



***Network Management System  
iBuilder User Guide***

***Release 7.0.1  
October 15, 2007***



.Copyright © 2007, 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](http://www.iDirect.net)

HQ: 1.703.648.8000  
Toll free from within the US 1.888.362.5475

# Contents

<b>Figures</b>	<b>xi</b>
<b>Tables</b>	<b>xii</b>
<b>1 Using this Guide</b>	<b>1</b>
1.1 Intended Audience	1
1.2 Document Conventions	1
1.3 Informational Conventions	1
<b>2 iDirect System Overview</b>	<b>3</b>
<b>3 Overview of the Network Management System for iBuilder</b>	<b>11</b>
3.1 Introduction	11
3.2 Gathering the Information You Need	11
3.3 Preparing Equipment in Advance	12
3.4 Components of the Network Management System	12
3.4.1 NMS Applications	12
<i>iBuilder</i>	13
<i>iMonitor</i>	13
<i>iSite</i>	13
3.4.2 Server Components	14
<i>Configuration Server</i>	14
<i>Real-time Data Server</i>	14
<i>Event Server</i>	14
<i>Latency Server</i>	14
<i>NMS Controller Server</i>	14
<i>PP Controller Servers</i>	14
<i>NMS Monitor Script</i>	14
<i>Consolidation Script</i>	14
<i>Database Backup Script</i>	15
<i>Database Restore Script</i>	15
3.5 Installing iBuilder, iMonitor, and iSite	15
3.5.1 System Requirements	15
3.5.2 Installation Procedure	15
3.6 Launching iBuilder	16
<i>Logging On To Additional Servers</i>	17
<i>Multiple Users or PCs Accessing the NMS</i>	17
<i>Accepting Changes</i>	18
3.7 Pre-defined Components and Components Folders in iBuilder	19
3.7.1 Bench Test Components	19
3.7.2 Components Folders	20

3.7.2.1 Folders Containing Critical Information	20
QoS	20
<i>Components: Remote Antenna Components</i>	21
<i>Components: Hub RFT Components</i>	22
3.7.2.2 Folders Containing Reference Information	22
3.7.2.3 Adding Entries to Folders	22
3.7.2.4 Canceling an Entry	23
3.8 Using iBuilder's Interface	23
3.8.1 Clicking on Elements and Folders: What Happens?	24
<i>Right-Clicking</i>	24
<i>Double-Clicking vs. Single-Clicking</i>	25
3.8.2 Globe	25
<i>Using the Docking Feature</i>	25
<i>Expanding Tree</i>	26
<i>Collapsing Tree</i>	26
<i>Sorting Columns</i>	27
<i>Sorting the Tree</i>	27
3.8.3 Network Tree	29
3.8.4 Using the Interface Toolbars and Menu Options	30
<i>Title Bar</i>	30
<i>Menu Bar</i>	31
<i>Toolbar</i>	31
<i>Find Toolbar</i>	32
<i>View Menu</i>	34
<i>Status Bar</i>	34
<i>Connection Details on Status Bar Icon</i>	35
<i>Active Users Pane</i>	35
<i>Legend Pane</i>	36
<i>Configuration Changes Pane</i>	37
<i>Configuration Status View</i>	37
<i>Properties View</i>	38
<i>Details</i>	38
<i>Collapse Details Hierarchy + Details</i>	39
<i>Choose Details</i>	40
3.9 Customizing and Creating New Detail Views	40
3.9.1 Customizing Detail Views for Configuration Reporting	40
3.9.2 Creating Additional Filters for Customized Reporting	44
3.10 Working with Multiple Elements Simultaneously	47
3.10.1 Working with Multiple Configurations and Image Files	47
3.10.2 Modifying Parameters on Multiple Elements	47
<i>Rules for Multiple Edit</i>	47



<i>Procedure for Group Editing</i>	47
3.11 Configuration Status of Elements	49
3.11.1 What is a Configuration State?	49
3.11.2 Possible Configuration States	50
3.11.3 Configuration State Transition	51
3.11.4 Viewing Configuration States	52
3.11.5 Why Did My Configuration States Change?	52
3.11.6 Configuration States and iMonitor	52
3.11.7 Accepting Configuration Changes and Locking the Database	53
3.12 Understanding the Database's Numbering Convention	53
3.13 In Color versus Shaded Icons	54
3.14 Configuring Warning Properties	55
3.14.1 Setting Global Warning Properties	56
3.14.2 Customizing Warning Properties for Individual Network Elements	58
3.14.3 Clearing Customized Warning Properties	59
<b>4 Defining Hub RFT Components and the Satellite</b>	<b>61</b>
4.1 Preparing the Hub RFT Components Folders	61
4.1.1 Adding an Antenna	61
4.1.2 Adding an Up or Down Converter	62
4.1.3 Adding a High Power Amplifier (HPA)	64
4.2 Adding a Spacecraft	65
4.3 Adding a Transponder	66
4.4 Adding Bandwidth	68
4.5 Adding Carriers	69
4.5.1 Adding Downstream Carriers	69
4.5.2 Adding Upstream TDMA Carriers	71
4.5.3 Adding Upstream SCPC Carriers	74
<b>5 Defining Network Components</b>	<b>77</b>
5.1 Adding a Teleport	77
5.2 Adding a Backup Teleport	78
5.3 Adding a Hub RFT	82
5.4 Adding a Protocol Processor	83
5.5 Setting Warning Properties for Protocol Processor Blades	85
5.6 Adding a Protocol Processor Blade	85
5.7 Adding a VLAN	88
<i>Special VLAN Configuration</i>	90
<b>6 Defining Networks, Line Cards, and Inroute Groups</b>	<b>93</b>
6.1 iDirect Line Card and Hub Models	93
6.2 Adding a Network	93

6.3	Adding a Tx Line Card, a Tx/Rx Line Card, or a 10000 Series Hub	94
6.4	Setting Warning Properties for Line Cards	97
6.5	Adding Receive (Rx) Line Cards	97
6.6	Adding an iSCPC Line Card	99
6.7	Defining a Standby Line Card	101
6.7.1	Selecting Automatic Failover	101
6.7.2	Failover Prerequisites	102
6.7.3	Basic Failover Concepts	102
6.7.4	Tx(Rx) versus Rx-Only Line Card Failover	103
6.7.5	Failover Sequence of Events	104
6.7.6	Failover Operation: User's Perspective	105
6.7.7	Recovering from a Line Card Failover	106
6.7.8	Recovering from a Repairable Line Card Failure On-site	106
6.8	Adding Inroute Groups	107
	<i>Carrier Grooming</i>	107
	<i>Frequency Hopping</i>	108
	<i>Mesh-Enabled Inroute Groups</i>	108
	<i>Adding an Inroute Group</i>	109
<b>7</b>	<b>Configuring Remotes</b>	<b>115</b>
7.1	iDirect Remote Satellite Router Models	115
7.2	Before You Start	115
7.3	Adding Remotes	115
7.4	Information Tab	116
7.4.1	Transmit and Receive Properties	120
7.4.2	Customers and Distributors	121
7.5	IP Config Tab	123
7.5.1	VLAN and LAN Information	123
	<i>Configuring LAN and Management Interfaces</i>	124
	<i>Adding VLANs to a Remote</i>	125
7.5.2	Domain Name Service (DNS)	127
7.5.3	Dynamic Host Configuration Protocol (DHCP)	127
7.5.4	Static Routes, NAT, Multicast Groups, and Port Forwarding	129
	<i>Static Routes</i>	129
	<i>Using Static Routes with Multiple Protocol Processor Blades</i>	130
	<i>Multicast Groups</i>	131
	<i>NAT and Port Forwarding</i>	132
7.5.5	Accelerated GRE Tunnels	133
7.6	Switch Tab	134
7.7	QoS Tab	138
7.7.1	QoS Profiles	138

7.7.2	Upstream and Downstream SAR	139
7.7.3	Upstream and Downstream Rate Shaping	140
7.7.4	PAD	141
7.8	Geo Location Tab	142
	<i>Mobile State</i>	142
7.9	VSAT Tab	143
7.10	Setting Warning Properties for Remotes	145
7.11	Adding a Remote by Cloning an Existing Remote	145
7.12	Roaming Remotes	145
7.12.1	Adding a Roaming Remote	147
7.12.2	Managing Roaming Remote Configuration	149
	<i>Managing "Must be the Same" Parameters</i>	149
	<i>Managing "Don't Care" Parameters</i>	150
7.12.3	Beam Switching for Roaming Remotes	152
	<i>Automatic Beam Selection</i>	152
	<i>Manual Beam Selection</i>	153
	<i>"Round Robin" Beam Selection</i>	153
7.13	Enabling IP Packet Compression Types	153
7.13.1	TCP Payload Compression	155
7.13.2	UDP Header Compression	155
	<i>UDP Header Compression Performance Characteristics</i>	155
7.13.3	CRTP	156
	<i>RTP Header Compression Performance Characteristics</i>	156
7.13.4	UDP Payload Compression	156
<b>8</b>	<b>Creating and Managing QoS Profiles</b>	<b>157</b>
8.1	What is a QoS Profile?	157
8.2	Storage of QoS Profile	158
8.3	Adding and Modifying Upstream and Downstream Profiles	159
8.4	Cloning a Profile	160
8.5	Adding a Service Level	160
8.6	Adding a Filter	163
8.7	Assigning a Profile to a Remote	166
8.8	Assigning QoS Profiles to Individual and Multiple Elements	167
	<i>How do I Tell What Remotes are Using a Given Profile?</i>	169
8.9	Icon Color Indicators for Profiles	169
<b>9</b>	<b>Configuring the Initial Hub Chassis</b>	<b>171</b>
9.1	Configuring the Chassis IP Address	171
9.2	Configuring and Controlling the Hub Chassis from iBuilder	172

<b>10</b>	<b>Controlling Remotes</b>	<b>177</b>
10.1	Activating and Deactivating Remotes	177
10.2	Moving Remotes	179
<b>11</b>	<b>Retrieving and Applying Saved and Active Configurations</b>	<b>181</b>
11.1	Configuration Options Files	181
11.2	Hub-side and Remote-side Options Files	181
11.3	Modifying, Deleting, and Viewing Configurations	182
11.4	Retrieving Configurations	183
11.4.1	Retrieving a Single Saved or Active Configuration	183
11.4.2	Retrieving Multiple Saved or Active Configurations	186
11.5	Comparing Configuration Changes	188
11.6	Applying Configuration Changes	190
	<i>Maintenance Window Consideration</i>	190
	<i>Sequence of Download</i>	190
11.6.1	Applying Multiple Configurations to Network Elements	191
	<i>Remote Protocol and Reset Options</i>	192
	<i>Reset Options</i>	192
	<i>Stopping the Download</i>	192
11.6.2	Applying Configurations to Individual Elements	193
	<i>Applying a Configuration to a Protocol Processor or Chassis</i>	193
	<i>Applying a Configuration to the Network</i>	194
	<i>Applying a Configuration to the Line Card</i>	194
	<i>Applying a TCP or UDP Configuration to a Remote</i>	196
11.7	Configuration Changes on Roaming Remotes	198
11.7.1	Roaming Options File Generation	198
11.7.2	Pending Changes across Networks	199
11.7.3	Applying Changes to Roaming Remotes	199
<b>12</b>	<b>Upgrading Software and Firmware</b>	<b>201</b>
12.1	Image Package Versions	201
12.2	Downloading an Image to Remotes and Line Cards Concurrently	201
12.2.1	Multicast via UDP	202
12.2.2	Download Procedure	202
	<i>Package Section</i>	202
	<i>Modems and Hubs Sections</i>	204
	<i>Download Parameters Section</i>	204
12.2.3	Downloading an Image to Out of Network Remotes	204
12.2.4	Interactions with Other iBuilder Operations	205
12.3	Resetting Remotes	206
12.4	Downloading an Image or Configuration File via TCP	207
12.5	Downloading Remotes Using Revision Server	207

12.5.1	How the Revision Server Works	208
12.5.2	When to Use the Revision Server	209
12.5.3	Starting the Revision Server	210
12.5.4	Monitoring Upgrades Using the Revision Server Status Pane	212
12.5.5	Cancelling an Upgrade	214
<b>13</b>	<b>Creating and Managing User Accounts and User Groups</b>	<b>215</b>
13.1	Conversion of User Accounts During 7.0 Upgrade Procedure	215
13.2	NMS User Groups	215
13.2.1	Visibility and Access for VNO User Groups	216
	<i>Visibility and Access for Network Elements</i>	216
	<i>Visibility and Access for Components Folders</i>	217
13.2.2	Visibility and Access for CNO User Groups	217
13.2.3	Creating and Managing VNO and CNO User Groups	218
	<i>Adding or Modifying a VNO or CNO User Group</i>	218
13.2.4	Setting Global Rate Limits for User Groups	221
13.2.5	Modifying per Node VNO Properties	222
13.3	Adding and Managing User Accounts	223
13.3.1	Adding a User and Defining User Privileges	224
13.3.2	Modifying a User	225
13.3.3	Adding a User by Cloning a User's Account	225
13.3.4	Viewing a User's Account Properties	226
13.3.5	Deleting an Existing User's Account	227
13.3.6	Managing Accounts from the Active Users Pane	227
13.4	Changing Passwords	229
13.5	User Privileges	230
13.5.1	Super User and Guest Level Privileges	232
13.5.2	Super User and Guest Privileges for VNOs	232
	<i>Super User within a VNO</i>	232
	<i>Guest User within a VNO</i>	233
13.6	NMS Database Locking	233
<b>14</b>	<b>Commissioning a Line Card, Private Hub or Mini Hub</b>	<b>235</b>
14.1	Before You Begin	235
14.2	Add the Line Card in iBuilder and Retrieve the Configuration	236
14.3	Power on the Line Card	236
14.4	Determine the IP Address	237
14.5	Download the Image Package and Options file	239
14.6	Connect the Transmit and Receive Ports	243
14.7	Perform 1 dB Compression Point Test with the Satellite Operator	244
14.8	Set the Transmit Power for the Outroute	245
14.9	Connect to the LAN and Apply the Line Card Configuration	247

14.10	Set the Clear Sky C/N Parameter for a Mesh Outroute	247
14.11	Set the UPC Margin for a Mesh Outroute	248
14.12	Set the Clear Sky C/N Parameters for a Mesh Inroute Group	248
14.13	Set the TDMA C/N Nominal Parameter for an Inroute Group	251
<b>15</b>	<b>Adding Mesh Capabilities to a Star Network</b>	<b>253</b>
15.1	Prerequisites for Converting an Existing Star Network to Mesh	253
15.2	Recalibrating a Star Outbound Channel for Mesh	253
15.3	Converting a Star Inbound Channel to Mesh	254
15.4	Reconfiguring Star Remotes to Carry Mesh Traffic	255
	<b>Appendix A Configuring a Distributed NMS Server</b>	<b>259</b>
A.1	Prerequisites	259
A.2	Distributed NMS Server Architecture	259
A.3	Logging on to iBuilder and iMonitor	260
A.4	Setting up a Distributed NMS Environment	261
A.5	Removing the SNMP Proxy Server from Auxiliary NMS Servers	264
A.6	Regenerating the Options Files	264
A.7	Granting Read Permissions to NMS 2 and NMS 3	265
A.8	Assigning QoS Profiles	266
A.9	Verifying Correct Operation	267
A.10	Running the NAT Script	268
A.11	Managing a Distributed NMS	269
A.12	dbBackup/dbRestore and the Distributed NMS	270
	<b>Glossary of Terms and Acronyms</b>	<b>273</b>
	<b>Index</b>	<b>281</b>

## Figures

Figure 2-1: Example iDirect Network	4
Figure 2-2: iDirect IP Architecture	5
Figure 2-3: iDirect IP Architecture – Multiple VLANs per Remote	6
Figure 2-4: iDirect IP Architecture – VLAN Spanning Remotes	7
Figure 2-5: iDirect IP Architecture – Classic IP Configuration	8
Figure 2-6: iDirect IP Architecture – TDMA and iSCPC Topologies	9
Figure 3-1: Desktop Shortcuts for NMS GUI Clients	15
Figure 3-2: Windows Start Menu Entries for NMS GUI Clients	16
Figure 3-3: Bench Test Components in Initial NMS Tree	20
Figure 3-4: Filter Profile Examples	21
Figure 3-5: Traffic Profile Examples	21
Figure 3-6: BUC Examples	21
Figure 3-7: LNB Examples	21
Figure 3-8: iBuilder's Main Screen	24
Figure 3-9: Expand Tree Selection	26
Figure 3-10: Expanded Tree with Child Elements	26
Figure 3-11: Collapse Tree Selection	27
Figure 3-12: Collapsed Tree	27
Figure 3-13: View Menu Options	34
Figure 3-14: Right-Click Options	34
Figure 3-15: Example of Configuration States	38
Figure 3-16: Clicking Details	38
Figure 3-17: Network Highlighted in Tree	39
Figure 3-18: Result in Details View	39
Figure 3-19: Network Highlighted in Tree	39
Figure 3-20: Result in Details View	39
Figure 3-21: Configuration States of an iDirect Remote	51
Figure 5-1: Uplink VLAN Segment in a PP Blade Environment	88
Figure 6-1: Failover Sequence of Events, NMS Server Perspective	104
Figure 6-2: Failover Sequence of Events, NMS User Perspective	105
Figure 6-3: Inroute Group Relationships	107
Figure 7-1: Sample VLAN Network Layout	123
Figure 7-2: Figure: Using the Console's beamselector Command	153
Figure 8-1: Remotes Associated with Profiles	158
Figure 8-2: Downstream QoS (Left side of QoS pane)	166
Figure 8-3: Upstream QoS (Right side of QoS pane)	166
Figure 11-1: Global NMS Options Files	198
Figure 12-1: Revision Server Duty Cycle	209
Figure A-1: Sample Distributed NMS Configuration	260
Figure A-2: dbBackup and dbRestore with a Distributed NMS	271

## Tables

Table 3-1: Toolbar Icons and Functions	31
Table 13-1: User Types and Access Privileges	231
Table 13-2: Custom Privileges	231



# 1 Using this Guide

This chapter discusses how to use this manual. It contains the following sections:

- [“Intended Audience”](#)
- [“Document Conventions”](#)
- [“Informational Conventions”](#)

## 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.

- 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 Network Tree 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.

## 1.3 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 iDirect System Overview

As depicted in [Figure 2-1 “Example iDirect Network”, p. 4](#), an iDirect network is a satellite based TCP/IP network with a star topology in which a Time Division Multiplexed (TDM) broadcast downstream channel from a central hub location is shared by a number of remote nodes. The iDirect Hub equipment consists of an iDirect Hub Chassis with Universal Line Cards, a Protocol Processor (PP), a Network Management System (NMS) and the appropriate RF equipment. Each remote node consists of an iDirect broadband router and the appropriate external VSAT equipment. The remotes transmit to the hub on one or more shared upstream carriers using Deterministic-TDMA (D-TDMA), based on dynamic timeplan slot assignment generated at the Protocol Processor.

Beginning with iDirect release 7.0, a mesh overlay can be added to the basic star network topology, allowing traffic to pass directly between remote sites without traversing the hub. This allows real-time traffic to reach its destination in a single satellite hop, significantly reducing delay. It also saves the bandwidth required to retransmit mesh traffic from the hub to the destination remote. For a description of iDirect’s mesh overlay architecture, see [chapter 3, “Mesh Technical Description,”](#) of the [iDirect Technical Reference Guide](#).

The choice of upstream carriers is determined either at network acquisition time or dynamically at run-time, based on a network configuration setting. iDS software has features and controls that allow the system to be configured to provide QoS and other traffic engineered solutions to remote users. All network configuration, control, and monitoring functions are provided via the integrated NMS. The iDS software provides packet-based and network-based QoS, TCP acceleration, 3-DES or AES link encryption, local DNS cache on the remote, end-to-end VLAN tagging, dynamic routing protocol support via RIPv2 over the satellite link, multicast support via IGMPv2, and VoIP support via voice optimized features such as CRTP.

An iDirect network interfaces to the external world through IP over Ethernet via 10/100 Base-T ports on the remote unit and the Protocol Processor at the hub. The following figures, beginning with [Figure 2-2 “iDirect IP Architecture”, p. 5](#) describe the IP level configurations available to a network operator.

The iDS system allows you to mix traditional IP routing based networks with VLAN based configurations. This capability provides support for customers that have conflicting IP address ranges in a direct fashion, and to support multiple independent customers at a single remote site by configuring multiple VLANs directly on the remote.

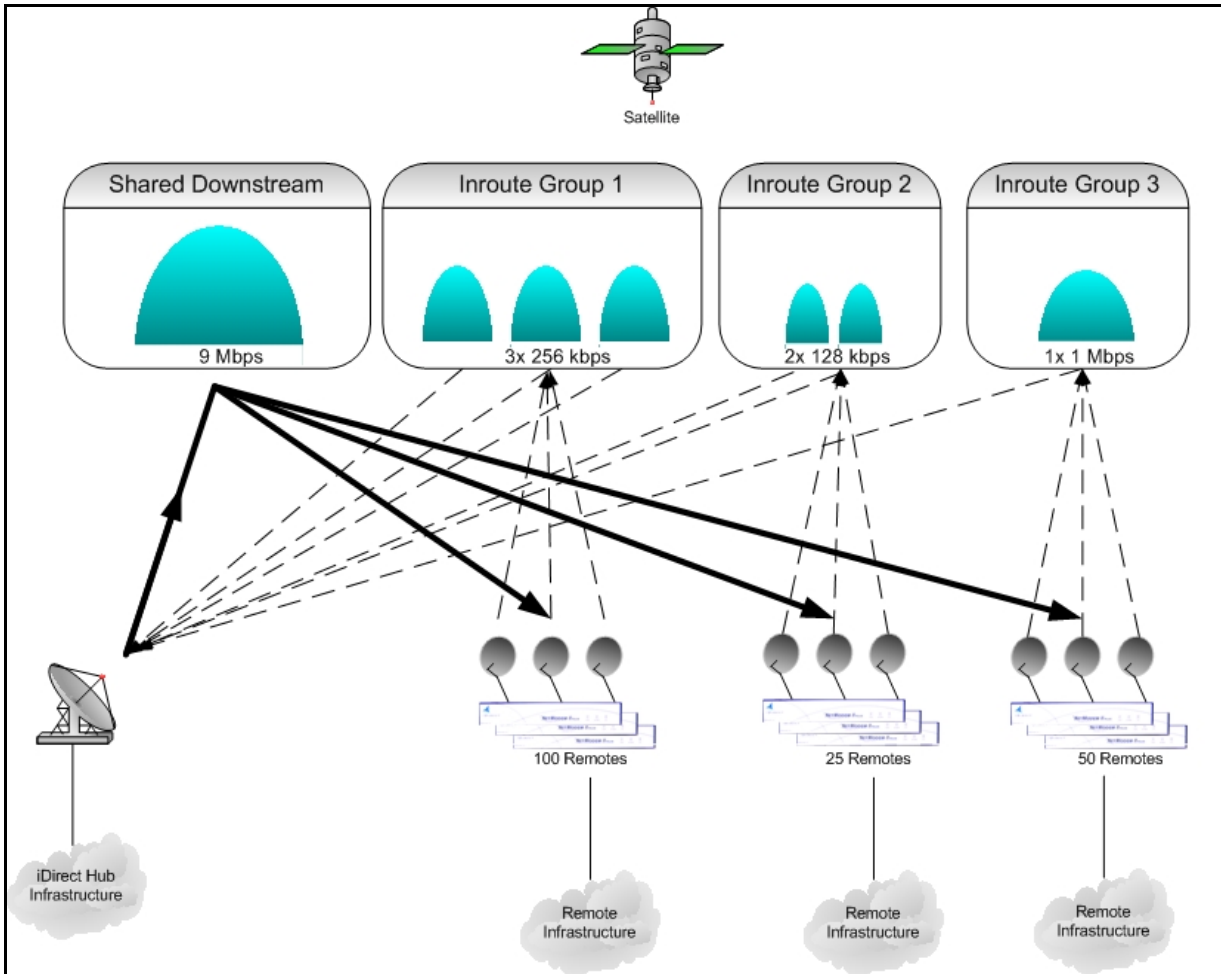


Figure 2-1: Example iDirect Network

In addition to end-to-end VLAN, the system supports RIPv2 in an end-to-end manner including over the satellite link; RIPv2 can be configured on per-network interface.

