



Network Management System
iMonitor User Guide

Release 6.0.9
November 30, 2005



Copyright © 2005, iDirect, Inc. All rights reserved. This manual may not be reproduced, in part or in whole, without the permission of iDirect, Inc.

The specifications and information regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual 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 manual 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.

iDirect, Inc.
International Headquarters
13865 Sunrise Valley Drive
Herndon, VA 20171
www.iDirect.net

HQ: 1.703.648.8000
Toll free from within the US 1.888.362.5475

Contents

Figures	viii
Tables	ix
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	1
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	4
<i>Configuration Server</i>	4
<i>Real-time Data Server</i>	5
<i>Event Server</i>	5
<i>Latency Server</i>	5
<i>PP Controller Server</i>	5
<i>NMS Monitor Script</i>	5
<i>Consolidation Script</i>	5
<i>Database Backup Script</i>	5
<i>Database Restore Script</i>	5
2.3 Installing iBuilder, iMonitor, and iSite	5
2.3.1 System Requirements	6
2.3.2 Installation Procedure	6
2.4 Launching iMonitor	7
<i>Logging On To Additional Servers</i>	8
<i>Multiple Users or PCs Accessing the NMS</i>	8
<i>Accepting Changes</i>	8
2.5 Overview of iMonitor Usage and Displays	9
2.5.1 iMonitor Time Frames in Requests	9
2.5.2 Saving Historical Time Ranges across Multiple Displays	9
2.5.3 Historical “Save to File” Capability	10
2.5.4 Types of iMonitor Displays	10
2.5.5 Multicolumn Details Displays	10

2.5.6 Multiple vs. Grouped Display Results	11
2.6 Using iMonitor's Interface	11
2.6.1 Clicking on Elements: What Happens?	12
<i>Right-Clicking</i>	12
<i>Single-Clicking vs. Double-Clicking</i>	12
2.6.2 Globe Functions	13
<i>Using the Docking Feature</i>	13
<i>Hiding Elements</i>	13
<i>Expanding Tree</i>	14
<i>Collapsing Tree</i>	14
<i>Sorting Columns</i>	15
<i>Sorting the Tree</i>	15
2.6.3 Network Tree	17
2.6.4 Using the Interface Toolbars and Menu Options	17
<i>Title Bar</i>	17
<i>Menu Bar</i>	18
<i>Toolbar</i>	18
<i>Audio Notification</i>	19
<i>View Menu</i>	20
<i>Find Toolbar</i>	20
<i>Workspace Toolbar</i>	22
<i>Operational Toolbar</i>	23
<i>Status Bar</i>	24
<i>Connection Details on Status Bar Icon</i>	24
<i>Conditions Pane</i>	24
<i>Legend Pane</i>	25
<i>Configuration Changes Pane</i>	25
<i>Monitor Menu</i>	26
3 Monitoring Conditions and Events	27
3.1 Conditions	27
3.1.1 Representing State of Element via Icons	27
3.1.2 Conditions View Tabs	28
3.1.3 Elements with Multiple Conditions	28
3.1.4 Offline State	29
3.1.5 Alarms and Warnings on Elements	29
3.2 Putting an Element under Observation for Conditions	30
3.2.1 Viewing Conditions or Events	34
<i>Viewing Conditions</i>	34
<i>Viewing Events</i>	35
3.2.2 Interpreting Conditions Results	42

3.3 Interpreting System Events	44
3.4 Snapshots	44
3.4.1 Network Condition Snapshot	44
<i>Multiple Selection Options in Condition Snapshot View</i>	48
3.4.2 Network Data Snapshot	50
4 Obtaining Performance and Status Information	55
4.1 Monitoring Blades in iMonitor	55
4.2 Retrieving Information on Remotes using Probe	57
4.2.1 CPU Usage (Blades Only)	62
4.2.2 Time Plan	64
<i>Pausing the Time Plan Graph and Highlighting Individual Entries</i>	67
4.2.3 Inroute Distribution	67
<i>Networks</i>	68
<i>Inroute Groups</i>	69
<i>Performing ACQ Bounce</i>	69
4.2.4 Latency	69
4.3 SAT Link Info	73
4.3.1 Line Card Statistics	73
4.3.2 SATCOM Graph	76
<i>Remote Status and UCP Info</i>	76
<i>Display</i>	76
<i>Procedure for Viewing SATCOM Graph, Remote Status and UCP Info</i>	76
<i>Remote Status and UCP Info Tabs</i>	80
4.3.3 Control Panel	80
4.4 Telnet	83
5 IP and SAT Traffic Graphs	85
5.1 IP Statistics	85
5.2 IP Statistics Changes	85
5.3 SAT Statistics	86
5.3.1 SAT Traffic Graph	87
5.3.2 IP Traffic Graph	90
5.3.3 Viewing Options	93
5.3.4 Bandwidth Usage	94
6 Reporting on Networks	97
6.1 Reports	97
6.1.1 Long-Term Bandwidth Usage Report	97
6.1.2 IP and SAT Long Term Bandwidth Usage Reports	97
<i>Results</i>	100
<i>Totals Tab</i>	100

<i>Averages Tab</i>	100
6.1.2.1 Interpreting the Report	102
<i>Percentage of Channel Capacity</i>	102
6.2 Remote Availability Report	103
Appendix A Accessing the NMS Statistics Archive	105
A.1 Improved NMS Statistics Archive Storage	105
A.2 Improved NMS Statistics Archive Lookup	105
A.3 Archive Consolidation	105
A.4 NMS Database Overview	106
<i>Connecting to the NMS Archive Database with ODBC</i>	106
<i>Obtaining the ODBC Connection Library</i>	106
<i>Setting up a Simple ODBC Access Account</i>	106
A.5 Basic Archive Database Information	107
<i>Types of NMS Databases and Supported Access</i>	107
<i>Structure Changes between Releases</i>	107
<i>Accessing Remote and Network Names from Configuration Database</i>	107
<i>Timestamps</i>	108
<i>Archive Consolidation</i>	108
<i>Overview of the Archive Database Tables</i>	108
A.6 Database Table Details	109
<i>IP Stats Tables</i>	109
<i>New Fields Beginning with Release 4.0.0</i>	110
<i>IP Stats Consolidation</i>	111
<i>Latency Measurements</i>	112
<i>Hub Line Card Statistics</i>	113
<i>Remote Status</i>	113
<i>Uplink Control Adjustments</i>	114
<i>Event Messages</i>	115
<i>Hub and Remote State Changes</i>	116
<i>Protocol Processor State Changes</i>	118
<i>Hub Chassis State Changes</i>	119
Appendix B Alarms and Warnings	121
B.1 Alarms	121
B.2 Warnings	122
B.3 Acronyms	124
B.4 Warning Limit Ranges	125
Appendix C SNMP Proxy Agent	127
C.1 How the Proxy Agent Works	127
C.1.1 Installing and Running the SNMP Proxy	127
C.1.2 The iDirect Management Information Base (MIB)	128
C.1.3 iDirect MIB SNMP Traps	129

C.1.4 Setting up SNMP Traps	130
C.2 Working with HP OpenView	131
C.2.1 Linux SNMP Tools	131
Index	133

Figures

Figure 2-1: Windows Start Menu Entries for NMS GUI Clients	6
Figure 2-2: Expand Tree Selection	14
Figure 2-3: Expanded Tree with Child Elements	14
Figure 2-4: Collapse Tree Selection	14
Figure 2-5: Collapsed Tree	14
Figure 2-6: The Workspace Toolbar in Action	22
Figure 3-1: Conditions Time Range	37
Figure 3-2: Events Time Range with Text Filter	38
Figure 3-3: Conditions Results in Multicolumn Format	39
Figure 3-4: Conditions Time Line Results in Graphical Format	40
Figure 3-5: Event Results	42
Figure 3-6: List View of Network Condition Snapshot	45
Figure 3-7: Remote Submenu in Condition Snapshot	46
Figure 4-1: Remote Status Raw Data	80
Figure 4-2: UCP Info Raw Data	80
Figure 5-1: Collection Points for IP Usage Statistics	86
Figure 5-2: Real-Time Bandwidth Usage Display	95
Figure 6-1: SAT Long Term Bandwidth Usage Report	101
Figure 6-2: IP Long Term Bandwidth Usage Report	102
Figure C-1: SNMP Proxy Architecture	127

Tables

Table 2-1: Toolbar Icons and Functions	18
Table 2-2: Operational Toolbar Icons and Functions	23
Table 3-1: Elements and Types of Information Provided	27
Table 3-2: Real-Time States and Icons	27
Table 3-3: Explanation of Alarms by Element	29
Table 3-4: Explanation of Warnings by Element	29
Table 3-5: Explanation of Alarms and Warnings on Hub Chassis	30
Table A-1: Archive Database Tables	108
Table A-2: IP Stats Record Format	109
Table A-3: Additional Consolidated IP Stats Table Fields	111
Table A-4: lat_stats Record Format	112
Table A-5: nms_hub_stats Table Format	113
Table A-6: nms_remote_status Record Format	114
Table A-7: nms_ucp_info Record Format	115
Table A-8: event_msg Record Format	115
Table A-9: state_change_log Record Format	116
Table A-10: pp_state_change_log Record Format	118
Table A-11: chassis_state_change_log Record Format	119
Table B-1: Alarms	121
Table B-2: Warnings	122
Table B-3: Warning Limit Ranges	125
Table C-1: iDirect MIB Contents	128
Table C-2: iDIRECT MIB Traps	129
Table C-3: SNMP Command Line Utilities	131

1 Using this Guide

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 (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

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 network 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 1db 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.

iSite also allows monitor-only capability to end-users, should you decide to provide it to them. For more information About iSite, see the book *Using iSite to Commission Equipment*.



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.

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.

PP Controller Server

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

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

Database Restore Script

This daemon 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 6.0**. The iBuilder, iMonitor, and iSite clients are displayed, along with an **Uninstall** selection.



Figure 6: Desktop Shortcuts for NMS GUI Clients



Figure 2-1: Windows Start Menu Entries for NMS GUI Clients



NOTE

The server portion of the NMS is installed on the primary and backup NMS servers. For more information About installing and/or upgrading these components, see the iDirect Technical Note titled *Installing iDS Software*.

2.4 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 [Appendix C, Creating and Managing User Accounts](#) in *Network Management System iBuilder User Guide*.

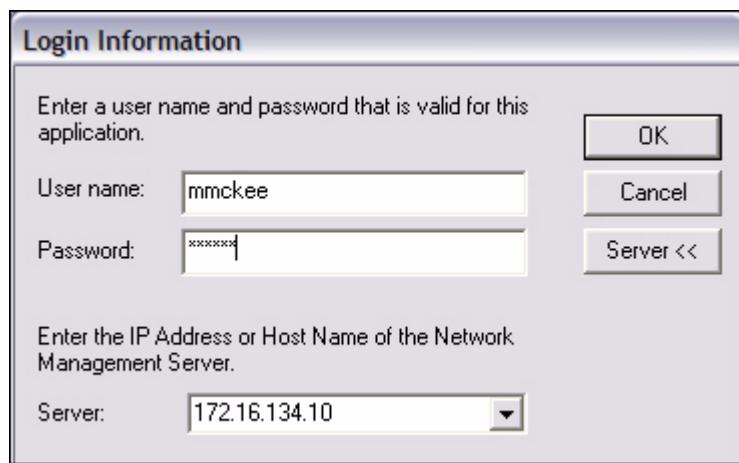
iDirect strongly recommends that you modify the **admin** user password as soon as possible after the installation. This is especially important if your NMS Server is accessible via the public Internet.

- 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

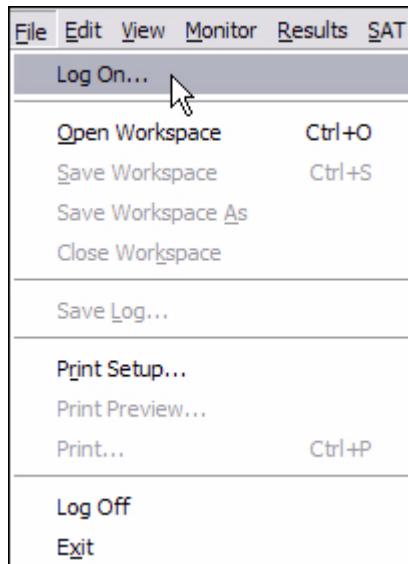
The NMS server version must match the iMonitor version in order for you to log in. For example, version 6.0.0 of iMonitor may connect only to version 6.0.0 of the NMS servers.



The iMonitor application automatically connects to the NMS server processes that are required to perform the NMS’s 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

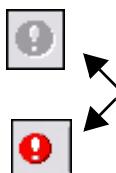
Multiple users or multiple sessions may run simultaneously on the NMS database. For example, the NMS offers the following capabilities:

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 iMonitor 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 the other user changes the configuration, 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 18](#).



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 25](#)). 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.

2.5 Overview of iMonitor Usage and Displays

2.5.1 iMonitor Time Frames in Requests

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

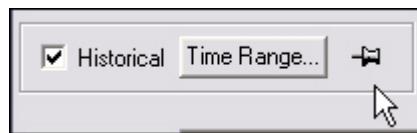
- **Real-time** requests display data as it arrives into the NMS back-end in real-time. These requests have no ending time period—they continue displaying data as long as you keep the display running. Closing either the specific display or the iMonitor application automatically cancels real-time requests.
- **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.

2.5.2 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.

2.5.3 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

2.5.4 Types of iMonitor Displays

The two data display types used in iMonitor are graphical displays and multicolumn lists. Conditions are shown only in multicolumn lists. Network statistical data 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.

2.5.5 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 FilePrint 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

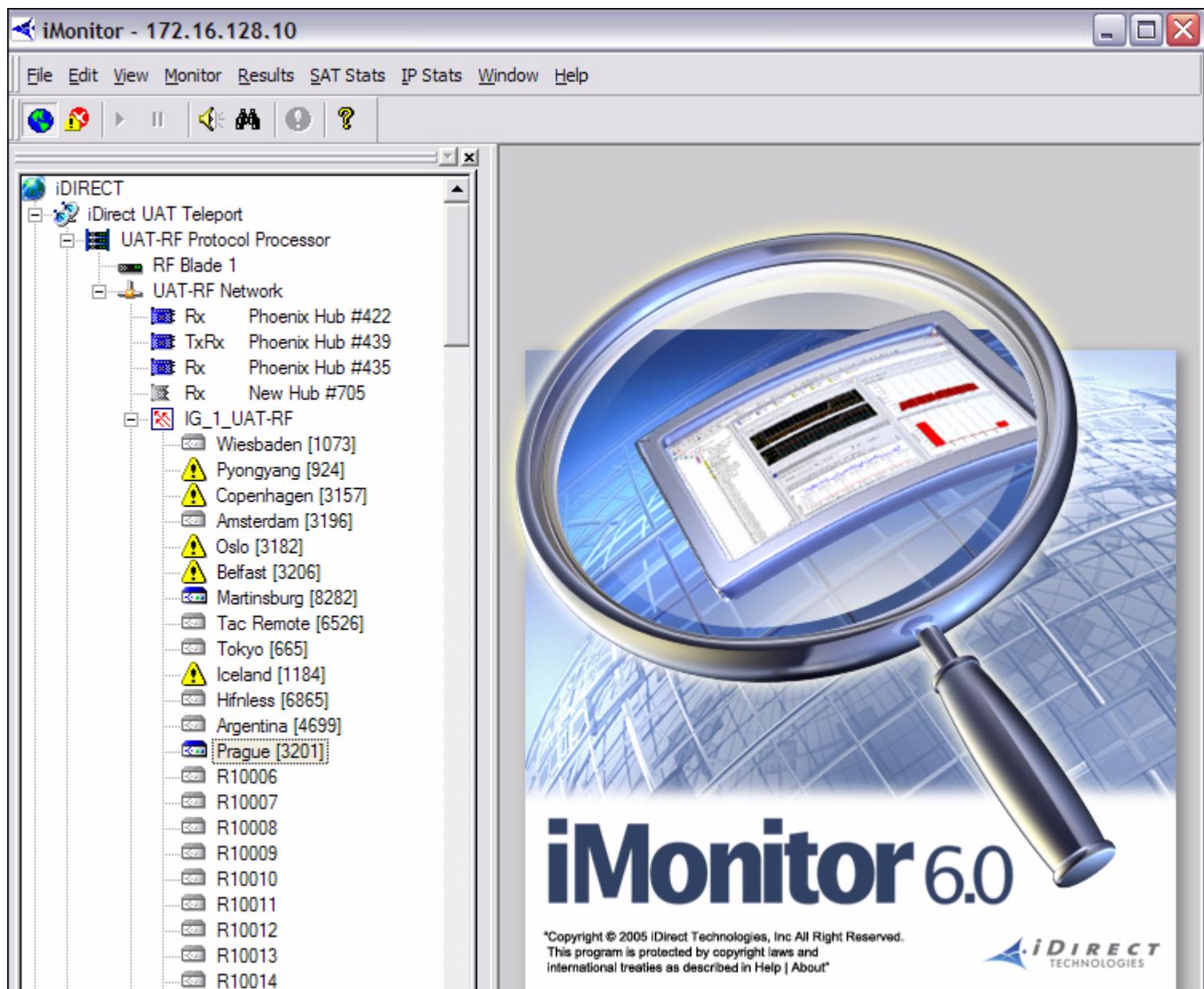
2.5.6 Multiple vs. Grouped Display Results

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.

2.6 Using iMonitor's Interface

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



2.6.1 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. Once an element has no plus (+) signs next to it, you can double-click any element to view the Properties for that element in read-only mode.

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

2.6.2 Globe Functions

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

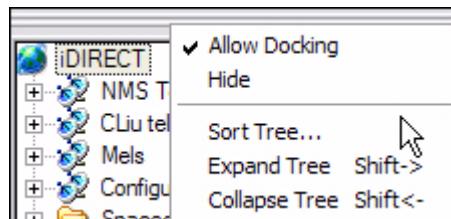
Using the Docking Feature

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. This feature is useful if you have two displays on a single PC and want to move this pane to the second display.

Hiding Elements

You can click **Hide** to remove 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.

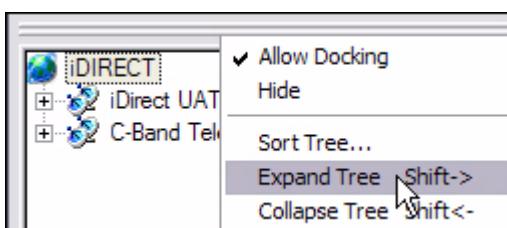


Figure 2-2: Expand Tree Selection

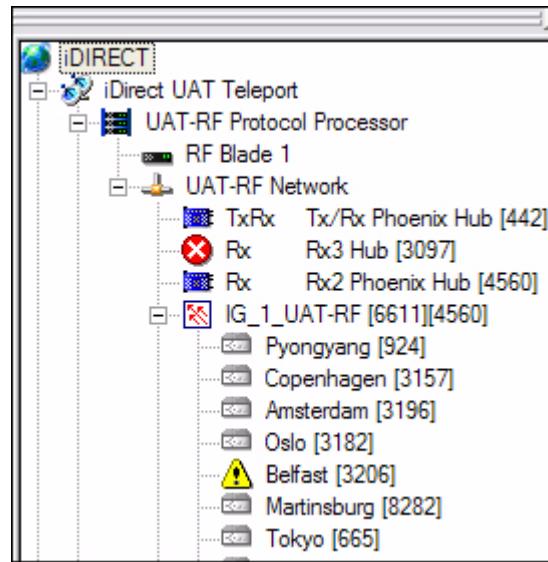


Figure 2-3: Expanded Tree with Child Elements

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.

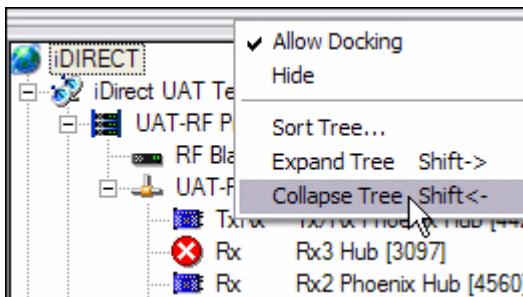


Figure 2-4: Collapse Tree Selection

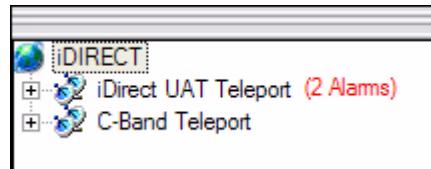


Figure 2-5: Collapsed Tree

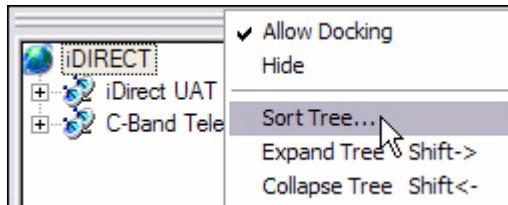
Sorting Columns

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

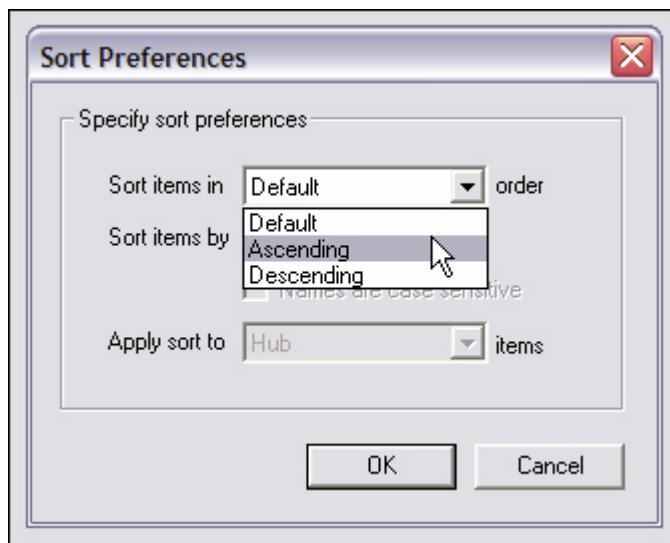
To sort the Tree, follow the steps below:

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

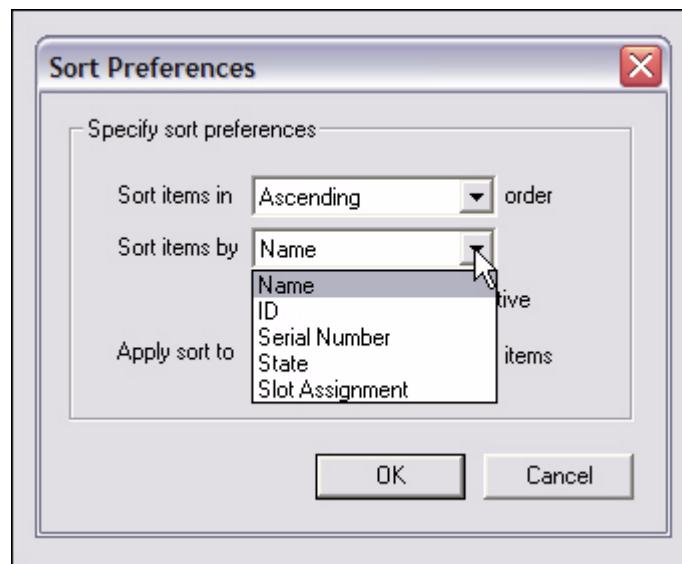


- Step 2 The **Sort Preferences** dialog box is displayed.

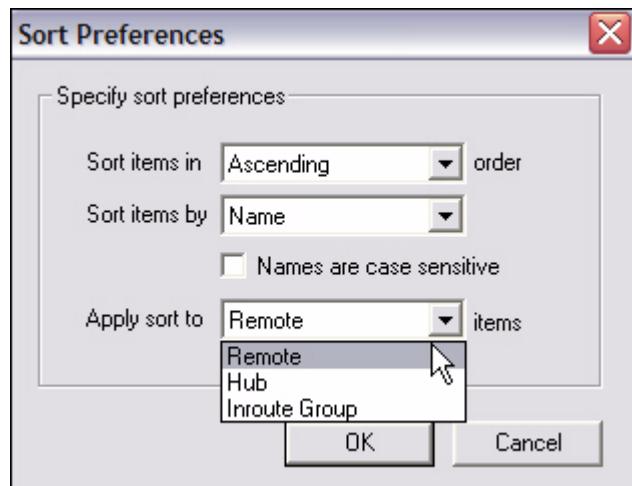
- Step 3 Click the **Sort items in** drop-down list and select either **Ascending** or **Descending**.



- 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

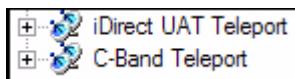


- Step 7 Click **OK**. The next time you log in, iMonitor will remember and display the last sort preference you chose.

2.6.3 Network Tree

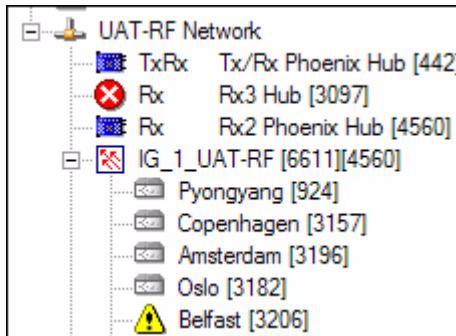
By right-clicking a tree element, a submenu of options appears, which you may click to view various types of data and other information used to monitor and troubleshoot your network. For specific information on how to use and interpret the information you view, see the section on that particular option. 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 collapsed and children are visible at the next level, or branch, in the Tree.

