

Data types and table entry names are available from the MIB itself, which is available in the following file on the NMS server machine:

```
/usr/share/snmp/mibs/IDIRECT-REMOTE-MIB.txt
```

C.2.2 iDirect MIB SNMP Traps

The iDirect SNMP Proxy Agent will send traps to any configured trap recipient based on network element state changes and raised or cleared element conditions. See the next section of this document for information on configuring trap recipients.

The complete list of traps is shown in the following table. You will receive each trap when the specified anomaly arises, and again when the condition clears. The trap-level field in the MIB specifies the severity.

Table C-3: iDIRECT MIB Traps

Trap Name	Generated When...	Severity	Network Elements
snmpProxyStart	SNMP Proxy Agent starts up	N/A	SNMP Proxy Agent
snmpProxyStop	SNMP Proxy Agent shuts down	N/A	SNMP Proxy Agent
upstreamSNR	Upstream SNR goes outside specified limits	Warning	Remotes
downstreamSNR	Downstream SNR goes outside specified limits	Warning	Remotes
tempLimit	Onboard temperature goes outside specified limits	Warning	Remotes
latency	Latency measurement exceeds high limit	Warning	Remotes
symbolOffset	Symbol offset goes outside specified limits	Warning	Remotes
ethernetUnplugged	The local LAN port is non-functional	Warning	Remotes
ucpLostContact	The protocol processor loses contact with a remote	Warning	Remotes
lldown	The protocol processor's link layer interface for a remote goes down	Alarm	Remotes
ucpOutOfNetwork	The protocol processor declares a remote out of network	Alarm	Remotes
latTimeout	Latency measurements are failing	Alarm	Remotes
remoteOffline	The remote has been commanded offline	Offline	Remotes
lackHubStats	The NMS is no longer receiving hub statistics	Alarm	Hub Modems
acqHubModemCRC	Acquisition CRC count exceeds high limit	Warning	Hub Modems

Table C-3: iDIRECT MIB Traps (Continued)

Trap Name	Generated When...	Severity	Network Elements
trafficHubModemCRC	Traffic CRC count exceeds high limit	Warning	Hub Modems
ppStateTrap	The NMS has stopped hearing from the protocol processor	Alarm	Protocol Processor
powerAlarm1, 2, 3	The specified power supply has failed	Warning	Chassis
fanAlarm	One of the fans has failed	Warning	Chassis
chassisDown	The NMS cannot contact the chassis	Alarm	Chassis
scpcRxErros	A remote has received SCPC errors on the downstream	Warning	Remotes
fllDacErrors	A remote's digital-to-analog converter (DAC) is operating outside the defined limits	Warning	Remotes

C.2.3 Setting up SNMP Traps

If you want the SNMP Proxy Agent to send traps for network element state changes, you must designate one or more machines to receive them. The machine name is a parameter in one of Net-SNMP's configuration files.

To designate a machine to receive traps, use the following procedure:

- Step 1 Log in to the NMS server machine as "root".
- Step 2 Using the vi editor, edit the Net-SNMP daemon configuration file:

```
# cd /etc/snmp/
# vi snmpd.conf
```



NOTE

In a few instances, the SNMP trap configuration has been moved into /home/nms/snmpsvr/para_cfg.opt. If the instructions above are not accurate, execute these commands instead:

```
# cd /home/nms/snmpsvr/
# vi para_cfg.opt
```

- Step 3 Add a line like the following for *each* machine to which you want to send SNMP Version 1 (v1) traps:

```
trapsink host [community [port]]
```

Replace host with the name of the desired recipient. The community and port strings are optional.

- Step 4 Add a line like the following for *each* machine to which you want to send SNMP Version 2 (v2) traps:

```
trap2sink host [community [port]]
```

Replace host with the name of the desired recipient. The community and port strings are optional.-



WARNING Do not change or remove any other lines in this file.

C.3 Working with HP OpenView

The SNMP product installed on the NMS server machine is an open-source package called *Net-SNMP*. The MIB syntax processing is slightly different between this package and HP OpenView. If you use HP OpenView as your SNMP client software, you will need to load the special HP OpenView-specific MIB instead of the MIB that comes standard with our agent.

The HP OpenView MIB can found on the NMS server machine in the following location:

`/home/nms/snmpsvr/IDIRECT-REMOTE-MIB.hpov.txt`

C.3.1 Linux SNMP Tools

The Net-SNMP package supplies a number of command-line utilities that perform various SNMP-related functions. These commands are listed below, along with a one-line description of what each one does.