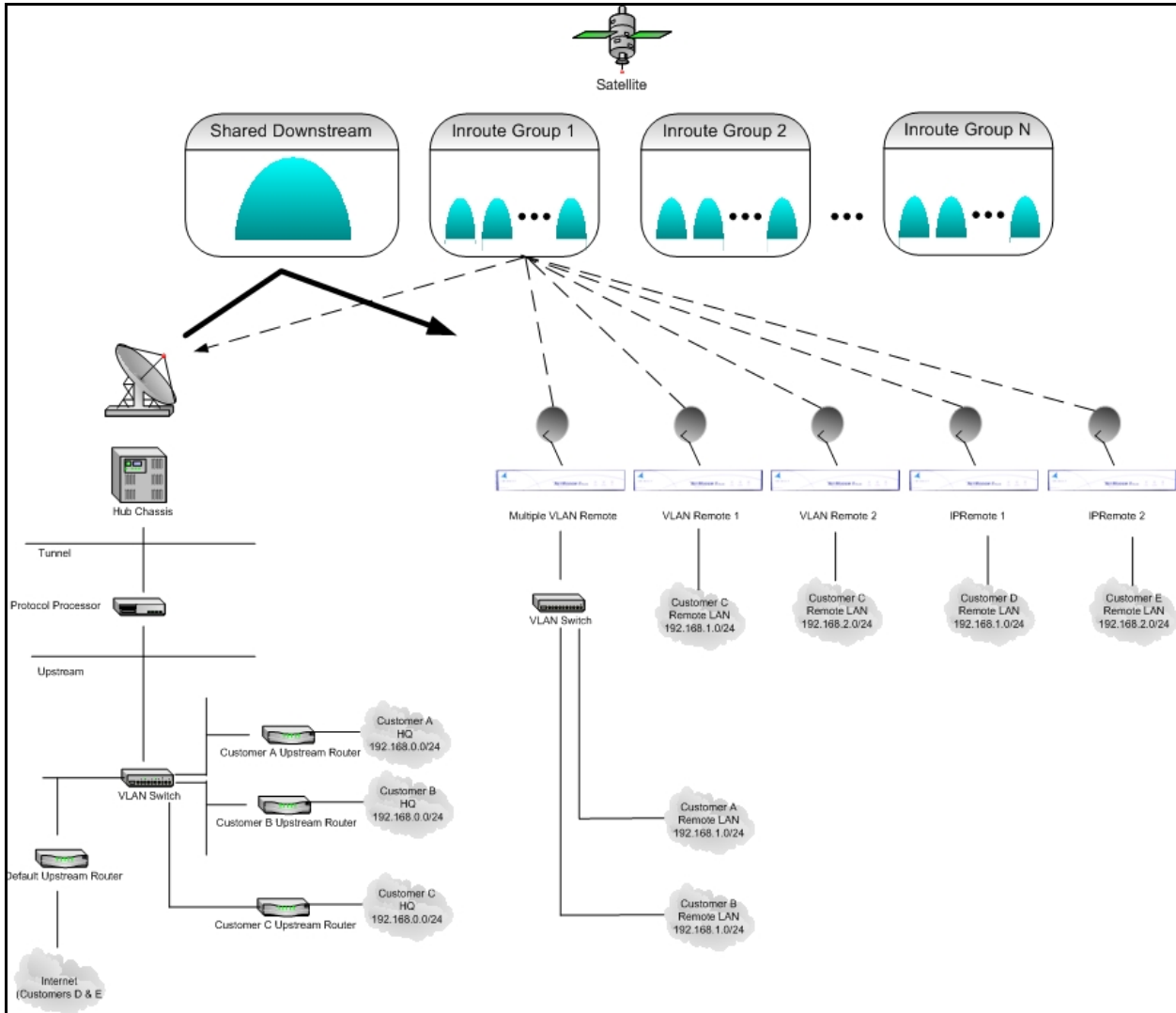


Figure 2-2: iDirect IP Architecture

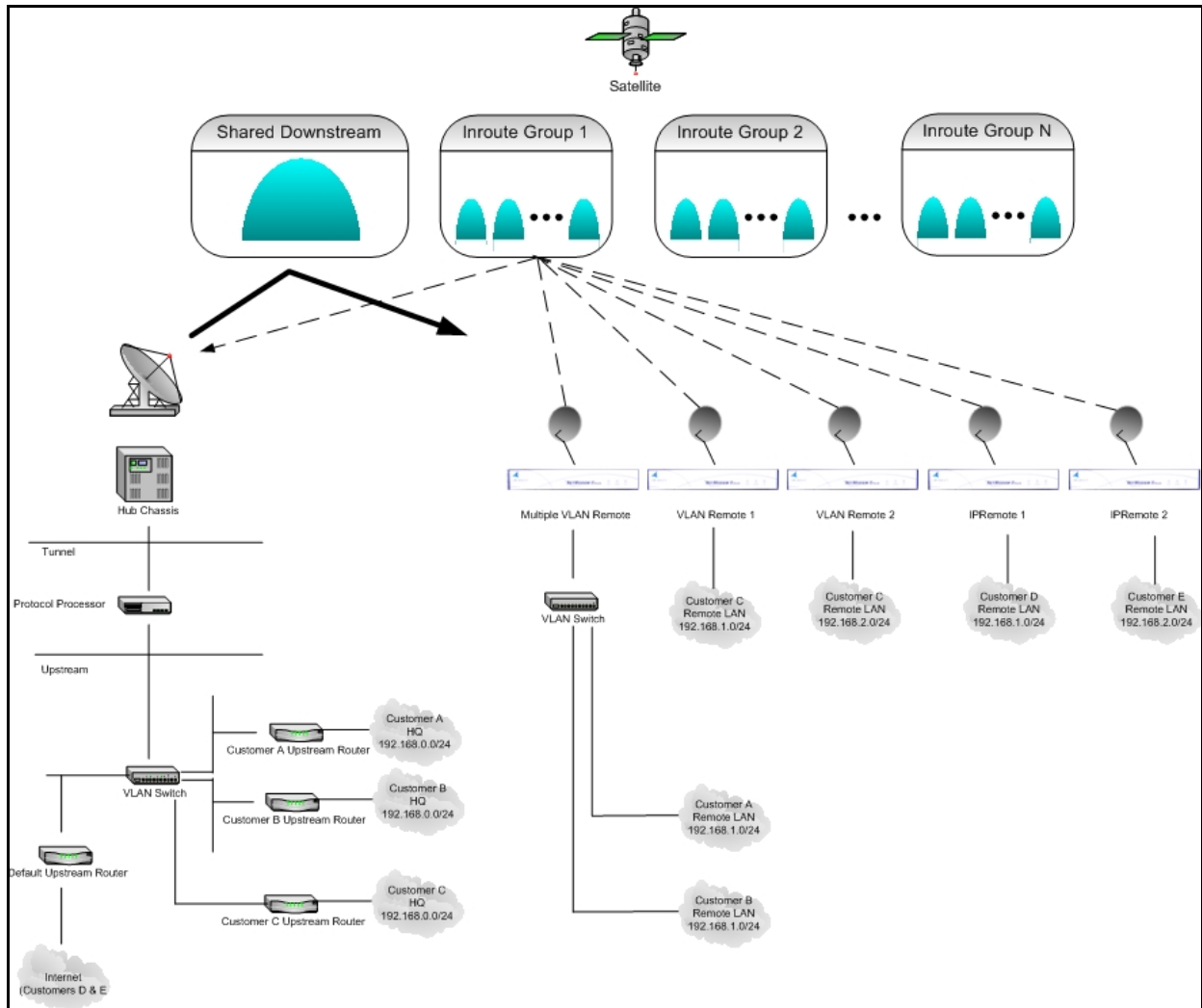


Figure 2-3: iDirect IP Architecture – Multiple VLANs per Remote

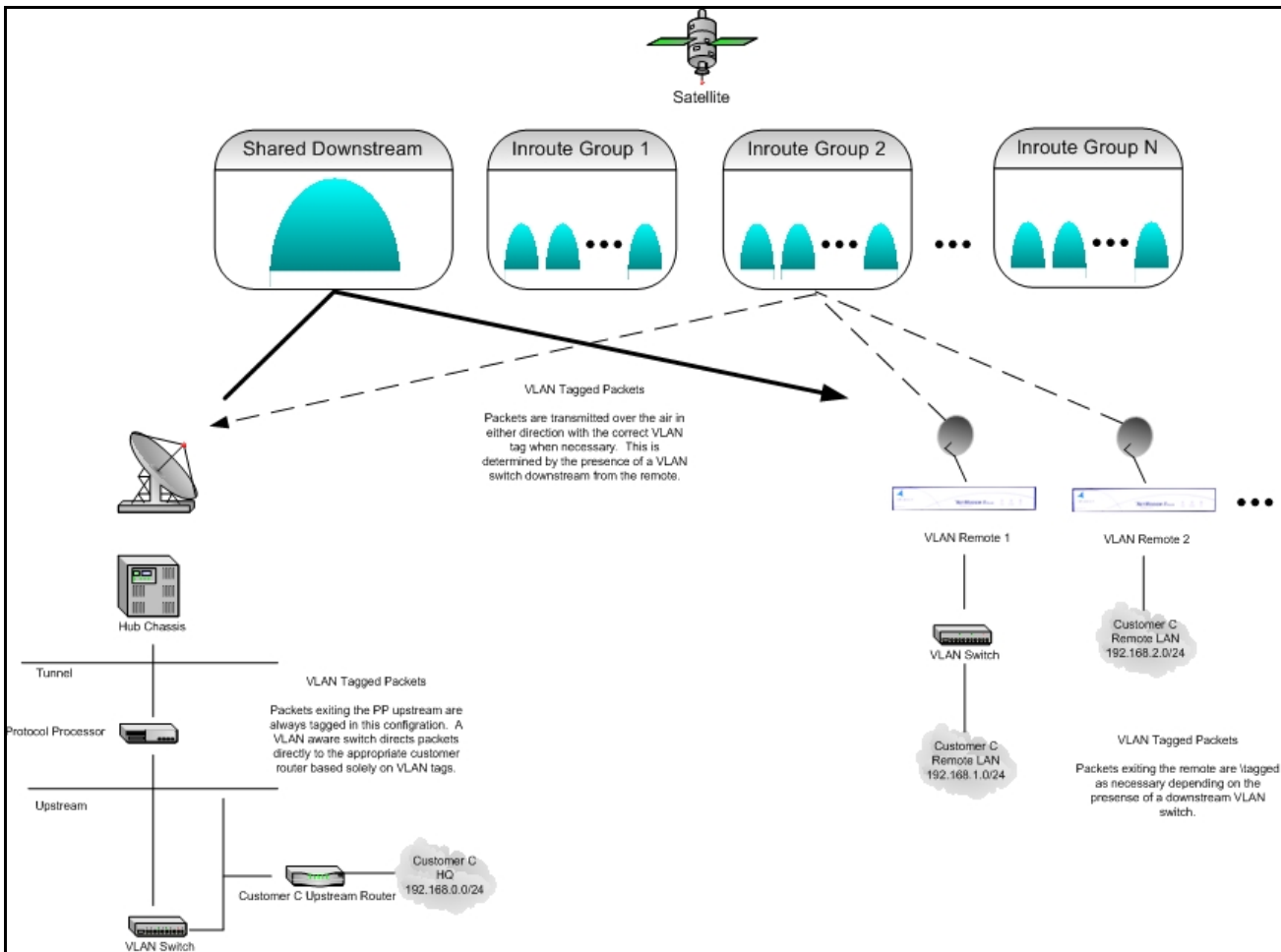


Figure 2-4: iDirect IP Architecture – VLAN Spanning Remotes

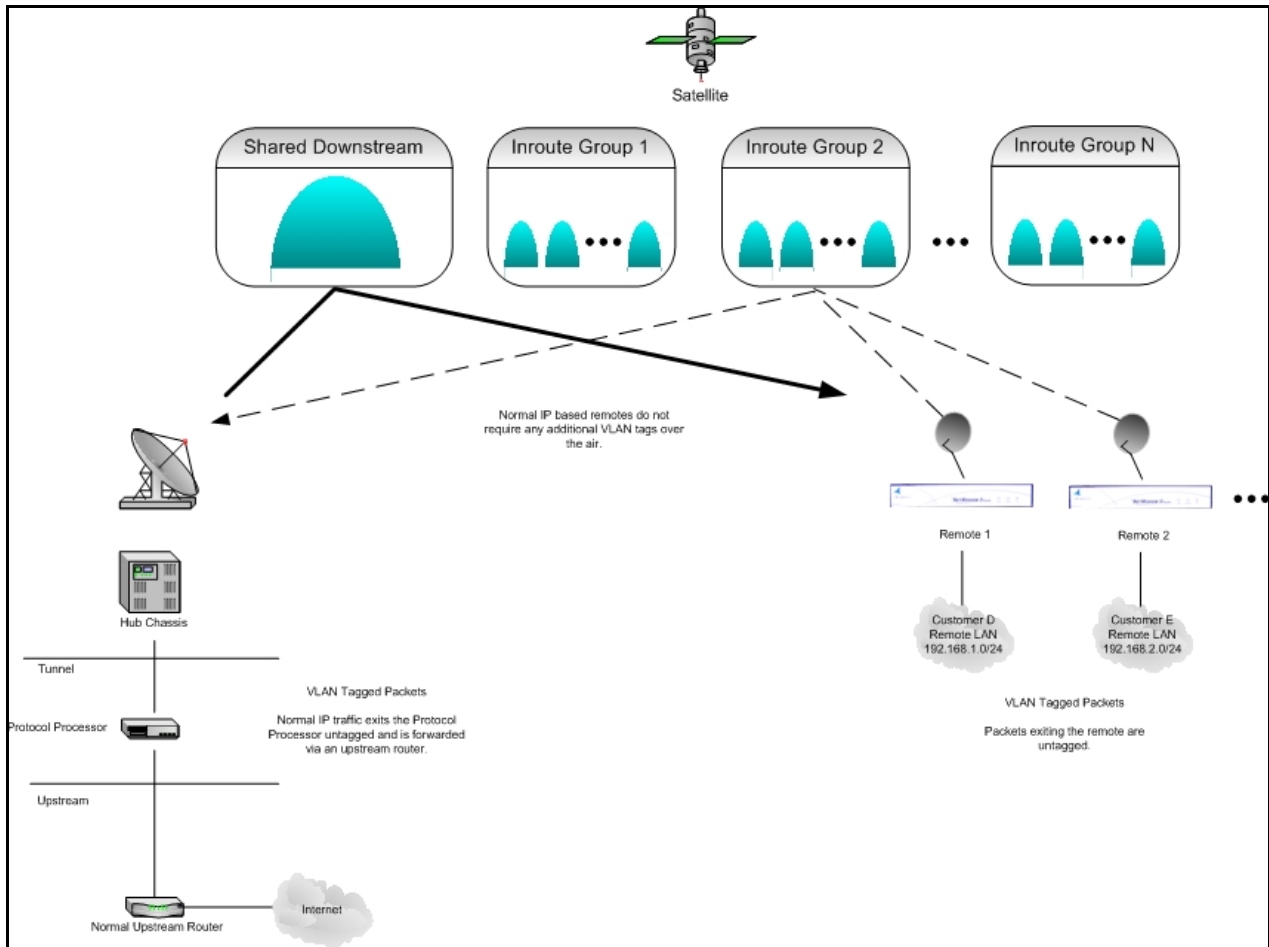


Figure 2-5: iDirect IP Architecture – Classic IP Configuration

In addition to the network architectures discussed so far, iDirect’s iSCPC solution allows you to configure, control and monitor point-to-point Single Carrier per Channel (SCPC) links. These links, sometimes referred to “trunks” or “bent pipes,” may terminate at your teleport, or they may be located elsewhere. Each end-point in an iSCPC link sends and receives data across a dedicated SCPC carrier. As with all SCPC channels, the bandwidth is constant and available to both sides at all times, regardless of the amount of data presented for transmission. SCPC links are less efficient in their use of space segment than are iDS TDMA networks. However, they are very useful for certain applications. [Figure 2-6](#) shows an iDirect system containing an iSCPC link as well as a TDMA network, all under the control of the NMS.



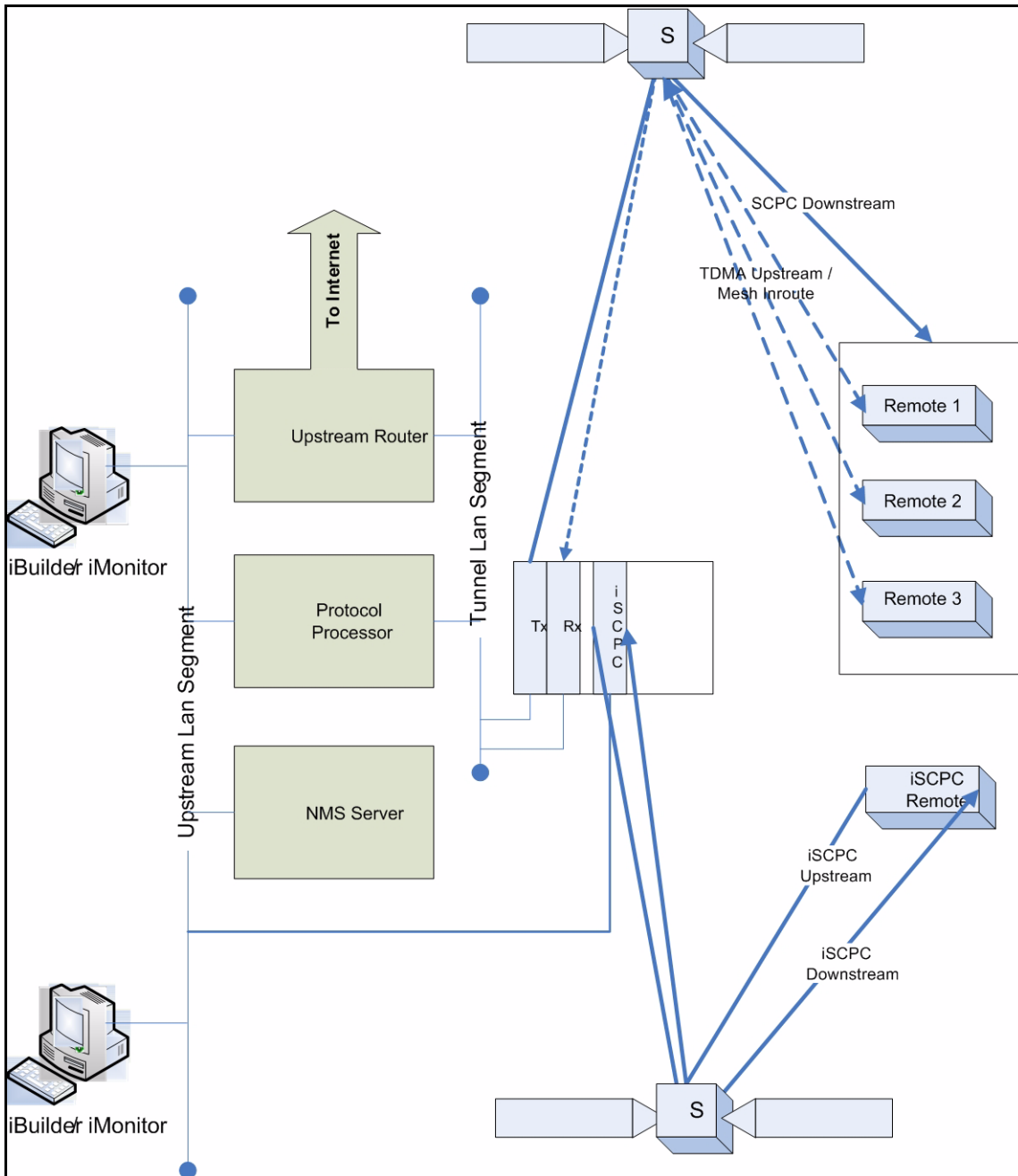


Figure 2-6: iDirect IP Architecture – TDMA and iSCPC Topologies



## 3 Overview of the Network Management System for iBuilder

This chapter presents an overview of the iBuilder network management tool for configuring your iDirect network. It contains the following sections:

- [“Introduction” on page 11](#)
- [“Gathering the Information You Need” on page 11](#)
- [“Preparing Equipment in Advance” on page 12](#)
- [“Components of the Network Management System” on page 12](#)
- [“Installing iBuilder, iMonitor, and iSite” on page 15](#)
- [“Launching iBuilder” on page 16](#)
- [“Pre-defined Components and Components Folders in iBuilder” on page 19](#)
- [“Using iBuilder’s Interface” on page 23](#)
- [“Customizing and Creating New Detail Views” on page 40](#)
- [“Working with Multiple Elements Simultaneously” on page 47](#)
- [“Configuration Status of Elements” on page 49](#)
- [“Understanding the Database’s Numbering Convention” on page 53](#)
- [“In Color versus Shaded Icons” on page 54](#)
- [“Configuring Warning Properties” on page 55](#)

### 3.1 Introduction

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

This chapter provides some of the most important information you will need to understand how iBuilder 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 iBuilder, how to use the many powerful tools available in iBuilder, how to create, customize, and print reports, and how to determine the configuration status of network elements.

### 3.2 Gathering the Information You Need

You must have the following information readily available when creating a new network.

- Spacecraft and carrier information, such as:

- Longitude (Geo location)
- Transponder translation frequency
- Hub Up/Down local oscillator
- LNB stability
- Carrier uplink and downlink frequencies
- FEC block sizes
- FEC blocks per outroute frame (See the *Network Planning Tool* and its *User Guide*.)
- Data rates
- Overall IP architecture plan for hub components
- Geographic location of the hub
- Line Card serial numbers and slot numbers
- Number of inroutes
- Tx/Rx or Tx-only line cards, depending on downstream/upstream data rates (Refer to [chapter 4, "iDirect Modulation Modes and FEC Rates,"](#) of the [iDirect Technical Reference Guide](#).)
- Frequency hopping (requires that a Reference Clock Module be installed on your hub chassis) or carrier grooming mode
- Remote serial numbers and geographic locations

### 3.3 Preparing Equipment in Advance

Before you begin configuring the network elements, you must have already commissioned your hub equipment. This involves the following:

- The NMS Server must already be installed and its interface defined.
- The Protocol Processor blades must already be installed and configured.
- The Chassis must already be installed and configured.
- Line Cards must have already been installed in the Chassis with their IP addresses defined using iSite.

### 3.4 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.

#### 3.4.1 NMS Applications

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

### **iBuilder**

The iBuilder application provides all configuration and control functions to network operators. **Configuration** options consist of creating network elements (e.g. networks, line cards, remotes) and specifying their operational parameters, such as QoS profiles or IP addresses. **Control** options consist of applying the specified configurations to the actual network elements, retrieving active configurations, resetting elements, and upgrading element software and firmware.

### **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. Refer to *Network Management System iMonitor User Guide* for 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 *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.

## 3.4.2 Server Components

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

### **Configuration Server**

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

### **Real-time Data Server**

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

### **Event Server**

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

### **Latency Server**

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

### **NMS Controller Server**

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

### **PP Controller Servers**

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

### **NMS Monitor Script**

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

### **Consolidation Script**

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

### **Database Backup Script**

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

### **Database Restore Script**

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

## **3.5 Installing iBuilder, iMonitor, and iSite**

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

### **3.5.1 System Requirements**

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

- Windows 2000 WorkStation, Service Pack 3 or later
- Windows XP WorkStation

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

### **3.5.2 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 the clients, copy the *nms\_clients\_setup.exe* file to the target PC, double-click it, and follow the prompts.

By default, the clients are installed on your desktop in the following folder:

- *iDIRECT NMS Clients <version>*, where *version* is the iDirect release number.

The installer automatically adds the appropriate entries in the Windows **Start** menu. Click **Start** → **All Programs** → **iDirect** → **NMS Clients 7.0**. The iBuilder, iMonitor, and iSite clients are displayed, along with an **Uninstall** selection.

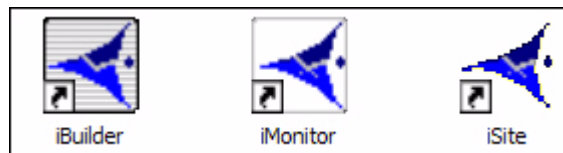


Figure 3-1: Desktop Shortcuts for NMS GUI Clients



Figure 3-2: 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*.

### 3.6 Launching iBuilder

iBuilder is initially installed with two default accounts: “admin” and “guest”. The admin user has full access privileges to all iBuilder 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 [chapter 13, “Creating and Managing User Accounts and User Groups.”](#)

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.

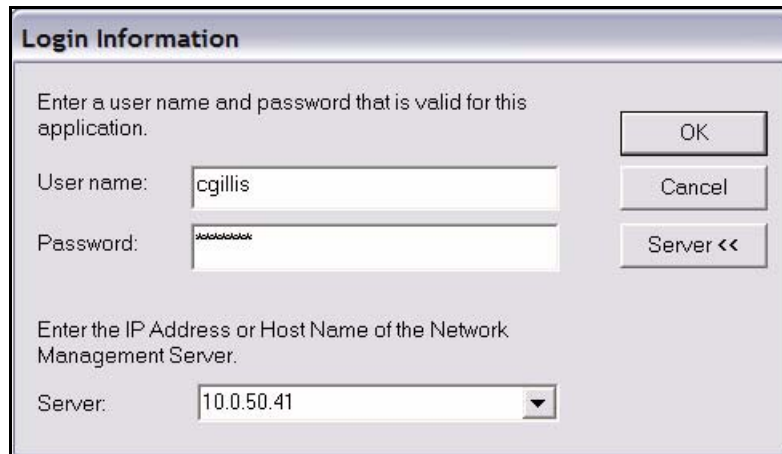
- Step 1 To launch iBuilder, double-click the desktop shortcut or select it from the Windows **Start** menu.
- Step 2 Enter your user name and password in the **Login Information** dialog box.
- Step 3 Click **Server** and select the IP address or host name of your primary NMS Server machine. The Server 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 the iBuilder version must match the NMS server version in order for you to log in. (For example, version 6.0.0 of iBuilder may connect only to version 6.0.0 of the NMS servers.)