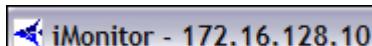
In the figure below, the UAT-RF Network has been collapsed as far as it can be. The UAT-RF Network cannot include children in another network; therefore, its only children are the TxRx and Rx line cards, and the IG_1_UAT-RF Inroute Group. The Inroute Group is a parent element that can be collapsed by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



2.6.4 Using the Interface Toolbars and Menu Options

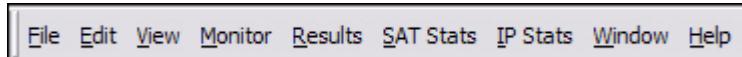
Title Bar

The **Title** bar identifies the name of the application (in this case, iMonitor) 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, “Toolbar Icons and Functions,” on page 18](#).

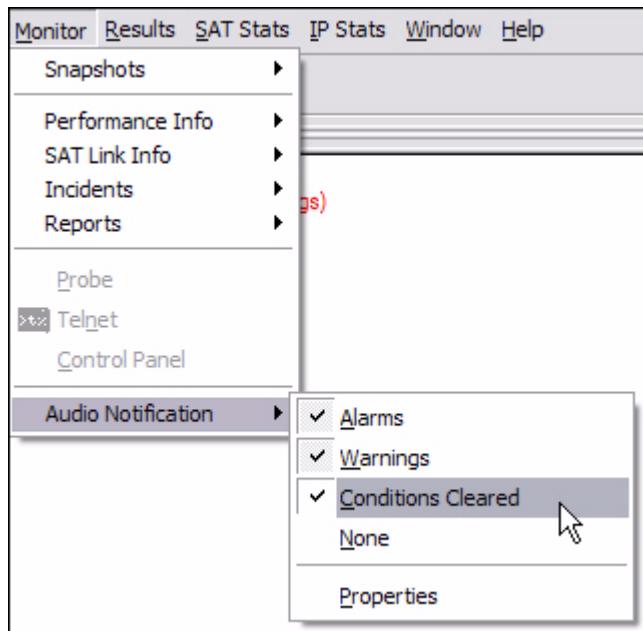


Table 2-1: Toolbar Icons and Functions

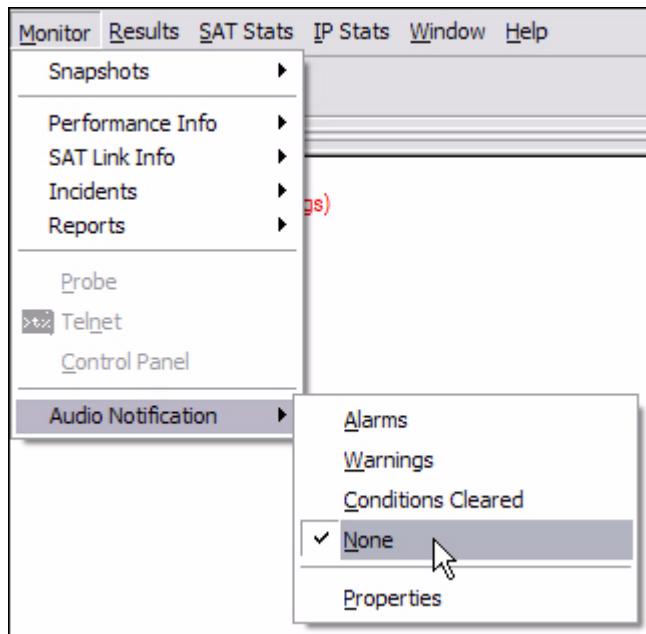
Toolbar Icon	Functionality
	Allows you to view elements in the Tree Menu hierarchy
	Allows you to view Conditions. The Conditions pane has three tabs you can select to view different aspects of the conditions: Active Conditions, Observation View, and Disabled Conditions. See Section 3.1.2 “Conditions View Tabs” on page 28 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.
	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

Audio Notification

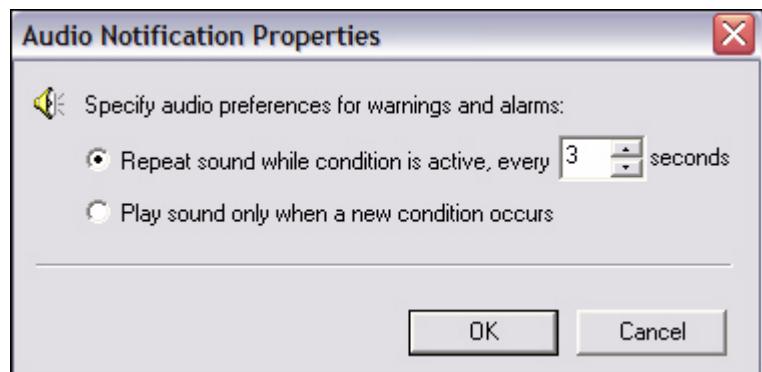
You can choose to turn on audio notification to alert you whenever a new alarm or condition is presented or a condition is cleared. Select **Monitor → Audio Notification**. You can click next to any of the three conditions under which you would like to have an audio notification presented.



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

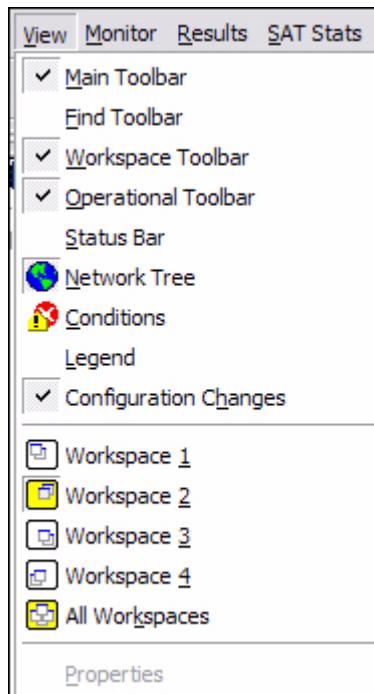


To set up how many times you want the audio to be repeated, select **Monitor → Audio Notification → Properties**. In this dialog box, you can also specify that the audio should play only when a new condition occurs. This relieves you of clicking on **Alarms** and **Warnings** separately in the above paths.



View Menu

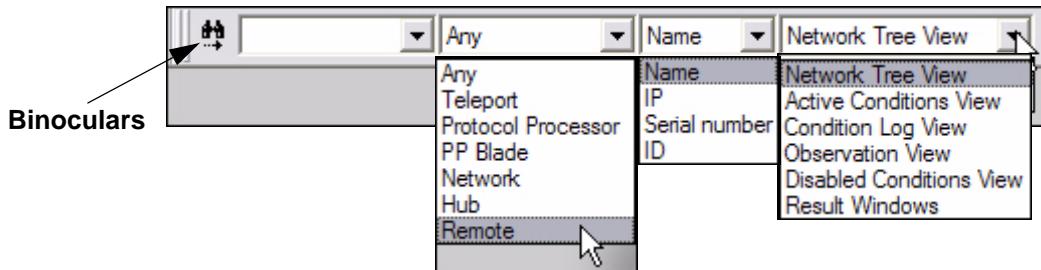
The **View** menu on the main menu toolbar allows you to display or hide the following toolbars and panes. You can also right-click your *context menu* button (typically the right mouse button) to see the same options as those in the **View** menu. If you have clicked an element in the Tree, the Properties option is available also.



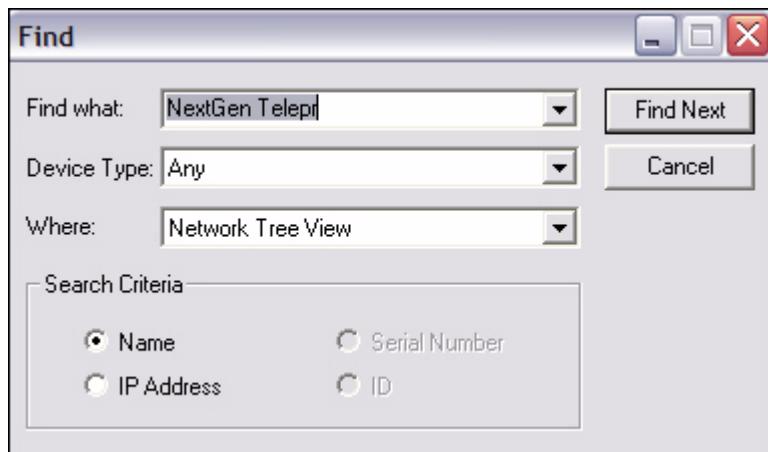
Find Toolbar

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.



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



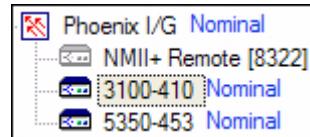
To perform a search, follow the steps below:

- 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 **Find Next** 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 task 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 2-6: 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, “Operational Toolbar Icons and Functions,” on page 23.](#)



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 Time Plan Slot Alignment Graph.
	Request latency results.
	Request a SATCOM Graph.
	Request a Remote Status/UCP report.

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

Toolbar Icon	Functionality
	Request modem events.
	Request conditions.
	Request a SAT Long Term Bandwidth Usage report.
	Request a Long Term Bandwidth Usage report.
	Put an element under observation.
	Open a telnet session.

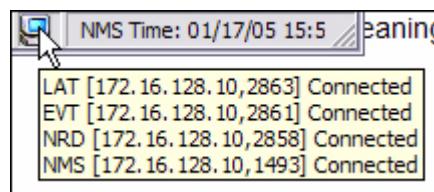
Status Bar

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** to open the pane.

Name	ID	Type-SN	Node T...	Network	Time
⚠️ Pyongyang [924]	195	II-924	Remote	UAT-RF Network	15:30:12
⚠️ Iceland [1184]	233	II-1184	Remote	UAT-RF Network	15:30:12
⚠️ Belfast [3206]	271	II+-3206	Remote	UAT-RF Network	11:35:05
❌ Rx3 Hub [3097]	673	II+-3097	Hub M...	UAT-RF Network	11:34:54
⚠️ Venice [3126]	676	II+-3126	Remote	UAT-RF Network	15:30:09
⚠️ Copenhagen [3157]	108	II+-3157	Remote	UAT-RF Network	15:30:02
⚠️ Phoenix Remote #492	697	5350-492	Remote	UAT-RF Network	15:30:00
⚠️ Phoenix Remote #492	697	5350-492	Remote	UAT-RF Network	15:30:00
⚠️ Phoenix Remote #459	698	5350-459	Remote	UAT-RF Network	15:30:00
⚠️ Oslo [3182]	124	II+-3182	Remote	UAT-RF Network	15:30:09

[Active Conditions](#) [Condition Log](#) [Observation View](#) [Disabled Conditions](#)

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 or...	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 Incompl...	Inroute Group not completely specified
CONDITION STATE	
🟢 OK	No alarms or warnings active
🔴 Offline	Remote Offline
🔴 Alarm	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.

Monitor Menu

The options listed under the Monitor Menu are discussed throughout this guide as follows:

- Snapshots
 - [Section 3.4.1 “Network Condition Snapshot” on page 44](#)
 - [Section 3.4.2 “Network Data Snapshot” on page 50](#)
- Performance Info
 - [Section 5.3.1 “SAT Traffic Graph” on page 87](#)
 - [Section 5.3.2 “IP Traffic Graph” on page 90](#)
 - [Section 4.2.2 “Time Plan” on page 64](#)
 - [Section 5.3.4 “Bandwidth Usage” on page 94](#)
 - [Section 4.2.3 “Inroute Distribution” on page 67](#)
 - [Section 4.2.4 “Latency” on page 69](#)
- SAT Link Info
 - [Section 4.3.2 “SATCOM Graph” on page 76](#)
 - [Section 4.3.1 “Line Card Statistics” on page 73](#)
 - [Section 4.3.2 “SATCOM Graph” on page 76](#)
- Incidents
 - [Chapter 3, Monitoring Conditions and Events](#)
- Reports
 - [Chapter 6, Reporting on Networks](#)
- Probe
 - [Section 4.2 “Retrieving Information on Remotes using Probe” on page 57](#)
- Telnet
 - [Section 4.4 “Telnet” on page 83](#)
- Control Panel
 - [Section 4.3.3 “Control Panel” on page 80](#)
- Audio Notification
 - [Section “Audio Notification” on page 19](#)

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, and chassis.
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.
Offline		The remote has been sent offline.

3.1.2 Conditions View Tabs

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

- **Active Conditions** – this tab shows all the currently-active conditions for all network elements. Details for each condition are shown in separate columns. You may click each column heading to sort the conditions in ascending or descending order.
- **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 all conditions that you have disabled. A disabled condition is one that you understand and no longer want to see in the Tree and Active Conditions list. The warning and/or alarm icon in the Tree turns gray when you disable a condition. You may re-enable the condition by right-clicking on the condition in the **Disabled Conditions** tab and selecting **Enable Condition**.

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

The tables below list all of the conditions that can be raised for the various elements.

Table 3-3: Explanation of Alarms by Element

Element	Alarm Condition	Explanation
Chassis	Down	Cannot talk to the EDAS
Protocol Processor	Down	Receipt (or lack of receipt) of a heartbeat from the PP
Hub Line Card	Down	

Table 3-4: Explanation of Warnings by Element

Element	Alarm Condition	Explanation
Chassis	Power Supply "n"	Failed
	Fan "n"	Failed
	RCM (Ref Clock Module) "n"	Failed
Hub Line Card	Rx Overflow of frames	Downstream Packets per sec. overdrive/Backplane lost 10 MHz clock
	Downstream Packets/sec. Overdrive	Protocol processor 's capability of the line card is being exceeded
	Back plane lost 10 MHz Clock	The 10 MHz reference timing signal is absent from the chassis backplane
Remote	Upstream C/N, low 7 high 25	Perceived signal 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

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

Element	Alarm Condition	Explanation
Remote	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 +/- 1/2 symbol off set
Remote	Remote Off-line State	
	Calibrated Transmit Power	Transmit power below -35 dbm detected
	GPS Signal Lost	Don't reset remote warning
	Remote Temperature	Temperature on board is higher than -77 C and lower than 15 C

Table 3-5: Explanation of Alarms and Warnings on Hub Chassis

Alert	Alarm Condition	Action to be Taken
Chassis Down	Alarm	Check unit power, validate network connectivity.
Fan Alert	Warning	Check fans, remove failed unit, replace.
Power Supply Alert	Warning	Check power supplies, remove failed unit, replace. The warning text includes the power supply number.
RCM A/B Alerts	Warning	Check the appropriate RCM for failure. If both warnings are on, check for loss of 10 MHz clock source.



NOTE

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

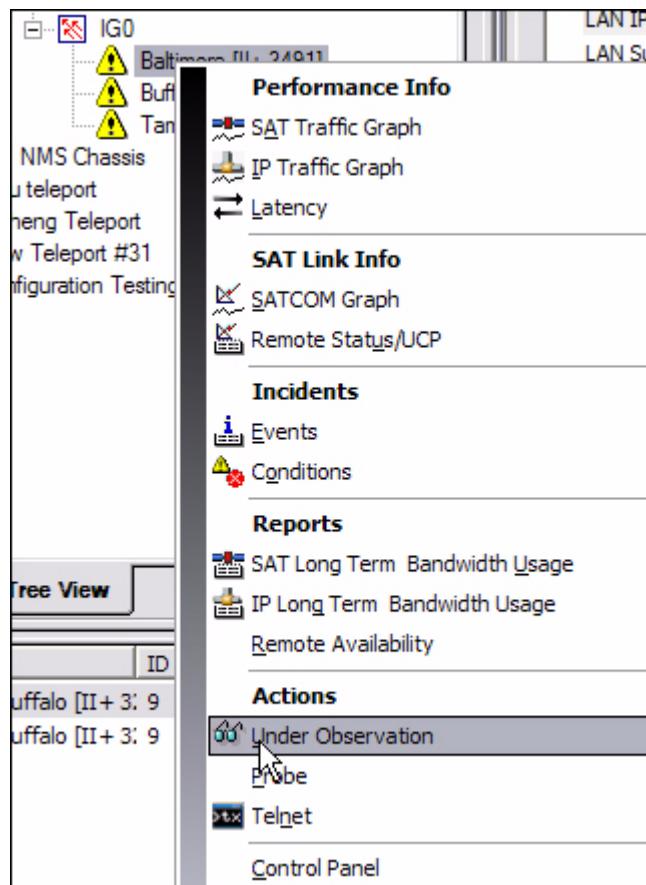
3.2 Putting an Element under Observation for Conditions

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):

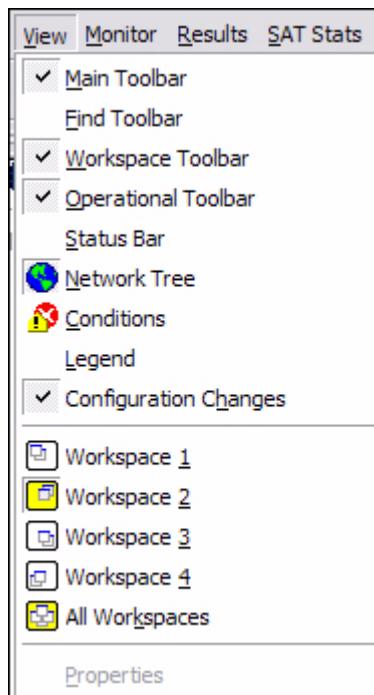
- Protocol Processor
- Blade
- Line Card
- Remote

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 Click **View → Conditions** or click **Conditions** in 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

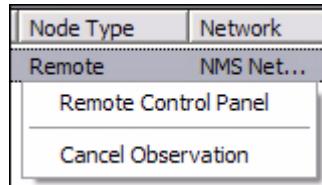
If you have previously put another element under observation, without canceling that observation view, the previous element's information will still be visible in the pane. To omit the unwanted information, right-click on the unwanted element and select **Cancel Observation**.

Name	ID	Type-SN	Node Type	Network	Time
66  Baltimore [II+ 3491] 213	II+-3491	II+-3491	Remote	NMS Net...	13:43:50
66  Baltimore [II+ 3491] 213	II+-3491	II+-3491	Remote	NMS Net...	13:36:15

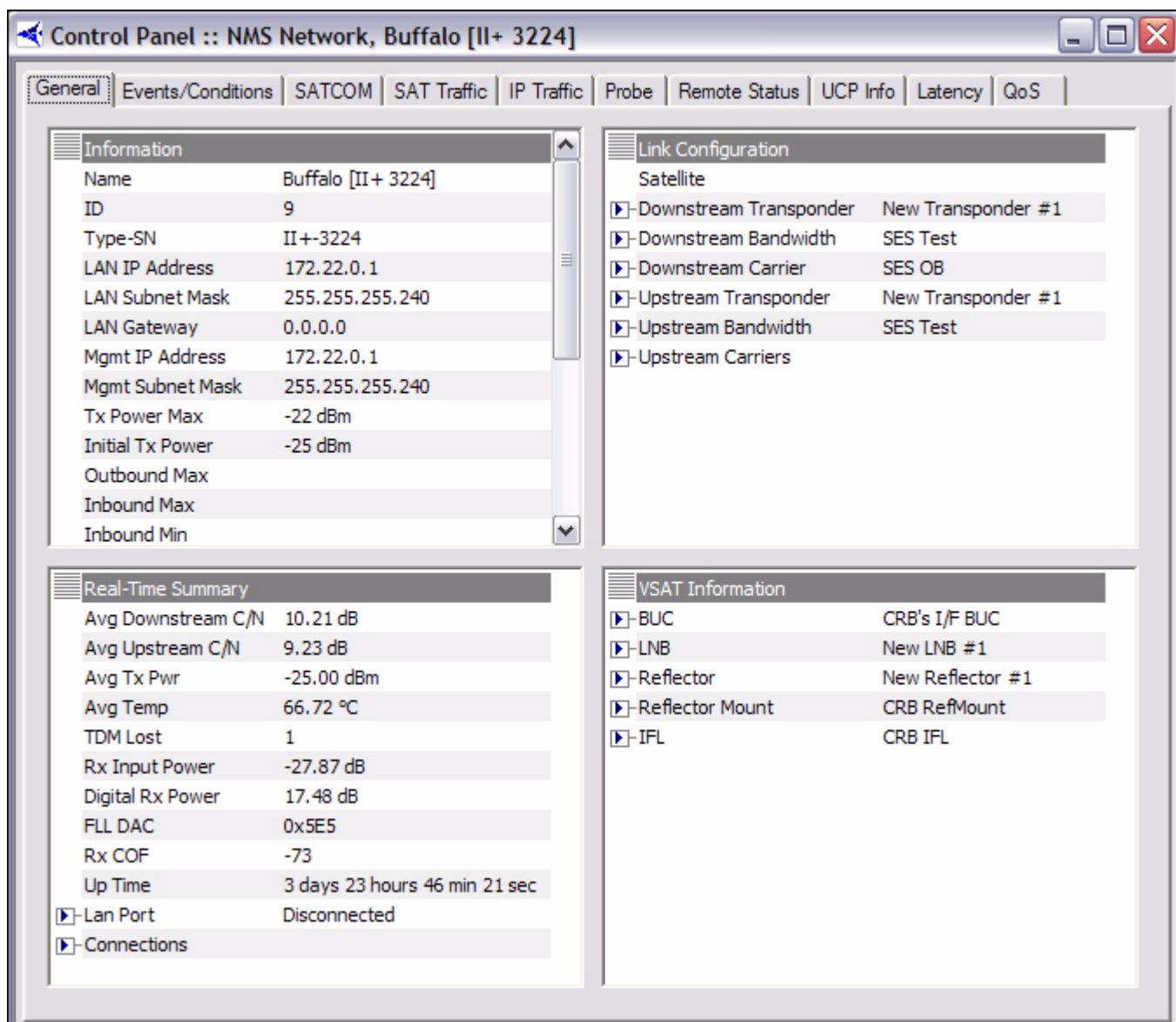
(|||)

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

- 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. Below 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 4.3.3 "Control Panel" on page 80.](#))
- Step 8 Follow the directions in [Section 3.2.1 "Viewing Conditions or Events" on page 34.](#)



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 30](#).

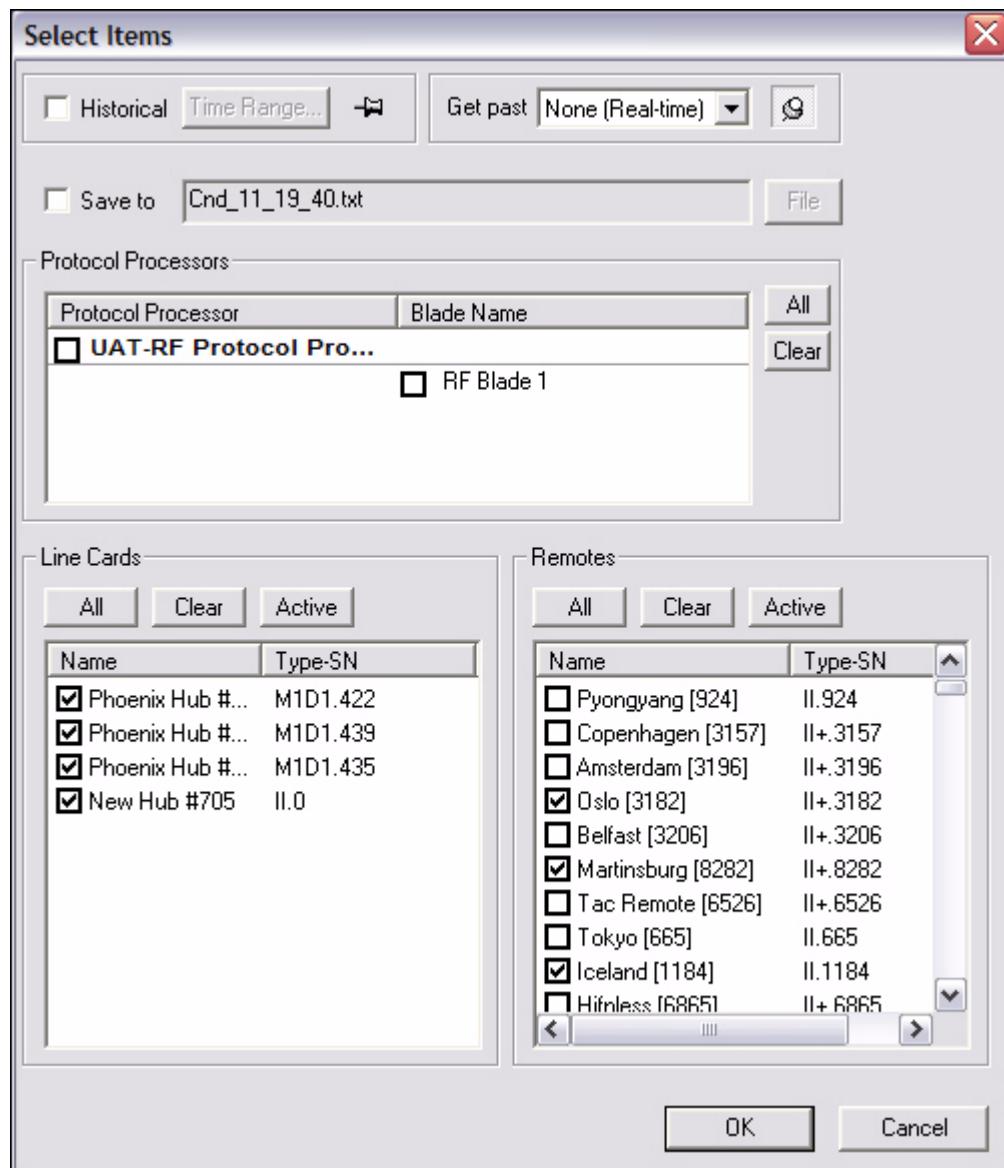
Viewing Events

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, p. 3-38](#)), 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 "telnet". Any event message text 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 an element in the **Tree** pane for which you want to view conditions or events.
- Step 2 Click on either **Conditions** or **Events**. The **Select Items** dialog box appears.