Table C-4: SNMP Command Line Utilities

Command Name	Severity
snmpbulkget	Communicates with a network entity using SNMP GETBULK Requests
snmpbulkwalk	Communicates with a network entity using SNMP BULK Requests
snmpcmd	Not a command, but a manual page that describes the common options for the SNMP commands
snmpconf	Creates and modifies SNMP configuration files
snmpdelta	Monitor deltas of integer valued SNMP variables
snmpdf	Gets a listing of disk space usage on a remote machine via SNMP
snmpget	Communicates with a network entity using SNMP GET Requests
snmpgetnext	Communicates with a network entity using SNMP GET NEXT Requests
snmpnetstat	Show network status using SNMP
snmpset	Communicates with a network entity using SNMP SET Requests
snmpstatus	Retrieves important information from a network entity
snmptable	Obtain and print an SNMP table
snmptest	Communicates with a network entity using SNMP Requests
snmptranslate	Translate SNMP object Id (OID) values into more useful information
snmptrap	Sends an SNMP trap to a manager
snmpusm	Creates and maintains SNMPv3 users on a remote entity
snmpwalk	Communicates with a network entity using SNMP GETNEXT Requests

For more information on any of the commands in this list, log in to the NMS server machine and type the following command:

```
# man <command name>
```

This will display the Linux manual entry or *man page* for the specified command that provides usage details, output descriptions, etc. Note that some of the commands above will not display anything about your iDIRECT networks, but instead display Linux system characteristics, such as disk space and network status.

Appendix D Rx CRC Error Correlation

Transmit problems on one or more remotes may cause CRC errors on the hub line card that is receiving the upstream carrier. CRC errors could be caused by any of a number of problems: a remote transmitting above the saturation point, a bad cable, interference, etc.

If the upstream carrier is being received by an iNFINITI line card, you can use the iDirect Rx CRC Correlation feature to identify which remote or remotes are causing the receive packet errors (Rx CRC errors) on the card.

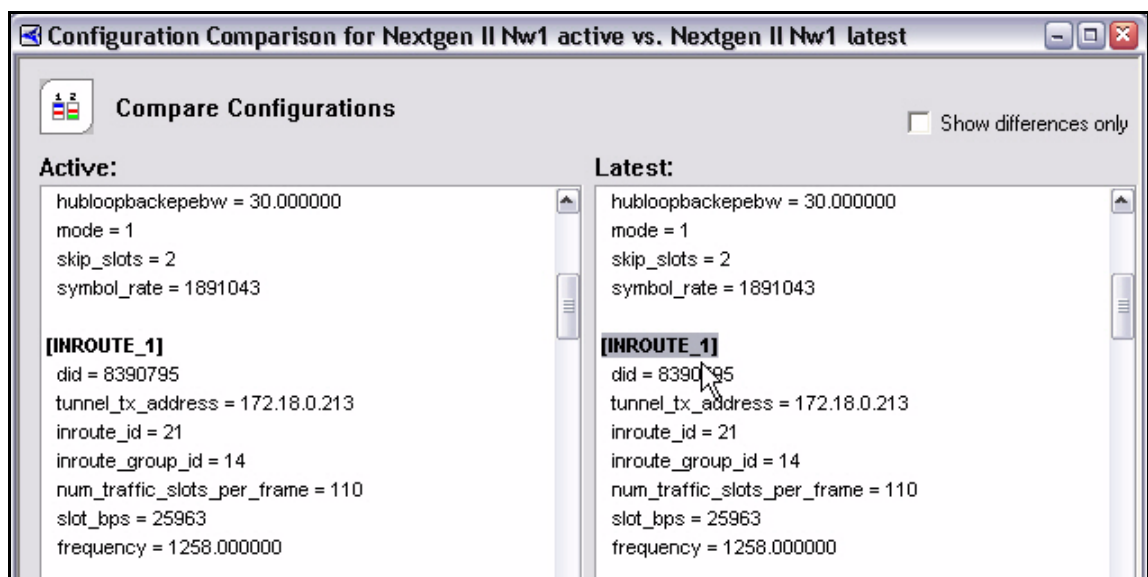


NOTE

CRC error checking is a processor-intensive operation. To avoid overloading the processes of your line cards, iDirect recommends that you delete the custom keys that enable Rx CRC Correlation when you are finished.

Follow these steps to correlate CRC errors on your receive line card with the remotes causing the errors:

- Step 1 Use iBuilder to determine the ID of the inroute being received by the line card as follows:
 - a In iBuilder, right-click on the Network and select **Compare Configurations** from the menu.
 - b In the **Configuration Comparison** dialog box, clear the **Show Differences Only** check box.
 - c Examine the **Latest** pane to determine the Inroute IDs for the Inroutes in your Network. Inroute IDs are displayed in the format **INROUTE_#**, where # represents the ID of the Inroute. Note the ID of each Inroute.