**Login Information**

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

User name:

Password:

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

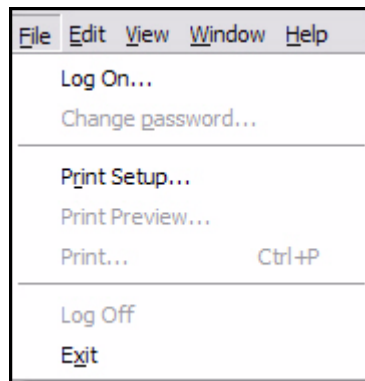
Server:

Buttons: OK, Cancel, Server <<

The iBuilder 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, iBuilder 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 iBuilder. 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.

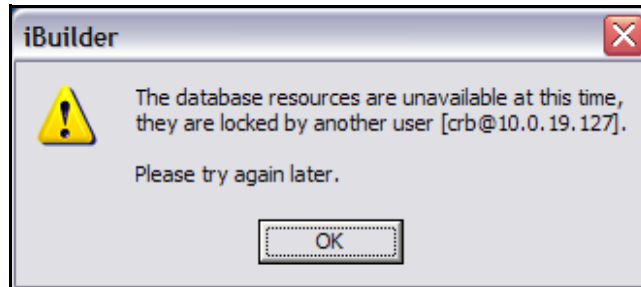


**Multiple Users or PCs Accessing the NMS**

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 iBuilder and/or 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 iBuilder and/or iMonitor at any given time and connect to the same server at the same time.

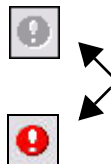
3. Only one iBuilder user may have a **Modify Configuration** dialog box open at any given time. If another user tries to modify a record when someone else already has a Modify, or configuration, dialog box open, an error message is displayed on the PC of the other user, and they are not allowed to change anything in the database.



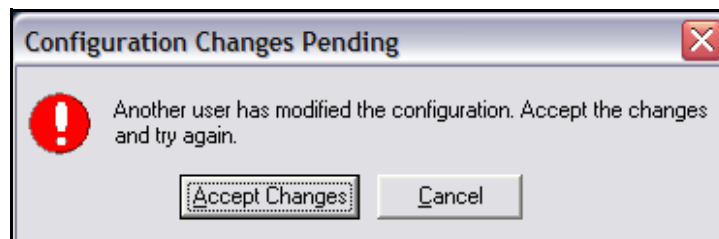
### **Accepting Changes**

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

When the other user changes the configuration, the **Accept Changes** button on your toolbar changes color from gray to red (For more information, see [Table 3-1, "Toolbar Icons and Functions,"](#) on page 31).



If you attempt to modify the network configuration without accepting changes, the following warning message appears:



Before you accept the changes, you may view the other user's changes by selecting **View → Configuration Changes** (see ["Configuration Changes Pane" on page 37](#)). To accept the changes and update your view of iBuilder, click **Accept Changes**. Any modifications the other user has made are now displayed in your copy of iBuilder.

## 3.7 Pre-defined Components and Components Folders in iBuilder

iDirect has designed the Network Management System to be as easy to use as possible, and therefore has added several components and components folder entries to iBuilder to get you started. These pre-defined components and folders exist in iBuilder when you launch it for the first time. The elements and folder entries can be re-used as you create new networks.

iBuilder is shipped with the following pre-defined and re-usable components and components folders:

- Bench Test Components for I/F Networks
  - Spacecraft
  - Transponder
  - Bandwidth
  - Up/Downstream Carriers
- Components Folders Containing Critical Information
  - Remote Antenna Components
    - BUCs
    - LNBS
  - QoS
    - Up/Downstream Filters
    - Up/Downstream Traffic Profiles
- Components Folders Containing Reference Information
  - Manufacturers

### 3.7.1 Bench Test Components

The components that exist in the system when it is displayed for the very first time at your site include:

- Bench Test Components for I/F Networks, that were set up for testing purposes prior to shipping. They include the following elements which can be modified to have their names and other properties changed to match the needs of your network:
  - a spacecraft
  - a transponder
  - a BUC
  - an LNB
  - bandwidth
  - an upstream and downstream carrier

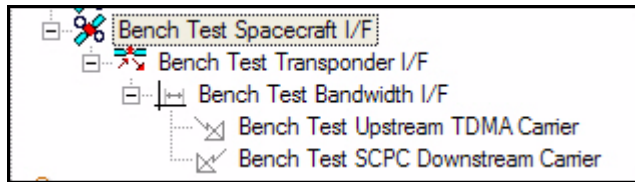


Figure 3-3: Bench Test Components in Initial NMS Tree

### 3.7.2 Components Folders

Several folders are built into iBuilder for your convenience, some of which have pre-defined entries, and others of which require you to add the entries yourself. Some of these folders contain entries that are critical to the configurations of various elements within the system, whereas other folders contain information that is used only for reference and network record-keeping. You can add additional entries to either type of folder. For instructions on how to add entries to folders, see [“Adding Entries to Folders” on page 22](#).

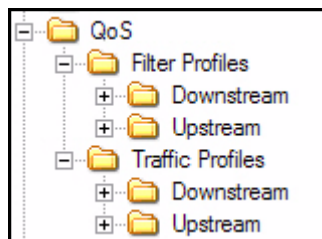
#### 3.7.2.1 Folders Containing Critical Information

These folders contain entries that are critical when configuring a given component. At initial deployment, these folders already contain entries that iDirect has defined. The folders containing critical information include:

- QoS
- Components
  - Remote Antenna Components
  - Hub RFT Components

#### QoS

This folder contains a number of subfolders, such as the Up/Downstream Filter Profiles and Up/Downstream Traffic Profiles folders shown below. The entries listed in the figures below are examples of default profiles developed by iDirect for use on iDirect products.



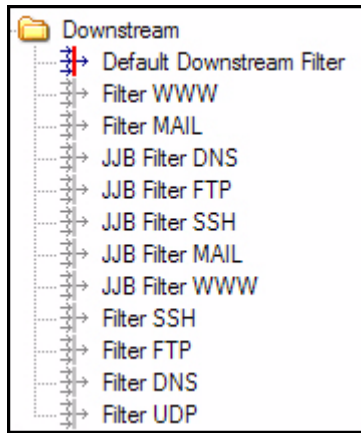


Figure 3-4: Filter Profile Examples

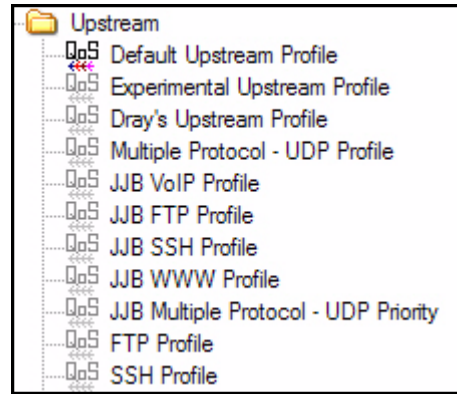


Figure 3-5: Traffic Profile Examples

**Components: Remote Antenna Components**

This folder contains a number of subfolders, such as the BUC and LNB folders shown below. The entries listed in the figures below are examples of BUCs and LNBs certified by iDirect for use on iDirect products. These lists are only partial lists.

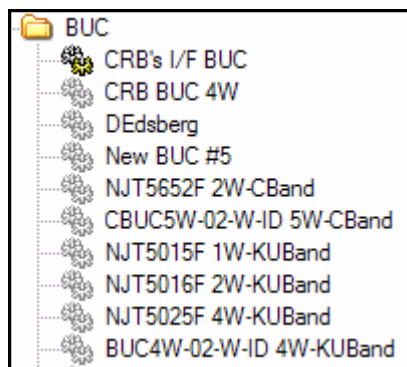
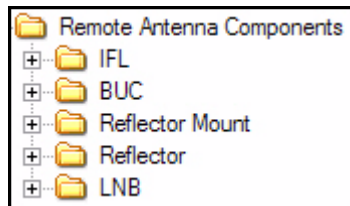


Figure 3-6: BUC Examples

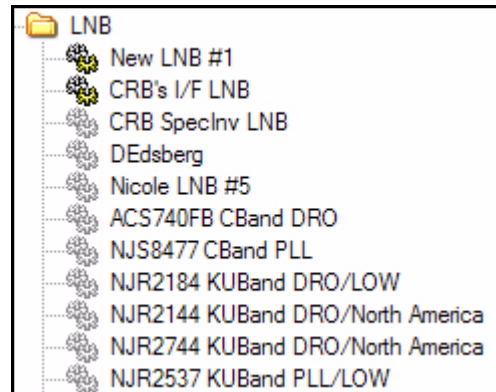


Figure 3-7: LNB Examples

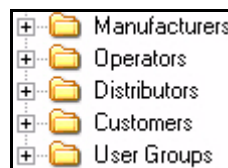
### **Components: Hub RFT Components**

For detailed instructions on defining components within the Hub RFT Components folder, see [“Preparing the Hub RFT Components Folders” on page 61.](#)

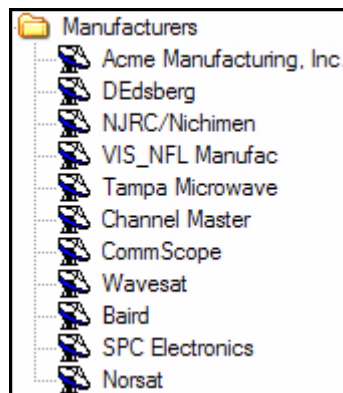
### **3.7.2.2 Folders Containing Reference Information**

The information in these folders are for convenience purposes only and are not used to operate the NMS or any of iDirect’s equipment. However, entries from these folders can be selected from drop-down lists on various configuration dialog boxes throughout the system so that the information is at your fingertips if you need it.

These folders include Manufacturers, Distributors, Operators, Customers and User Groups, as shown below.



An example of entries in the Manufacturers folder is shown below.

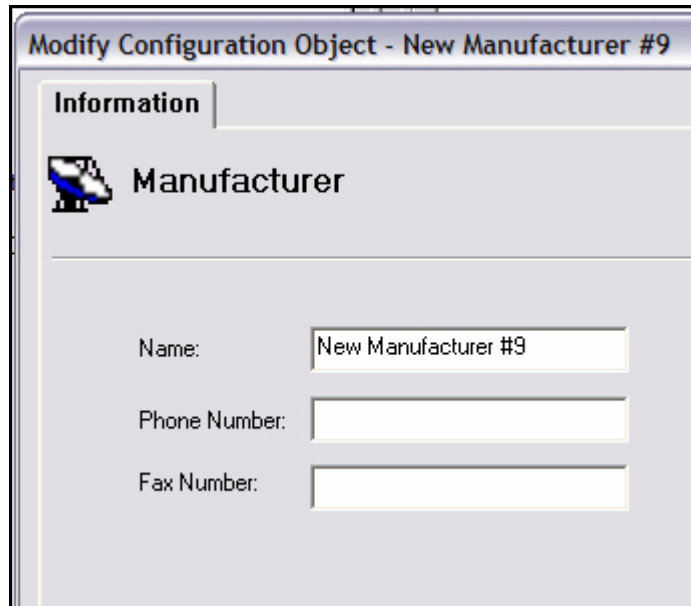
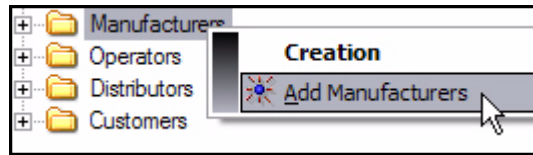


### **3.7.2.3 Adding Entries to Folders**

You can add entries to any folder, whether it has pre-defined entries in it or not. Selections in these folders should be added prior to configuring other elements of the system, as the information in the folders listed above will be requested in various configuration panes throughout the system. Not having a selection defined in a given folder will result in your not being able to select that entry when a configuration dialog box requests it. This could add additional steps to the configuration process because an element may remain “Incomplete” until a required component or subcomponent entry is created and selected on a given element’s configuration dialog box.

You can add additional entries to any folder by right-clicking on the folder and selecting **Add [type of component]**. For example, you can right-click **Manufacturers** and select **Add Manufacturer**. A

dialog box appears allowing you to define a new manufacturer. When you have input the information, click **OK** in the lower right corner of the dialog box (not shown).



### 3.7.2.4 Canceling an Entry

Clicking Cancel in any of the dialog boxes will cancel your current entries.

## 3.8 Using iBuilder's Interface

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



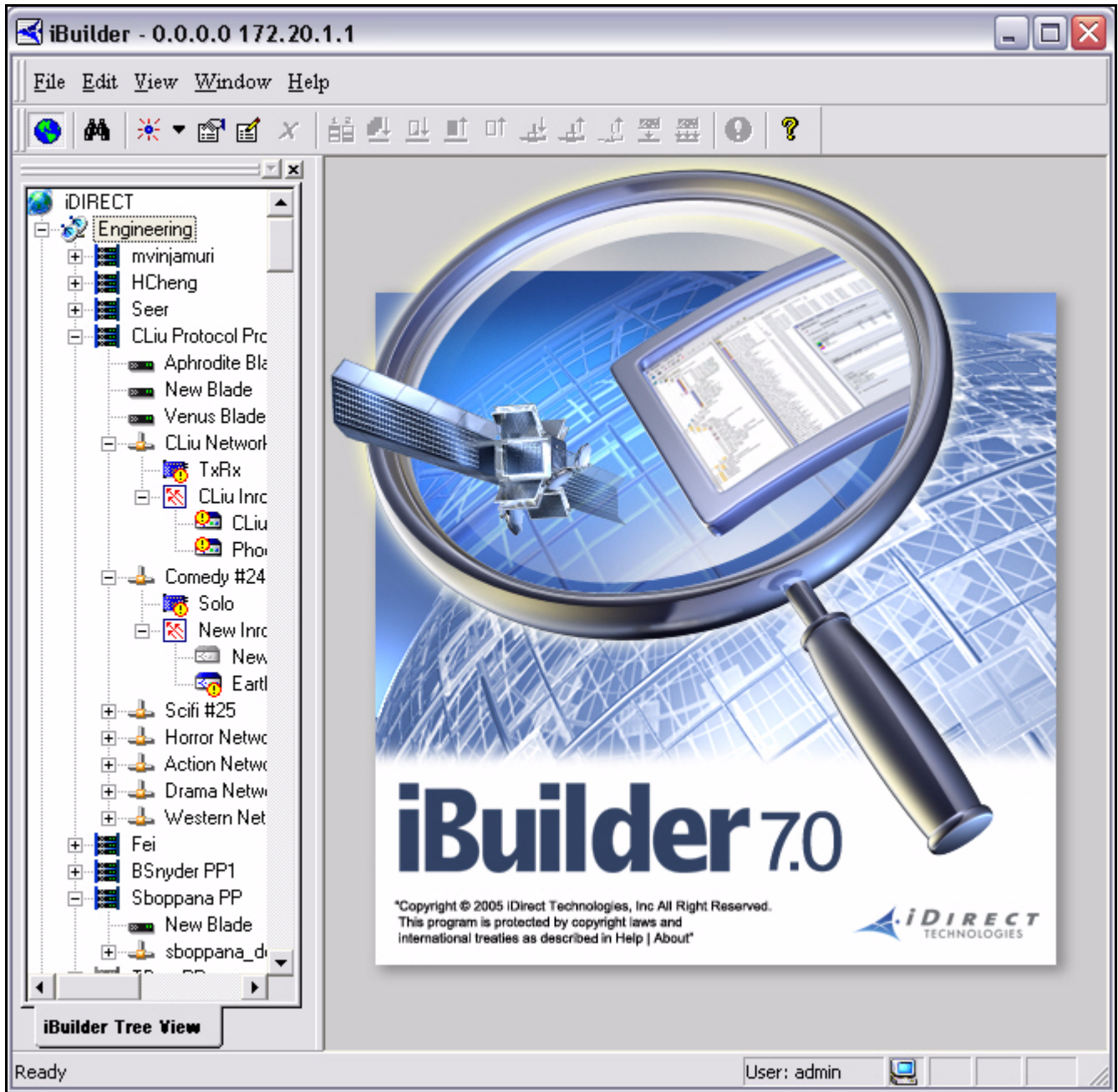


Figure 3-8: iBuilder's Main Screen

### 3.8.1 Clicking on Elements and Folders: What Happens?

#### Right-Clicking

In general, you must right-click (or use the context-sensitive mouse button) on your mouse to display any list of options that can be performed on the element you currently have selected.



### **Double-Clicking vs. Single-Clicking**

You can double-click any network element/component in the Tree to automatically display its properties in read-only mode.

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 or folder. Once an element has no plus sign or minus sign next to it, you can double-click any element to view the Properties for that element in read-only mode.

For example, if the Hub RFT Components folder has a plus sign (+) next to it, you can double-click it to expand it to see the four folders at the next level: Antenna, Up Converter, Down Converter, and HPA. You can double-click any folder with a plus sign next to it to expand it to the next level. However, once the folder is fully expanded and the elements within it are displayed, if you double-click the actual element, the Properties for that element are displayed in read-only mode.

## **3.8.2 Globe**

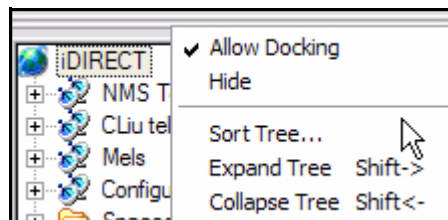
### **Using the Docking Feature**

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

### **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.

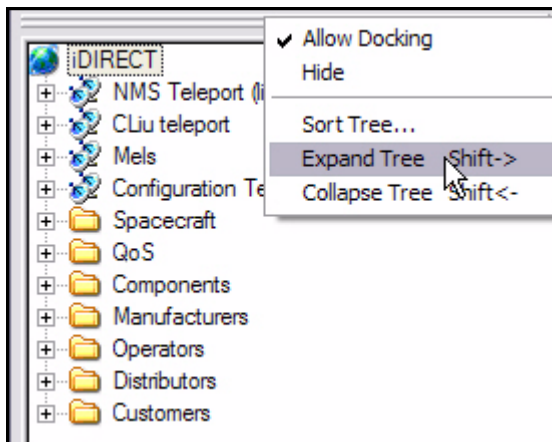


Figure 3-9: Expand Tree Selection

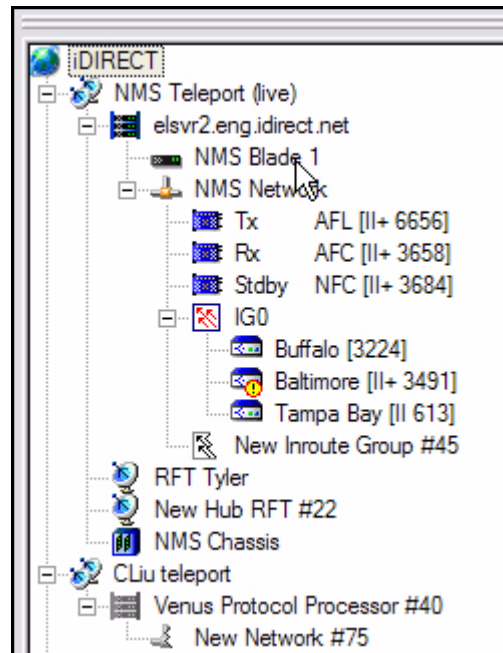


Figure 3-10: Expanded Tree with Child Elements

### **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.

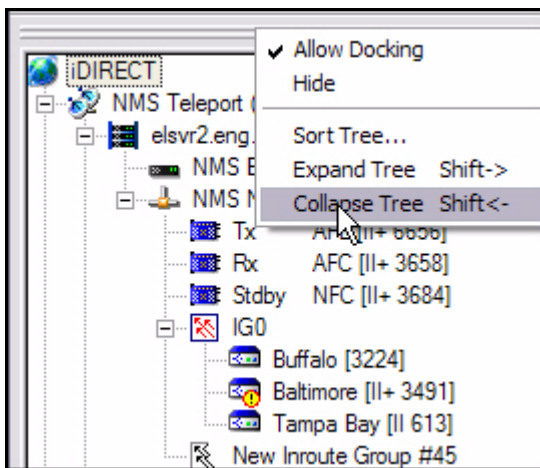


Figure 3-11: Collapse Tree Selection

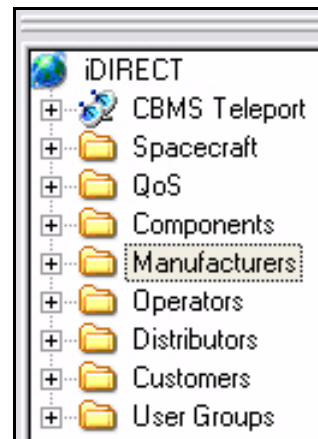


Figure 3-12: Collapsed Tree

### Sorting Columns

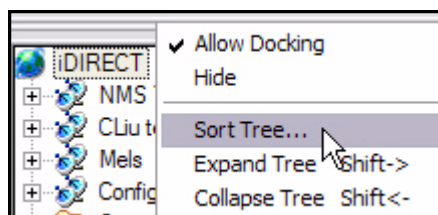
In any pane with columns, or list controls, you can sort the entries in the pane by the values in any column by clicking on the column heading. In the example below, the Active Users Pane has been sorted on **Group** by clicking the column heading.

Name	Group ▲	Permissions	Logged On
C1	CNO1	Super User	No
C2	CNO1	Guest	No
admin	System	Super User	Yes - iBuilder(4), iMonitor(3)
guest	System	Guest	No
V1	VNO1	Super User	No
V2	VNO1	Guest	No

### Sorting the Tree

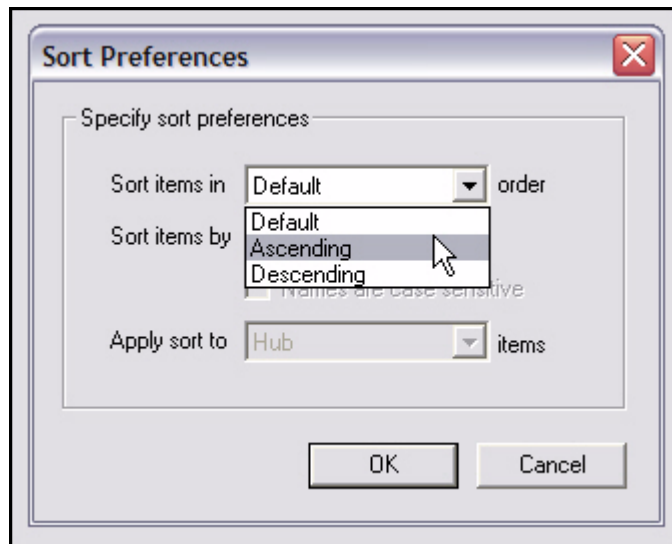
To sort the Tree, follow the steps below:

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

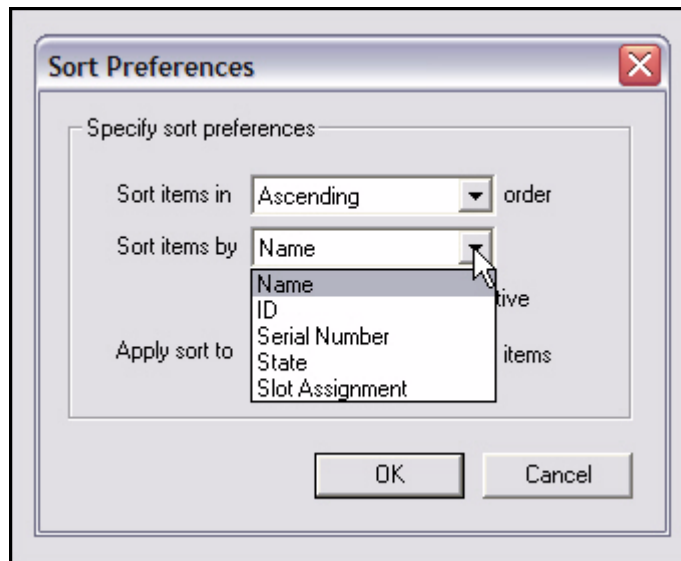


- Step 2 The **Sort Preferences** dialog box is displayed.

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.

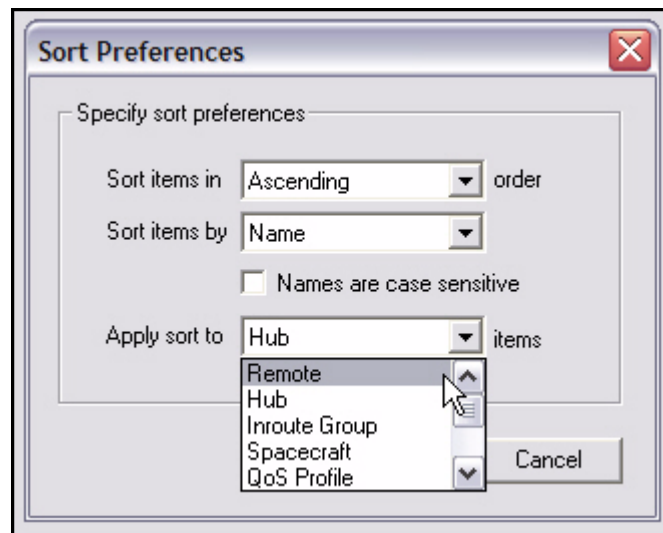


Step 5 If you select **Name**, either click the **Names are case sensitive** check box or clear it.