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.

- 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](#).

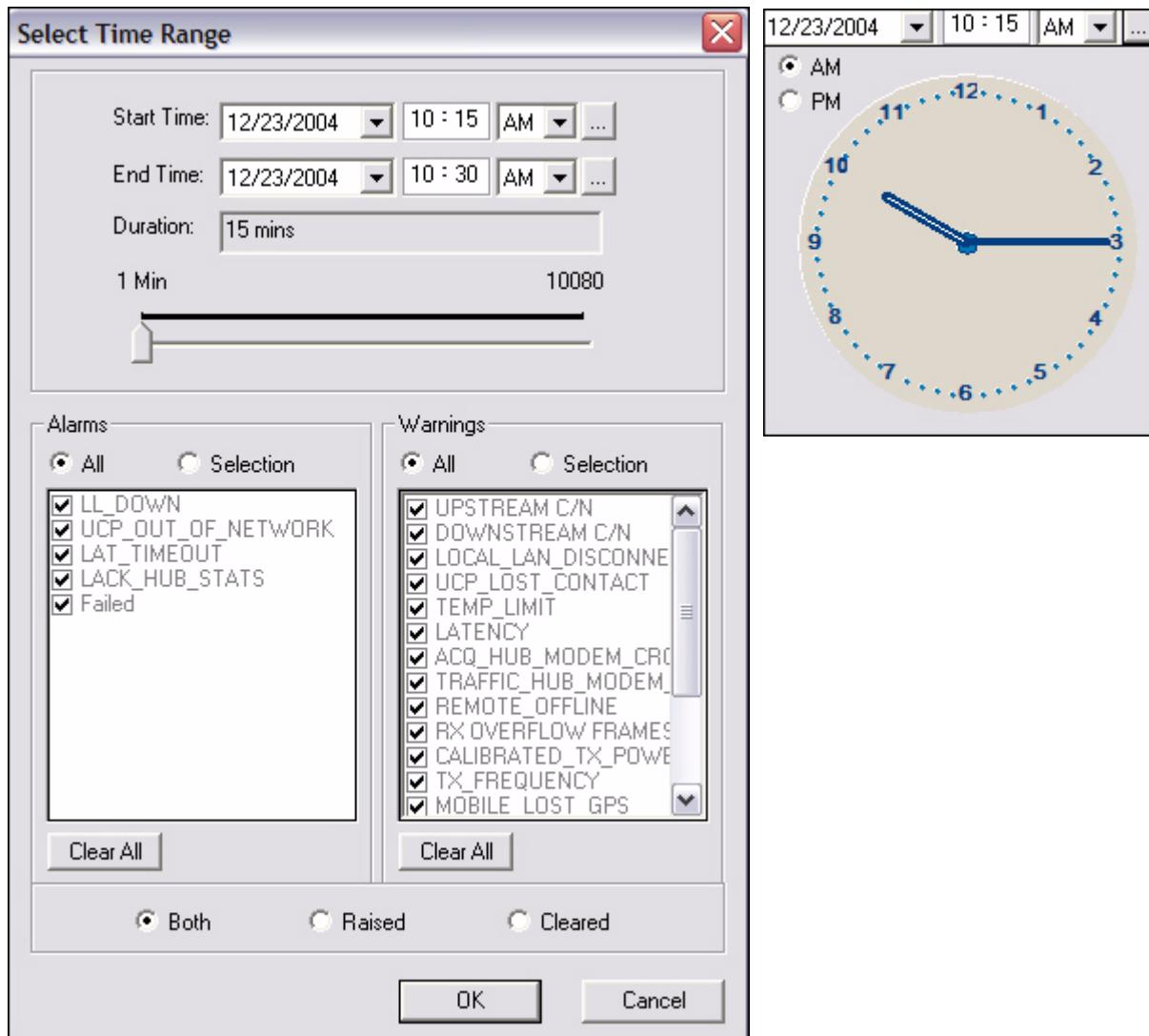


Figure 3-1: Conditions Time Range

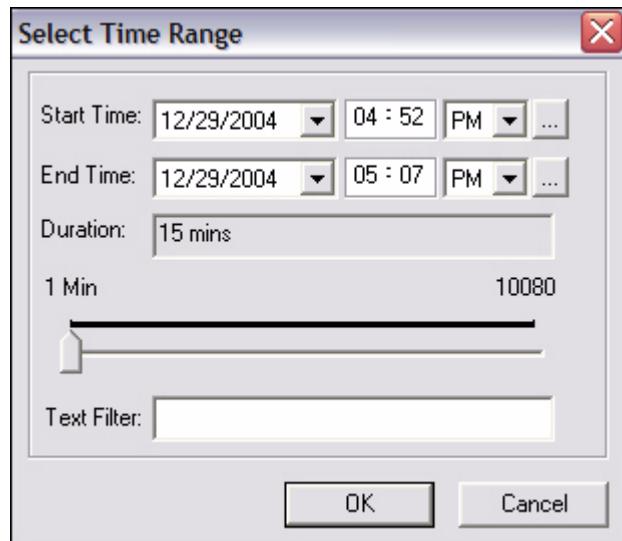
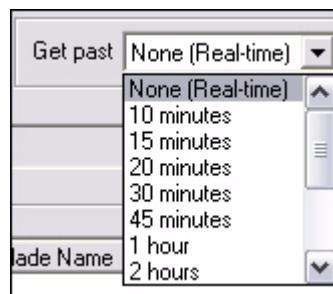


Figure 3-2: Events Time Range with Text Filter

- 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. You can right-click on a remote that has an arrow or click on the condition for that remote and select either **Remote Control Panel** (see [Section 4.3.3 “Control Panel” on page 80](#)) or **Clear List**, which will clear the condition from the Condition Log. Be careful not to clear the list unless you want the conditions to disappear. (The **Remote Control Panel** and **Clear List** options are not available from displays other than the Tab views.)

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.

Conditions :: Network ID: 0, Modems: M1D1.422 M1D1.439 M1D1.435 II.0 II+.3182 II+.82										
Conditions		Time Line								
<input type="checkbox"/> Historical	Time Range...		Get past	None (Real-time)			Restart			
Name	ID	T...	N...	Network	Time	Date	Type	Severity	Details	
Oslo [3182]	124	II...	R...	UAT-RF ...	11:53:19	02/01/05	LOCAL_LAN_DISC...	Warning	Local LAN	
Iceland [1184]	233	II...	R...	UAT-RF ...	11:53:19	02/01/05	LOCAL_LAN_DISC...	Warning	Local LAN	

Figure 3-3: Conditions Results in Multicolumn Format

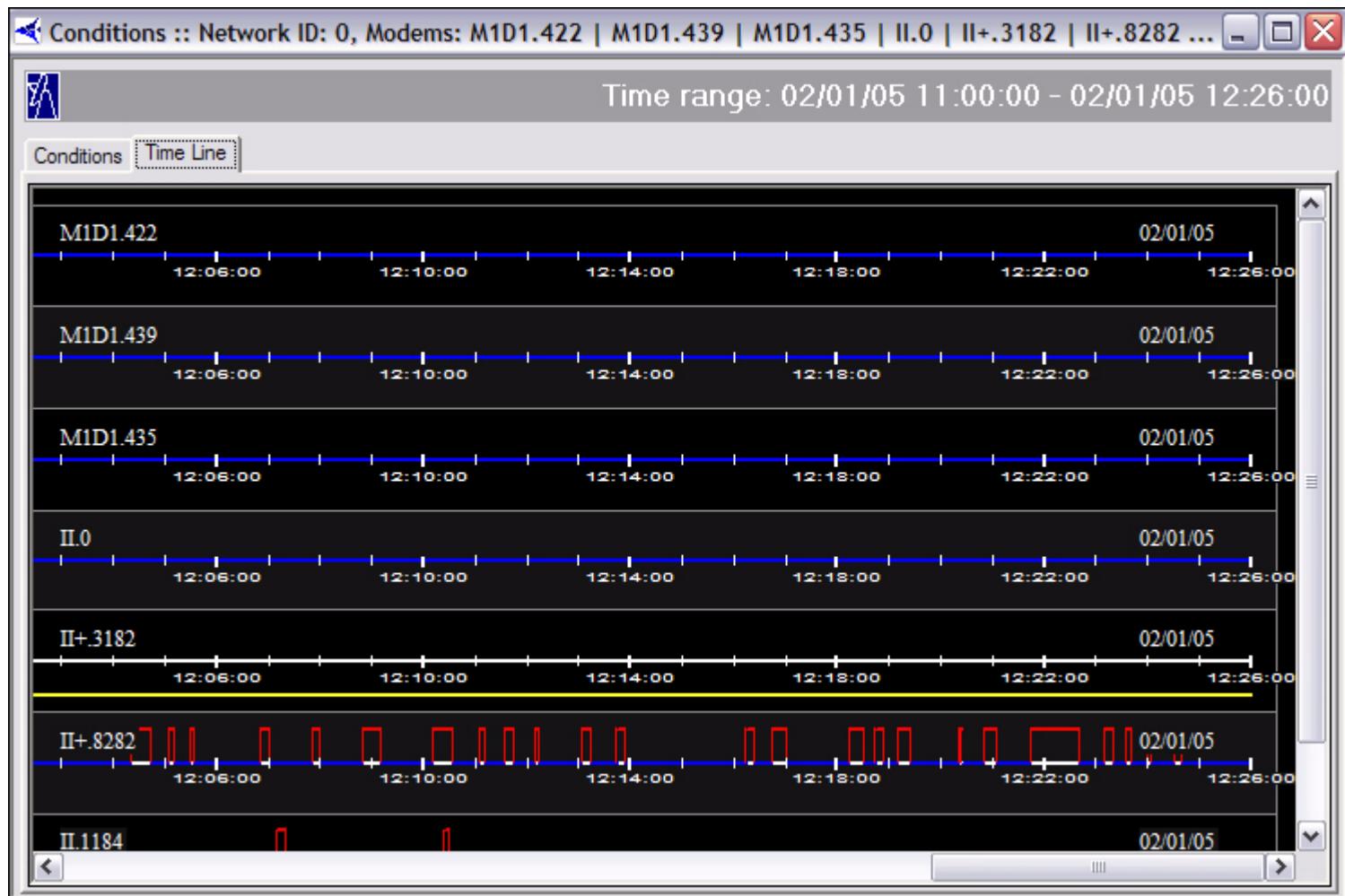
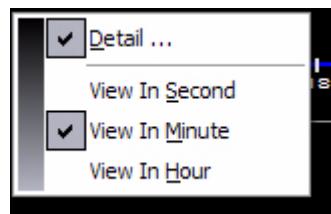


Figure 3-4: Conditions Time Line Results in Graphical Format

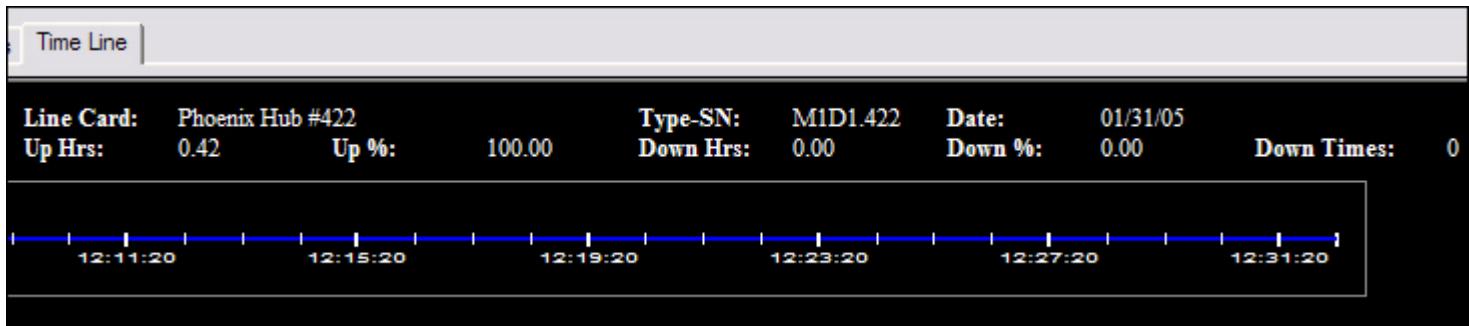
Step 8 On the **Time Line** display, you can right-click to elect to view the results in Seconds, Minutes, or Hours.



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 Line Card
- Type and Serial Number of 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 %)
- Number of times the card has gone 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.

Modem Events :: UAT-RF Network, Modems: II-924 | II+-3157 | II+-3196 | II+-3182 | II+-3206 | II-6...

Time	Date	Name	Ty...	Type	Event Level	Event Description
17:11:31	12/29/04	Phoenix Remote ...	53...	Remote	Info	ACQ_TX remote_id =6816236 cmd =SWEEP: afo=+13050, fr
17:11:35	12/29/04	Phoenix Remote ...	31...	Remote	Info	ACQ_TX remote_id =4981150 cmd =SWEEP: afo=+29700, fr
17:11:36	12/29/04	Phoenix Remote ...	53...	Remote	Info	ACQ_TX remote_id =6816236 cmd =SWEEP: afo= -1350, fr .
17:11:40	12/29/04	Phoenix Remote ...	31...	Remote	Info	ACQ_TX remote_id =4981150 cmd =SWEEP: afo=-18000, fr
17:11:41	12/29/04	Phoenix Remote ...	53...	Remote	Info	ACQ_TX remote_id =6816236 cmd =SWEEP: afo=-19800, fr
17:11:42	12/29/04	Pyongyang [924]	II...	Remote	Info	UCP!: SO(+69), FO(+10193), PO(+0.0)
17:11:43	12/29/04	Prague [3201]	II...	Remote	Info	UCP!: SO(+67), FO(+10262), PO(+0.0)
17:11:43	12/29/04	Iceland [1184]	II...	Remote	Info	UCP!: SO(+68), FO(+10168), PO(+0.0)
17:11:43	12/29/04	Oslo [3182]	II...	Remote	Info	UCP!: SO(+68), FO(+10286), PO(+0.0)
17:11:43	12/29/04	Belfast [3206]	II...	Remote	Info	UCP!: SO(+67), FO(+10259), PO(+0.0)
17:11:43	12/29/04	Venice [3126]	II...	Remote	Info	UCP!: SO(+67), FO(+10211), PO(+0.0)
17:11:43	12/29/04	Copenhagen [3157]	II...	Remote	Info	UCP!: SO(+67), FO(+10273), PO(+0.0)
17:11:45	12/29/04	Phoenix Remote ...	31...	Remote	Info	ACQ_TX remote_id =4981150 cmd =SWEEP: afo= +6300, fr
17:11:46	12/29/04	Phoenix Remote ...	53...	Remote	Info	ACQ_TX remote_id =6816236 cmd =SWEEP: afo= +8100, fr
17:11:50	12/29/04	Phoenix Remote ...	31...	Remote	Info	ACQ_TX remote_id =4981150 cmd =SWEEP: afo= +24750, fr
17:11:51	12/29/04	Phoenix Remote ...	53...	Remote	Info	ACQ_TX remote_id =6816236 cmd =SWEEP: afo= +26550, fr
17:11:55	12/29/04	Phoenix Remote ...	31...	Remote	Info	ACQ_TX remote_id =4981150 cmd =SWEEP: afo= -13050, fr
17:11:56	12/29/04	Phoenix Remote ...	53...	Remote	Info	ACQ_TX remote_id =6816236 cmd =SWEEP: afo= -14850, fr
17:12:01	12/29/04	Phoenix Remote ...	31...	Remote	Info	ACQ_TX remote_id =4981150 cmd =SWEEP: afo= +1350, fr
17:12:01	12/29/04	Phoenix Remote ...	53...	Remote	Info	ACQ_TX remote_id =6816236 cmd =SWEEP: afo= +3150, fr
17:12:02	12/29/04	Pyongyang [924]	II...	Remote	Info	UCP!: SO(+69), FO(+10166), PO(+0.0)
17:12:03	12/29/04	Prague [3201]	II...	Remote	Info	UCP!: SO(+67), FO(+10251), PO(+0.0)

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.



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	DOWNTREAM_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 DOWNTREAM_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:

- Telnet 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:

- networks
- inroute groups

3.4.1 Network Condition Snapshot

The **Network Condition Snapshot** shows all remotes in an inroute group or network 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 the directions below:

- Step 1 Right-click the network or inroute group for which you want to view a snapshot of the conditions.
- Step 2 Select **Network Condition Snapshot**. The **Network Condition Snapshot** pane appears. Below is an example of a **Network Condition Snapshot** at the network level.

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

Network Condition Snapshot :: UAT-RF Network							
II+-6611	II+-10011	II+-10028	II+-10045	II+-10062	II+-10079	II+-10096	II+-10111
II+-3097	II+-10012	II+-10029	II+-10046	II+-10063	II+-10080	II+-10097	II+-10111
II+-4560	II+-10013	II+-10030	II+-10047	II+-10064	II+-10081	II+-10098	II+-10111
II-924	II+-10014	II+-10031	II+-10048	II+-10065	II+-10082	II+-10099	II+-10111
II-3157	II+-10015	II+-10032	II+-10049	II+-10066	II+-10083	II+-10100	II+-10111
II+-3196	II+-10016	II+-10033	II+-10050	II+-10067	II+-10084	II+-10101	II+-10111
II-3182	II+-10017	II+-10034	II+-10051	II+-10068	II+-10085	II+-10102	II+-10111
II-3206	II+-10018	II+-10035	II+-10052	II+-10069	II+-10086	II+-10103	II+-10120
II-665	II+-10019	II+-10036	II+-10053	II+-10070	II+-10087	II+-10104	II+-10121
II-1184	II+-10020	II+-10037	II+-10054	II+-10071	II+-10088	II+-10105	II+-10121
II+-4699	II+-10021	II+-10038	II+-10055	II+-10072	II+-10089	II+-10106	II+-10121
II-3201	II+-10022	II+-10039	II+-10056	II+-10073	II+-10090	II+-10107	II+-10121
II+-10006	II+-10023	II+-10040	II+-10057	II+-10074	II+-10091	II+-10108	II+-10121
II+-10007	II+-10024	II+-10041	II+-10058	II+-10075	II+-10092	II+-10109	II+-10121
II+-10008	II+-10025	II+-10042	II+-10059	II+-10076	II+-10093	II+-10110	II+-10121
II+-10009	II+-10026	II+-10043	II+-10060	II+-10077	II+-10094	II+-10111	II+-10121
II+-10010	II+-10027	II+-10044	II+-10061	II+-10078	II+-10095	II+-10112	II+-10121

Figure 3-6: List View of Network Condition Snapshot

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

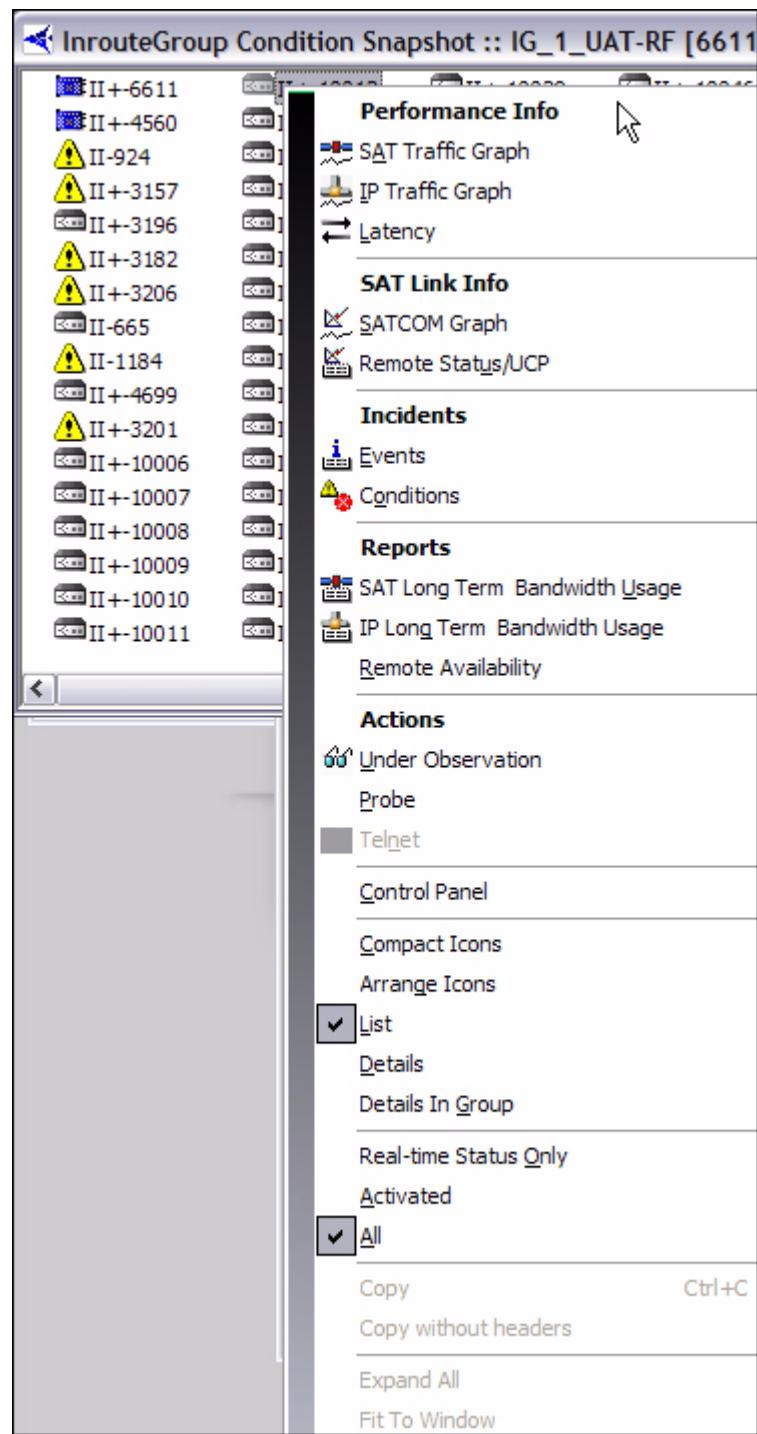


Figure 3-7: Remote Submenu in Condition Snapshot

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 You can click on any of these options to create a specific view. [Figure 3-6](#) above is an example of right-clicking **List** in the submenu (see [Figure 3-7](#)). The example below is a result of right-clicking **Details**.

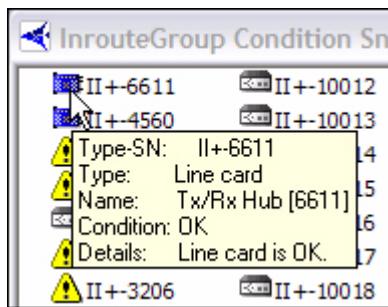
InrouteGroup Condition Snapshot :: IG_1_UAT-RF [6611][4560]				
Type-SN	Type	Name	Condition	Details
II+-3157	Remote	Copenhagen [3157]	Alarm	LOCAL_LAN_DISCONNECT
II+-3196	Remote	Amsterdam [3196]	Deactivated	Remote is not activated.
II+-3182	Remote	Oslo [3182]	Warning	LOCAL_LAN_DISCONNECT
II+-3206	Remote	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 4.3.3 "Control Panel" on page 80](#) 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:

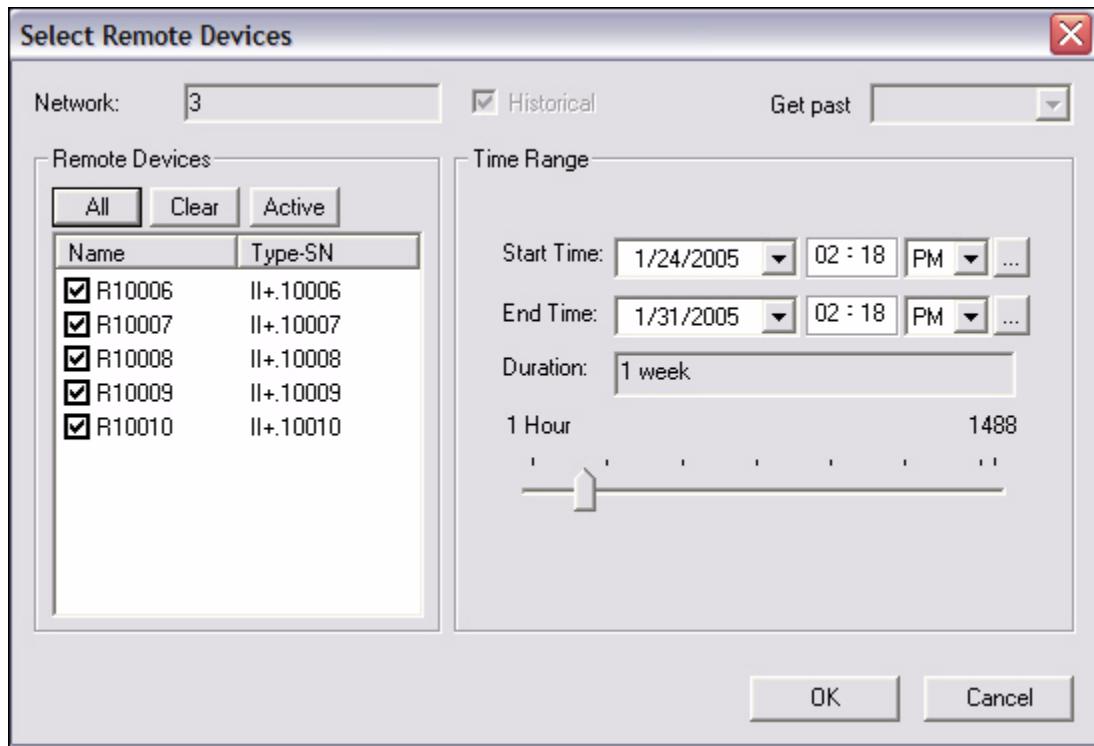
- SAT/IP Traffic Stats
- Latency
- Events
- Conditions
- Network Data Snapshot
- SAT/IP Long Term Bandwidth Reports
- Remote Availability Report

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.