Step 2 Enable Rx CRC correlation for your Inroutes as follows:

- a Right-click the Network in the iBuilder tree and select **Modify→Item** from the menu.
- b Click the Custom tab.
- c Enter a network-level custom key in the following format:

```
[INROUTE_#]  
disable_lock = 0
```

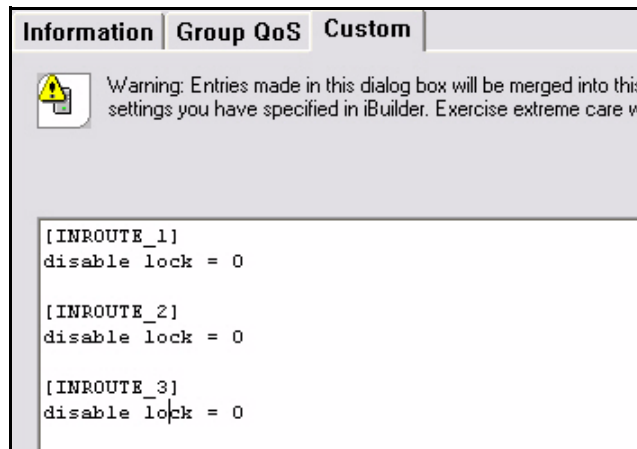
where # is the Inroute ID determined in the previous step.

If you have multiple Inroutes in the Network, you need to create a custom key for each. For example:

```
[INROUTE_1]  
disable_lock = 0
```

```
[INROUTE_2]  
disable_lock = 0
```

etc.



- d Click **OK** to save your changes.
- e Right-click the Network in the iBuilder tree and select **Apply Configuration→Network** from the menu.

Step 3 Connect to your protocol processor blades as follows:

- a Using a terminal emulator (such as PuTTY), log on to your NMS server using SSH.
- b From the command line of the NMS server, enter the following command to log onto a blade:

```
> telnet <IP Address> 13255
```

where **<IP Address>** is the address of the protocol processor blade.

- c Log on to the blade with Username: admin.

Step 4 To view the Rx CRC errors for the Networks configured to use the blade, run the CRC error correlation report as follows:

- a From the command line, enter the command **sarnt** to access the sarnt functions on the blade:

```
> sarnt;
```

- b Enter the **net list** command to determine the networks available on this blade. You will see a list of valid networks, as in the following example:

```
Valid Networks are: 1 4 6
```

- c Enter the **net** command to select the Network you want to examine. For example:

```
> net 1  
NETWORK 1
```

- d Enter the **crc report** command to see the number of CRC errors generated by each remote over time. The **crc report** command has several forms shown in the syntax below:

```
> crc report  
Usage:  
crc report {data|acq|all} [reset]
```

- e Enter the following command to see a count of data CRC errors for each remote:

```
> crc report all  
3100.3235 : DATA CRC [ 1]  
3100.3502 : DATA CRC [5818]  
3100.4382 : DATA CRC [ 20]  
3100.4463 : DATA CRC [ 3]  
3100.4656 : DATA CRC [ 11]  
3100.7249 : DATA CRC [1369]  
3100.8963 : DATA CRC [ 1]  
3100.9162 : DATA CRC [ 1]
```

- f You can clear the counts by entering:

```
> crc report all reset
```

- g Repeat steps b through d for each Network on current blade, or enter the following command to see all CRC errors for all Networks on the blade:

```
> net * crc report all
```

If you have more protocol processor blades to check, execute this procedure again, beginning with [Step 3](#). When you have finished, iDirect recommends that you delete the custom keys you configured for your Network(s) and re-apply the changes.

Index

A

alarms	
see conditions	
archive, see statistics archive	
audio notification	20

B

blades	
cpu usage	66
monitoring	59
button	
accept changes	11

C

conditions	33
acknowledging	22
alarms and warnings on elements	36
audio notification	20
condition log tab	34
interpreting	48
observation view tab	34
viewing	42
conditions pane	27, 34
configuration changes	29
connecting to network elements	98
CRC errors	
Identifying Rx errors on line cards caused by remote transmissions	82
cw carrier	
enabling from remote probe	63
modifying timeout duration	65

E

elements	
putting under observation	39
events	33
interpreting	50
viewing	42
external device monitoring	
alarm state vs warning state	51
displaying conditions for all remote devices per inroute	51
displaying conditions for remote devices	51
displaying conditions for teleport devices	51