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

- Remote

- Hub
- Inroute Group
- Spacecraft
- QoS Profile
- Component
- Manufacturer
- Operator
- Distributor



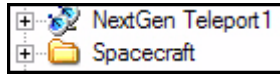
Step 7 Click **OK**. The next time you log in, iBuilder will remember and display the last sort preference you chose.

### 3.8.3 Network Tree

The Network Tree is the primary navigation tool in iBuilder. It contains all of the elements of your network, structured hierarchically. Each element in the tree contains a context-sensitive menu accessible from your mouse's *context menu* button (typically the right mouse button). By right-clicking a tree element, a submenu of options appears, which you may click to use to configure or view various types of data and other information used to operate your network. For example, Teleport or Transponder appear in the submenus of Tree elements. For specific information on these selections, see the section on that particular option. Use the **Contents** or **Index** of this book to locate this information.

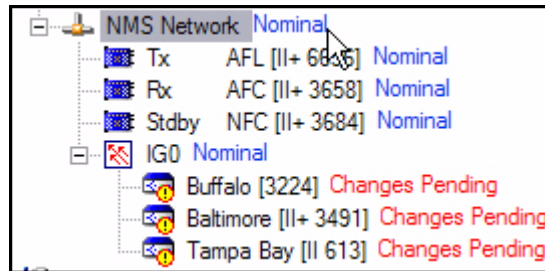
Most elements and entries in the Tree are necessary to operate the network. However, some folders are provided simply to enable you to add informational entries for reference and record-keeping. These reference folders include the Manufacturers folder, Operators folder, Distributors folder, and Customers folder.

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

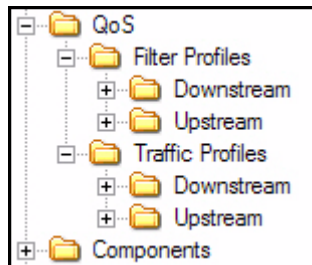


A *minus sign (-)* next to an element or folder indicates that the element or folder has been completely expanded and has no other child entries below this level, or branch, in the Tree, other than the children that are currently visible.

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



In the example below, the QoS folder has been expanded as far as it can be. The QoS folder cannot include children in another folder on the same branch of the tree; therefore, its only children are the Filter Profiles and Traffic Profiles folders. The Filter Profiles and Traffic Profiles folders are parents to the Downstream and Upstream folders that can be expanded by clicking their *plus signs (+)* to reveal their children folders or elements below them in the Tree.



### 3.8.4 Using the Interface Toolbars and Menu Options

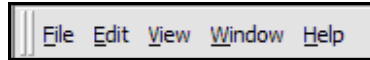
#### Title Bar

The **Title** bar identifies the name of the application (in this case, iBuilder) 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 **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 3-1, “Toolbar Icons and Functions,” on page 31](#).



**Table 3-1: Toolbar Icons and Functions**

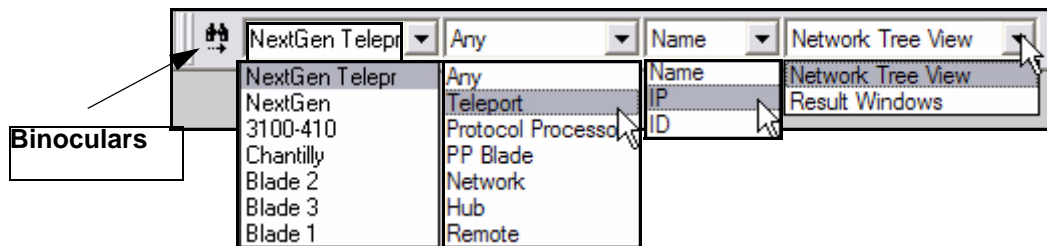
Toolbar Icon	Functionality
	Allows you to view elements in the Network Tree Menu hierarchy
	Displays the Find dialog box
	Opens the Modify Configuration dialog box of a highlighted parent element in the Tree, allowing you to create a new child element for that parent. If the highlighted element you select before clicking this button has no children elements, this icon will become unselectable and is displayed in gray.
	Allows you to add an element to the Tree. If the element in the Tree that is highlighted before you click this icon does not have the capability to allow you to add anything, the icon will become unselectable and be displayed in gray.
	Allows you to view the properties of the highlighted element in the Tree in Read-Only mode
	Allows you to view and edit the highlighted element in the Tree.
	Allows you to delete a highlighted element in the Tree. You CANNOT delete parent node elements if they have children (sub) elements.
	Allows you to compare two configurations
	Allows you to apply multiple configurations

**Table 3-1: Toolbar Icons and Functions (Continued)**

Toolbar Icon	Functionality
	Allows you to apply a TCP configuration
	Allows you to retrieve the Active Configuration
	Allows you to retrieve the Saved Configuration
	Allows you to apply a TCP network configuration
	Allows you to retrieve the Active Network Configuration
	Allows you to retrieve the Saved Network Configuration
	Allows you to download firmware images to remote modems and line cards
	Allows you to perform a multicast package download
	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 means that you are accepting the fact that changes have been made since the time of your last login.
	Allows you to view the version number of the NMS as well as system information

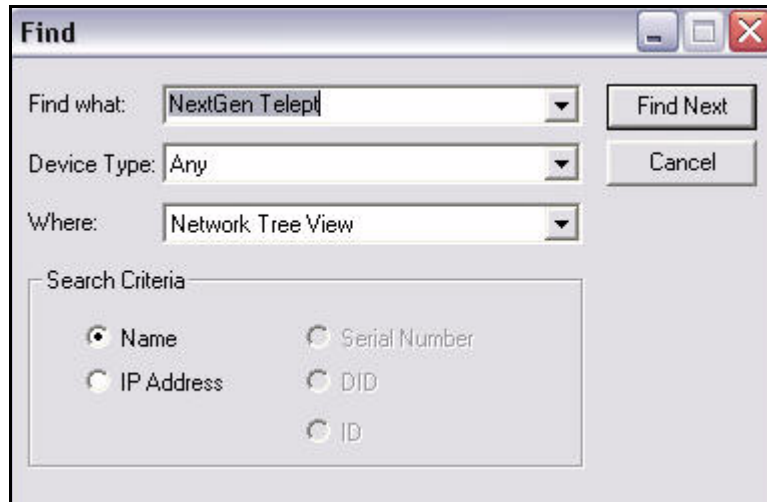
### **Find Toolbar**

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 illustrates the various options within each category.



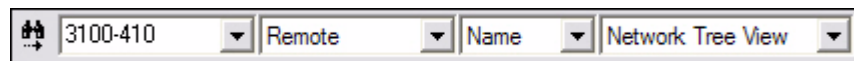


You can also click the **Find** button on the toolbar to open a dialog box that gives you the same options.

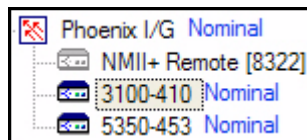


To perform a search, follow the steps below:

- 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.



## 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.

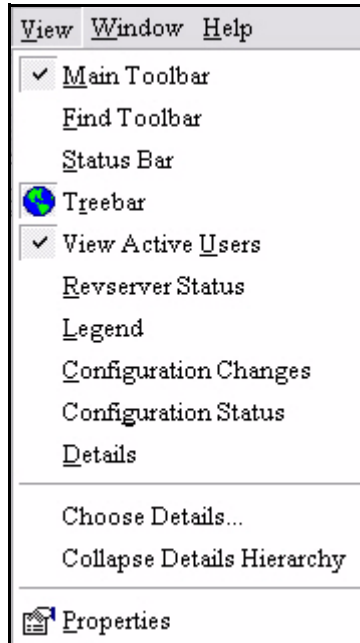


Figure 3-13: View Menu Options

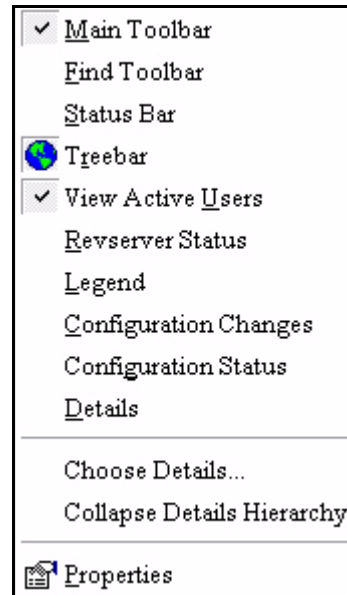
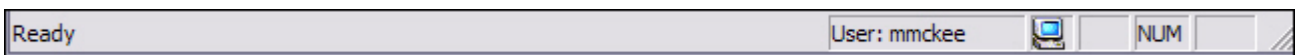


Figure 3-14: Right-Click Options

As you can see, the options on the View menu and those available by right clicking at the top of the window are the same.

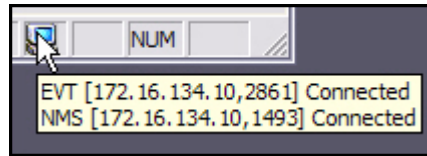
## Status Bar

The **Status** bar is located at the bottom of the iBuilder 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 server that you are currently connected to is displayed.

























### Active Users Pane

The **Active Users** option and usage is discussed in more detail in [“Managing Accounts from the Active Users Pane” on page 227](#). However, if you select **View** → **Active Users**, the pane displays a list of all defined users, along with their permissions, user groups, and current log in status.

Name ▲	Group	Permissions	Logged On
 admin	System	Super User	Yes - iBuilder(1)
 advance	System	DatabaseRe...	No
 bsnyder	System	Super User	No
 cliu	System	Super User	No
 dedenberg	System	Super User	No
 dray	System	Super User	No
 fzhao	System	Super User	No
 guest	System	Guest	No
 hcheng	System	Super User	Yes - iBuilder(1)
 Maruthi	System	Super User	No
 seer	System	Super User	Yes - iBuilder(1)
 sushmitha	System	Super User	Yes - iBuilder(1), iMonitor(1)
 vokan	System	Super User	No

## **Legend Pane**

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

CONFIGURATION STATE	DESCRIPTION
<b>REMOTE MODEM</b>	
 Nominal	Activated, no changes to apply
 Changes Pending	Activated, configuration changes not yet applied
 Deactivated or Never Applied	Not active in the network or configuration not yet applied
 Incomplete	Configuration not completely specified
 Unknown	Unknown configuration status
<b>HUB MODEM</b>	
 Nominal	No changes to apply
 Changes Pending	Configuration changes not yet applied
 Never Applied	Configuration not yet applied
 Incomplete	Configuration not completely specified
 Unknown	Unknown configuration status
<b>INROUTE GROUP</b>	
 Nominal	Normal
 Incomplete	Inroute Group not completely specified
<b>NETWORK</b>	
 Nominal	No changes to apply
 Changes Pending	Configuration changes not yet applied
 Never Applied	Configuration not yet applied
 Incomplete	Configuration not completely specified
 Unknown	Unknown configuration status
<b>CHASSIS</b>	
 Nominal	No changes to apply
 Changes Pending	Configuration changes not yet applied
 Never Applied	Configuration not yet applied
 Incomplete	Configuration not completely specified
 Unknown	Unknown configuration status

### **Configuration Changes Pane**

If another user changes the database, the **Accept Configuration Changes** icon on your toolbar will become active.



If you want to view the changes in iBuilder before you click the icon to accept them, select **Configuration Changes** from the View menu to display the **Configuration Changes** pane. You can click the arrow to the left of each item to see more detail. The figure below shows the changes that will appear if another user creates a new remote.

Events (8 items)	Objects
13:15:25 ADD	
Object Type	Remote Antenna
Object ID	5
User	admin@10.0.50.61
▶ 13:15:25 ADD	New Remote
▶ 13:15:25 ADD	
▶ 13:15:25 ADD	
▶ 13:15:25 ADD	
▶ 13:15:25 ADD	
▶ 13:15:25 ADD	
▶ 13:15:25 ADD	
▶ 13:15:25 MODIFY	New Remote #8

Note that creating a single remote results in a number of separate objects being created: antenna, remote, default VLAN, etc. When you click the **Accept Configuration Changes** Icon, all entries will be cleared from the Configuration Changes Pane.

### **Configuration Status View**

**Configuration Status** is discussed in detail in [“Configuration Status of Elements” on page 49](#). Configuration States are identified by both icons and color-coded words on either side of their corresponding element in the network as shown below. The legend details the meanings of the various icons and color-coded words. (See [“Legend Pane” on page 36](#).)

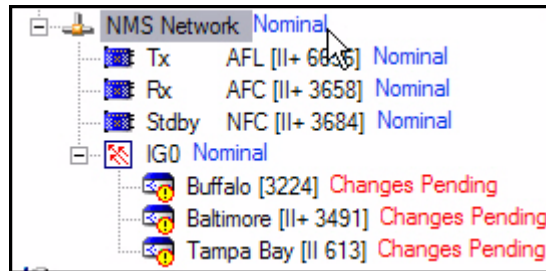


Figure 3-15: Example of Configuration States

### Properties View

The Properties view shows the properties of a highlighted element in the Tree, in Read-Only mode. To view properties via the **View** menu, click an element in the **Tree** and select **View** → **Properties**, or simply double-click on the element.

### Details

The NMS is shipped with predefined sets of details that may be viewed for any given element in the Tree. Different elements have different predefined details. To view the details of a given element's children who reside at the next level down in the tree, select **View** → **Details**.

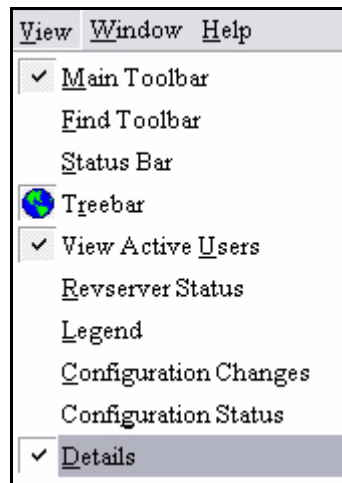


Figure 3-16: Clicking Details

The **Details** view allows you to sort, view and print a number of details, including the real-time states, of all or some of the elements under the parent node you have highlighted in the Tree. For example, if you click a **Network** in the Tree, as shown in [Figure 3-17](#), you can view the details about that network's children (such as line cards and Inroute Groups) who reside on the same level of the Tree, as shown in [Figure 3-18](#). Notice that the remote in the Tree is not displayed in the **Details**

view. You do not see, however, the details of the Network, itself. If you want to view the Network details, you must select its parent in the Tree.

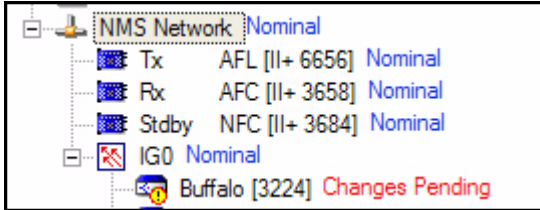


Figure 3-17: Network Highlighted in Tree

Name	ID
..	
AFL [II+ 6656]	7
AFC [II+ 3658]	414
NFC [II+ 3684]	420
IG0	1

Figure 3-18: Result in Details View

To print a report of all the elements in the **Details** view, click anywhere in the **Details** view and select **File** → **Print**. You can print a portion of the view by using the Windows Explorer style functionality to select any elements in the **Details** view (using the CTRL key and clicking on individual elements, or using the Shift key to select a group of consecutive elements). Once the desired elements are highlighted in the **Details** view, you can print a report of those elements' details by selecting **File** → **Print**. (To customize the details you want in the report, see [“Customizing Detail Views for Configuration Reporting” on page 40.](#))

### **Collapse Details Hierarchy + Details**

In the preceding “**Details**” section, we learned that the **Details** option, when used alone, allows you to view details about the children at the next level down from the parent you highlight in the Tree *but does not allow* you to view any sub-elements beneath the children. For example, if you click a **Network** in the Tree, you can view the details about that network’s children (such as line cards) who reside on the same level of the Tree, but you CANNOT VIEW details about the children’s sub-elements (such as remotes) which reside at the second level down from the network you highlighted. Notice that the remote is displayed in the **Details** view now.

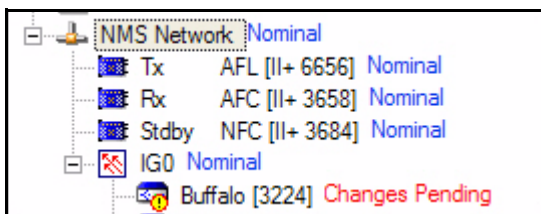


Figure 3-19: Network Highlighted in Tree

Name	ID
..	
AFL [II+ 6656]	7
AFC [II+ 36...	414
NFC [II+ 36...	420
IG0	1
Buffalo [3224]	9
Baltimore [II...	213
Tampa Bay [...]	227

Figure 3-20: Result in Details View

The **Details + Collapse Details Hierarchy** view collapses, or flattens, the hierarchy beneath a highlighted element in the Tree so that you can view the details of all children elements at every level of the Tree below the parent you selected. For example, if you click a **Network** in the Tree, you can view the details about that network’s children (such as line cards) who reside on the same

level of the Tree, and you CAN VIEW the details about the children's sub-elements (such as remotes) which reside at the second level down from the network you highlighted.

To view the details of all children elements at every level of the Tree below the parent you selected, select **View** → **Details** and **View** → **Collapse Details Hierarchy**.

### **Choose Details**

This option in the **View** menu allows you to modify the system's predetermined set of details for any given element so that you can view only the details you need. For a detailed description on using this feature, see ["Customizing Detail Views for Configuration Reporting" on page 40](#).

## **3.9 Customizing and Creating New Detail Views**

The NMS allows you to use not only the **Details** and **Collapse Tree** buttons to display predefined details about a given highlighted element and its sub-elements, but it gives you the ability to customize a **Details** display with any set of details or to create permanent new detail views that you can use with any element in the system.

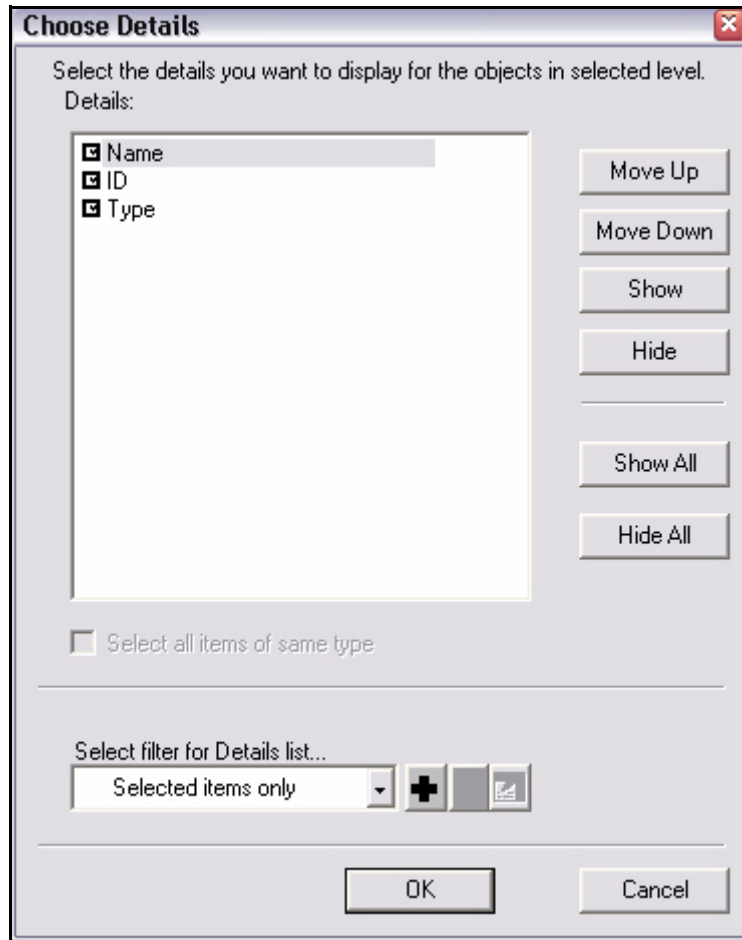
### **3.9.1 Customizing Detail Views for Configuration Reporting**

As mentioned in ["Details" on page 38](#), the NMS is shipped with predefined sets of details that may be viewed for any given element in the Tree. However, you can customize your **Details** views for any element, using the advanced **Choose Details** feature.

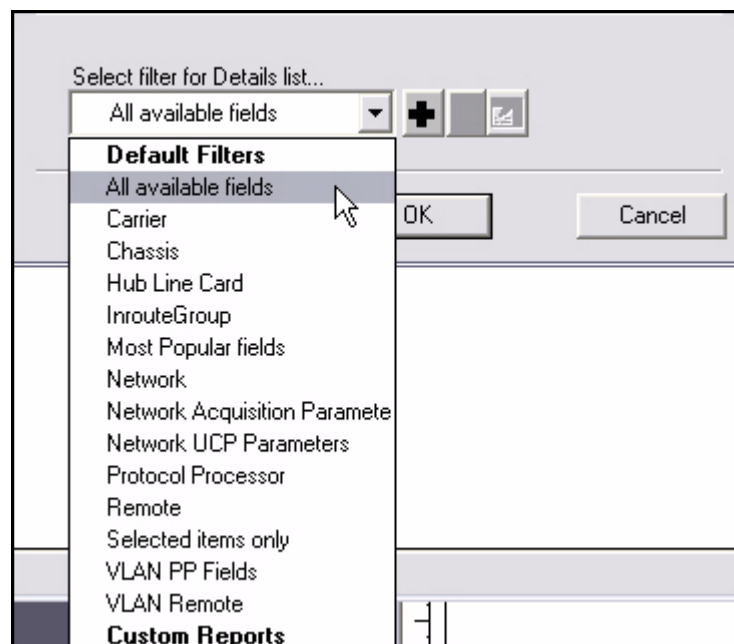
To customize a **Details** view, follow the procedure below:

- Step 1 Click an element in the Tree for which you want to view details.
- Step 2 Select **View** → **Choose Details** from the Main Menu. The **Choose Details** dialog box is displayed.



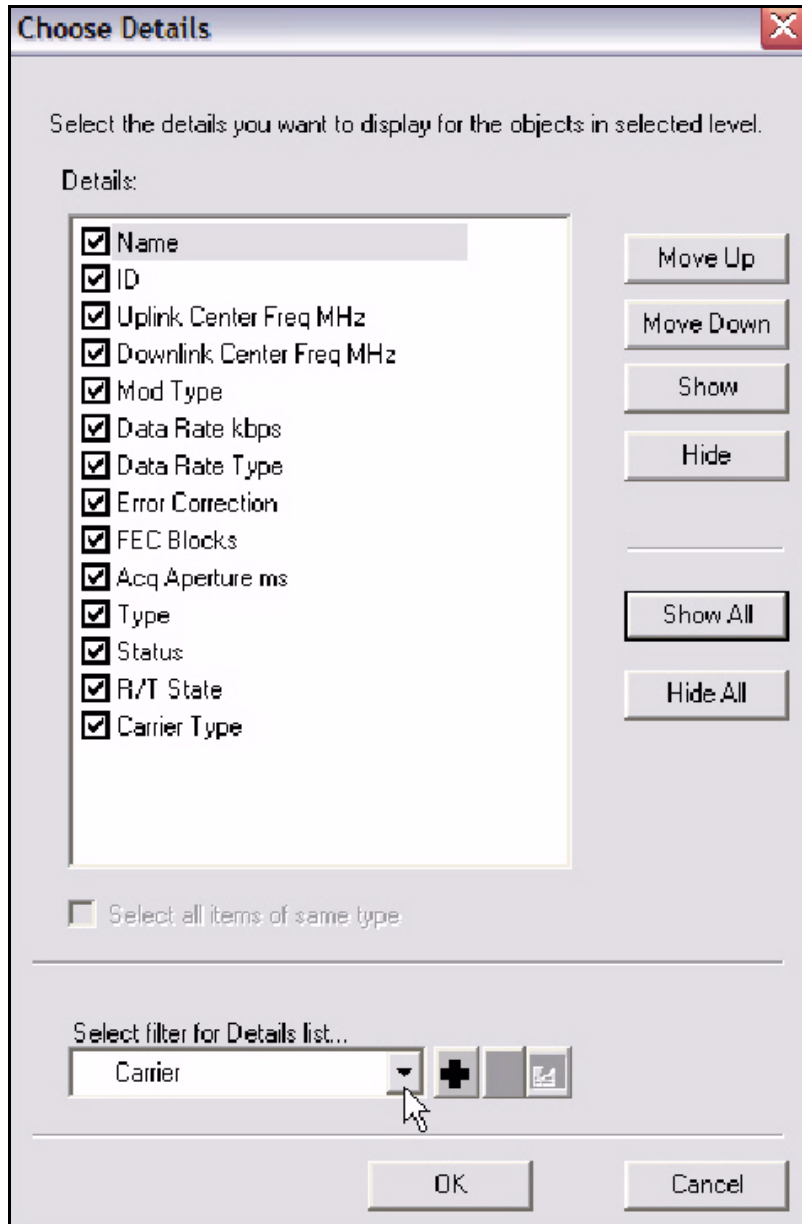


Step 3 Click the **Select filter for Details list...** drop-down list in the **Choose Details** dialog box.