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.

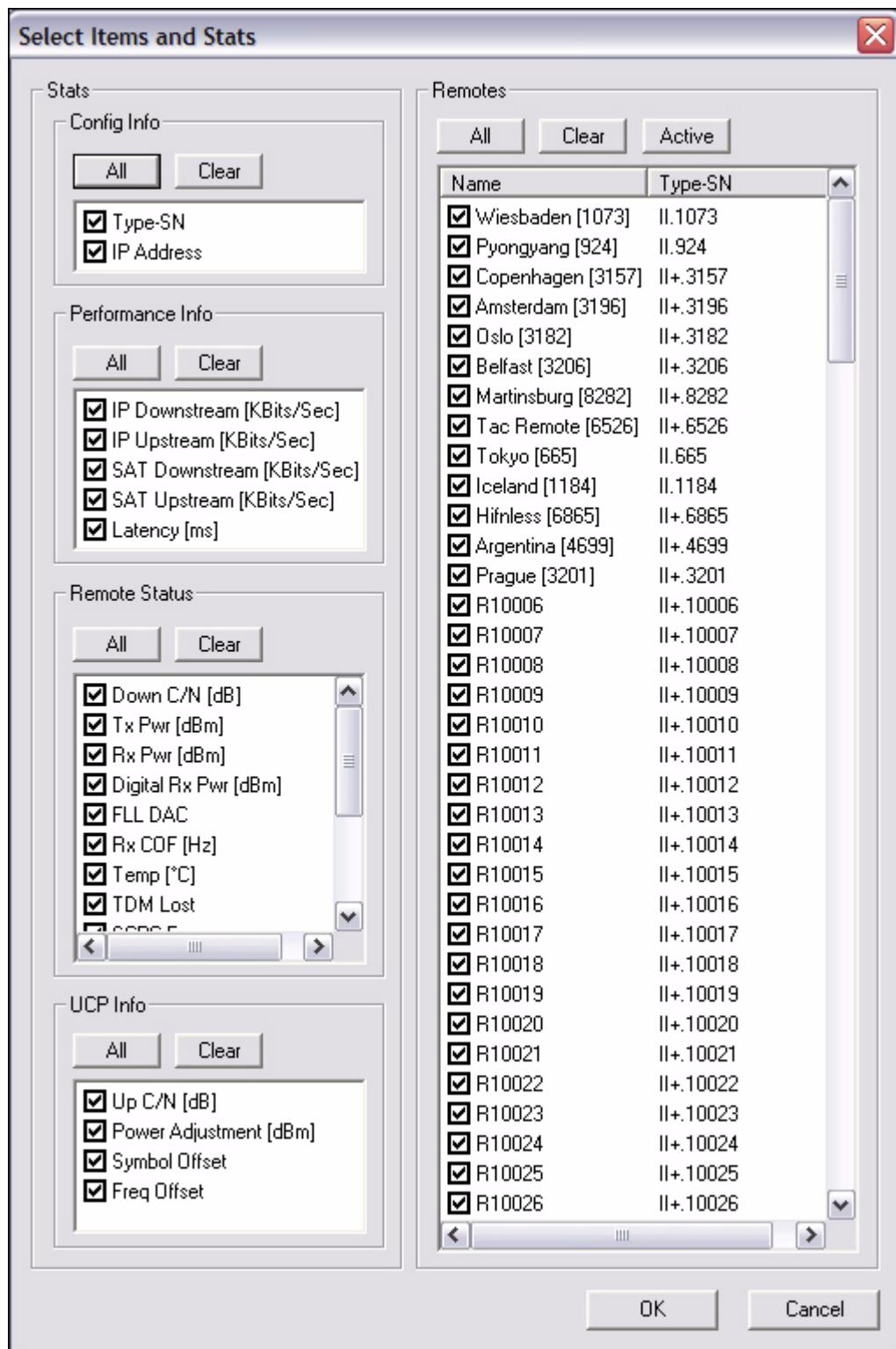


3.4.2 Network Data Snapshot

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)

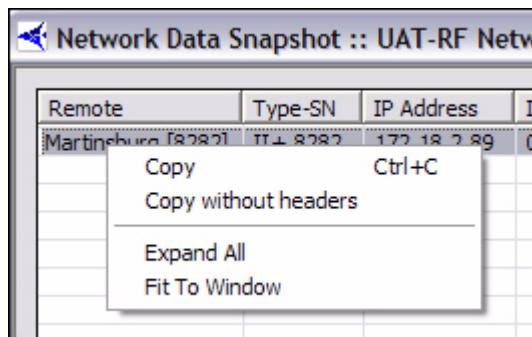
Step 4 By default all remotes are displayed in the **Remotes** section. To select only Activated remotes, select **Active**. To clear all remotes, select **Clear**. In this example, **Clear** was selected, and then only the Martinsburg remote was selected for the snapshot.

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.

Network Data Snapshot :: UAT-RF Network, Martinsburg [8282]							
Remote	Type-SN	IP Address	IP Down...	IP Upst...	S...	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, discussed on page 55](#)
- [Retrieving Information on Remotes using Probe, discussed on page 57](#)
- [CPU Usage \(Blades Only\), discussed on page 62](#)
- [Time Plan, discussed on page 64](#)
- [Bandwidth Usage, discussed on page 94](#)
- [Inroute Distribution, discussed on page 67](#)
- [Latency, discussed on page 69](#)
- [Line Card Statistics, discussed on page 73](#)
- [SATCOM Graph, discussed on page 76](#)
- [Control Panel, discussed on page 80](#)
- [Telnet, discussed on page 83](#)

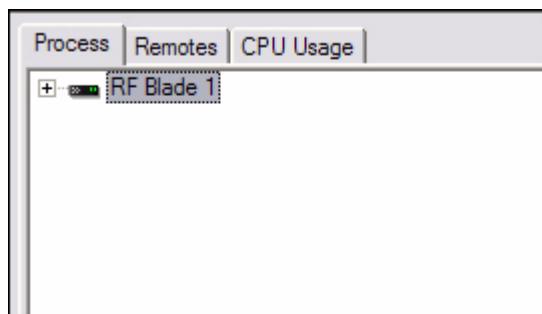
4.1 Monitoring Blades in iMonitor

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).

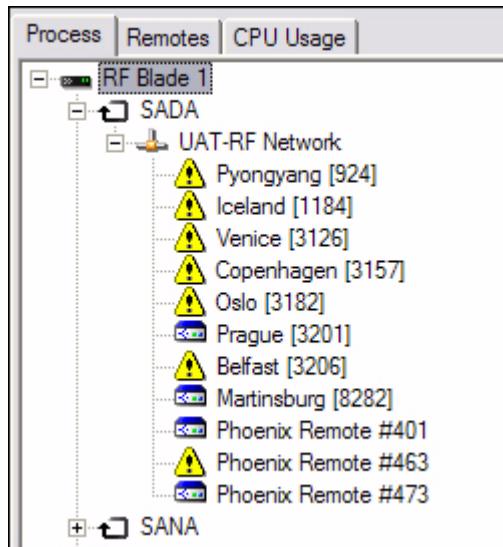
To view blade information, follow the directions below:

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.



Blade	Network	Remote	Type-SN
RF Bla...	UAT-RF Net...		
		Pyongyang [924]	!!.924
		Iceland [1184]	!!.1184
		Venice [3126]	!!+.3126
		Copenhagen [3157]	!!+.3157
		Oslo [3182]	!!+.3182
		Prague [3201]	!!+.3201
		Belfast [3206]	!!+.3206
		Martinsburg [8282]	!!+.8282
		Phoenix Remote ...	3100.401
		Phoenix Remote ...	5350.463
		Phoenix Remote ...	5350.473

Blade Info :: NMS Blade 1			
Process	Remotes	CPU Usage	
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 more information about CPU usage on blades. See [Section 4.2.1 "CPU Usage \(Blades Only\)" on page 62](#) for instructions on how to obtain and use this information.

4.2 Retrieving Information on Remotes using 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 the remote's transmit power value
- view, save, clear and reset the remote's statistics
- view, save and clear its parameters, LL Bounce and Acq Bounce on all protocol layers
- monitor its temperature
- telnet into the remote
- connect to its protocol processor

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:

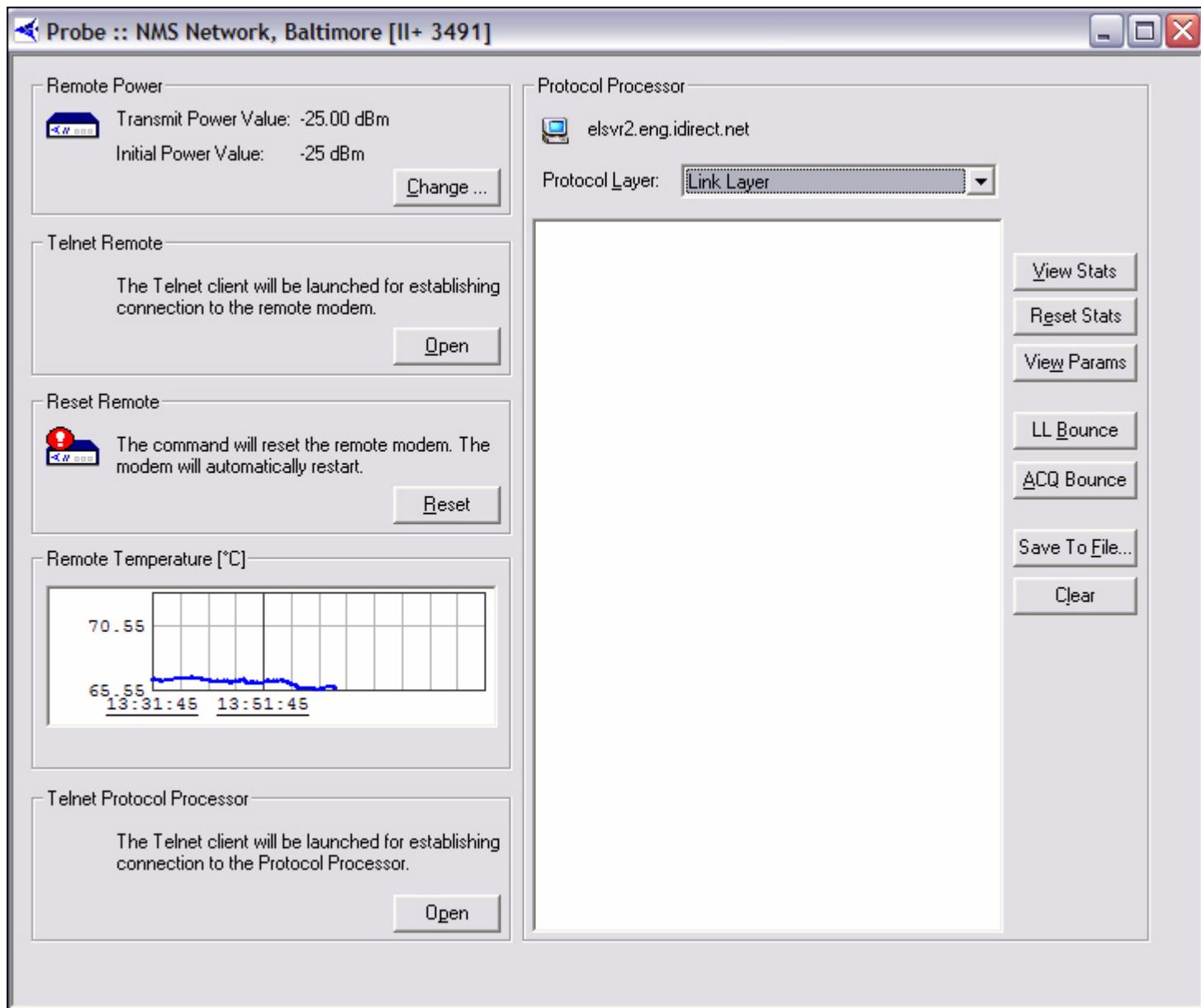
- **Remote Power** – allows you to dynamically change the remote's transmit power using a MAC-level message from the Protocol Processor. The remote does not have to be in the network to receive this message, but it must be locked onto the downstream carrier.
- **Telnet Remote** – a convenience function that launches a telnet window to this remote. The remote must be in the network for this feature 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.
- **Remote Temperature** – graphs the remote temperature for the time period you have the pane open.
- **Telnet Protocol Processor** – convenience function that launches a telnet window to the Protocol Processor's internal console.
- **Protocol Processor** – using the drop-down box, select a protocol layer and press View Stats, Reset Stats, or View Params for detailed information about that protocol layer.

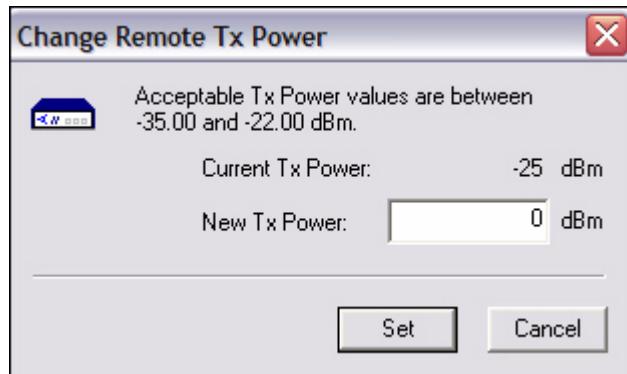
The Protocol Processor section of the Probe pane also allows you to “bounce” the link layer, which causes it to go through its initialization handshake sequence and perform the “ACQ Bounce” function on this remote. ACQ Bounce is discussed in [Performing ACQ Bounce, discussed on page 69](#). Inroute Distribution is discussed in [Section 4.2.3 “Inroute Distribution” on page 67](#).

Step 1 Right-click a remote.

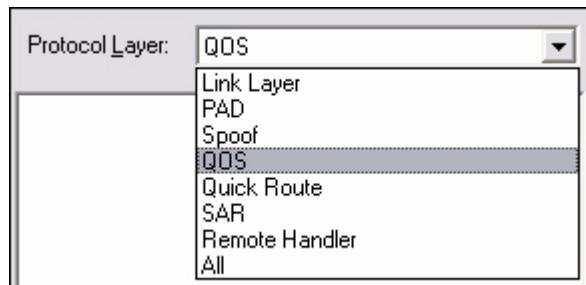
Step 2 Click **Probe**. The **Probe** dialog box appears.



- Step 3 If desired, click **Open** in the **Telnet Remote** box to type commands that will allow you to directly view or manipulate the remote.
- Step 4 If desired, click **Open** in the **Telnet Protocol Processor** box to type commands that will allow you to directly view or manipulate the protocol processor.
- Step 5 If desired, click **Reset** to reset the modem.
- Step 6 If necessary, click **Change...** to alter the **Transmit Power Value**. The **Change Remote Tx Power** dialog box appears.



- Step 7 Type the desired value and click **Set**. Note that you cannot set the power outside of the Min/Max range defined for this remote in iBuilder.
- Step 8 Select a layer in the **Protocol Layer** drop-down list. All of the buttons to the right will display information for the layer you select.



- Step 9 Select the button to the right that will provide the desired data. You can save this data to a file, clear the data, or reset the statistics.

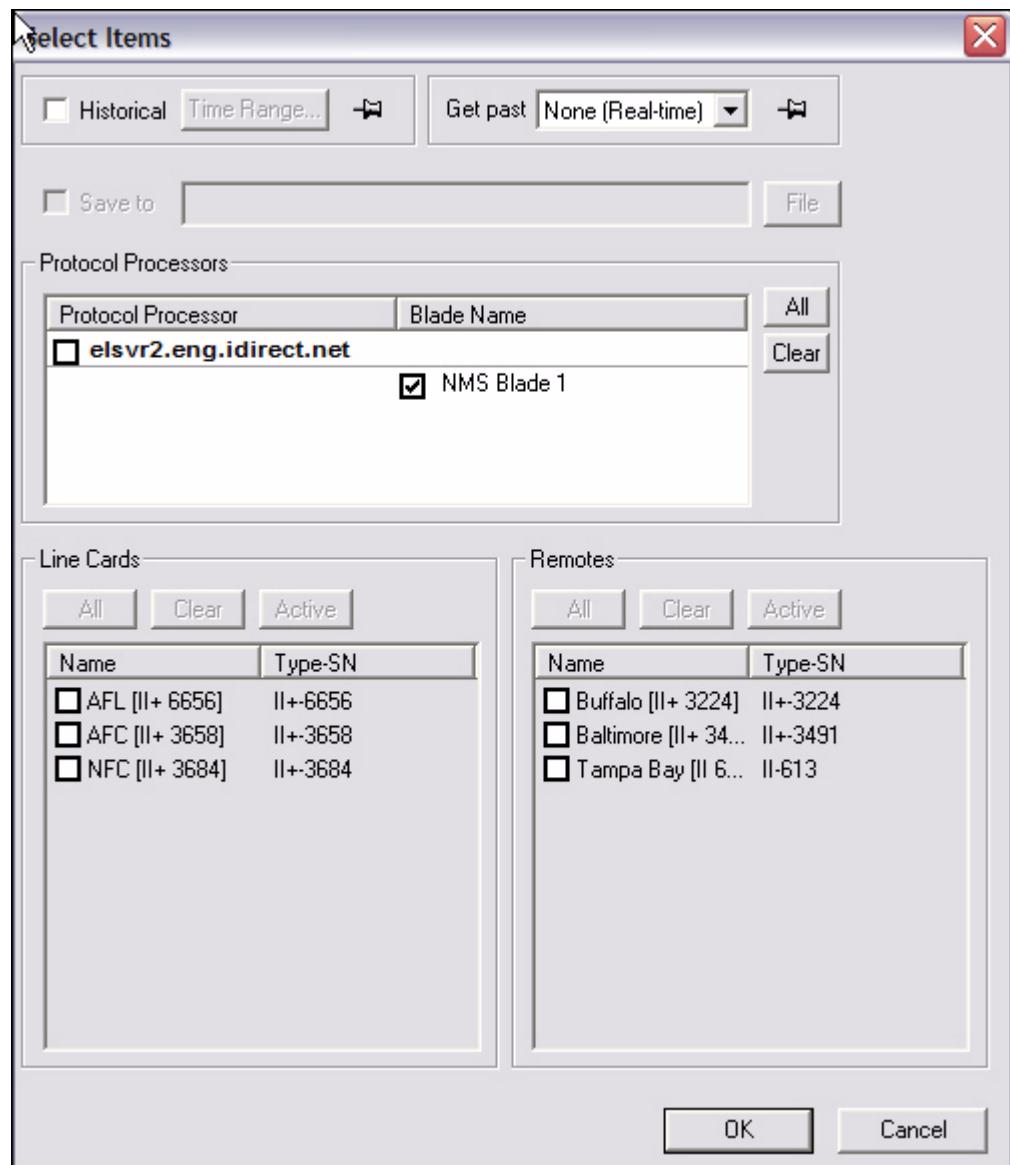
Protocol Layer: QOS	
Get QoS Stats	14:13:09
Return Code	OK
filtered_packets	0
service	DEFAULT
packet_count	204932
byte_count	5745312
dropped_packets	0
rejected_packets	0
service	NMS_TCP
packet_count	11450
byte_count	659192
dropped_packets	0
rejected_packets	0
service	NMS_UDP
packet_count	0
byte_count	0
dropped_packets	0
rejected_packets	0
service	UDP
packet_count	0
byte_count	0
dropped_packets	0
rejected_packets	0
service	TCP
packet_count	10
byte_count	362
dropped_packets	0
rejected_packets	0

[View Stats](#)
[Reset Stats](#)
[View Params](#)
[LL_Bounce](#)
[ACQ_Bounce](#)
[Save To File...](#)
[Clear](#)

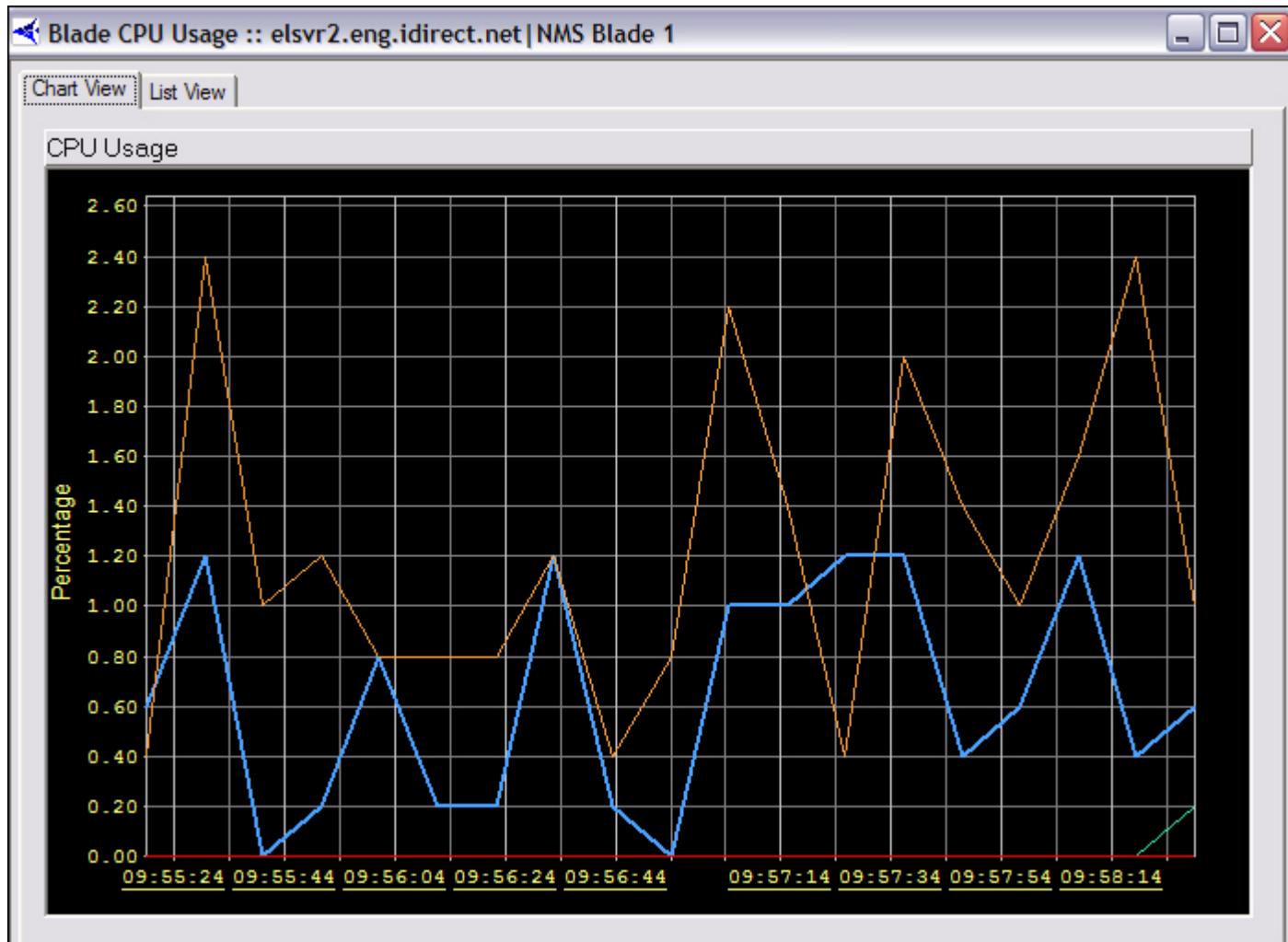
4.2.1 CPU Usage (Blades Only)

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.