F

find toolbar	23
--------------	----

G

geographic map	
clearing remote tracks	141
components of	7
determining a remote's past locations	141
enabling remote tracking	141
filtering	144 to 146
filtering criteria	144
filtering using the context menu	145
filtering using the toolbar	145
installing on PC	8
installing server license	8
launching	135
launching with historical tracking	136
license for	8
monitoring remotes with	135
PC requirements	7
selecting remotes to view	135
toolbar	137
tracking mobile remotes	140
using the map to select from Network Tree menu	142
viewing the toolbar	137
globe	
hiding elements	15
sorting elements	15
tree	15
graphs	
IP traffic	114
mesh traffic	121
mesh UCP	86
SAT traffic	111
SATCOM	82
timeplan	68
Group QoS	
explanation of statistics displayed	92
exporting statistics to excel or CSV	95
limitation of BW Req statistic	92
viewing statistics	90
viewing statistics for a single node	91
viewing statistics for a single remote	92

H

HDLC addresses, viewing on remotes	98
------------------------------------	----

I

iBuilder	
description	3
installing	6
iMonitor	
description	4
launching	9
using the interface	14
installation	
NMS applications	6
IP long term bandwidth usage	127
IP routing table, viewing on remotes	98
IP statistics	109
IP traffic graph	114
iSite	4
iVantage NMS components	xi

L

latency, monitoring round-trip	74
launching iMonitor	9
legend	28
line cards	
identifying remotes causing Rx CRC errors on	82
statistics on	79
logging in	
passwords	9
to other servers	10

M

main toolbar	23
map, see geographic map	
mesh	
mesh long term bandwidth usage	127
mesh statistics	120
mesh traffic graph	121
mesh UCP tab	86
probe mesh	77
selecting UCP parameters for viewing	87
UCP parameter definitions	88
mobile remotes	
determining past locations	141
tracking on geographic map	140
modifying	
accepting changes	10

N

NetManager, replaced by iSite	4
network condition snapshot	50
network data snapshot	56
network tree	19
see also: tree	
NMS	
applications	3
iVantage NMS components	xi
main components	3
multiple users accessing	10
servers used	5
NMS database	
overview	148

O

observation	
putting elements under	39
offline state	36

P

panes	
conditions	27
configuration changes	29
legend	28
probe	61
probe mesh	78
<i>See also</i> dialog boxes	
selecting columns for viewing	30
sorting columns in	16
passwords	9
pn carrier	
enabling from remote probe	63
modifying timeout duration	65
probe	61
adjusting remote transmit power	63
functions of	61
transmitting a modulated or unmodulated carrier	63
probe mesh	77

R

remotes	
viewing IP and HDLC information on	98
reports	127 to 134

long-term bandwidth usage	127
remote availability	133
requirements	
system	6
right-click	
menu options	22

S

SAT long term bandwidth usage	127
SAT statistics	109
SAT traffic graph	111
SATCOM graph	82
saving data to files	12
saving workspaces	25
selecting columns for viewing	30
servers	5
SkyMonitor	
capturing a bitmap image of the display	107
changing RF port settings	103
described	100
launching from the iMonitor tree	100
recalling and viewing saved data	105
saving data to the NMS server	104
viewing carriers and pre-defined bandwidth	100
snapshots	50 to 57
SNMP	
iDirect MIB	192
iDirect traps defined	197
resetting MIB statistics	195
setting up traps	198
statistics in MIB	192
support on iDirect	191 to 201
sorting columns	16
sorting the tree	17
statistics	
IP	109
SAT	109
statistics archive	
accessing	
basic information	149
changing the 6.1 table structure	173
converting data between table formats	172
installing the partitioning calculator on your PC	174
optimized storage	147
partitioning the database	174
querying the restructured database tables	180
restructuring for release 6.1	167

table details	151
using the partitioning calculator	175
status bar	26
system requirements	6

T

teleport condition snapshot	50
time periods	
for requesting data	11
time ranges, saving	11
timeplan graph	68
toolbars	
configuration changes	29
find	23
geographic map	137
icons	23, 26
legend	28
main	20, 23
main menu	22
status bar	26
view menu	22
tree	
description	19
sorting the tree	17

U

upstream carriers	
Rx CRC errors on	82
users	
multiple	10

W

windows, <i>See</i> panes	
<i>See also</i> dialog boxes	
workspaces	
saving and reloading	25

iDirect, Inc.

13865 Sunrise Valley Drive

Herndon, VA 20171

+1 703.648.8000

+1 866.345.0983

www.idirect.net

Advancing a Connected World