Step 4 Select one of the filters. Each filter offers a different set of details. For example, the **Carrier** filter offers a list of all the predefined details that are viewable when you highlight a carrier in the Tree and select **Details** from the **View** menu.

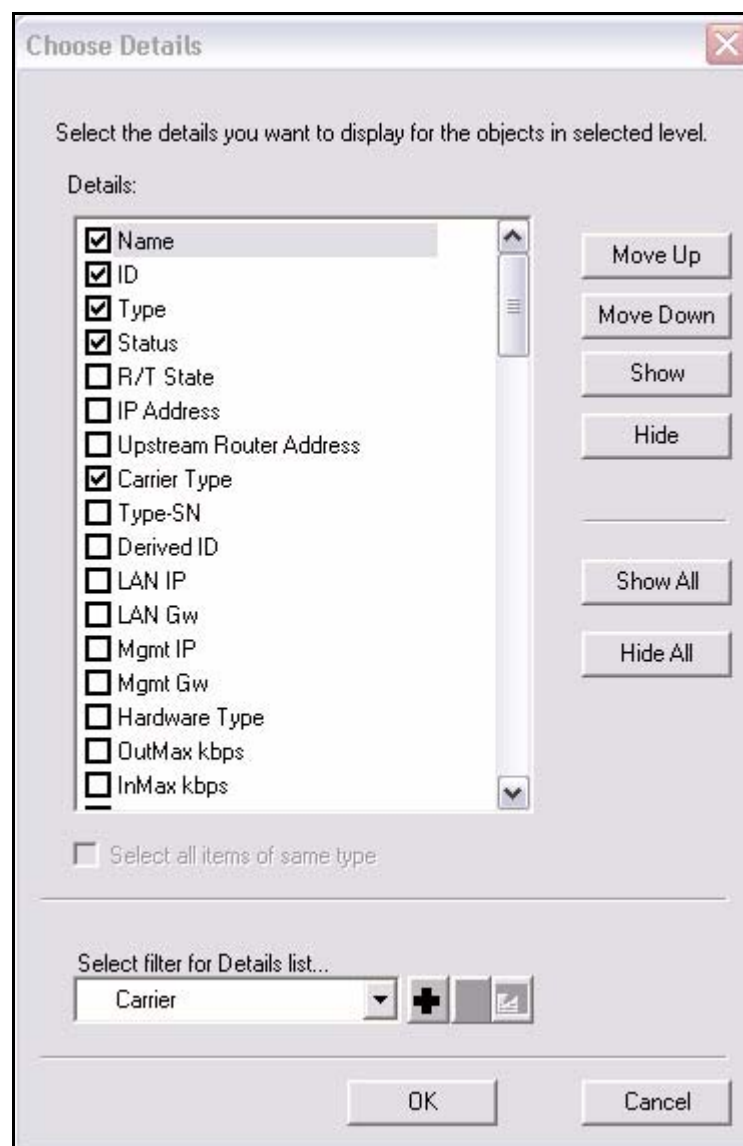
When you select a filter, the detail choices appear in the **Choose Details** dialog box, as shown below. The example below shows the details for **Carrier**.



Step 5 From the list of available choices, click the details you want to view for the element you have highlighted in the Tree.

- a Use the **Show All** button on this dialog box to select all of the details with one click.
- b Use the **Move Up** and **Move Down** buttons to arrange the details in the sequence in which you want them to appear from left to right on the **Details** pane.
- c Use the **Hide All** button to clear checkmarks from detail options you have already checked.

Step 6 In the example below, only five details were chosen to remain in the Carrier view: Name, ID, Type, Status and Carrier Type.



- Step 7 When you are finished customizing the view, click **OK** to save the list of details for this filter. The next time you open iBuilder, the last saved list of details for any given filter are retained.
- Step 8 Now that the details in the **Carrier** view have been altered to include only these five details, you can select any element in the Tree (the element may be a carrier or any other element), and select **View → Details**, and only the details you chose for the *new Carrier* view will be displayed for that element.
- Step 9 In the following example, a carrier was selected in the tree. The user selected **View → Choose Details → Carrier → OK**. The user also selected **View → Details** for this element. If these options are selected, the following details on the selected carrier are displayed in the **Details** view:

Name	ID	Type	Status	IP Address	Carrier Type
..					
<input checked="" type="checkbox"/> P2P_DownStream_SCPC	73	carrier	Unknown		Outroute
<input checked="" type="checkbox"/> P2P_UpStream_SCPC	74	carrier	Unknown		Inroute

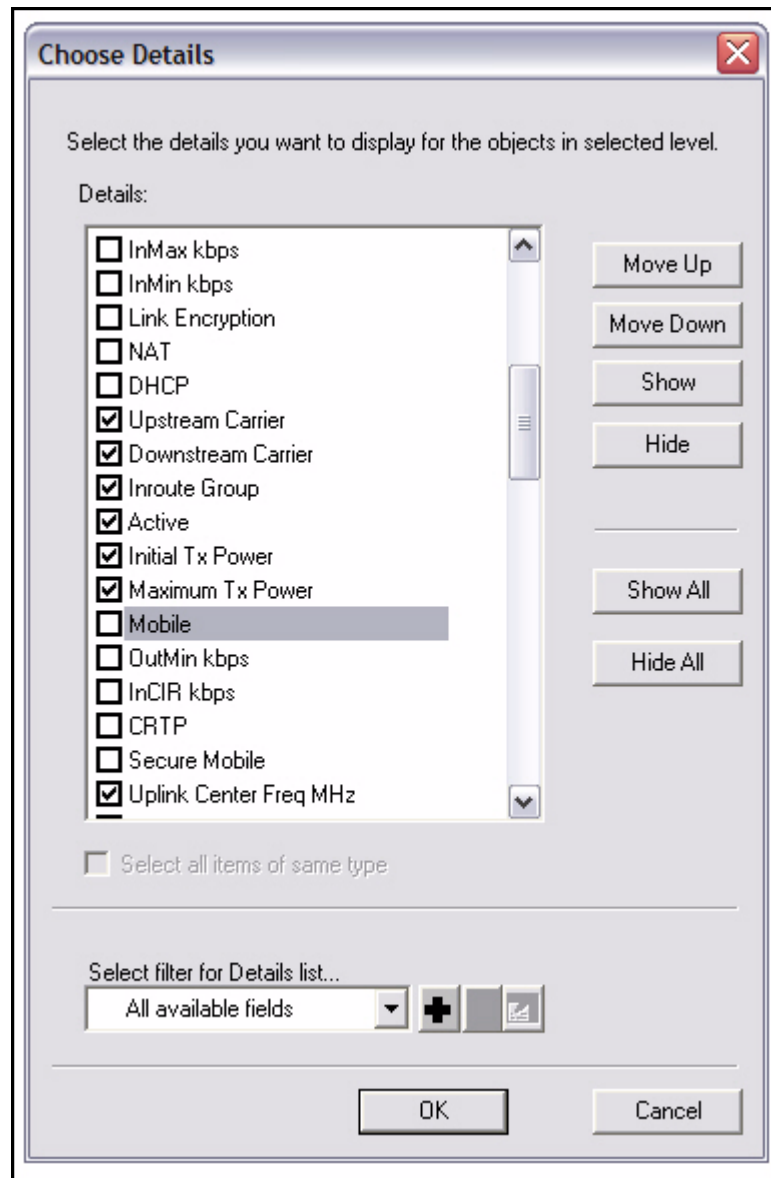
- Step 10 If desired, you can now view **Details** or **Details + Show All** and print a report.

### 3.9.2 Creating Additional Filters for Customized Reporting

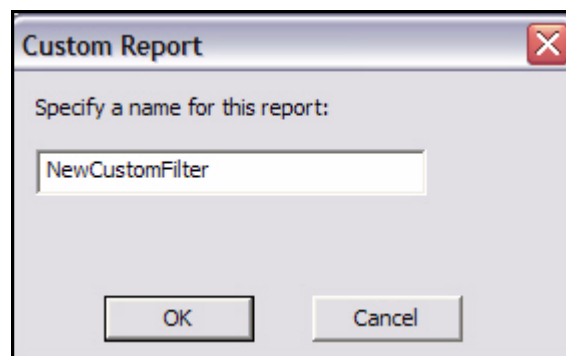
You can also create your own sets of details for generating and printing reports, using the **Choose Details** feature. To create customized **Detail** or **Details + Collapse Tree** views, follow the procedure below:

- Step 1 Select **View → Choose Details** from the Main Menu. The **Choose Details** dialog box is displayed.
- Step 2 Select a list of details that you want to display in your **Details** view by clicking the arrow in the **Select filter for details list** drop-down box at the bottom of the dialog box and choosing a set of details from which to start.

In the example below, the user selected **All Available Fields** to be displayed, and then cleared some of the check boxes so that those details would not appear in the **Details** view they were creating.



Step 3 Click the **Plus (+)** button to assign this custom filter a name. The **Custom Filter** dialog box is displayed.



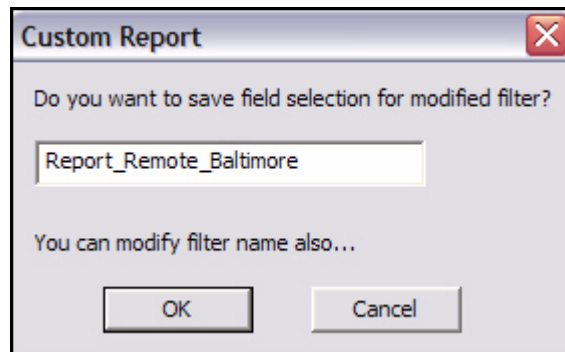
Step 4 Type a name into the field and click **OK**. When you add a filter, the buttons at the bottom of the **Choose Details** pane change from:



Step 5 To modify the field selection for a new filter, make the desired changes to the detail selections for the filter and click the Modify button shown below:



Step 6 A message appears, asking if you want to change the name.



Step 7 Change the name and click **OK**. A new filter is created.

Step 8 To delete a filter, click the **X** button at the bottom of the **Choose Details** dialog box. A message appears to confirm that you want to delete the filter.



Step 9 Click **OK** to delete the filter.

Step 10 If desired, you can now view **Details** or **Details + Collapse Details Hierarchy** and print a report.

## 3.10 Working with Multiple Elements Simultaneously

The sections below describe how to modify parameters on multiple elements at the same time and direct you to sections that describe how to work with multiple configurations and Image files.

### 3.10.1 Working with Multiple Configurations and Image Files

In [chapter 11, “Retrieving and Applying Saved and Active Configurations,”](#) see the following sections:

- [“Retrieving Configurations” on page 183](#)
- [“Applying Configuration Changes” on page 190](#)

In [chapter 12, “Upgrading Software and Firmware ,”](#) see the following sections:

- [“Multicast via UDP” on page 202](#)
- [“Downloading an Image to Remotes and Line Cards Concurrently” on page 201](#)
- [“Downloading an Image to Out of Network Remotes” on page 204](#)

### 3.10.2 Modifying Parameters on Multiple Elements

You can modify parameters on multiple elements simultaneously as long as the elements are all the same type. For example, you can modify parameters on any number of Networks, or any number of Remotes, or any number of Receive Line Cards, etc.

#### **Rules for Multiple Edit**

There are some restrictions and requirements regarding the use of group editing, as follows:

1. You may select multiple elements only from the **Details** view. You cannot select multiple elements from the Tree. Select **View** → **Details** from the main menu to display the **Details** pane.
2. All the elements you select must be of the same type. For example, elements to be edited in a group must *all* be remotes or *all* be line cards, etc. You cannot edit, for example, a remote and a line card in the same *group*.
3. You may only modify items in a group that have the same value, or have no value yet assigned to them. For example, when editing a group of remotes, you may give them all the same custom key or modify the custom key if they all have the same custom key value. However, you will probably not be able to change the GEO location, because this value is generally different on every remote in the group.

#### **Procedure for Group Editing**

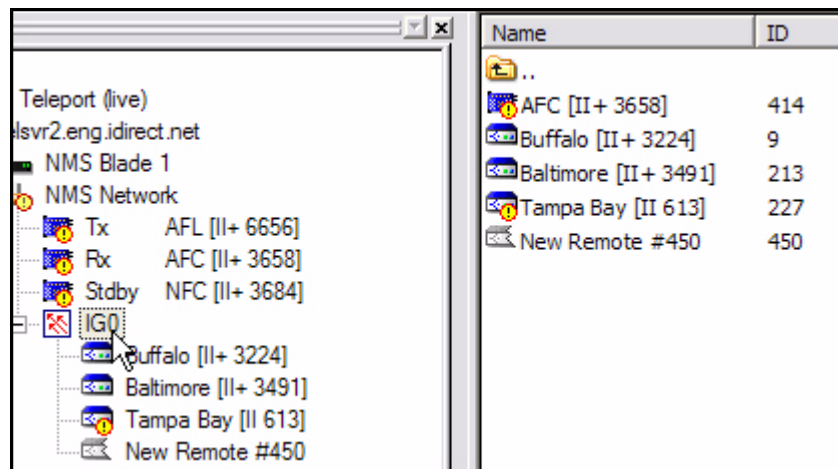
To perform this function, follow the procedure below:

- Step 1 Highlight an element in the Tree that is a parent to the elements to which you want to make changes.

For example, *Network* is a parent element for *line cards*. However, any element above *Network* can also serve as a parent element for line cards, such as the *Teleport* or *Protocol Processor*.

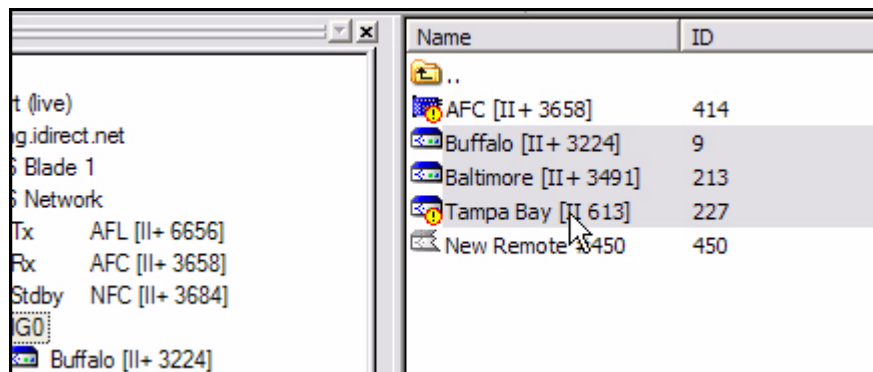
- Step 2 With a parent element highlighted in the Tree, select **View → Details** from the Main Menu. The **Details** pane is displayed to the right of the Tree, and the elements to which you want to make changes appear in the list of elements.

In this example, changes will be made to the remotes in the **IG0** inroute group. Therefore, **IG0** has been selected as the parent element. The elements on the next branch down from the inroute group parent level are displayed in the **Details** pane. In other words, the “child” elements are the only elements displayed. In this example, a line card and several remotes are displayed.



- Step 3 Use the Control (CTRL) key or the Shift key on your keyboard to highlight the elements to which you want to make changes. In this example, changes will be made to three remotes.





- Step 4 Right-click the highlighted elements in the **Details** pane (in this case, the remotes) to open the **Configuration** or **Configuration and Control** dialog box.
- Step 5 To modify all of them, click **Modify**. The **Modify Configuration** dialog box for those elements appears.
- Step 6 Make the changes you want to apply to ALL of the selected elements, and click **OK**. The changes are saved in the database.

## 3.11 Configuration Status of Elements

Central to the operation of iDirect’s NMS is the concept of “configuration state”. Configuration states represent elements of the network in terms of their condition. This section describes the concept of configuration state and what it means for both iBuilder and iMonitor.

### 3.11.1 What is a Configuration State?

iBuilder divides the configuration process into three steps:

- Step 1 Make your changes to the database;
- Step 2 Review those changes by selecting **Compare Configuration** on the element you are changing (this step is optional but recommended), and if necessary, make any necessary modifications
- Step 3 Once you’re satisfied with the changes, make them active in the network by applying them to the components that you changed via the **Apply Configuration** or a multicast download feature

This three-step change process gives the network operator ultimate control over operational network components, because no change takes place without the operator initiating it. However, it creates a situation where the NMS database is temporarily out-of-sync with the actual network. This occurs after the operator has made database modifications, but before they have been applied to the network.

To help operators easily manage this situation and others like it, iDirect implements the concept of configuration state. Configuration states show the current configuration status of key components of the network: Hub Chassis, individual networks, line cards, and remote modems.

Using a specific modification as an example, we can see how configuration state changes over time:

1. Remote “r\_123” is configured, commissioned, and all previous changes have been applied. Its configuration state is “Nominal”.
2. User changes the upstream QOS settings for remote r\_123.
3. The configuration state for r\_123 becomes “Changes Pending”.
4. User reviews the changes, determines they are correct, and then applies them to the remote.
5. The configuration state for r\_123 returns to “Nominal”.



#### **NOTE**

Remote and line card configuration state returns to “Nominal” immediately after a new configuration file is applied; iBuilder does not attempt to track whether or not the modem was reset. Please ensure you reset remote modems or line cards to activate your changes.

### **3.11.2 Possible Configuration States**

The following table lists all of iBuilder’s configuration states and the network elements to which they apply. See also [chapter 3, “Overview of the Network Management System for iBuilder,”](#) sections:

- [“Legend Pane” on page 36](#)
- [“Configuration Changes Pane” on page 37](#)
- [“Configuration Status View” on page 37](#)

**Table 3-2: Configuration States**

Configuration State	Network Element	Definition	Applies to
Nominal	Network Chassis Line Card Remote	The element is completely configured, is alive in the network, and there are no unapplied changes.	Remote Hub Network Chassis
Changes Pending	Network Chassis Line Card Remote	The element is completely configured and is alive in the network. There are changes in the database that have not been applied.	Remote Hub Network Chassis
Incomplete	Network Chassis Line Card Remote	The element is only partially configured; one or more key components of the configuration are unspecified (e.g. carriers, IP address, serial number)	Remote Hub Network Chassis
Never Applied	Network Chassis Line Card Remote	The element is completely configured but the configuration has never been applied to the element.	Remote Hub Network Chassis
Deactivated	Remote	The remote modem was at one time active in the network, but it has been deactivated.	Remote

### 3.11.3 Configuration State Transition

The following diagram illustrates typical state transition for a remote modem in iBuilder from creation to steady-state.

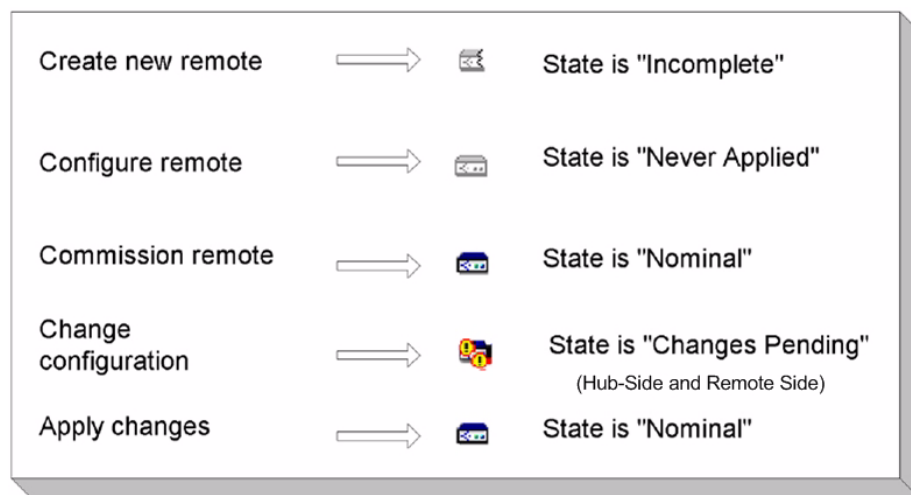


Figure 3-21: Configuration States of an iDirect Remote

An explanation of all configuration states for all elements, their meaning, and their respective icons is available in iBuilder by selecting **View** → **Legend** from the main menu.

### 3.11.4 Viewing Configuration States

Configuration states are displayed in iBuilder's network Tree. Each network element in the tree shows its current configuration state with these icons. You can also view the configuration state as color-coded words next to the corresponding element by selecting **View** → **Configuration Status** from iBuilder's main menu.

See also ["Configuration Changes Pane" on page 37](#) and ["Configuration Status View" on page 37](#).

### 3.11.5 Why Did My Configuration States Change?

Configuration states can change for a variety of reasons, including:

- *You changed configuration.* Whenever you change the configuration, the **Changes Pending** icon appears beside all affected network elements.
- *Someone else changed configuration.* iBuilder supports multiple simultaneous logins. If another user changes configuration, your network tree icons will change to reflect the current configuration state.
- *Someone changed a modem's configuration directly.* When a modem comes into the network, the configuration server uploads the active configuration from the remote and re-calculates configuration state. If this configuration is different from the latest iBuilder configuration, you will see the **Changes Pending** icon for that modem. This can happen if someone changes a modem's configuration from the console or the iSite utility. This potentially dangerous situation is flagged by the configuration state.
- *You installed a new version of the Configuration Server.* When the configuration server starts up, it re-generates the configuration files for all networks, hubs, and remotes. The new server may generate additions, deletions, or changes to the configuration files. If so, all affected elements will display the **Changes Pending** icon after the new server starts up.

### 3.11.6 Configuration States and iMonitor

Configuration states are shown in iMonitor in the following circumstances:

- When a Chassis, Network, Hub, or Remote is "Incomplete", iMonitor displays the Incomplete icon.
- When a remote modem is "Deactivated" or "Never Applied", iMonitor shows the deactivated icon. In this case historical requests may still be made, since a deactivated remote may have archived data.
- When a remote modem is either "Nominal" or "Changes Pending", iMonitor's real-time state icons take over, so you will see either the **OK**, **Warning**, or **Alarm** icon depending on the real-time status of the modem.

An explanation of the configuration states, their meaning, and their respective icons is available in iMonitor by selecting **View** → **Legend** from the main menu.

### 3.11.7 Accepting Configuration Changes and Locking the Database

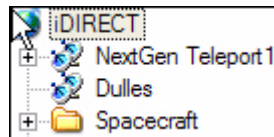
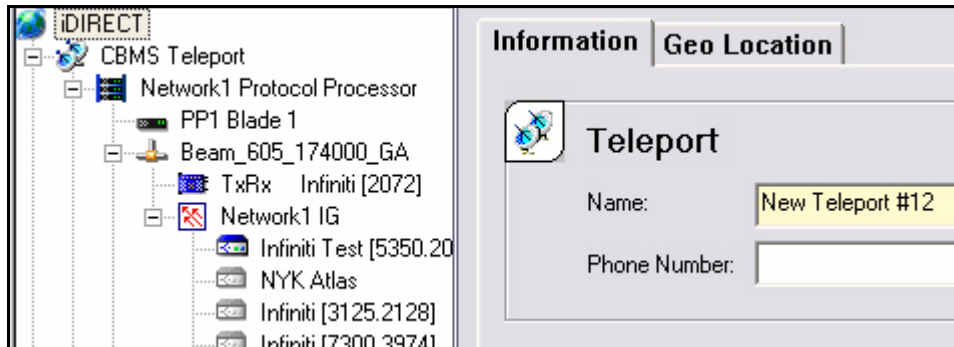
For a discussion on how to accept changes made by others to the database, see [“Multiple Users or PCs Accessing the NMS” on page 17](#). For the steps to unlock the database in the event that someone makes changes and forgets to log out, see [“NMS Database Locking” on page 233](#).

## 3.12 Understanding the Database’s Numbering Convention

When an element in the Tree is created, a sequenced number is assigned to that element by the database, and The new component or element appears in the Tree at the bottom of the list of like-elements on its branch level in the tree. In the example below, a user has right-clicked on the Globe to create a new Teleport. The **Modify Configuration** dialog box is displayed with “New Teleport #12” in the Name box, and at the bottom of the teleport’s level in the Tree, a Teleport is automatically displayed with the same name. When you change the name on the **Modify Configuration** dialog box and save it by clicking OK, the name of the teleport in the Tree will also change.

When you exit iBuilder and log back in, the teleport will move from the bottom of the Tree to the bottom of the list of teleports. In the example below, we named the new teleport “Dulles”. Notice that the teleport names are not sorted alphabetically.

The NMS database assigned a system-generated number to each element when it is created. The first teleport is assigned the number “1”. The second teleport is assigned the number “2”, and so on. The same number assignment takes place with every element created in the tree. Therefore, the first spacecraft would be named “New Spacecraft #1”, and so on. This number is always associated with its original element. This is how the database keeps track of the elements and the configurations and management control associated with it as long as it exists in the Tree. If an element is deleted, the numbers of the elements created after it do not change numbers. For example, if you have five teleports and teleport number 3 is deleted, teleport number 4 does not become teleport number 3. Teleport number 4 remains teleport 4 forever. If a sixth teleport is created, it becomes teleport number 6, not number 3.