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.

Blade CPU Usage :: elsvr2.eng.idirect.net|NMS Blade 1

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 55.](#)

4.2.2 Time Plan

The Time Plan graph shows you the number of TDMA timeslots 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 time plan slot allocations.

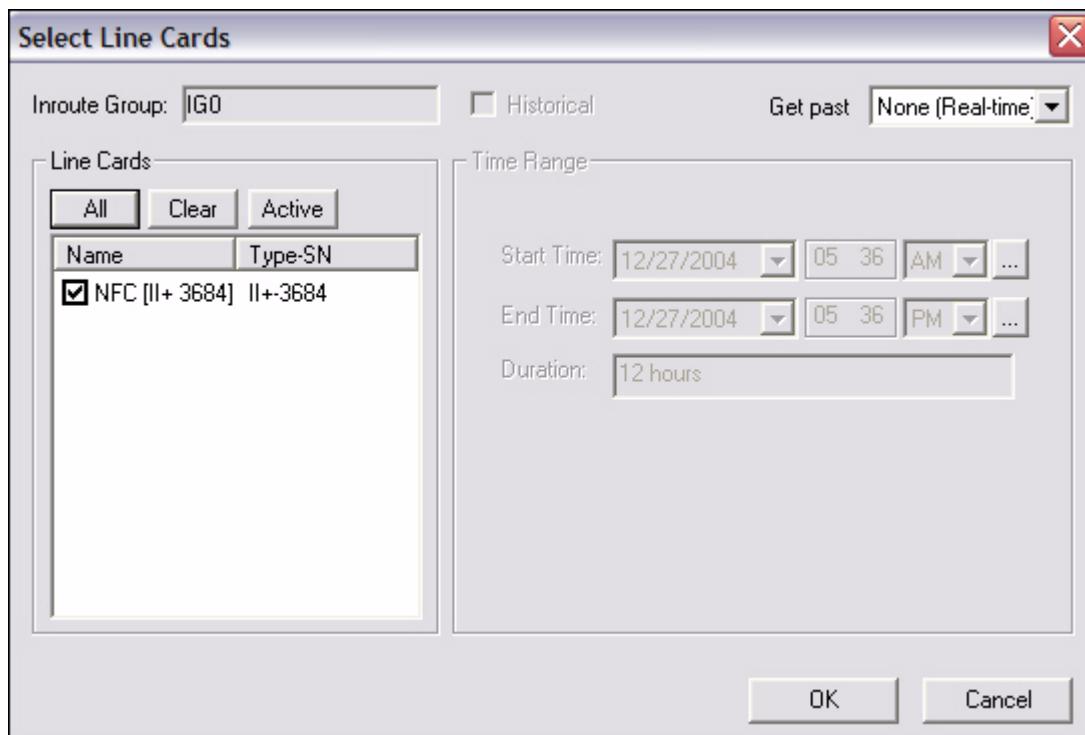
The Time Plan display can be selected from:

- receive line cards
- inroute groups

To view time plan information, follow the directions below:

Step 1 Right-click a receive line card or an inroute group.

Step 2 Click **Time Plan**. The **Select Line Cards** dialog box appears.



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**.

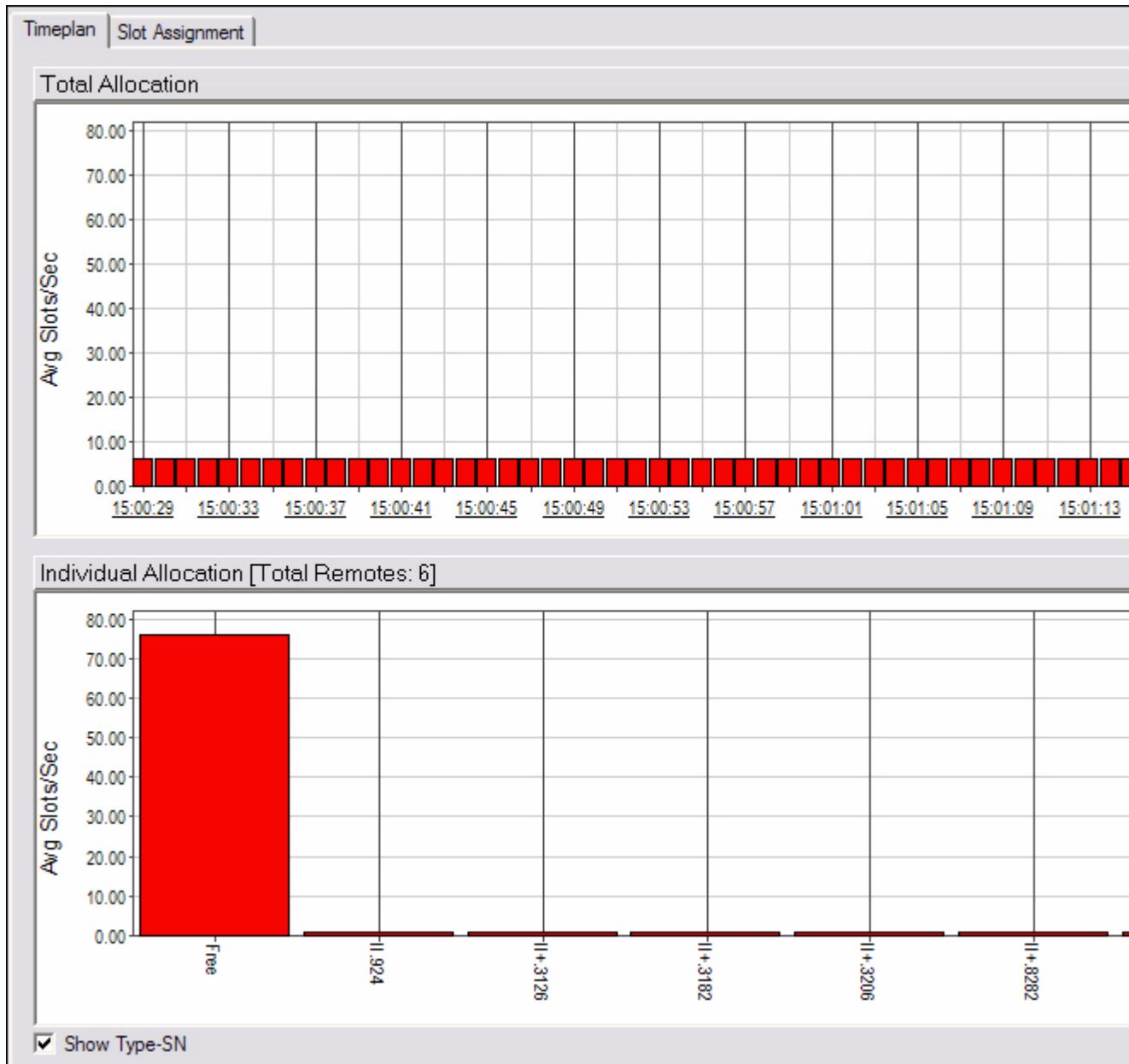
Step 5 The **Timeplan** graph appears.

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 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 time plan message as it is sent to the remotes.

Pausing the Time Plan 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 Time Plan graph. On iMonitor's task 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).

4.2.3 Inroute Distribution

The Inroute Distribution display also shows time plan 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 time plan 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:

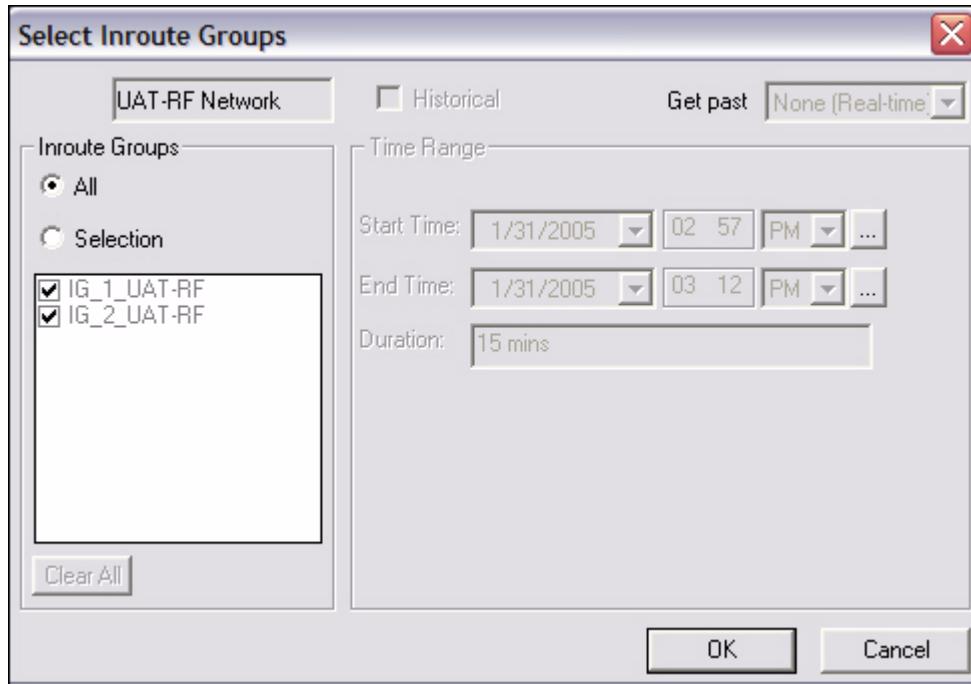
- Remote name and serial number
 - Total slots allocated to this remote across ALL inroutes

- 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 time plans
- 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 time plan

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.
- 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.

Inroute Distribution :: IG_1_UAT-RF				
Remote Name	Type-SN	Total, Slots/frame	Phoenix Hub #422 ...	Phoenix Hub #435...
Phoenix Remote #401	3100.401	1.00	1.00	
Phoenix Remote #463	5350.463	1.00		1.00
Phoenix Remote #473	5350.473	1.00	1.00	
Pyongyang [924]	II.924	1.00		1.00
Iceland [1184]	II.1184	1.00	1.00	
Venice [3126]	II+.3126	1.00		1.00
Copenhagen [3157]	II+.3157	1.00	1.00	
Oslo [3182]	II+.3182	1.00		1.00
Prague [3201]	II+.3201	1.00	1.00	
Belfast [3206]	II+.3206	1.00		1.00
Martinsburg [8282]	II+.8282	1.00		1.00
Total Allocated (%)		11.00 (6.71%)	5.00 (6.10%)	6.00 (7.32%)
Maximum		164	82	82

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.

4.2.4 Latency

The NMS measures the round-trip time from the hub to each remote and back every five seconds. These values are available from iMonitor in either real-time or from the historical archive. Latency measurements are saved for one week by default; see the section entitled Back-End Functionality for more information on archive consolidation.

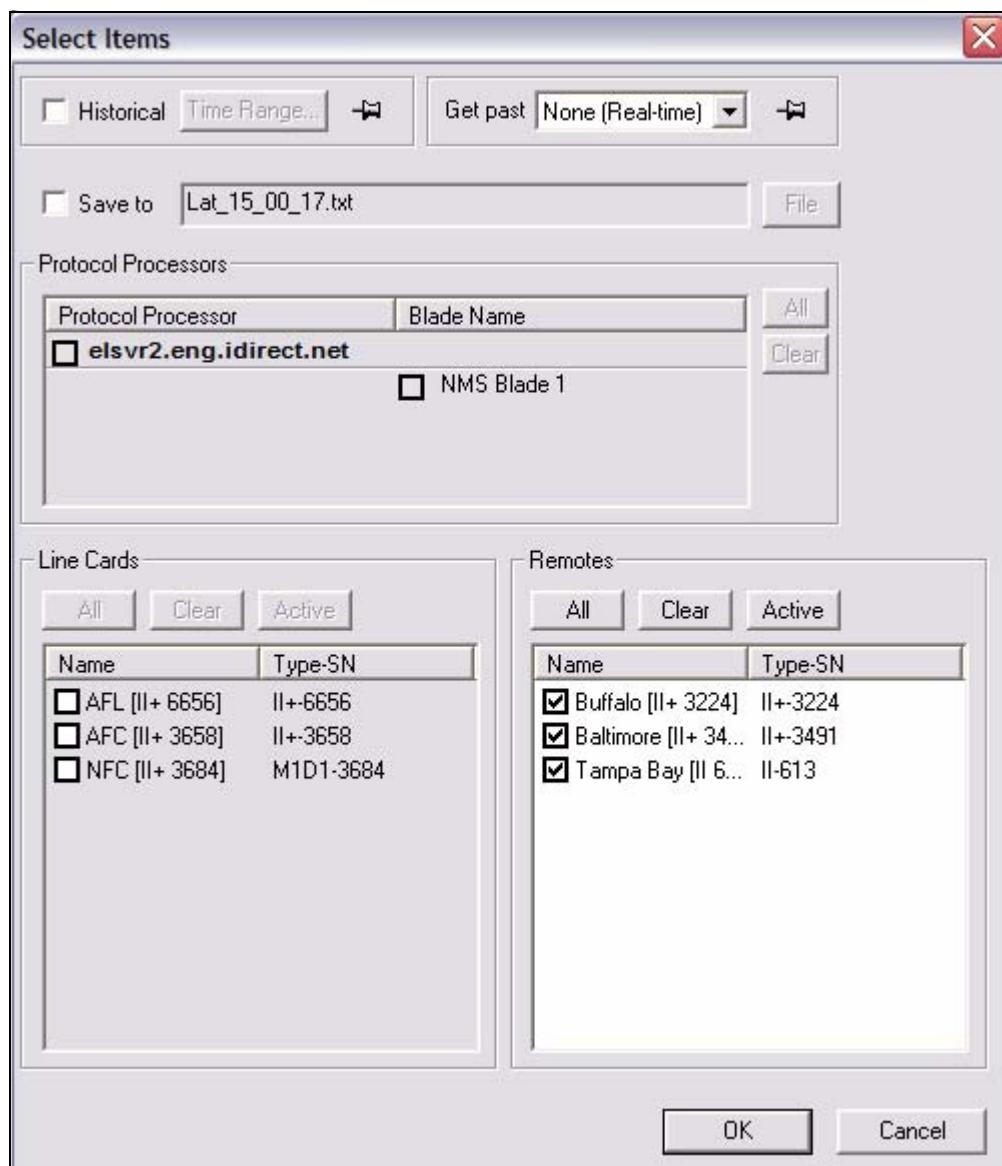
The Latency display can be selected from:

- networks
- inroute groups
- remotes

To view latency, follow the directions below:

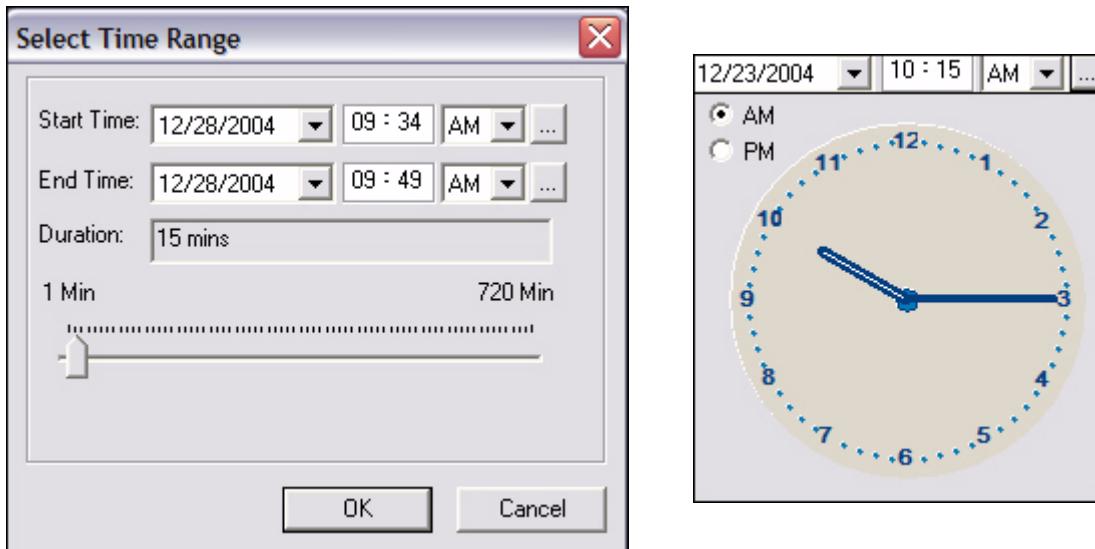
Step 1 Right-click a network, inroute group, or remote.

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

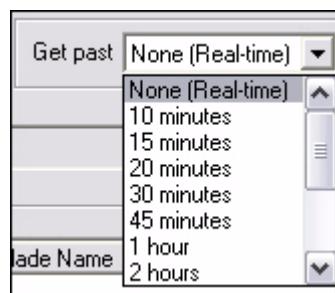


Step 3 Select the remotes for which you want to view information. Notice that all but the Remotes section are unavailable for selection.

- Step 4 Click either **Historical** or **Get Past**, or press **OK** to begin viewing latency in real-time.
- a If you click **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 Latency pane appears, as shown below.

Latency :: UAT-RF Network, Martinsburg [8282]								
<input type="checkbox"/> Historical	Time Range...	-	Get past	None (Real-time)	-	-	Restart	
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.

4.3 SAT Link Info

SAT (satellite) link information can be selected from:

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

4.3.1 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

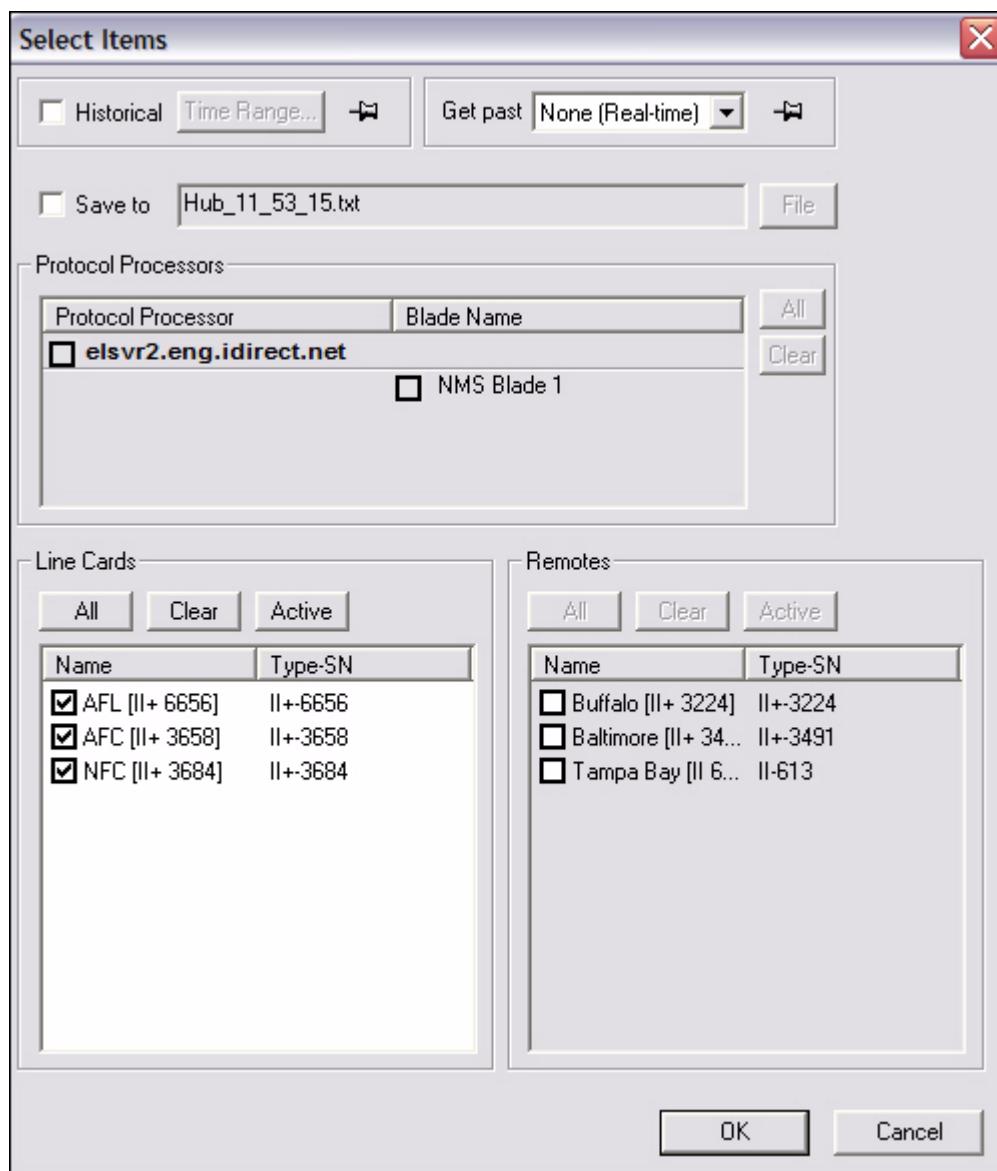
Because the information in the display is specific to an individual line card, when you select multiple line cards from the network level, iMonitor launches a separate pane for each line card.

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 errors

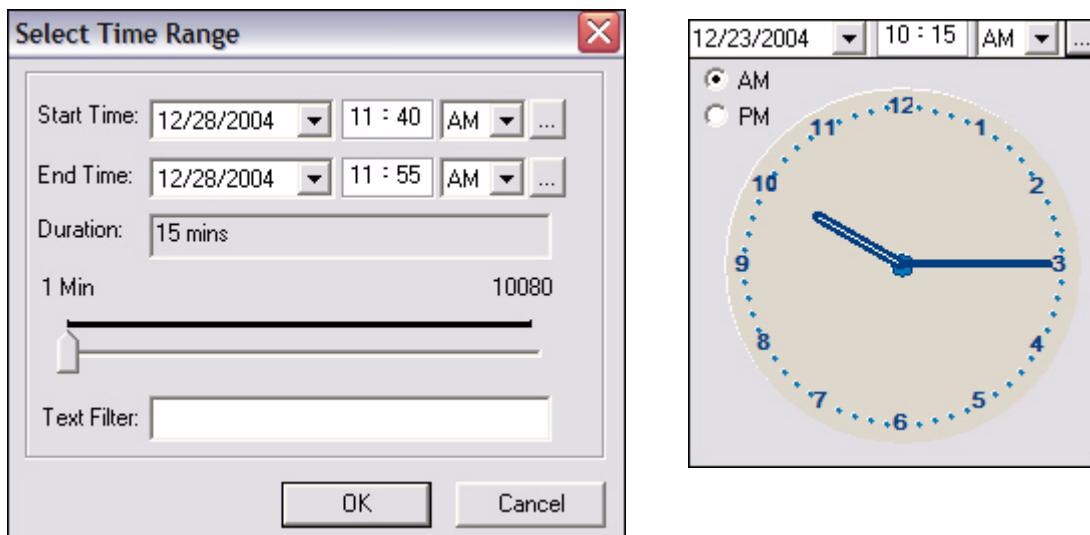
To view line card statistics on networks and line cards, follow the directions below:

- 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.

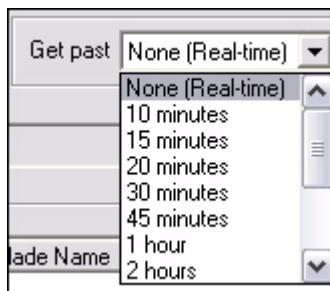


Step 3 Click either **Historical** or **Get Past**, or click **OK** for real-time.

- a If you click **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.

Hub Stats :: UAT-RF Network, Rx3 Hub [3097]

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

4.3.2 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.