### 3.13 In Color versus Shaded Icons

If an icon next to a component (such as a user, QoS profile, BUC, LNB, Converters, etc.) in the Tree is in color, it indicates that component is being used somewhere in the network. Therefore, if you perform any configuration or control functions on that element, it will affect other elements in the network. If you modify the element, a message is displayed warning you that if you make changes to this element, any other element in the database that is using it will be changed also. As long as the icon is in color, you cannot delete the element.

If the icon next to an element in the Tree is unavailable and displayed in gray, you can make modifications without it affecting other elements in the network.

## 3.14 Configuring Warning Properties

Warnings that indicate anomalous conditions on your iDirect equipment are generated by the iDirect network and displayed in iMonitor. You can configure the properties that determine how individual warnings are generated for the following network elements:

- Line cards
- Remotes
- Protocol processors

There are two categories of warnings:

- *Limit-based* warnings are generated when either the high or low limit defined for the warning is violated. A warning's range can specify a low limit, a high limit or both.
- *Boolean* warnings have two states: the warning is either off or on. A boolean warning is generated when the value being monitored by the warning changes from the nominal state to the anomalous state. For example, if a line card loses the chassis backplane 10 MHz timing signal, then the BackplaneLost10MHz warning is generated for the line card.

You can perform the following operation when configuring warning properties:

- Enable or disable a warning.
- Set the upper and lower limits that determine when certain warnings are generated. (Limit-based warnings only.)
- Configure a warning to be generated only when a limit is violated, or to be generated each time a value changes when outside the normal operating range. (Limit-based warnings only.)

All warning modifications are processed dynamically; you do not need to restart any NMS processes for the warning changes to take effect. For example, if you disable a warning all currently active warnings of this type will clear in iMonitor. Similarly if you modify a limit such that some active warnings now fall in the normal range, those warnings are automatically cleared.



### NOTE

The installation of iDS 7.0 drops your current warning definitions from the database and recreates them. If you have custom limits defined in your network, you must redefine them after your upgrade.

You can use iBuilder to modify both global properties of warnings and warning properties for individual network elements. When you customize a warning for an individual element, the new setting overrides the global setting. Changes to global warning settings apply only to those elements that do not have their settings customized on an individual basis.

The behavior of the system with regard to global properties and individual overrides is as follows:

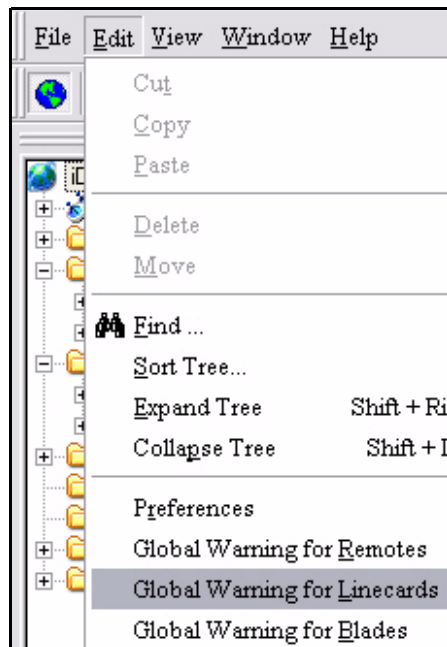
- A warning whose properties have not been modified for an individual element uses the global properties for that warning. In the event that the global properties of the warning are modified, the new global properties will be used by the element.
- A warning whose properties have been modified for an individual element uses the customized properties for that warning for that element. Changes to the global properties of the warning have no effect on the warning properties configured for that element; the element will continue to use the modified properties.
- When a warning that has been modified for an individual element is reset for that element, any properties that were previously modified for the warning take on the current, global values.

### 3.14.1 Setting Global Warning Properties

Global warning properties are configured from iBuilder's **Edit** menu.

To set global warning properties for your line cards, remotes or blades, follow these steps:

- Step 1 Click the **Edit** menu and select Global Warnings for the element type. In this example, **Global Warning for Linecards** is selected from the menu.



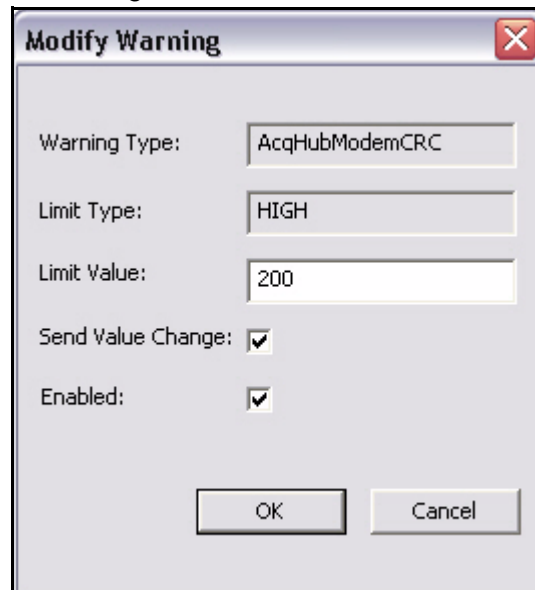


The **Modify Global Warning** dialog box appears with all warnings appropriate to the selected network element type.

Warning Type	Limit Type	Limit Value	Send Value Change	Enabled	Details
MeshHubRxTDMASNR	HIGH	3.00	1	1	The TDMA signal quality in C/N, ....
AcqHubModemCRC	HIGH	200.00	1	1	The number of acquisition-based....
TrafficHubModemCRC	HIGH	10.00	1	1	The number of traffic-based CR.....
RxOverflowFrames	HIGH	0.00	1	1	The Rx linecard's maximum DMA ....
FlldacErrors	LOW	512.00	1	1	The remote's or linecard's intern.....
FlldacErrors	HIGH	3584.00	1	1	The remote's or linecard's intern.....
MeshHubRxSCPCCLBSNR	HIGH	3.00	1	1	The SCPC loopback signal qualit.....
BackplaneLost10MHz	Boolean		0	1	The line card has stopped detec.....

Step 2 Select the **Warning Type** for the warning you want to modify and click the **Edit** button.

Step 3 Enter the new settings in the **Modify Warning** dialog box and click **OK** to save the changes.



**Modify Warning**

Warning Type:

Limit Type:

Limit Value:

Send Value Change:

Enabled:

You can modify the following parameters:

- The **Limit Value** setting determines the high or low limit of the normal range of values for the network parameter being monitored. When this limit is crossed, a warning is generated. You can only set the **Limit Type** for limit-based warnings. This field does not apply to boolean warnings.

- The **Send Value Change** setting determines whether or not the warning will be generated each time a value changes while that value is outside normal operating limits. If the check box is selected, a new warning will be generated each time the abnormal value changes. If the check box is cleared, a warning will be generated the first time an abnormal value is detected, but not if the abnormal value changes. You can only set the **Send Value Change** property for limit-based warnings. This field does not apply to boolean warnings.
- The **Enabled** setting enables or disables the warning. If you clear this check box, the warning will not be generated.



**NOTE**

Changes to global warning settings do not affect warnings that have been customized on the **Warning Properties** tab. You must reset the customized warning to return to the global settings. (See [“Clearing Customized Warning Properties” on page 59.](#))

### 3.14.2 Customizing Warning Properties for Individual Network Elements

To customize warning properties for individual network elements, follow these steps:

- Step 1 Right-click the network element in the network tree and select the appropriate **Modify** option from the context menu.
- Step 2 When the dialog box for the network element appears, click the **Warning Properties** tab.

Information						Warning Properties						Custom					
Warning Type	Limit Type	Limit Val...	Send Value Change	Enabl...	Details												
MeshHubRxTDMA...	HIGH	3.00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The TDMA signal quality in C/N, as r												
AcqHubModemCRC	HIGH	200.00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The number of acquisition-based CF												
TrafficHubModemC...	HIGH	10.00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The number of traffic-based CRC (C												
RxOverflowFrames	HIGH	0.00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The Rx linecard's maximum DMA tra												
FIIDacErrors	LOW	512.00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The remote's or linecard's internal o:												
FIIDacErrors	HIGH	3584.00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The remote's or linecard's internal o:												
MeshHubRxSCPC...	HIGH	3.00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The SCPC loopback signal quality in												
<b>BackplaneLost10...</b>	<b>Boolean</b>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<b>The line card has stopped detectin</b>												

Rows in BOLD indicate customized

Reset Edit

- Step 3 Select the **Warning Type** for the warning you want to reconfigure and click the **Edit** button.

- Step 4 Follow the procedure beginning with [Step 2](#) in [“Setting Global Warning Properties” on page 56](#) to reconfigure the warning properties.

Warnings that have been customized are highlighted in **bold** text on the **Warning Properties** tab. In the example, the **BackplaneLost10MHz** warning has been disabled for this specific line card.



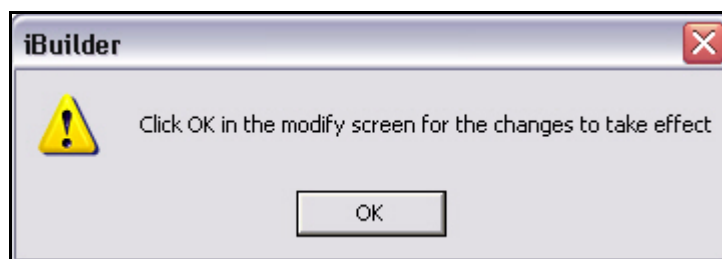
## NOTE

Customized warning settings configured on the **Warning Properties** tab apply only to the individual element being modified. These settings override the global settings for the element being reconfigured. (For more details see [“Configuring Warning Properties” on page 55](#).)

### 3.14.3 Clearing Customized Warning Properties

When you set warning properties on an element’s **Warning Properties** tab, the customized settings override the global settings for that element until you clear the customized settings. To clear the customized settings for a warning and return the warning to the global settings, follow these steps:

- Step 1 Right-click the network element in the network tree and select the appropriate **Modify** option from the context menu.
- Step 2 When the dialog box for the element appears, click the **Warning Properties** tab.
- Step 3 Select the warning for which you want to clear the customized settings. (Warnings with customized settings are highlighted in **bold** text.) Then click the **Reset** button at the bottom of the screen. The following dialog box will appear:



Click **OK** in the dialog box. Then click **OK** on the **Warning Properties** tab. The warning that you reset will be reconfigured with the global settings.



## 4 Defining Hub RFT Components and the Satellite

A spacecraft must exist in the Tree before the Hub RFT (Radio Frequency Terminal) can be defined. However, before you define the spacecraft, you must define the Hub RFT Sub-Components. This includes:

- [“Preparing the Hub RFT Components Folders” on page 61](#)
- [“Adding a Spacecraft” on page 65](#)
- [“Adding a Transponder” on page 66](#)
- [“Adding Bandwidth” on page 68](#)
- [“Adding Carriers” on page 69](#)

### 4.1 Preparing the Hub RFT Components Folders

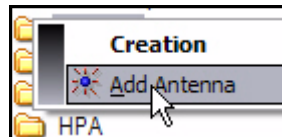
In order to configure the HUB RFT, you must select certain pre-defined subcomponents for each field in the HUB RFT configuration dialog box. When you expand the HUB RFT folder, you will see the subcomponent folders listed below. These subcomponents have been previously configured and contain critical settings used to establish the Hub RFT operational parameters.

- Antenna
- Up Converter
- Down Converter
- High Power Amplifier (HPA)

You should add entries to these folders in advance and define the parameters of the components you add so that the appropriate information is already in the drop-down lists on the Hub RFT configuration dialog box. The steps below carry you through the configuration of these sub-components.

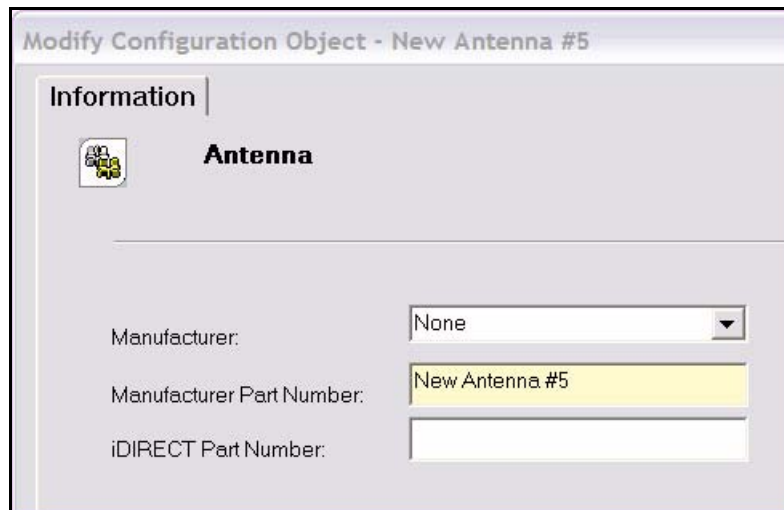
#### 4.1.1 Adding an Antenna

- Step 1 Under the Hub RFT Components folder, right-click the Antenna folder and select **Add Antenna**. The new antenna appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its parameters.



- Step 2 In **Manufacturer Part Number**, enter a part number or name for the antenna. You may enter any information you like in this field, or leave it blank.
- Step 3 You may also select a manufacturer in the **Manufacturer** drop down box by selecting the appropriate manufacturer from the available list. The items

in this list were either pre-existing or were added when you populated the folder earlier. See [“Adding Entries to Folders” on page 22](#).



- Step 4 You may also enter an **iDirect Part Number** for the antenna (optional). You may enter any information you like in this field, or leave it blank.
- Step 5 Click **OK**. The new antenna appears in the Tree under the antenna folder.
- Step 6 If you have more than one antenna, repeat this procedure and assign the new antenna a different name.

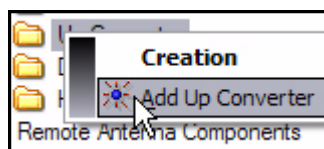
## 4.1.2 Adding an Up or Down Converter



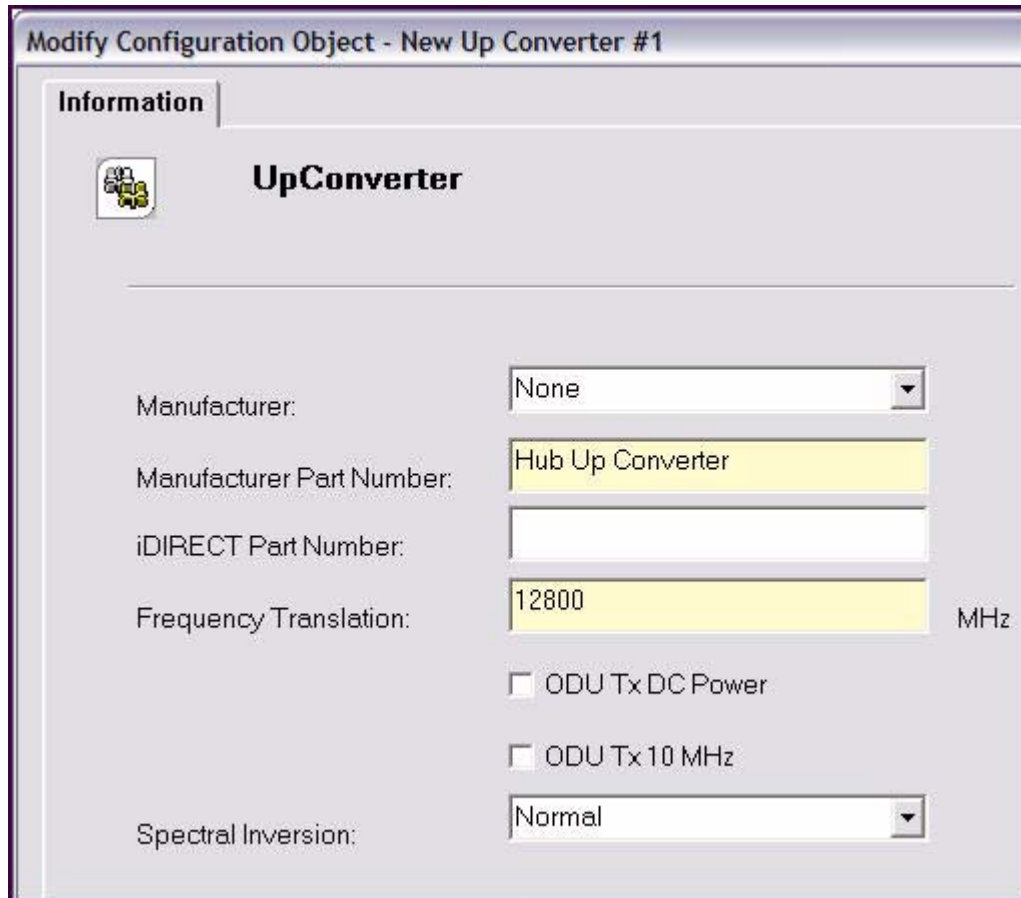
### NOTE

Be sure to enter the correct frequency translation values for all of your Up and Down Converters. The NMS will use these values later to generate network configurations.

- Step 1 Under the Hub RFT Components folder in the Tree, right-click the Up Converter folder, and select **Add Up Converter** or **Add Down Converter**. The new converter appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its parameters. The examples below show an Up Converter being added; however, the procedure is the same for adding a Down Converter.



- Step 2 In **Manufacturer Part Number**, enter a part number or name for the Up Converter. You may enter any information you like in this field, or leave it blank.



**Modify Configuration Object - New Up Converter #1**

**Information**

**UpConverter**

Manufacturer: None

Manufacturer Part Number: Hub Up Converter

iDIRECT Part Number:

Frequency Translation: 12800 MHz

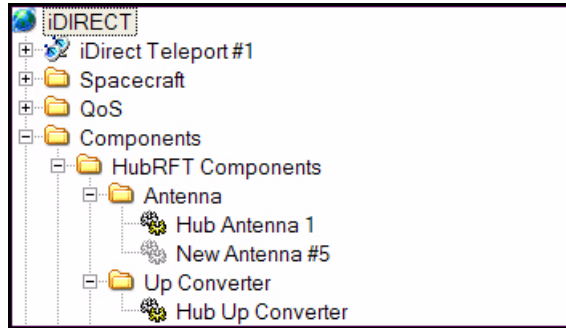
ODU Tx DC Power

ODU Tx 10 MHz

Spectral Inversion: Normal

- Step 3 In **Frequency Translation**, enter a frequency in MHz. This information is provided on the specifications sheet for the Up Converter.
- Step 4 You may also select a **Manufacturer** for the Up Converter (optional).
- Step 5 Enter an **iDirect Part Number** for the Up Converter (optional). You may enter any information you like in this field.
- Step 6 Select **ODU Tx DC Power** and **ODU Tx 10 MHz** if you require the iDirect modem to supply DC power and the 10 MHz clock. These settings are applicable only if you are operating a small teleport whose BUC and LNB are not built into the antenna. (The iDirect chassis and line cards do not provide these capabilities; private hubs, mini hubs and remote modems have these capabilities built into them.)
- Step 7 In **Spectral Inversion**, leave it at Normal UNLESS you are using C-band. If the local oscillator is higher in frequency than the one being transmitted or received, then the spectrum must be inverted.

Step 8 Click **OK**. The new Up Converter appears in the Tree under the Up Converter folder.

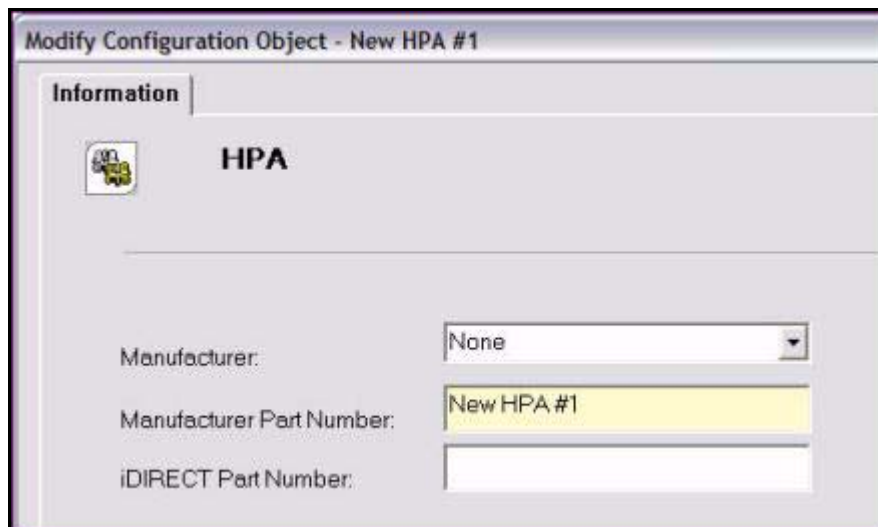
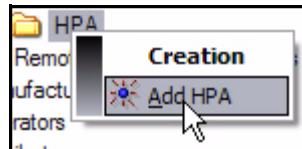


Step 9 If you have more than one Up Converter, repeat this procedure and assign it a different name.

Step 10 Repeat these steps for all of the Down Converters at your teleport.

### 4.1.3 Adding a High Power Amplifier (HPA)

Step 1 Under the Hub RFT Components folder in the Tree, right-click the HPA folder, and select **HPA**. The new HPA appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its parameters.

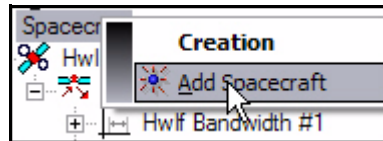
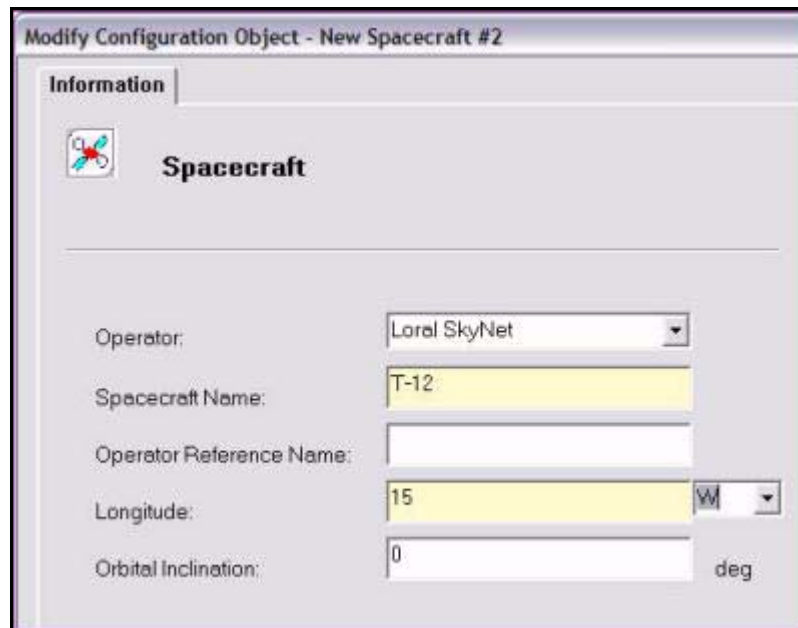




- Step 2 In **Manufacturer Part Number**, enter a part number or name for the HPA, or use the system-generated generic name.
- Step 3 You may also select a **Manufacturer** for the HPA (optional).
- Step 4 You may also enter an **iDirect Part Number** for the HPA (optional). You may enter any information you like in this field, or leave it blank.
- Step 5 Click **OK**. The new HPA appears in the Tree under the HPA folder.
- Step 6 If you have more than one HPA, complete this procedure again and assign it a different name.


## 4.2 Adding a Spacecraft

- Step 1 To create a Spacecraft, right-click the **Spacecraft** folder and select **Add Spacecraft**. A new spacecraft appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its parameters.

Modify Configuration Object - New Spacecraft #2

**Information**

 **Spacecraft**

Operator: Loral SkyNet

Spacecraft Name: T-12

Operator Reference Name:

Longitude: 15 W

Orbital Inclination: 0 deg

- Step 2 In **Spacecraft Name**, enter a name for the spacecraft.

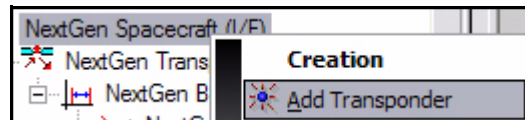
- Step 3 Enter the exact **Longitude** (between 0 and 180 degrees) of the satellite. This information can be obtained from your satellite service provider.
- Step 4 To the right of the **Longitude** box, enter the Hemisphere: **E** (East) or **W** (West).
- Step 5 You rarely have to enter the **Orbital Inclination**. This is necessary only if the satellite is experiencing difficulty or is coming to the end of its life cycle, in which case the satellite provider will provide you with the orbital inclination.
- Step 6 Select the name of the **Operator** (normally the service provider, assuming that your company is not the provider). (Optional.) You can click the Operator drop-down box to view a list of operators you have entered into the NMS, and select one of them.
- Step 7 Enter an **Operator Reference Name**. (Optional)
- Step 8 Click **OK**. The spacecraft appears in Tree under the Spacecraft folder.

### 4.3 Adding a Transponder

The transponder transmits and receives the signals to and from the satellite. Once you have configured the transponder, you can add bandwidth regions, which consists of one or more upstream and downstream carriers.


To define a transponder, you must first have a spacecraft defined in the Tree. To add and define a transponder, follow the procedure below:

- Step 1 Right-click to select a **Spacecraft** and select **Add Transponder**. The new transponder appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.



Modify Configuration Object - Hub Transponder #2

**Information**

 **Transponder**

---

Operator Reference Name:

Center Frequency:  MHz

Bandwidth:  MHz

Tx Polarization:

Rx Polarization:

Translation Frequency:  MHz

Uplink Footprint:

Downlink Footprint:

EIRP:  dBW

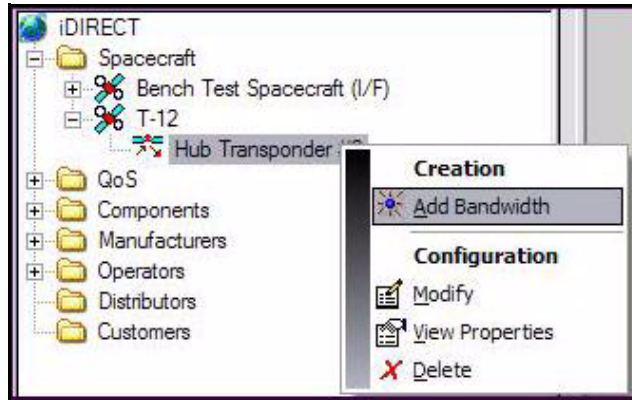
OBO:  dB

- Step 2 In **Operator Reference Name**, enter a name for the transponder to identify it in the Tree.
- Step 3 Enter the **Translation Frequency**. This information can be obtained from your satellite provider. The frequency, in MHz, is transponder specific. It is that frequency used to down convert the radio frequency (RF) uplink to the RF downlink for retransmission from the satellite. This information must be correct for your networks to function correctly.
- Step 4 Enter the information for the remaining fields, which can also be obtained from your service provider. This information is for reference purposes only.
- Step 5 Click **OK**. A transponder appears in the Tree.

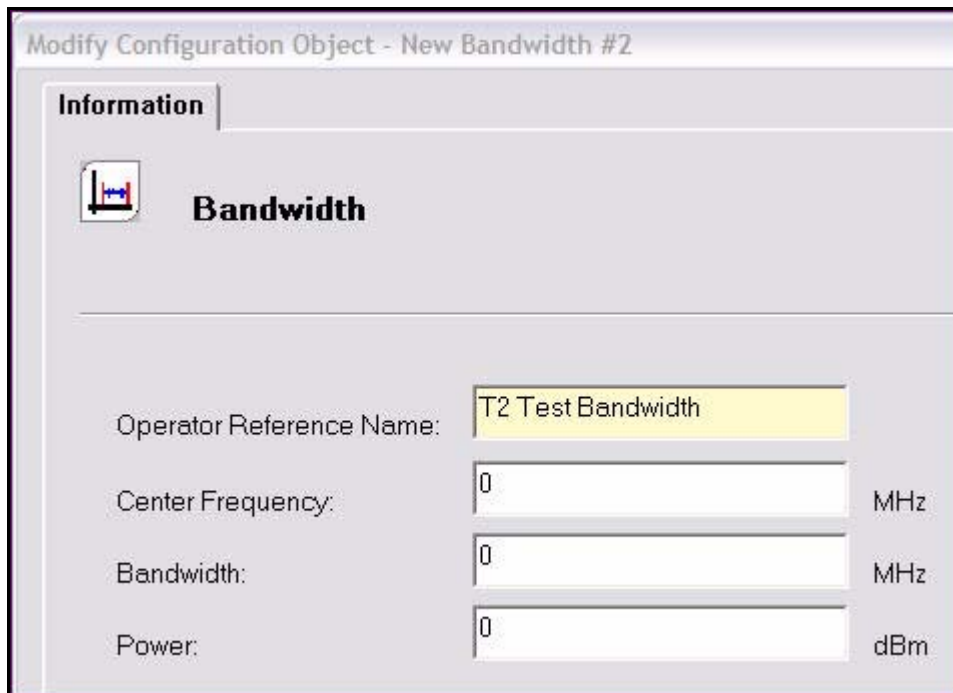
## 4.4 Adding Bandwidth


A bandwidth region defines a specific portion of the satellite's transponder within which you can define transmit and receive bandwidth carriers. You must define at least one bandwidth region in order to create carriers. To add and define a bandwidth region, follow the procedure below:

- Step 1 Right-click the transponder and select **Add Bandwidth**. The new bandwidth entry appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.



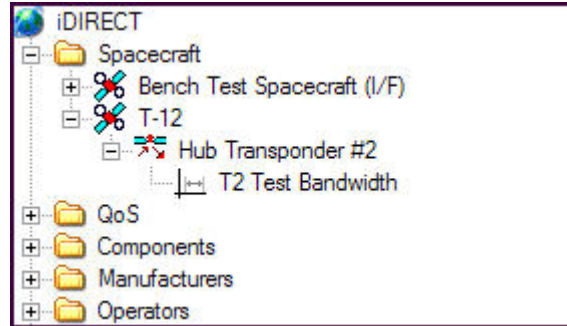
- Step 2 On the **Information** tab, in the **Operator Reference Name** box, enter a name to identify the bandwidth in the Tree.



Modify Configuration Object - New Bandwidth #2	
<b>Information</b>	
 <b>Bandwidth</b>	
Operator Reference Name:	<input type="text" value="T2 Test Bandwidth"/>
Center Frequency:	<input type="text" value="0"/> MHz
Bandwidth:	<input type="text" value="0"/> MHz
Power:	<input type="text" value="0"/> dBm

- Step 3 Enter the **Center Frequency**, **Bandwidth**, and **Power** values, which can be obtained from your service provider. This information is for reference purposes only.

Step 4 Click **OK**. A bandwidth entry appears in the Tree.



## 4.5 Adding Carriers

Each upstream carrier defined becomes available for assignment to a line card once configured. They are made available for selection for the line card configuration, but only after selecting the associated Hub RFT and its assigned spacecraft.

### 4.5.1 Adding Downstream Carriers

Each Network may have only one Downstream (Outbound) Carrier. The information for creating a carrier should be obtained from your satellite provider, as it is part of the satellite link budget process.

In addition to providing the outbound carrier for a network of TDMA remotes, a dedicated downstream carrier can be used to send data on a point-to-point connection from an iSCPC line card at the hub to a single iSCPC remote. In that case, the iSCPC remote transmits back to the hub on an iSCPC upstream carrier. (For details, see [“Adding Upstream SCPC Carriers” on page 74.](#))



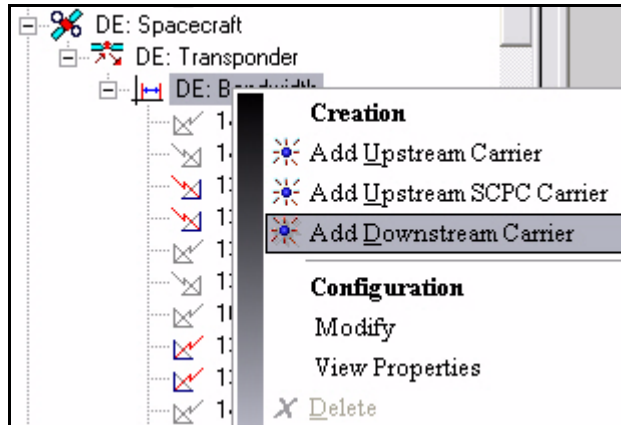
#### NOTE

When using a downstream SCPC carrier for iSCPC operation, the transmit power is based on the SCPC line card configuration, *not* on the downstream carrier configuration. For further information, please see [“Adding an iSCPC Line Card” on page 99.](#)

To add a downstream carrier, follow the procedure below:


Step 1 Right-click on the bandwidth for your transponder and select **Add Downstream Carrier**. The new carrier appears in the Tree with a system-

generated generic name, and a dialog box appears allowing you to define its basic parameters.



**Modify Configuration Object - New Carrier #30**

**Information**

 **Downstream Carrier - SCPC**

Outroute ID:

Name:

Uplink Center Freq:  MHz

Downlink Center Freq:  MHz

Power:  dBm

Carrier Spacing:

Error Correction:

Modulation:

Assigned to Line Card:

Transmission Parameters

Transmission Rate:  kbps

Information Rate:  kbps

Symbol Rate:  ksym

Timeplan Parameters

FEC Blocks per Frame:

Frame Length:  ms

Other Parameters:

Scrambling	IDR
Differential Encoding	OFF

- Step 2 Enter a name for the downstream SCPC carrier.
- Step 3 Enter the Uplink Center Frequency. The Downlink Center Frequency will automatically be calculated when you press **Tab** or click in the **Downlink Center Freq** box. This information can be obtained from your satellite provider, as it is part of the satellite link budget process.
- Step 4 In the **Error Correction** drop-down list, select the type of forward error correction (FEC). See also [chapter 4, "iDirect Modulation Modes and FEC Rates,"](#) of the [iDirect Technical Reference Guide](#).
- Step 5 In **Power**, enter a value for the transmit power. The default is -25dBm.
- Step 6 Enter either a **Transmission Rate**, **Information Rate**, or **Symbol Rate**. See also [chapter 4, "iDirect Modulation Modes and FEC Rates,"](#) of the [iDirect Technical Reference Guide](#). Entering any of the rate values will cause the remaining rates to be automatically calculated. Typically, you would enter a desired transmission rate and the service provider would determine if that could be accomplished.
- a The Maximum Downstream **Information Rate** for NetModems is 9.1 Mbps, and for Series 3000s, 5000s and 7000s is 18 Mbps.
  - b **Symbol Rate** is related to **Transmission Rate** based on the selected **Modulation** as follows:
    - For BPSK, the **Symbol Rate** is equal to the **Transmission Rate**.
    - For QPSK, the **Symbol Rate** is half the **Transmission Rate**.
    - For 8PSK, the **Symbol Rate** is one third the **Transmission Rate**.

For example, if you enter 2800 kbps into the **Transmission Rate** box, the **Symbol Rate** box is automatically calculated to be 2800 ksym for BPSK, 1400 for QPSK, or 933.33 ksym for 8PSK.

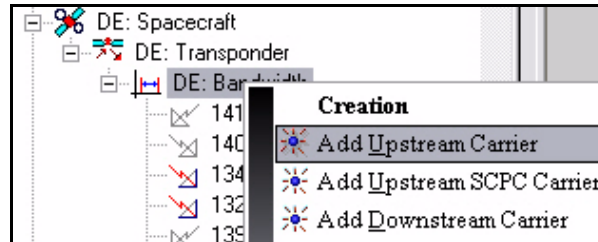
Note that the symbol rate must be between 64 and 5750 ksym.
- Step 7 In the **Assigned to Line Card** box, select the line card to which this carrier is to be assigned.
- Step 8 In **Timeplan Parameters**, enter the number of **FEC Blocks** in each frame. The frame length is automatically calculated, based on FEC Blocks, FEC rates and transmission data rate. iDirect recommends that the number of FEC blocks is set such that the frame length is ~125 ms.
- Step 9 **Frame Length** is automatically calculated based on transmission data rate.
- Step 10 Click **OK**. The outbound carrier appears in the Tree.

## 4.5.2 Adding Upstream TDMA Carriers

The Upstream carrier frequency is used to send data from remotes to the hub.

To add an Upstream carrier (Inbound Carrier), follow the procedure below:

- Step 1 Right-click **Bandwidth**, and select **Add Upstream Carrier**. The new carrier appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.



Modify Configuration Object - Network3 Upstream [128K]

**Information**

**Upstream Carrier - TDMA**

Inroute ID: 8

Name: Network3 Upstream [128K]

Uplink Center Freq: 1435 MHz

Downlink Center Freq: 1435 MHz

Power: -25 dBm

Carrier Spacing: 1.2

Error Correction: TPC-441/1024 (.431)

Modulation: BPSK

Assigned to Line Card: Infini 40018

Transmission Parameters

Transmission Rate: 594.43 kbps

Information Rate: 256 kbps

Symbol Rate: 594.43 ksym

Timeplan Parameters

Acquisition Aperture: 1020 sym

Guard Band: 8 sym

Frame Length: 125.636 ms

Traffic Slots: 66

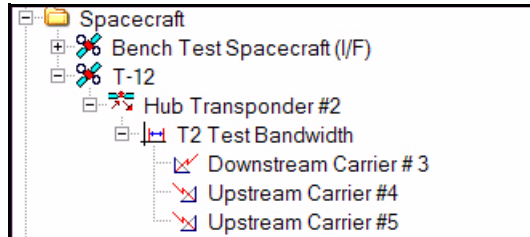
Other Parameters: Scrambling Differential Encoding IDR OFF



- Step 2 Enter a name for the upstream TDMA carrier.
- Step 3 Enter the **Uplink Center Frequency**. This frequency assignment is provided as part of the satellite link budget process and comes from the satellite provider.
- Step 4 The Downlink Center Frequency will automatically be calculated when you click in the **Downlink Center Freq** box, based on the previous transponder translation frequency.
- Step 5 In the **Error Correction** drop-down list, select the type of forward error correction (FEC). See also [chapter 4, "iDirect Modulation Modes and FEC Rates,"](#) of the [iDirect Technical Reference Guide](#).
- Step 6 Select the **Modulation** for your carrier: **BPSK**, **QPSK** or **8PSK**.
- Step 7 When building a new carrier, the **Assigned to Line Card** box is not available. The field is populated automatically after the Hub RFT is assigned to this satellite and this carrier is assigned under the hub line card configuration.
- Step 8 Enter either a **Transmission Rate**, **Information Rate**, or **Symbol Rate**. See also [chapter 4, "iDirect Modulation Modes and FEC Rates,"](#) of the [iDirect Technical Reference Guide](#). Entering any of the rate values will cause the remaining two rates to be automatically calculated.
- a The Maximum Downstream **Information Rate** for NetModems is 9.1 Mbps, and for Series 3000s, 5000s and 7000s is 18 Mbps.
- b **Symbol Rate** is related to **Transmission Rate** based on the selected **Modulation** as follows:
- For BPSK, the **Symbol Rate** is equal to the **Transmission Rate**.
  - For QPSK, the **Symbol Rate** is half the **Transmission Rate**.
  - For 8PSK, the **Symbol Rate** is one third the **Transmission Rate**.
- For example, if you enter 2800 kbps into the **Transmission Rate** box, the **Symbol Rate** box is automatically calculated to be 2800 ksym for BPSK, 1400 for QPSK, or 933.33 ksym for 8PSK.
- Note that the symbol rate must be between 64 and 5750 ksym.
- Step 9 In the **Timeplan Parameters** section:
- a The **Acquisition Aperture Length** is the size of the acquisition window in the Time Plan. It is automatically calculated for you.
- b **Guard Band** is the time between bursts on the TDMA upstream carrier. This parameter is typically set to eight symbols.
- c **Frame Length** and **Traffic Slots** for an upstream carrier are determined when the carrier is assigned to a line card in a network with a downstream

carrier already assigned. **Frame Length** is the size of the Time Plan frame in msec. Each frame is composed of or divided into many timeslots, based on data rate, FEC, etc. Each time slot is a slice of time allotted to a remote to send its data traffic.

Step 10 Click **OK** to save your settings. The Upstream Carrier appears in the Tree.

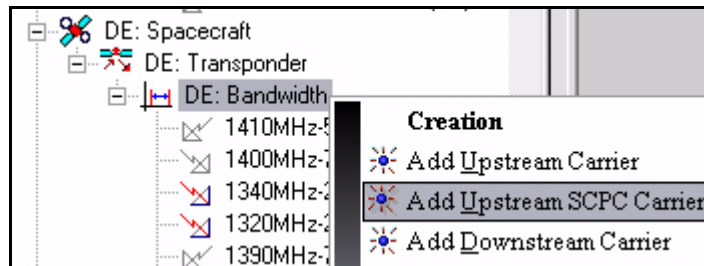


### 4.5.3 Adding Upstream SCPC Carriers

An Upstream SCPC carrier frequency is used to send data on a point-to-point connection between an iSCPC remote and the hub. An iSCPC line card or 5000/7000 iNFINITI series remote modem receives the SCPC upstream carrier at the hub. In the downstream direction, the iSCPC remote receives the SCPC carrier transmitted by the iSCPC line card, completing the point-to-point connection.


To add an Upstream SCPC carrier, follow the procedure below:

Step 1 Right-click on the bandwidth for your transponder and select **Add Upstream SCPC Carrier**. The new carrier appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.



**Modify Configuration Object - New Carrier #72**

**Information**

 **Upstream Carrier - SCPC**

Inroute ID:

Name:

Uplink Center Freq:  MHz

Downlink Center Freq:  MHz

Power:  dBm

Carrier Spacing :

Error Correction:

Modulation:

Assigned to Line Card:

Transmission Parameters

Transmission Rate:  kbps

Information Rate:  kbps

Symbol Rate:  ksym

Timeplan Parameters

FEC Blocks per Frame

Frame Length:  ms

Other Parameters:

Scrambling	IDR
Differential Encoding	OFF

Step 2 Enter a name for the upstream SCPC carrier.

Step 3 The remaining configuration of an upstream SCPC carrier is similar to that of a downstream carrier. Follow the instructions beginning with [Step 3](#) of [“Adding Downstream Carriers” on page 69](#) on to complete the carrier definition.



**NOTE**

When using an upstream SCPC carrier for iSCPC operation, the transmit power is based on the SCPC line card configuration, *not* on the upstream carrier configuration. For further information, please see [“Adding an iSCPC Line Card” on page 99](#).



## 5 Defining Network Components

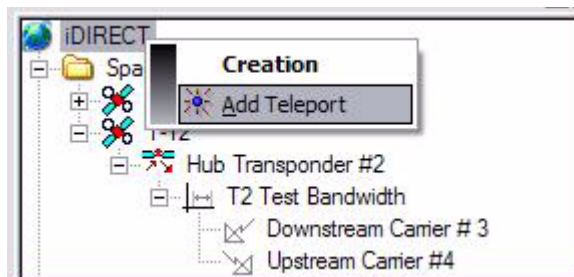
The Teleport is the highest component in the Tree hierarchy and represents the facility where the antenna and, typically, the rest of the Hub equipment is housed. After adding a Teleport, you can add a Protocol Processor (PP), Blades, Hub RFT, and Chassis to the Tree. This chapter discusses how to configure all of these components, with the exception of the chassis. Because the chassis requires a different type of configuration process, it is discussed in another chapter. See [chapter 9, “Configuring the Initial Hub Chassis.”](#)

This chapter contains the following sections:

- [“Adding a Teleport” on page 77](#)
- [“Adding a Backup Teleport” on page 78](#)
- [“Adding a Hub RFT” on page 82](#)
- [“Adding a Protocol Processor” on page 83](#)
- [“Adding a Protocol Processor Blade” on page 85](#)
- [“Setting Warning Properties for Protocol Processor Blades” on page 85](#)
- [“Adding a VLAN” on page 88](#)

### 5.1 Adding a Teleport

- Step 1 To add a Teleport, right-click the iDirect Globe at the top of the Tree and select **Add teleport**. The new teleport appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.





Modify Configuration Object - iDirect Teleport #1

Information | Geo Location

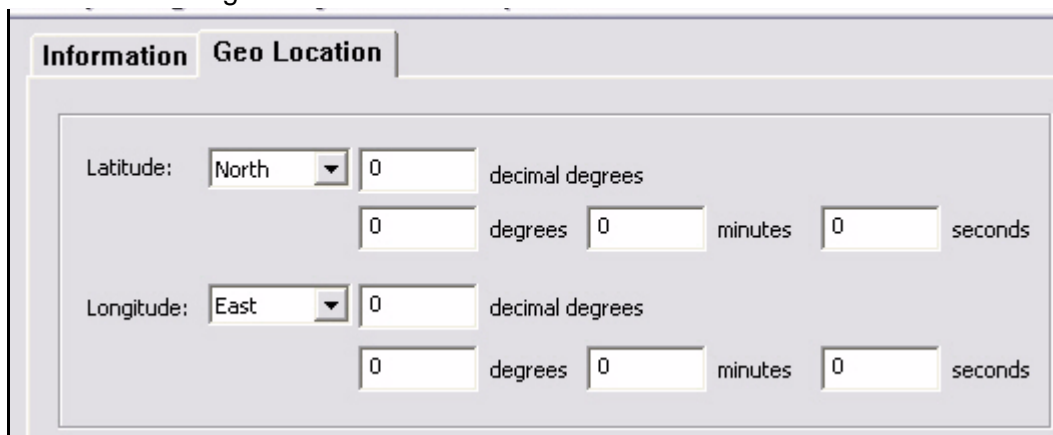
**Teleport**

Name: iDirect Teleport #1

Phone Number:

Step 2 On the **Information** tab, enter a name and a phone number for your Teleport facility.

Step 3 Click the **Geo Location** tab. The Geo Location identifies precisely where the Uplink facility (the Hub RFT) is geographically located on the Earth. The teleport transmits the uplink signal to the satellite and receives the downlink signal from the satellite.



Information | **Geo Location**

Latitude: North 0 decimal degrees  
0 degrees 0 minutes 0 seconds

Longitude: East 0 decimal degrees  
0 degrees 0 minutes 0 seconds

Step 4 Enter the exact **Latitude** and **Longitude** of your teleport facility. This information can be obtained from your service provider or can be determined with a GPS device. Be sure to select the correct hemisphere for each. Latitude represents North and South; longitude represents East and West.

Step 5 Click **OK** to save your settings. The Teleport appears in the Tree.

## 5.2 Adding a Backup Teleport

As part of the iDirect Geographic Redundancy feature, iBuilder allows you to create a fully-redundant backup teleport which can assume the role of your primary teleport in the event that the primary teleport becomes unavailable.

The procedure for configuring your backup teleport assumes that your primary teleport is already operational and that your backup teleport has been installed. Generally, the iBuilder configuration

of the backup components should be identical to the configuration of the primary teleport. During operation, any configuration changes that you make at the primary teleport should also be made at the backup teleport. This can be accomplished using the NMS database backup and restore utility described in the iDirect Technical Note [NMS Redundancy and Failover](#).



## NOTE

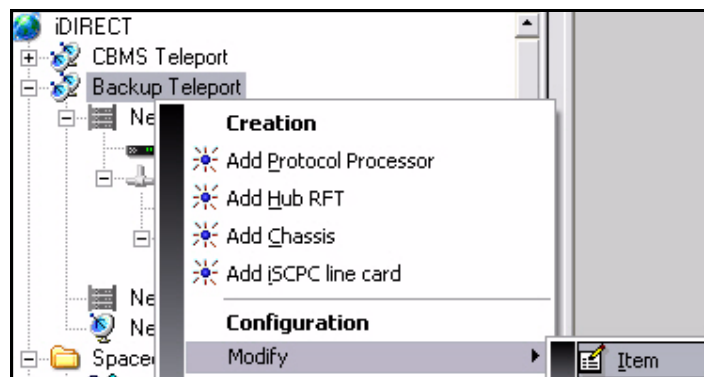
If you are using the same outbound carrier for your primary and backup teleports, the teleport operator must disable the backup transmitter while the primary teleport is operational. In the event of failure of the primary site, the teleport operator must enable the backup transmitter for the backup teleport to become operational.

Using iBuilder at the primary teleport, follow these steps to configure your backup teleport hub equipment and to add your existing remotes to the backup teleport's networks. The procedure assumes that your primary teleport and the networks it controls are already configured in iBuilder and operational.

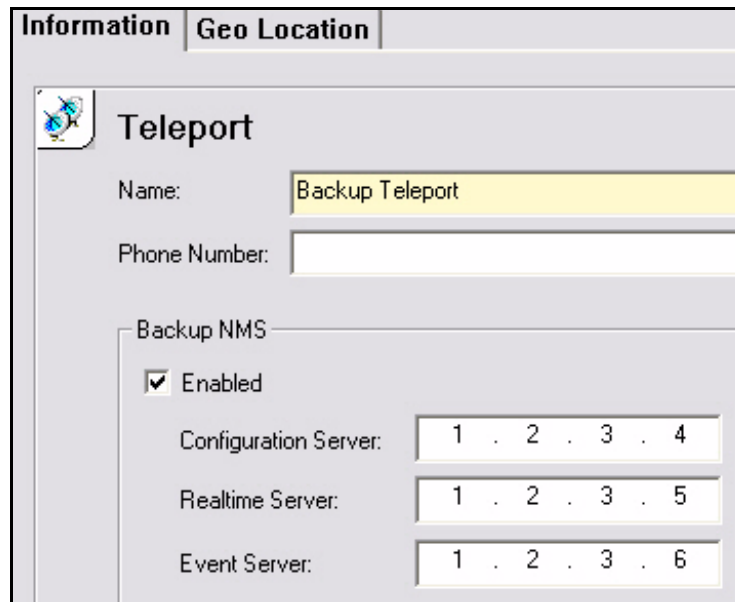
**Step 1** Add the backup teleport to your network by following the steps in the section [“Adding a Teleport” on page 77](#). Then configure all the components of the backup teleport, including:

- The Hub RFT (See [“Adding a Hub RFT” on page 82](#))
- The Protocol Processor (See [“Adding a Protocol Processor” on page 83](#))
- Protocol Processor Blades (See [“Adding a Protocol Processor Blade” on page 85](#))
- Networks (See [“Adding a Network” on page 93](#))
- Line Cards (See [“Adding a Tx Line Card, a Tx/Rx Line Card, or a 10000 Series Hub” on page 94](#))
- Inroute Groups (See [“Adding Inroute Groups” on page 107](#))

**Step 2** Right-click the backup teleport in the network tree and select **Modify** → **Item**.



Step 3 In the **Backup NMS** area of the **Teleport** dialog box, select **Enabled**. Then enter the IP address (or addresses) of the NMS server(s) at your backup teleport.)