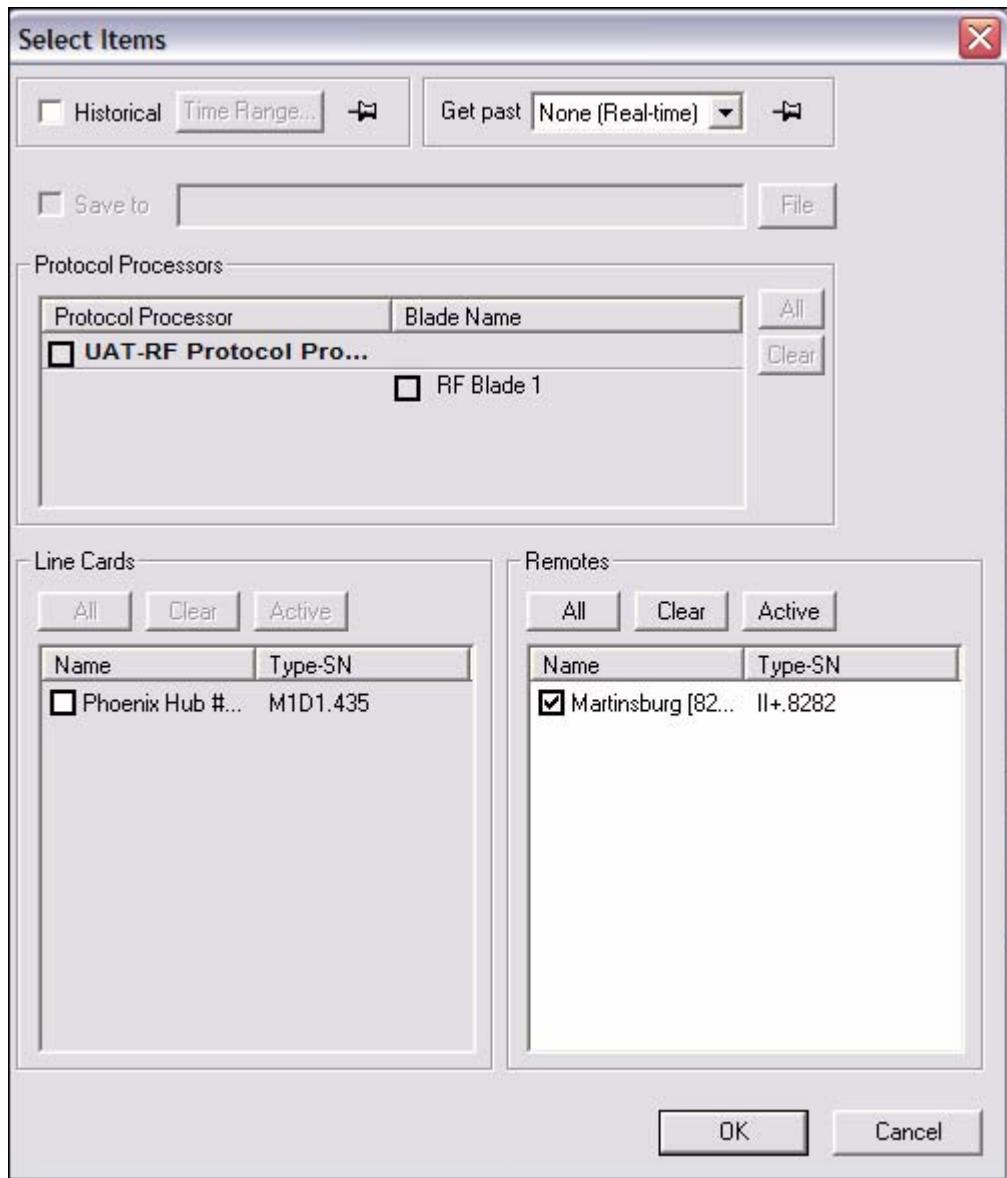
Display

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

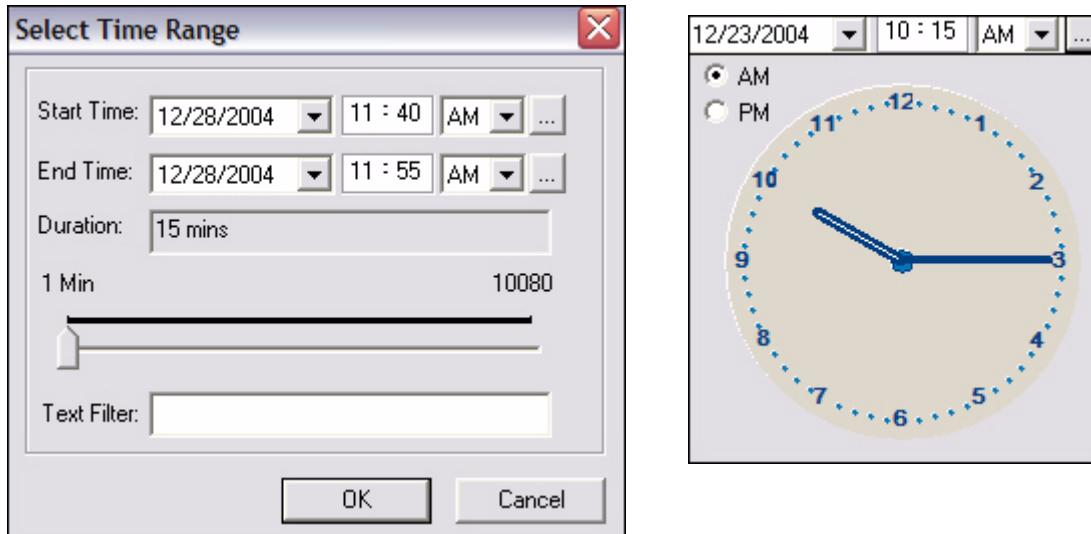
To view the **SATCOM Graph**, **Remote Status**, or **UCP Info** on remotes, follow the directions below:

Step 1 Right-click the remote for which you want to view information. Select **SATCOM Graph**, **Remote Status**, or **UCP Info**. The **Select Items** dialog box appears.

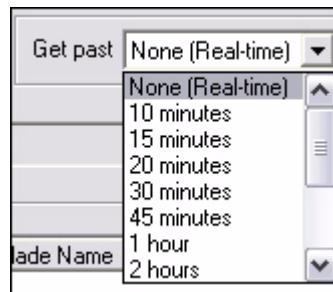


Step 2 Click either **Historical** or **Get Past**, or **OK** for real-time.

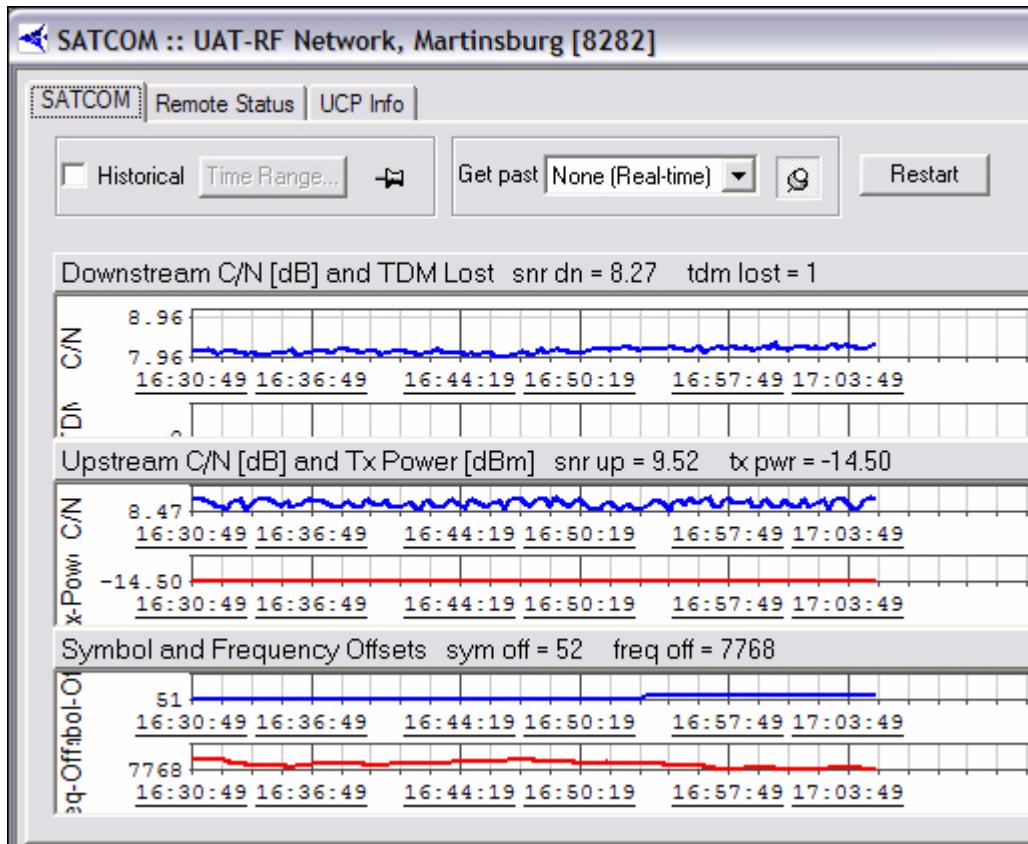
- a If you click **Historical**, click **Time Range....** The **Select Time Range** dialog box appears (see below). If desired, click the ellipses next to the Start and End times to set the time via the graphical clock display. If you selected **Get Past**, see [Step b](#).



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



The **SATCOM Graph** pane appears with three tabs. The Remote Status and UCP Info tabs contain the raw data used to draw the graph.



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

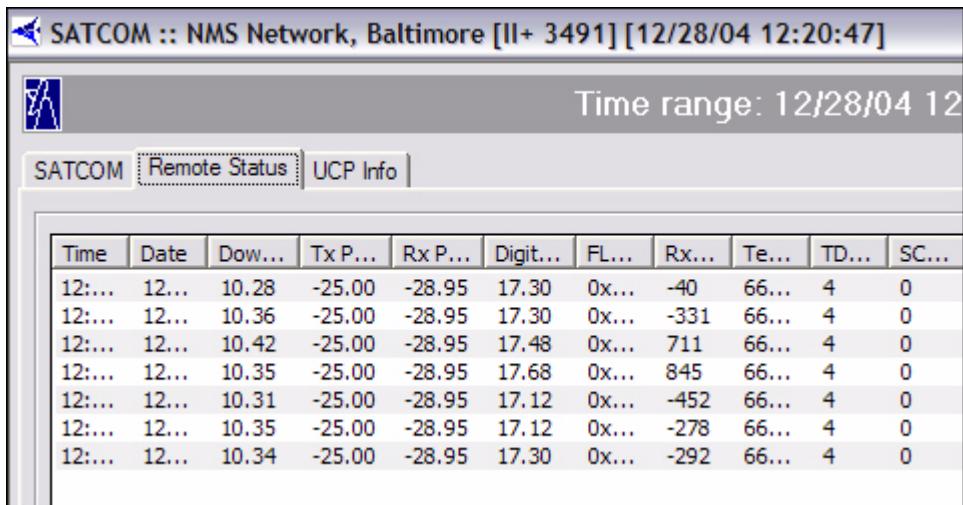
- **Graph 1** – The downstream signal-to-noise ratio as perceived at the remote, superimposed on top of the number of times the remote has lost lock on the downstream carrier (TDM lost). The TDM lost value is cumulative since the remote was last powered-up, but this graph shows only deltas from message 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.

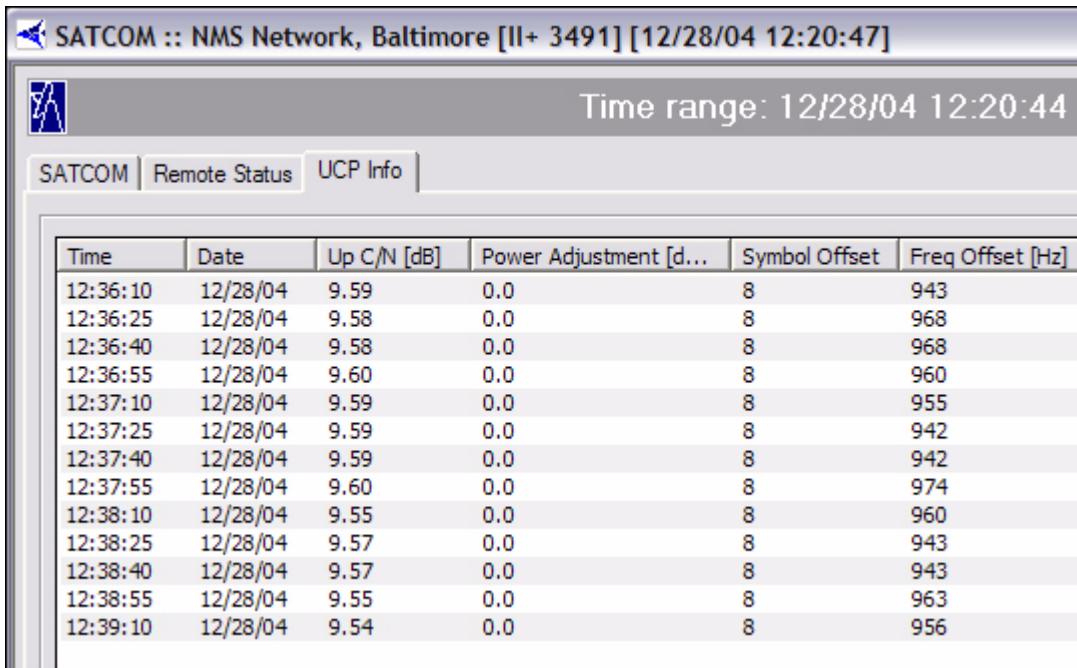
Remote Status and UCP Info Tabs

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



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 4-1: Remote Status Raw Data



Time	Date	Up C/N [dB]	Power Adjustment [dB]	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 4-2: UCP Info Raw Data

4.3.3 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, IP Stats, Probe, QoS settings, latency, and events/conditions simply by clicking from tab to tab in this single pane.

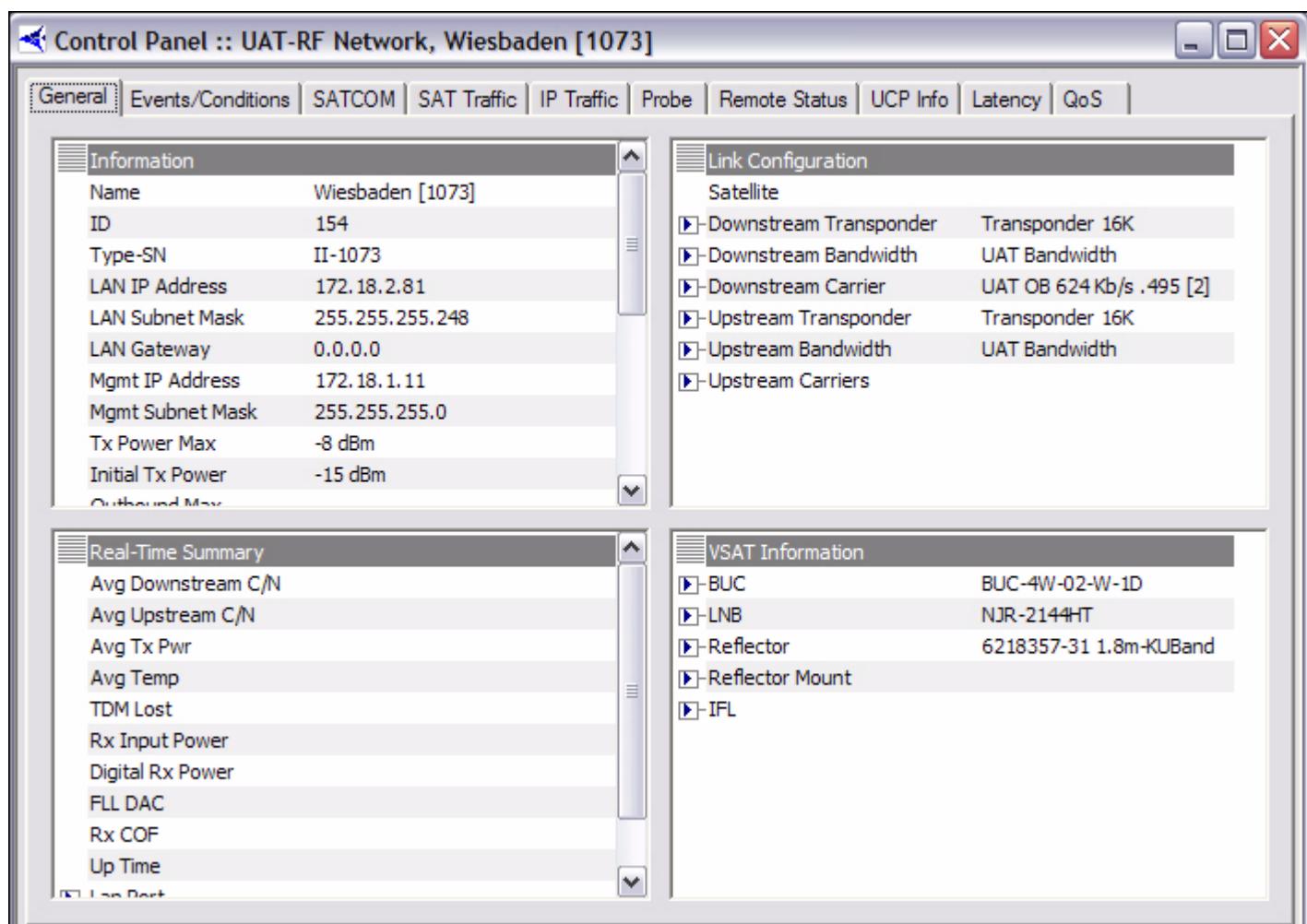
The Control Panel is available only from individual remotes in the network tree view. Additionally, you may have only four Control Panel panes launched at the same time.

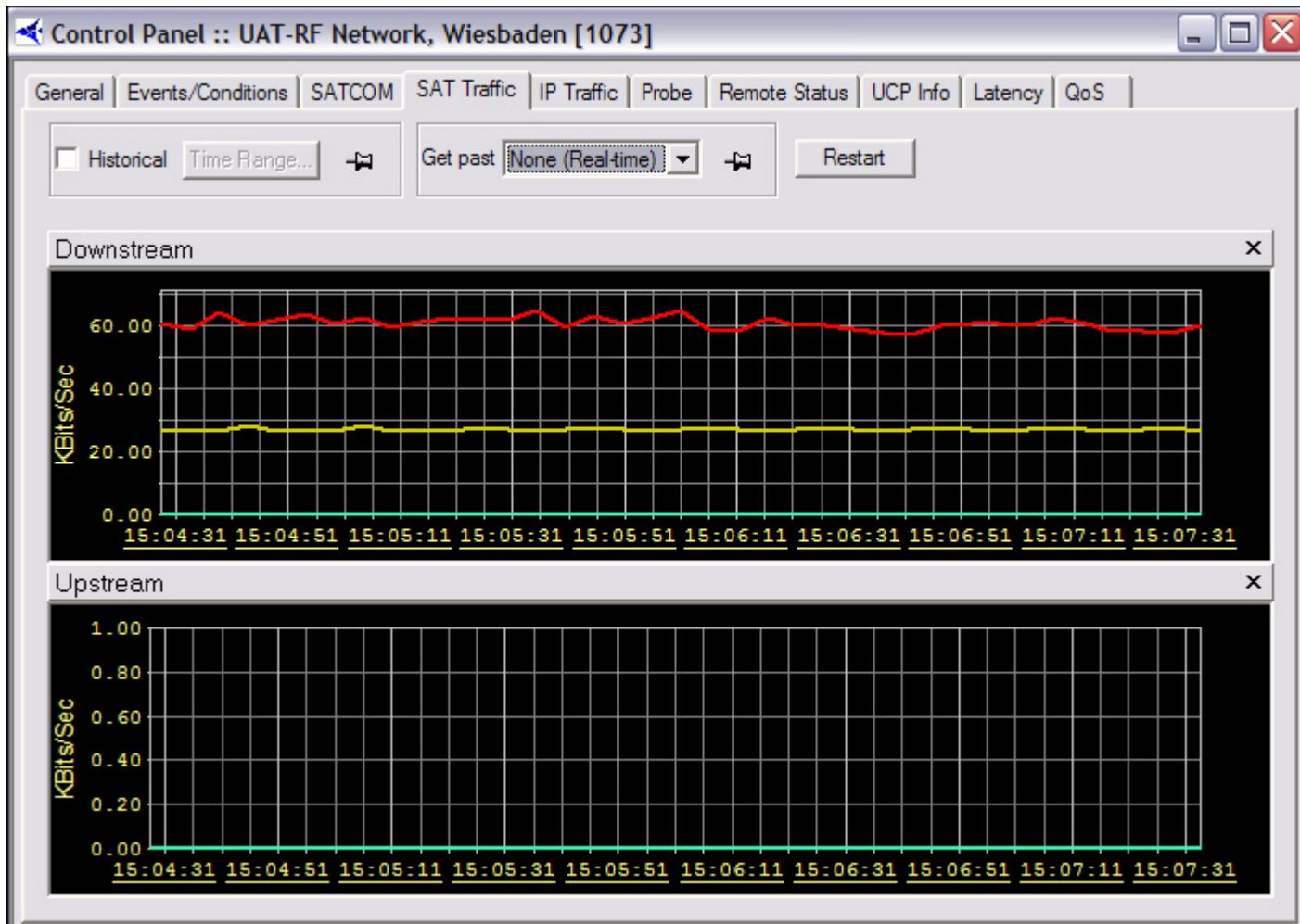
When you launch the Control Panel it automatically requests real-time data for each tab in the pane; you may also request historical data for any tab in the pane using the Historical or Get Past tools at the top of each tab.

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.
- **IP Stats** – shows IP statistics on the downstream and/or upstream for this remote.
- **SAT Stats** – 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.





4.4 Telnet

You can access the **Telnet** 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 Telnet command opens a telnet session to the selected element for detailed anomaly investigation. Please contact iDirect's Technical Assistance Center for further information on using system consoles.



5 IP and SAT Traffic Graphs

5.1 IP Statistics

iMonitor's IP stats 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 IP Statistics Changes

Release 6.0 contains a significant improvement in the IP statistics collection and presentation process. Specifically, bandwidth usage statistics are now divided into two different displays in iMonitor, each representing different classes of usage: actual over-the-air bytes and actual 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 PP.

This technique allows TCP traffic to flow at line rate across the satellite, and it minimizes the amount of TCP acks that get sent over the air. However, it causes *different* amounts of traffic to flow upstream from the PP (eth0 to the Internet) than flows across the satellite. A large TCP download, for example, can cause significant traffic out of the upstream interface of the PP, even though little of that traffic goes across the satellite.

In previous iDS releases, IP statistics ignored the upstream traffic generated by TCP acceleration in favor of showing satellite traffic more accurately. This compromise has been eliminated in release 6.0 by splitting traffic statistics into two collections: IP Stats (upstream side of PP), and SAT Stats (tunnel side of PP). Figure 1 illustrates where each collection takes place.

The IP Stats display remains unchanged in iMonitor, except it now represents the traffic sent and received on the upstream interface of the PP.

Note: Due to the changes described above, the IP Stats display may now 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.

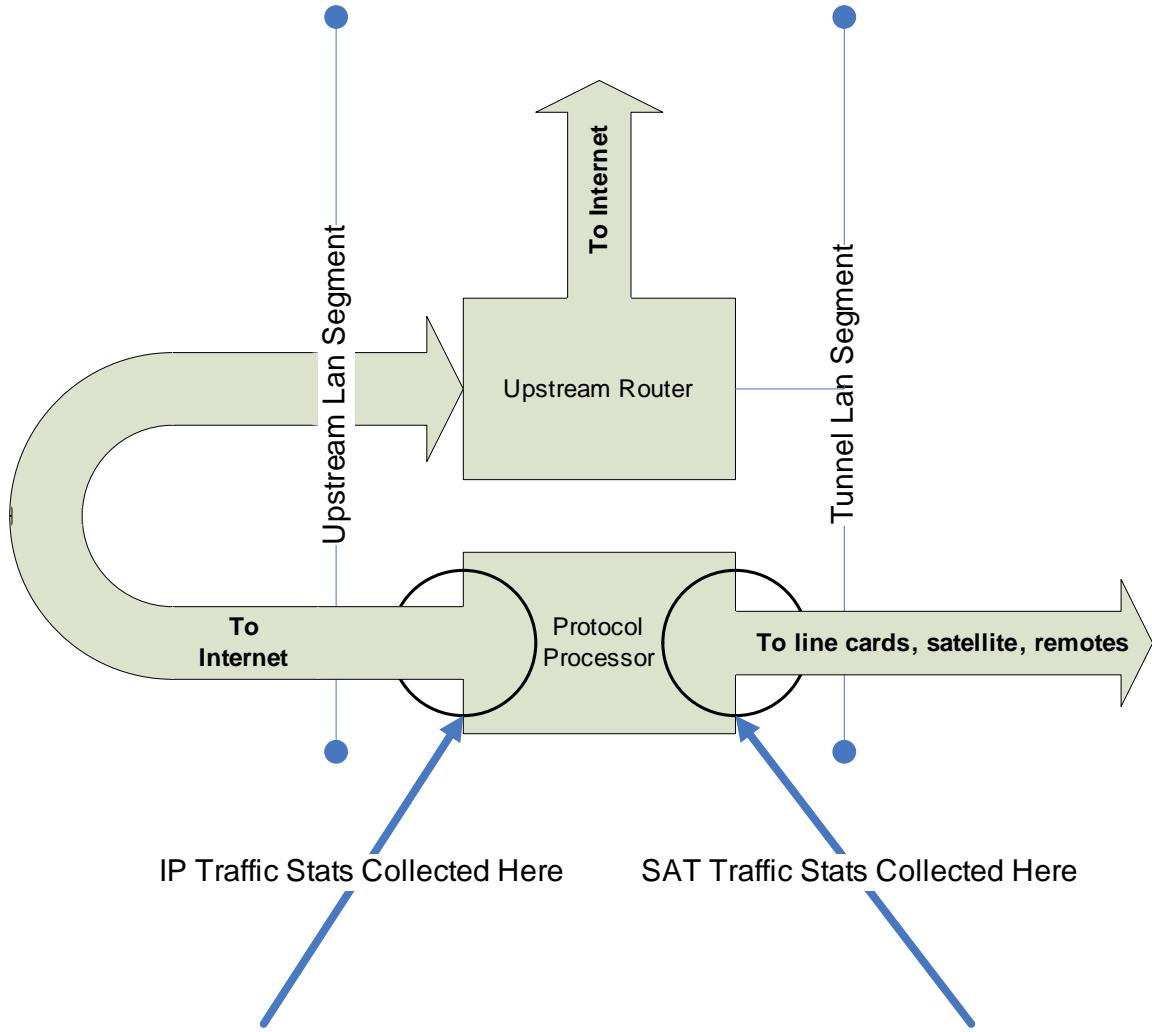


Figure 5-1: Collection Points for IP Usage Statistics

5.3 SAT Statistics

The new 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.

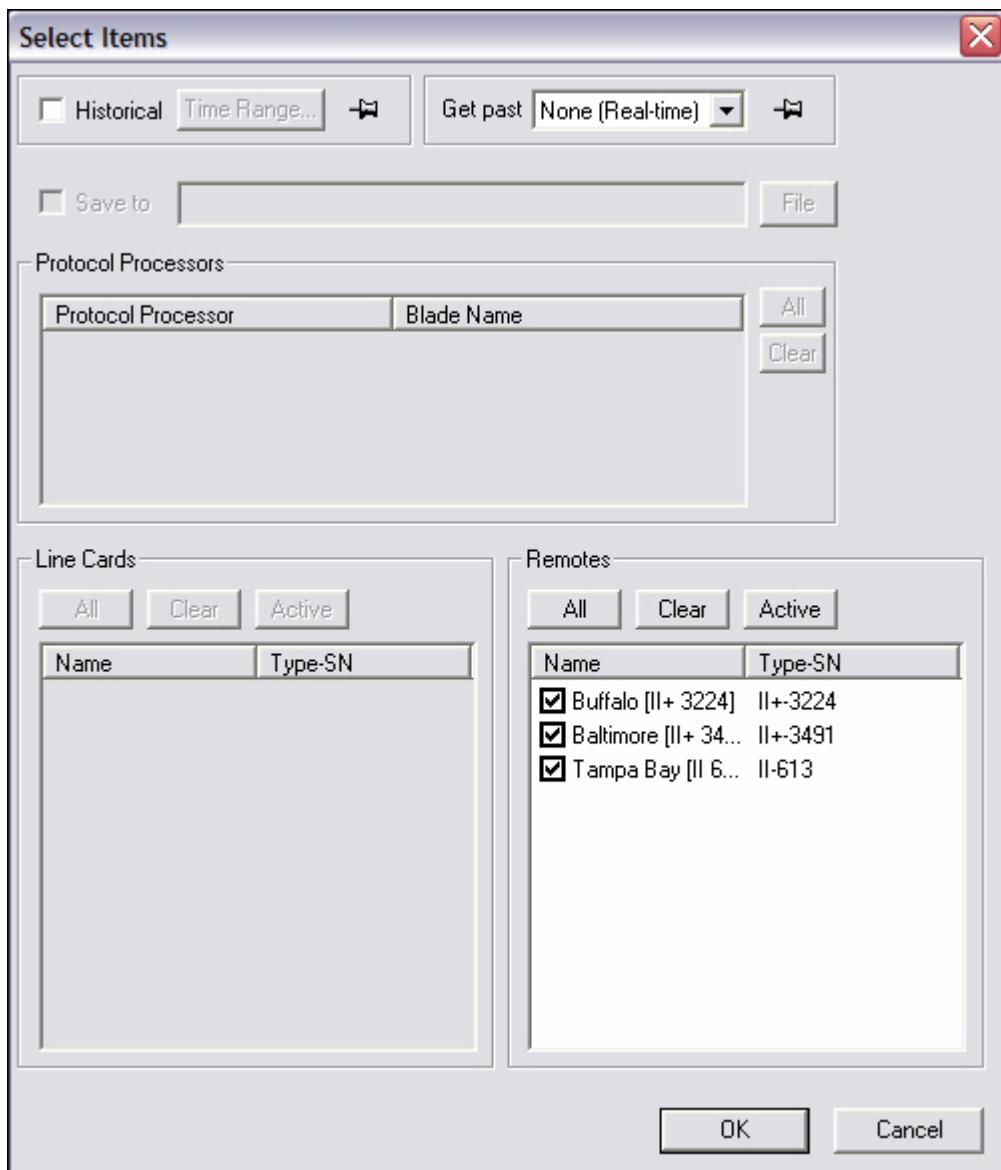
5.3.1 SAT Traffic Graph

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.



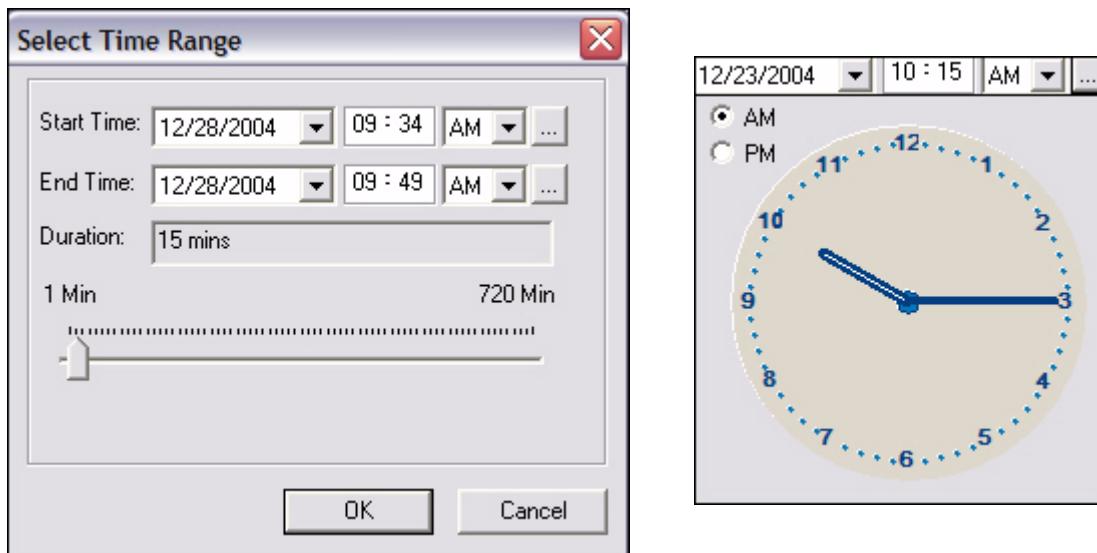
Step 3 Select the remote for which you want to view information. Notice that all but the Remotes section are unavailable for selection.

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

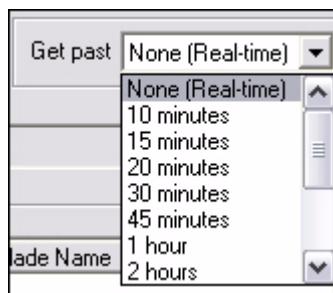
You may specify a historical time range or Get Past value from the parameters dialog. The maximum interval you can select is 12 hours. The farther you go back in time, less granularity will be available from the database due to archive consolidation.

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 click **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](#).

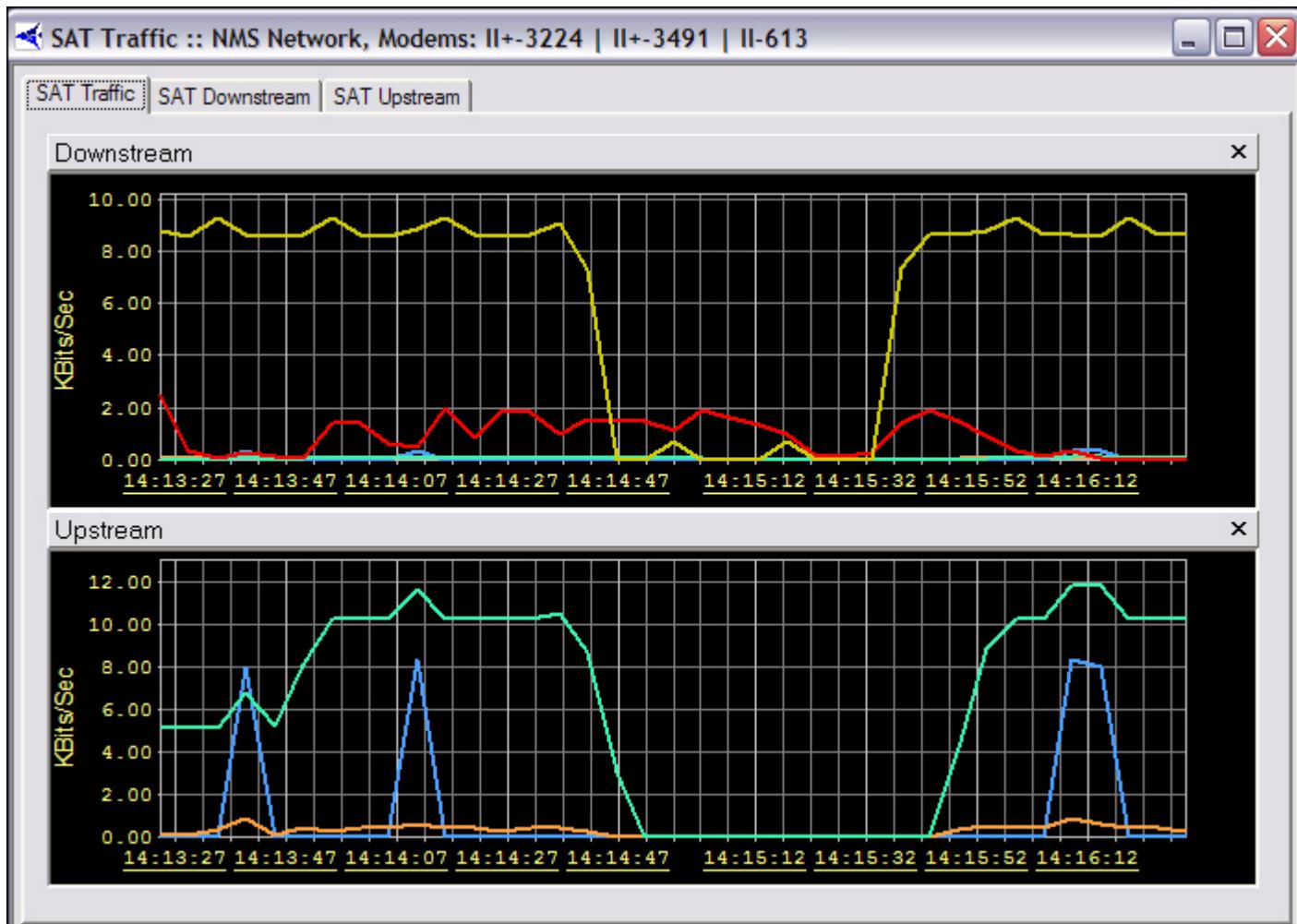


- b If you selected **Get Past**, the **Get Past** drop-down list appears. Select an interval of time.



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

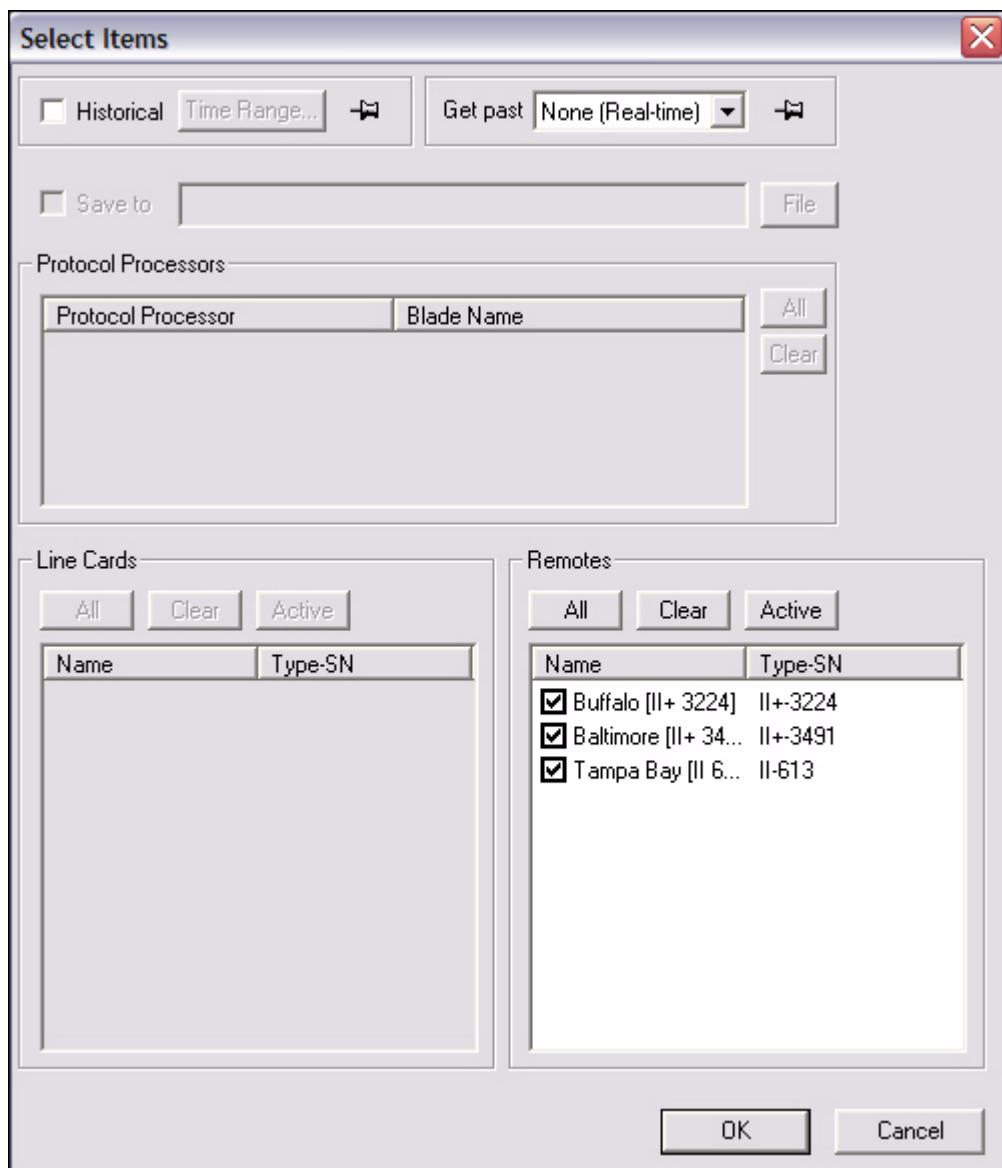
5.3.2 IP Traffic Graph

IP traffic information can be selected from:

- networks
- inroute groups
- remotes

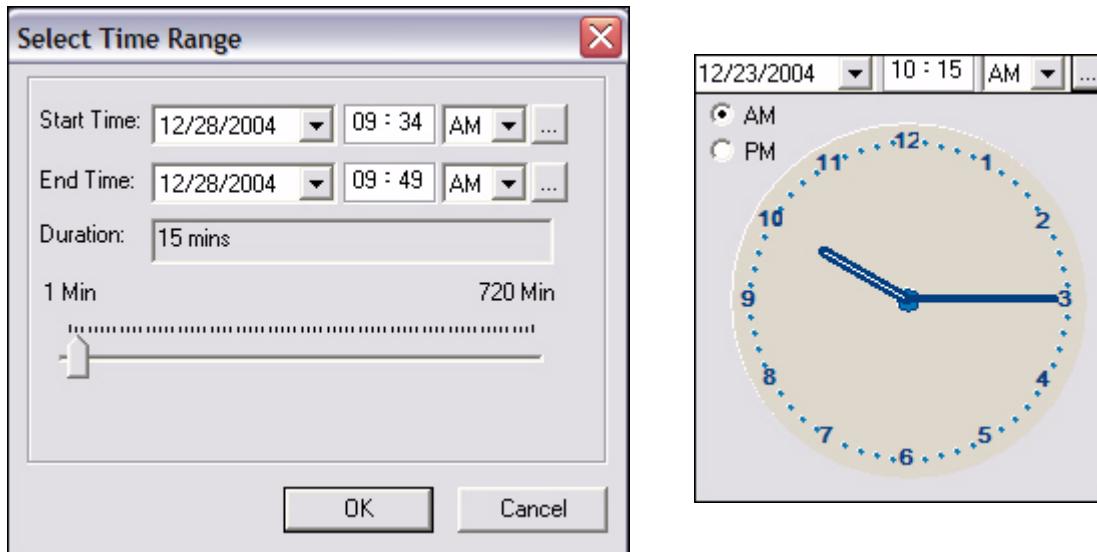
To view the IP traffic graph, follow the directions below:

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

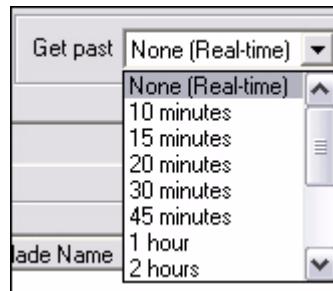


- Step 3 Select the remote for which you want to view information. Notice that all but the Remotes section are unavailable for selection.
- Step 4 Click either **Historical** or **Get Past**, or **OK** to view real-time.

- a If you click **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](#).

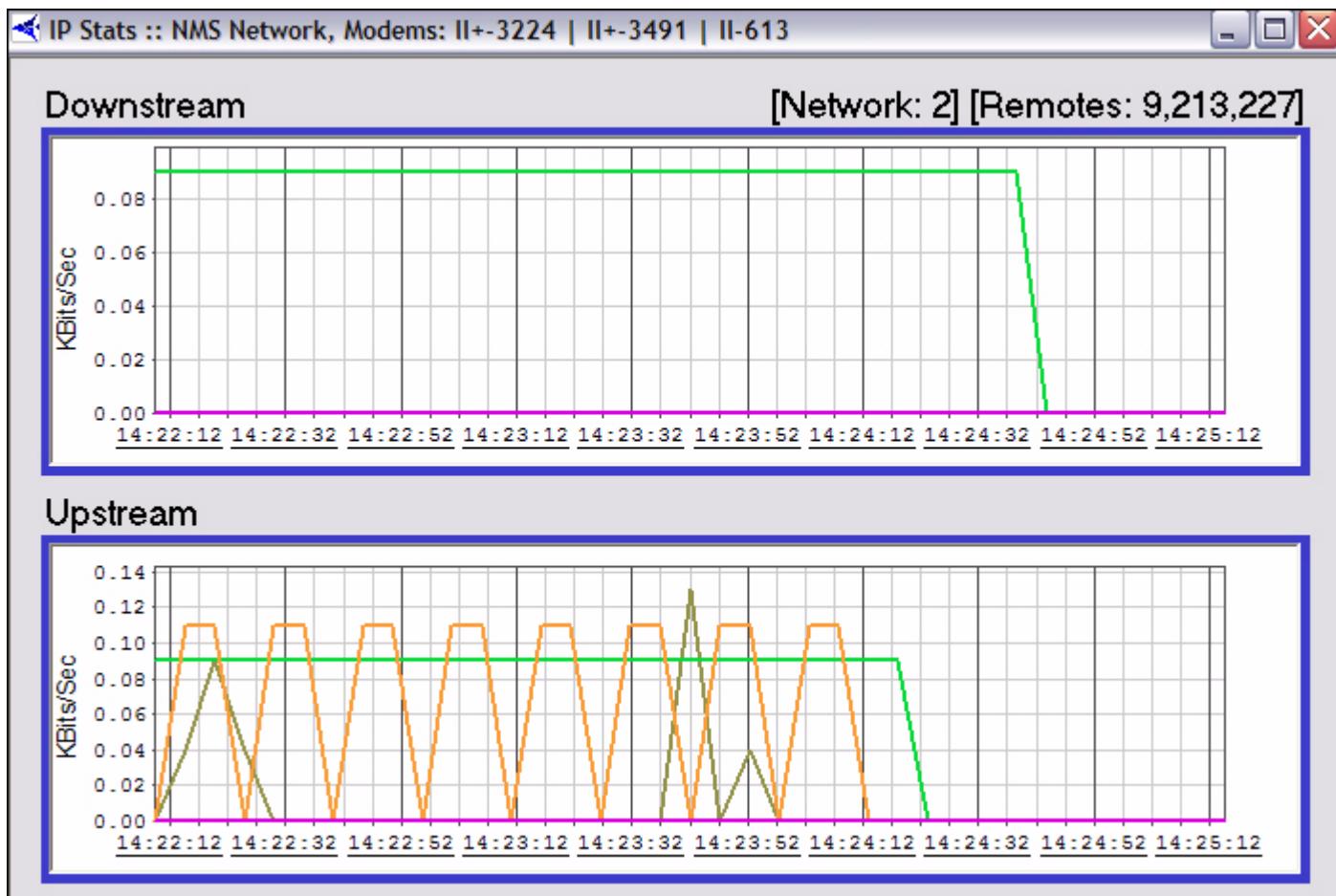


- b If you selected **Get Past**, the **Get Past** drop-down list appears. Select an interval of time.



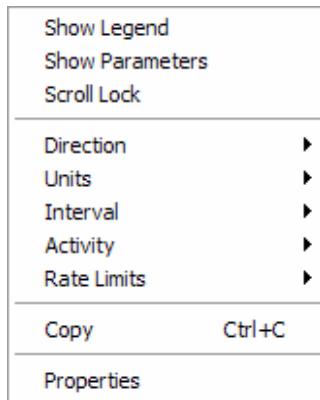
Step 5 Click **OK**.

Step 6 The **IP Traffic Stats** pane appears, as shown below. Refer to the [IP Stats Tables](#), discussed on page 117 for information on these results.



5.3.3 Viewing Options

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



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 option is only available if you're displaying traffic for a single remote
- **Copy** – copies the current graph display to your PC's clipboard
- **Properties** – allows to you modify the default color settings

5.3.4 Bandwidth Usage

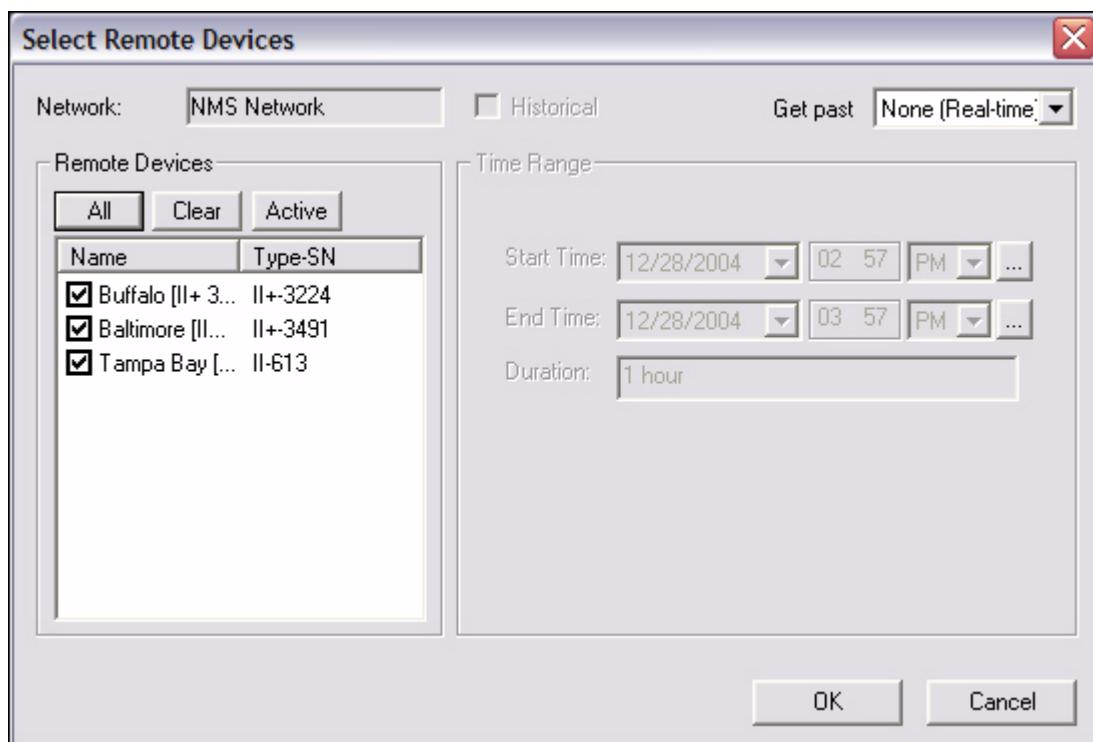
This display is useful as an at-a-glance display of the total kbps traffic in both directions for a selected group of remotes. The information is shown in real-time only in a multi-column list. You can sort each column in ascending or descending order.

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.

Bandwidth Usage :: NMS Network, Modems: II+-3224 II+-349...				
Remote	ID	Ty...	Downstream [KBits/Sec]	Upstream [KBits/Sec]
Tampa Bay [II 613]	227	II-...	0.00	0.00
Buffalo [II+ 3224]	9	II+...	0.04	0.20
Baltimore [II+ 3491]	213	II+...	0.04	0.04
Total			0.09	0.24

Figure 5-2: Real-Time Bandwidth Usage Display

6 Reporting on Networks

iMonitor provides two 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

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

- SAT Long Term Bandwidth Usage
- IP Long Term Bandwidth Usage
- Remote Availability

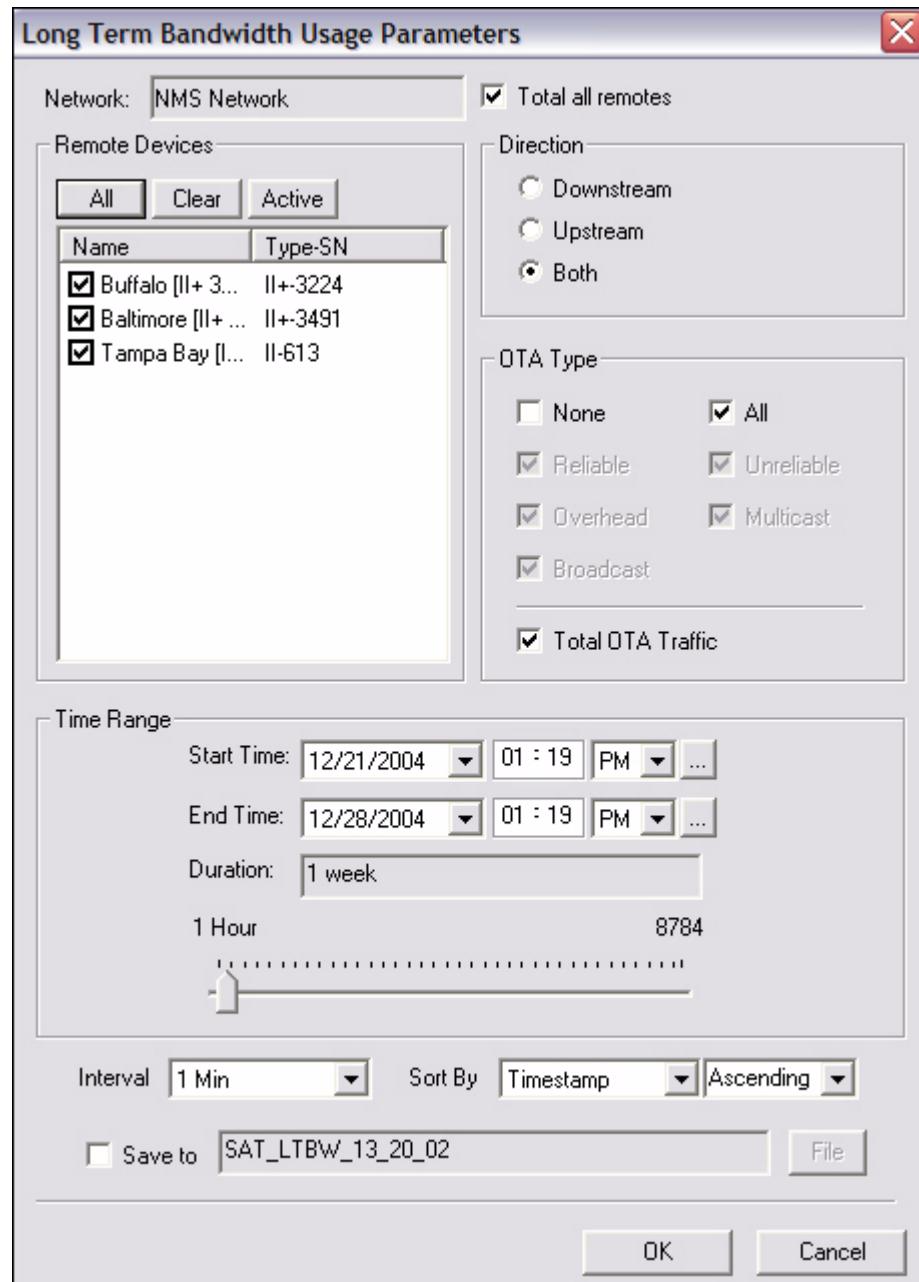
6.1.1 Long-Term Bandwidth Usage Report

Long-term bandwidth usage reports can be generated in iMonitor, providing you with a fast and flexible way to show bandwidth utilization. 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 and SAT Long Term Bandwidth Usage Reports

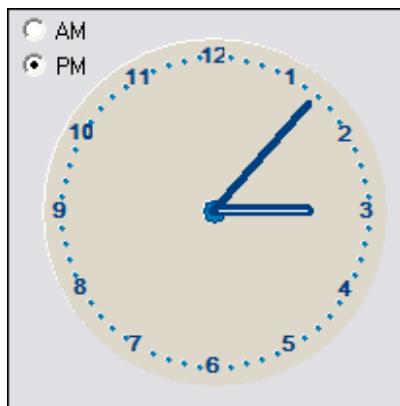
To generate, view, save, or print the SAT Long Term Bandwidth Usage report, follow the directions below:

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



- 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**, 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 IP 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 the technical note titled, **Accessing the NMS Statistics Archive**.

- 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 **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.

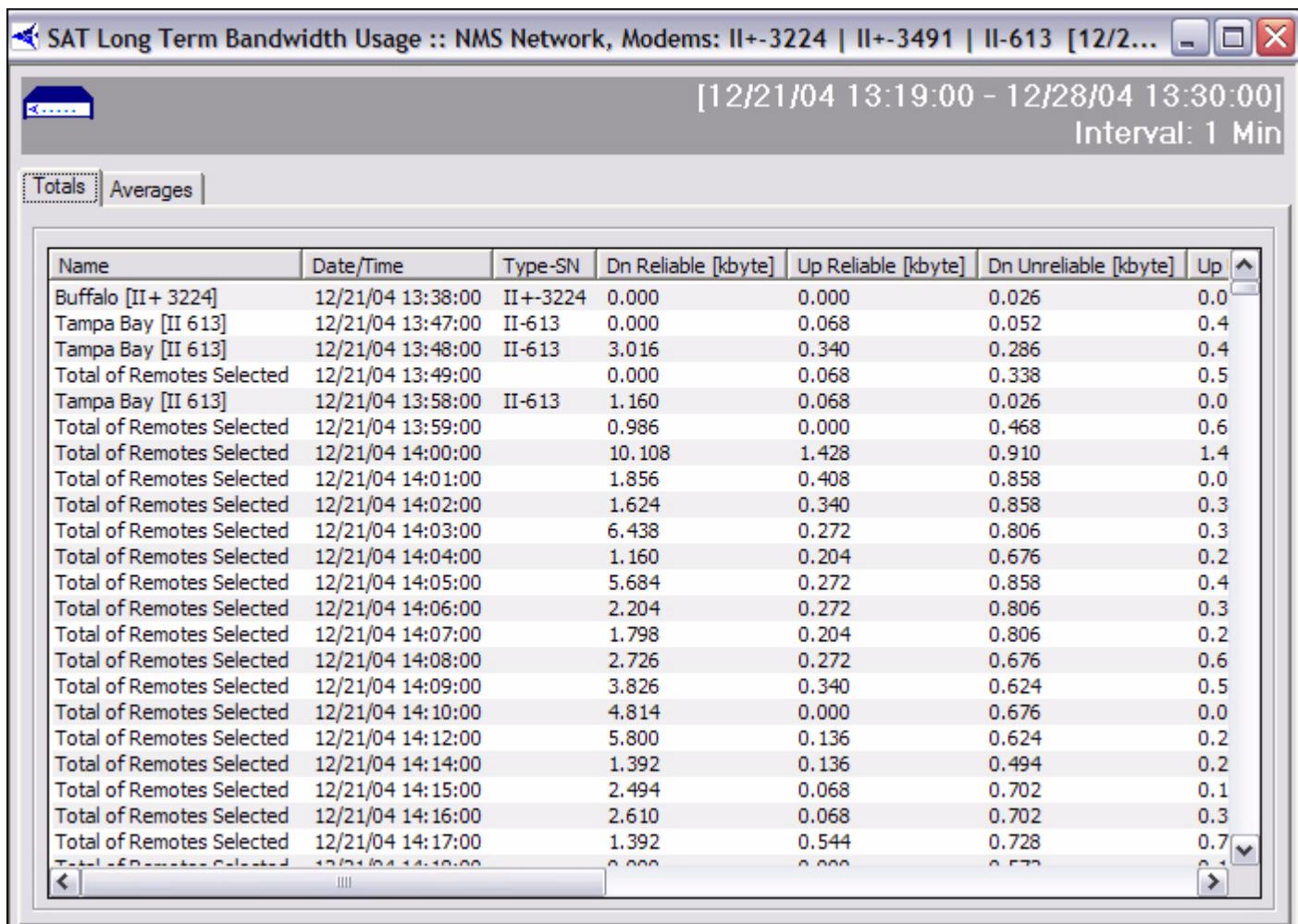


Figure 6-1: SAT Long Term Bandwidth Usage Report

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

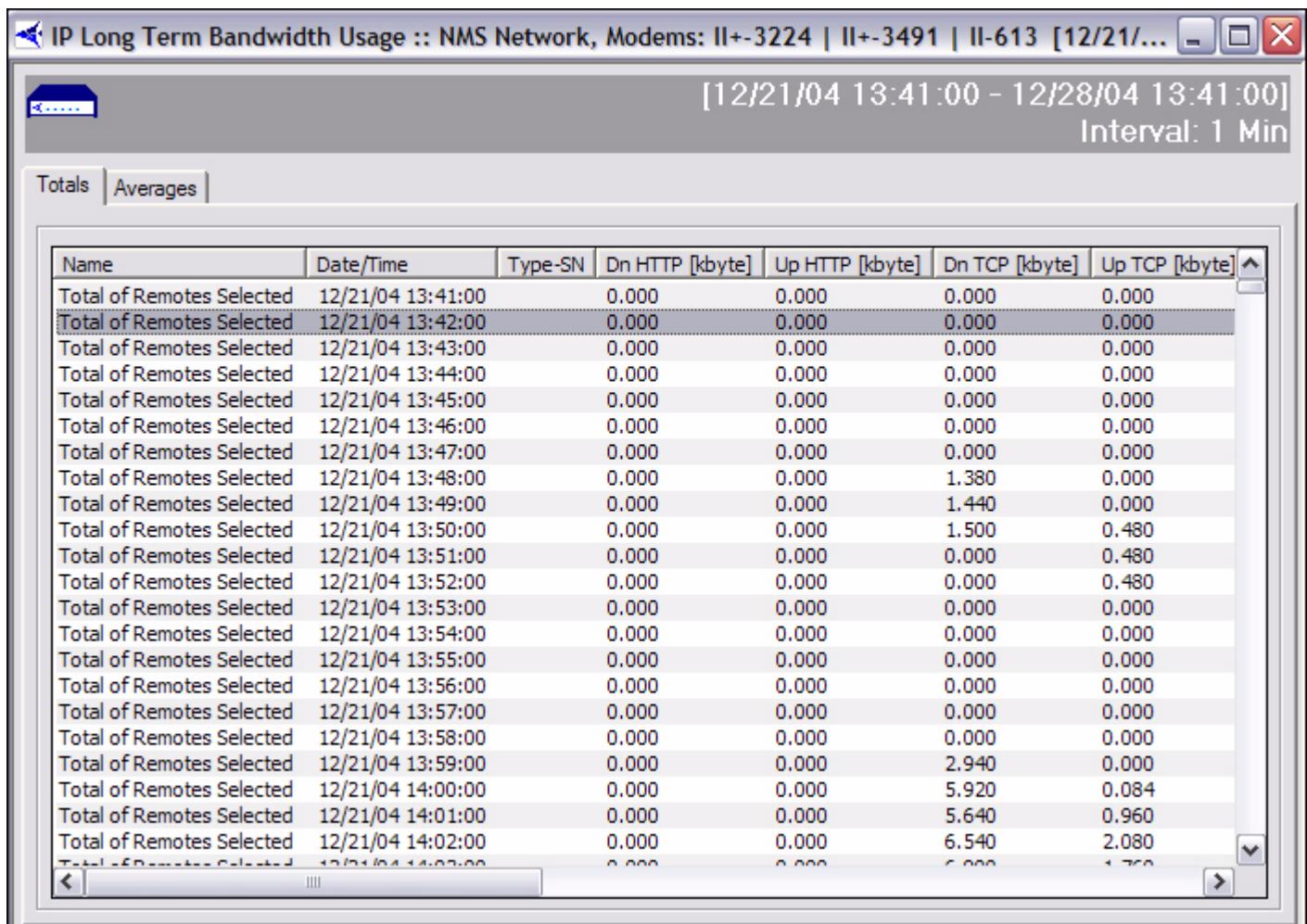


Figure 6-2: IP Long Term Bandwidth Usage Report

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 SAR 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, time plans, 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:

```
(bytes per slot) * (slots per frame) * (1000/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 bytes per slot) * (109 slots) * (1000/125) = 488.320 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 Availability Report

The Remote Availability report allows 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 Remote Availability Report also includes a count of the number of times a remote was out-of-network during the reporting period.

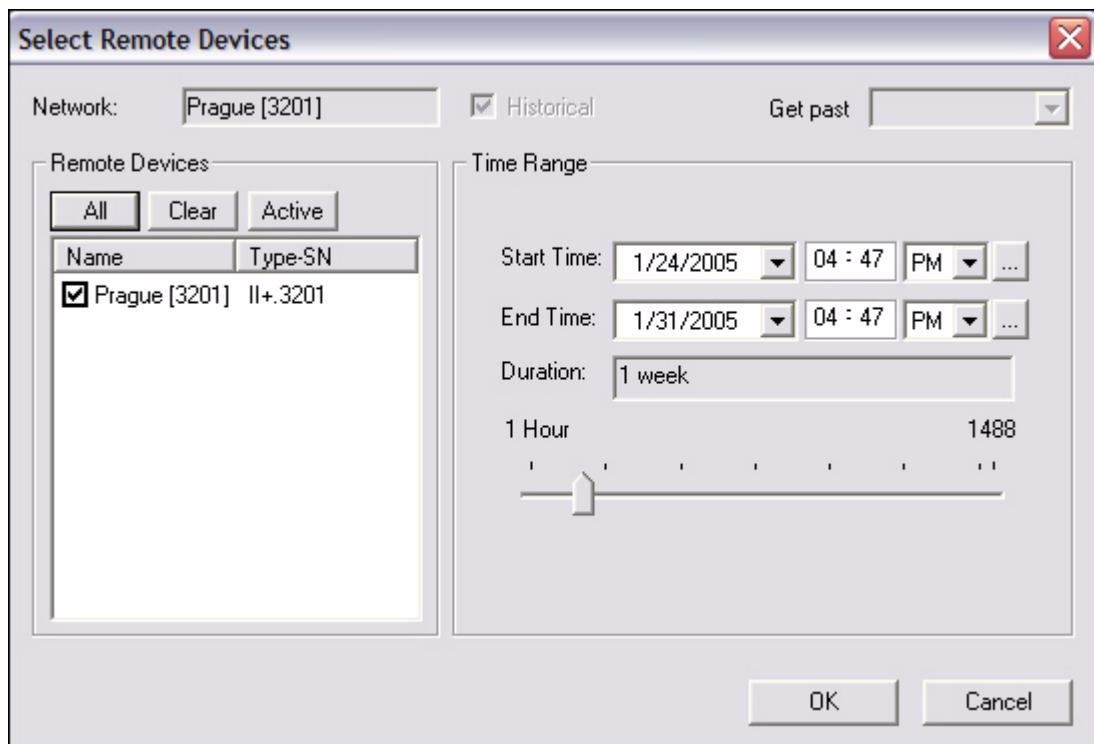
This report is available from the following levels of the network tree view:

- Network
- Inroute Groups
- Individual Remotes

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 remotes 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 remote was up and down, and the total number of hours during the time period the remote 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 remotes for which you generated the report.

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

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. (For more information on this feature, please see the technical note entitled *Long-Term Bandwidth Reporting in iMonitor*.)

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 memo is a technical person who has experience developing relational database applications, preferably using ODBC.

A.1 Improved NMS Statistics Archive Storage

The statistics archive now stores some types of archive data more efficiently, specifically:

- 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.2 Improved NMS Statistics Archive Lookup

Large historical requests are now 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.3 Archive Consolidation

To prevent filling up the NMS server's hard disk, a consolidation process runs every night at approximately midnight. 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 1 below.

A.4 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 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, the double quotes around password and single quotes around the percent sign are required.

Step 4 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.5 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.

Archive Consolidation

To prevent filling up the NMS server's hard disk, a consolidation process runs every night at approximately midnight. 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 1 below.

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 tech note.

Table A-1: Archive Database Tables

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

Table A-1: Archive Database Tables (Continued)

Table Name	Contains	Data Saved For
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

A.6 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.

IP Stats Tables

As shown in [Table A-1](#), there are three separate tables for IP stats, each one containing records that cover a particular period of time. Prior to release 4.0, the format of all three tables is the same and is shown in [Table A-2](#) below. Beginning with release 4.0, the ip_minute_stats and ip_hour_stats tables have additional fields containing maximum and standard deviation calculations for all IP types. These new 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.

Important 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

Table A-2: IP Stats Record Format (Continued)

Column Name	Data Type	Meaning
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

New Fields Beginning with Release 4.0.0

The two consolidated tables, ip_minute_stats and ip_hour_stats, contain additional fields beginning with release 4.0.0. These fields 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_kbyte	double	As above, for tx_http_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 rx_tcp_kbyte.
rx_udp_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

IP Stats Consolidation

The IP stats 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 daemon performs the following tasks on the IP stats tables (default values are used here):

- Step 1 Delete all records from the ip_hour_stats table older than 4464 hours.
- Step 2 Consolidate all records from the ip_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 ip_minute_table older than 744 hours.
- Step 4 Consolidate all records from the raw_ip_stats table older than 24 hours into one record per minute and write that record to the ip_minute_table.
- Step 5 Delete all records from the raw_ip_stats table older than 24 hours.

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. [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
rtt	double	the measured round trip time in milliseconds (-1 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.

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.

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.

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_ticks	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)
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
fll_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

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
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
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

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

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
<code>timestamp</code>	<code>timestamp(14)</code>	<code>time_t</code> that the condition was raised or cleared
<code>unique_id</code>	<code>int(10) unsigned</code>	uniquely identifies the remote or hub line card
<code>modem_sn</code>	<code>int(10) unsigned</code>	remote's or line card's serial number
<code>current_state</code>	<code>enum</code>	<p>current state of the modem after this condition is processed; values are:</p> <ul style="list-style-type: none"> • OK • WARNING • ALARM • OFFLINE • UNKNOWN <p>NOTE: MySQL enumeration types are 1-based, not 0-based.</p>
<code>occurred_at</code>	<code>timestamp(14)</code>	<code>time_t</code> of original condition in the case of multiple simultaneous conditions
<code>error_type</code>	<code>smallint(6)</code>	<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

Table A-9: state_change_log Record Format (Continued)

Column Name	Data Type	Meaning
error_type	smallint(6)	<ul style="list-style-type: none"> • SYMBOL_OFFSET • REMOTE_OFFLINE • RX_OVERFLOW_FRAMES
error_severity	enum	<p>severity of the condition; values are:</p> <ul style="list-style-type: none"> • EVTWarning • EVTAck • EVTcleared • EVTOffline <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.

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
current_state	enum	<p>current state of the protocol processor after this condition is processed; values are:</p> <ul style="list-style-type: none"> • OK • WARNING • ALARM • UNKNOWN • OFFLINE • STATE_NONE <p>currently, only OK, ALARM, and UNKNOWN are raised for protocol processors.</p>
occurred_at	timestamp(14)	time_t the condition was first raised in case of multiple simultaneous conditions
error_severity	enum	<p>severity of the condition; values are</p> <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.

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 • EVCleared • EVTOffline • EVTNone
reason	varchar(255)	text explanation of this condition



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, tracert). 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, tracert). 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, tracert). 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. <p>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.</p>
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.

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

Table B-2: Warnings (Continued)

Device	Warning Condition	Description	Action, Troubleshooting
	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_OVER_DRIVE	Downstream packets-per-second count above fixed limit	
	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 (7 dB/25 dB)	<ul style="list-style-type: none"> Weak signal could be due to rain fade. Check transmit power levels in iBuilder.
	DOWNSTREAM_SNR	Downstream C/N as perceived at remote is below/above limits (7 dB/25 dB)	<ul style="list-style-type: none"> Weak signal could be due to rain fade. Check transmit power levels in iBuilder.

Table B-2: Warnings (Continued)

Device	Warning Condition	Description	Action, Troubleshooting
	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 (+15°C/+77°C)	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 (-35dBm/+7dBm)	
	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 Warning Limit Ranges

Table B-3: Warning Limit Ranges

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
Calibrated TxPower	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 and basic configuration information to any interested SNMP client.

C.1 How the Proxy Agent Works

The SNMP Proxy Agent is a client of both the NMS Configuration Server and the NMS Event Server. It gets a list of network elements from the Configuration Server and the real-time status of each element from the Event Server. The following figure illustrates how the SNMP Proxy Agent fits into the overall NMS architecture.

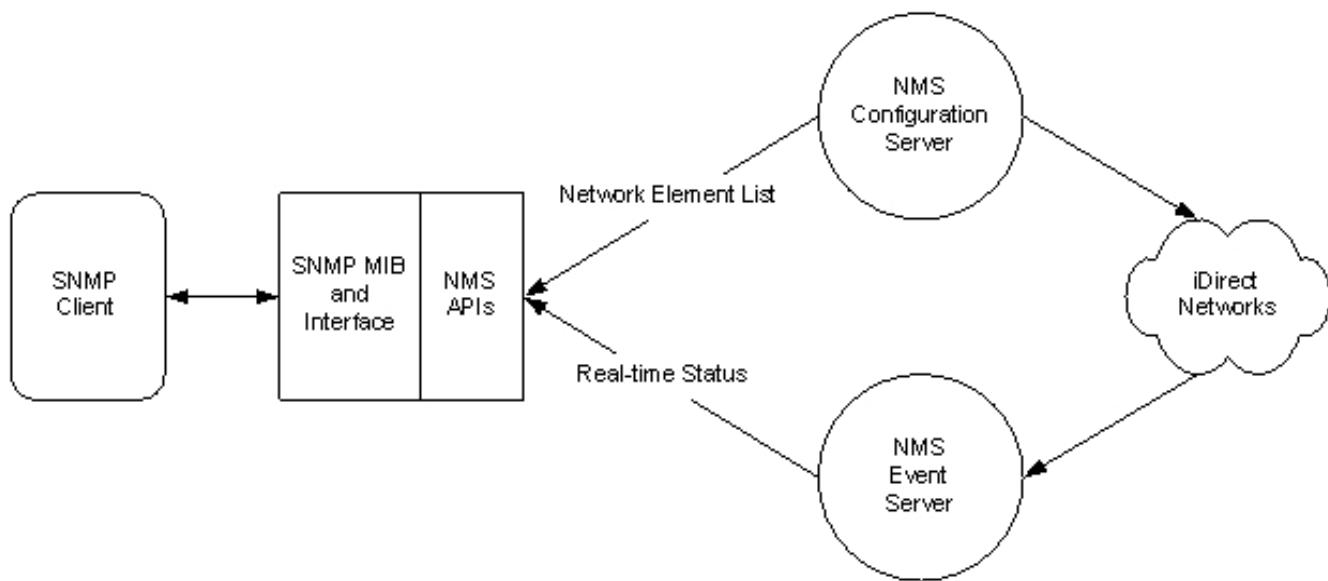


Figure C-1: SNMP Proxy Architecture

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.

C.1.1 Installing and Running the SNMP Proxy

iDirect distributes the SNMP Proxy Agent in its own RPM file. For instructions on installing this RPM, see the document entitled *Installing the Net-SNMP Option*.

Once you have completed the installation, the SNMP Proxy Agent becomes part of the normal NMS server startup and shutdown procedure (`service idirect_nms start/stop/restart`). It will also be started automatically whenever the server machine is restarted.

C.1.2 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)
NetModem	<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)

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/local/share/snmp/mibs/IDIRECT-REMOTE-MIB.txt`

C.1.3 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/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-2: 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-2: 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

C.1.4 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 /usr/local/share/snmp
# vi snmpd.conf
```

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]]
```

Step 4 Replace *host* with the name of the desired recipient. The community and port strings are optional.

Step 5 Add a line like the following for *each* machine to which you want to send SNMP Version 2 (v2) traps:

```
trap2sink host [community [port]]
```

Step 6 Replace *host* with the name of the desired recipient. The community and port strings are optional.

Step 7 Do not change or remove any other lines in this file.

C.2 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/snmpsrv/IDIRECT-REMOTE-MIB.hpov.txt

C.2.1 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-3: 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
snmpptest	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 (disk space, network status, etc.).

Index

B

button
accept changes 8

C

conditions 27
configuration changes 25

D

dialog box
Select Items 34

E

events 27

F

find toolbar 20

G

Globe 13
globe
sorting
globe
hide element 13
tree 13

I

iBuilder
description 3
installing 6
iMonitor
description 4
installation
NMS applications 6
iSite 4

L

legend 25
logging in
passwords 7
to other servers 8

M

main toolbar 20
modifying
accepting changes 8

N

NetManager, replaced by iSite 4
NMS
applications 3
main components 3
multiple users accessing 8
servers used 4

P

panes
configuration changes 25
legend 25
See also dialog boxes
passwords 7

R

requirements
system 6
right-click
menu options 20

S

Select Items dialog box 34
servers 4
status bar 23
system requirements 6

T

toolbars

- configuration changes 25
- find 20
- icons 20
- legend 25
- main 20
- main menu 20
- status bar 23
- view menu 20

tree

- description 17

U

users

- multiple 8

W

windows, See panes

See also dialog boxes