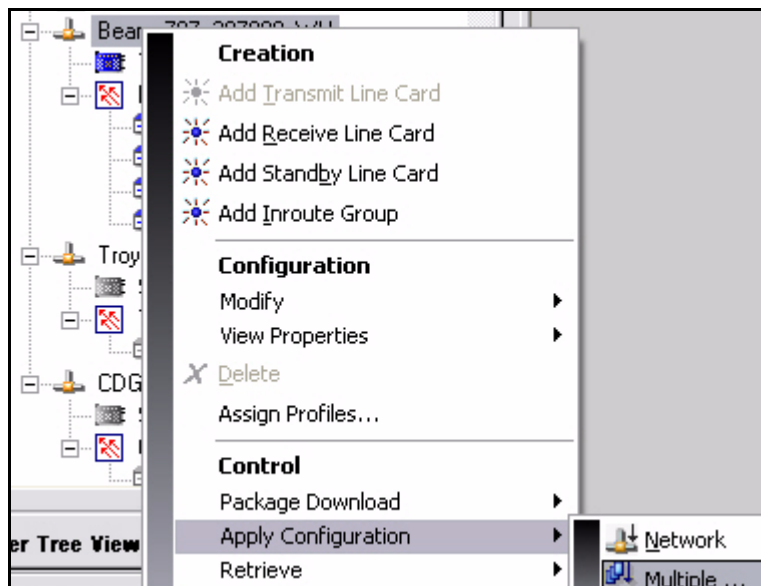


**NOTE**

A distributed NMS requires up to three IP addresses for the NMS servers. If you do not have a distributed NMS at the backup site, all three IP addresses should be identical.

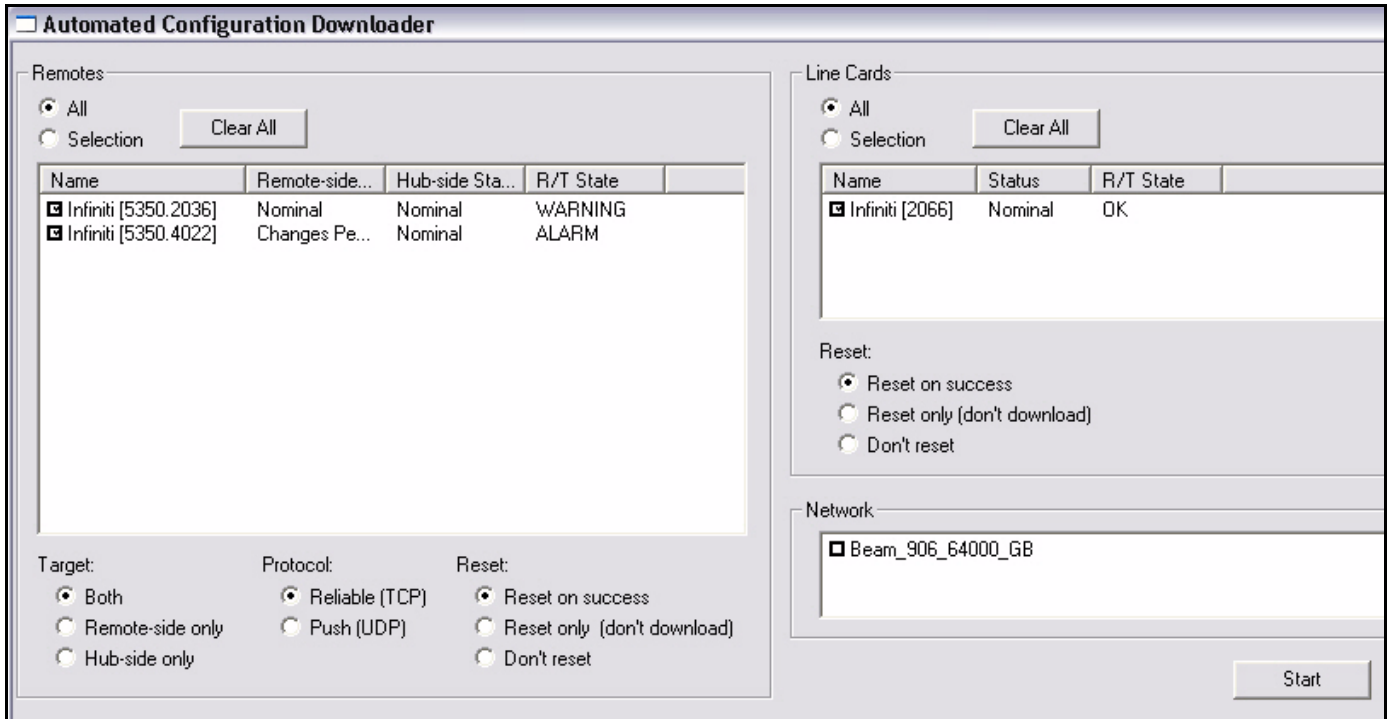
Step 4 After you have enabled the **Backup NMS**, all remotes will have changes pending. Apply the changes for each network as follows:

- a Right-click the network in the tree and select **Apply Configuration → Multiple**.





- b In the **Automated Configuration Downloader** dialog box, select all remotes and line cards.

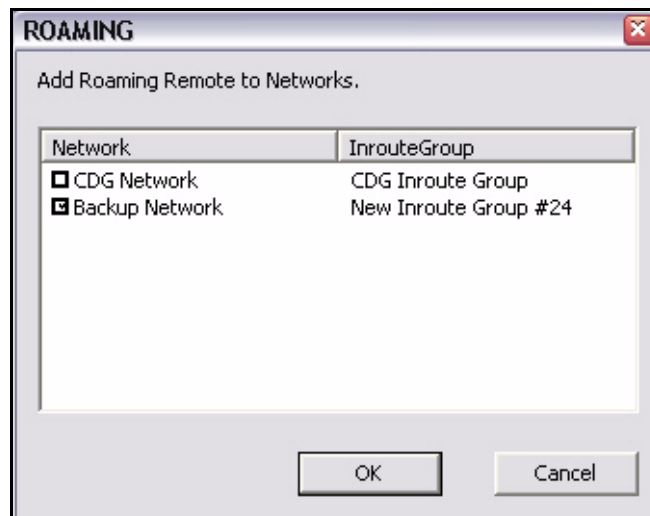


- c Click the **Start** button.

Step 5 Right-click the protocol processor and select **Apply Configuration** from the menu. Then click **Yes** in the confirmation dialog box to update the protocol processor and blades.

Step 6 Add each of your remotes to the backup teleport as follows:

- a Right-click the remote in the network tree and select **Add to Networks** from the menu to display the **Roaming** dialog box.

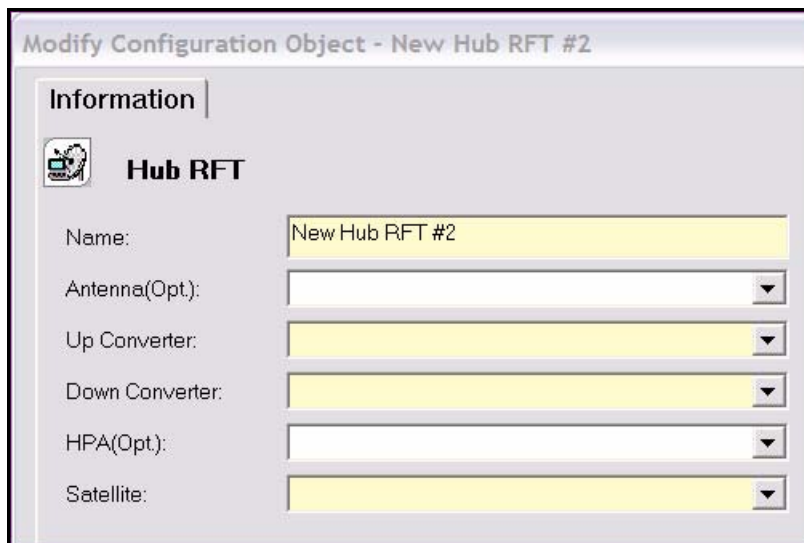
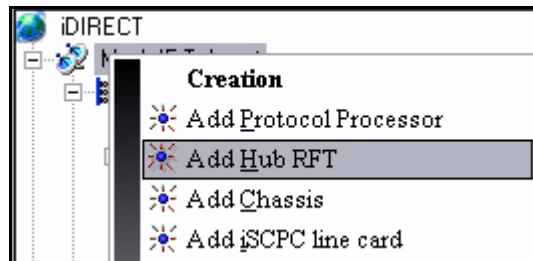


- b In the **Roaming** dialog box, select the remote's **Network** under the backup teleport.
- c Click **OK** to save your changes.

### 5.3 Adding a Hub RFT

Before you define the Hub RFT, you should define the elements in the Hub RFT Components folders. See [“Defining Hub RFT Components and the Satellite” on page 61](#).

- Step 1 To create a Hub RFT, right-click **Teleport**, select **Add Hub RFT**. The new Hub RFT appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.



- Step 2 Enter a name for the Hub RFT, and then select the subcomponents for the Hub RFT from each of the drop-down list boxes.
- Step 3 Select the Satellite to which this Hub RFT is assigned.
- Step 4 Click **OK**. The Hub RFT appears in the Tree with its new name.

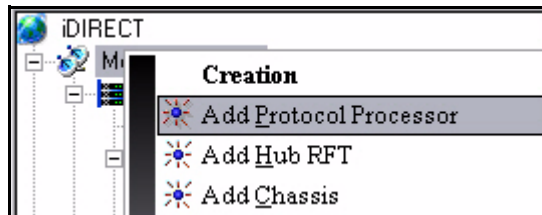
## 5.4 Adding a Protocol Processor

After adding the Hub RFT, create the Protocol processor. Networks can be expanded by adding additional processing elements, referred to as Blades, to the Protocol Processor. The Protocol Processor architecture provides both scalability and automatic failover. If a blade fails, its load is automatically distributed across the remaining blades; the previous manual switchover process is obsolete.



**WARNING** iDirect strongly recommends changing your default password on the protocol processor as soon as possible.

- Step 1 To create a Protocol Processor (PP), right-click the **Teleport**, and select **Add Protocol Processor**. The new Protocol Processor appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.



Information | Blades | VLans | **Warning Properties** | Custom

### Protocol Processor

Name: UAT-IF Protocol Processor

User Password:

Admin Password:

Download Monitor Credentials: 2886762762

Upstream Gateway: 172 . 16 . 128 . 1

Enabled RIPv2 (default VLAN only)

Upstream Interface: eth0

Tunnel Interface: eth1

Multicast Groups

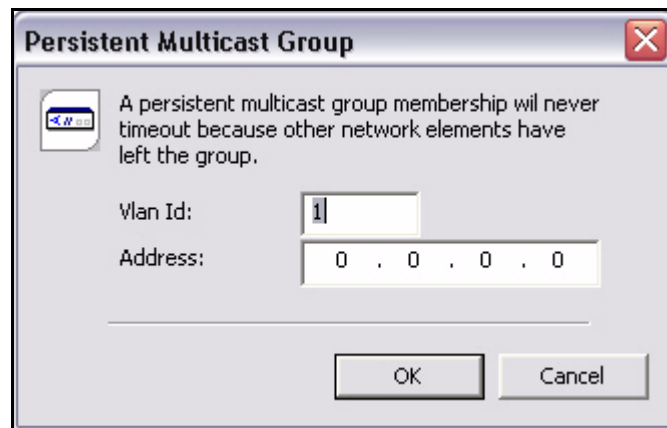
Vlan Id	Address

Add... Edit... Remove

- Step 2 On the **Information** tab, enter a name for your Protocol Processor (PP).
- Step 3 Enter your **User Password** and the **Admin Password**. The default passwords are shown in the dialog box above. These passwords are used for the Console and telnet logins. Make sure you record any changed password in case you forget it. You will not be able to log in with the default passwords once they are changed.
- Step 4 In **Download Monitor Credentials**, enter any value greater than one and less than four billion. (This number is used for multicast firmware image download and can be duplicated across multiple PPs.)
- Step 5 In **Upstream Gateway**, enter the IP address of your upstream router. This should be the address of the router interface connected to the upstream LAN segment.
- Step 6 Click **Enabled RIPv2** if you want the Protocol Processor to advertise remote routes to your upstream router using the protocol RIPv2. This setting affects your default VLAN only.

- Step 7 Select the **Upstream** and **Tunnel** Interfaces. The tunnel is the LAN segment between the Protocol Processor and the line cards.
- Step 8 A persistent multicast group is a multicast group that includes all remotes communicating with this protocol processor. A remote will be a member of this group even if it has not been acquired into the network.

To add a persistent multicast group, click **Add** in the **Multicast Groups** section of the **Information** tab. When the **Persistent Multicast Group** dialog box appears, enter the **Vlan Id** and the **IP Address** of the multicast group you want to add.



## 5.5 Setting Warning Properties for Protocol Processor Blades

You can use iBuilder to modify both global properties of protocol processor blade warnings and warning properties for all blades of individual protocol processors. To change the global warning properties, select **Global Warnings for Blades** from the **Edit** menu. To change warning properties for individual protocol processors, click the **Warning Properties** tab for the protocol processor you want to modify.



### NOTE

When you override global blade warnings on the Protocol Processor **Warning Properties** tab, the new settings are applied to all blades of that protocol processor. You cannot override the settings for the individual blades of a protocol processor.

For details on configuring warning properties for line cards, remotes and protocol processors, please see [“Configuring Warning Properties” on page 55](#).

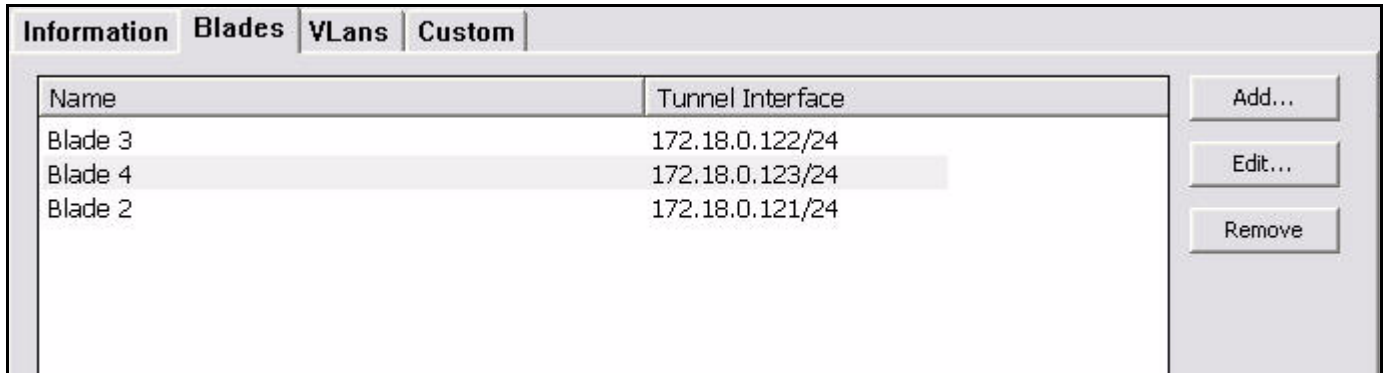
## 5.6 Adding a Protocol Processor Blade

The Protocol Processor level of the tree represents a set of one or more blades. If a blade fails, its load is automatically distributed across the remaining blades; the previous manual switchover process is obsolete.

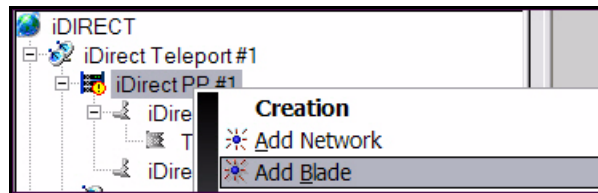
To add a Blade to a Protocol Processor, follow these steps:

Step 1 You can use either the **Blades** tab of the Protocol Processor or the Tree context menu to add a Blade. Both methods are shown here.

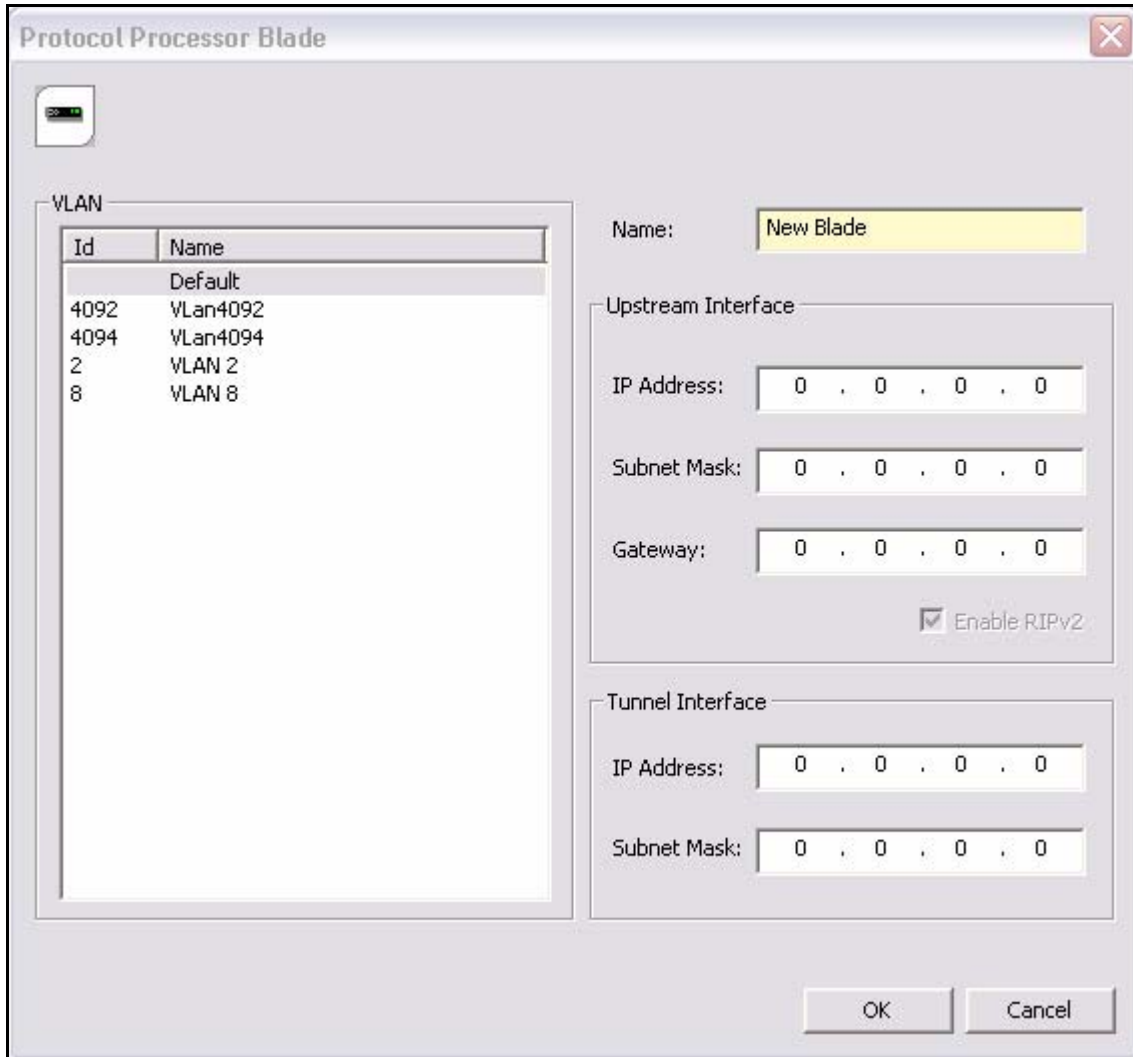
- a Right-click the Protocol Processor in the Tree and select **Modify → Item**. Then select the **Blades** tab and click the **Add** button.



- a Alternatively, right-click the Protocol Processor in the Tree and select **Add Blade**.



In either case, the **Protocol Process Blade** dialog box appears allowing you to define its parameters.



The dialog box titled "Protocol Processor Blade" contains a "VLAN" section with a table listing VLANs. To the right, there are input fields for "Name" (set to "New Blade"), "Upstream Interface" (with IP Address, Subnet Mask, and Gateway fields, all set to "0 . 0 . 0 . 0"), and "Tunnel Interface" (with IP Address and Subnet Mask fields, both set to "0 . 0 . 0 . 0"). There is also a checked checkbox for "Enable RIPv2". "OK" and "Cancel" buttons are at the bottom right.

Id	Name
	Default
4092	Vlan4092
4094	Vlan4094
2	VLAN 2
8	VLAN 8

- Step 2 Enter a name for the blade.
- Step 3 Enter the Upstream Interface information for the default VLAN. (iBuilder will automatically assign the Upstream Interface information for other existing VLANs.)
- Step 4 Enter the Tunnel Interface information for the default VLAN.

## 5.7 Adding a VLAN

Due to the distributed architecture of the Protocol Processor, all blades in a blade set combine to form a single, logical, upstream interface. However, each blade must have a distinct IP address for each VLAN. This is illustrated below for a single VLAN.

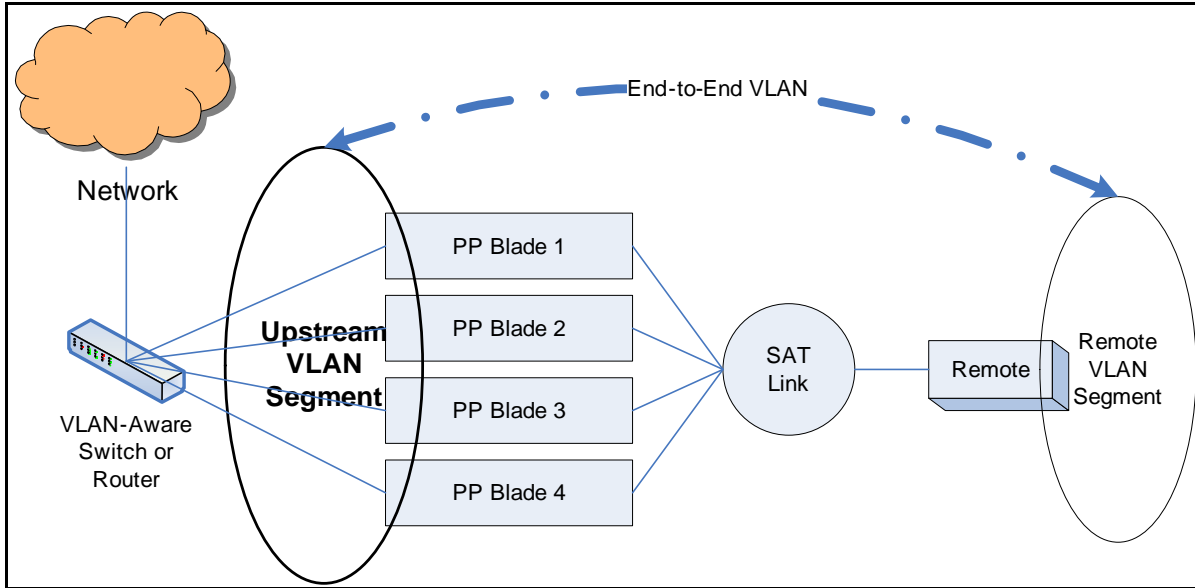
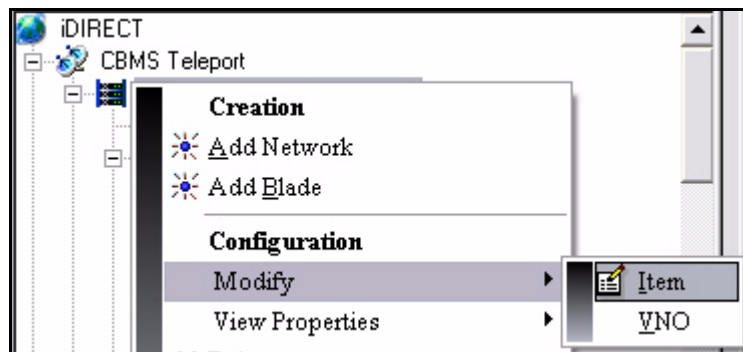


Figure 5-1: Uplink VLAN Segment in a PP Blade Environment

For more information on VLANs, see [“VLAN and LAN Information” on page 123](#).

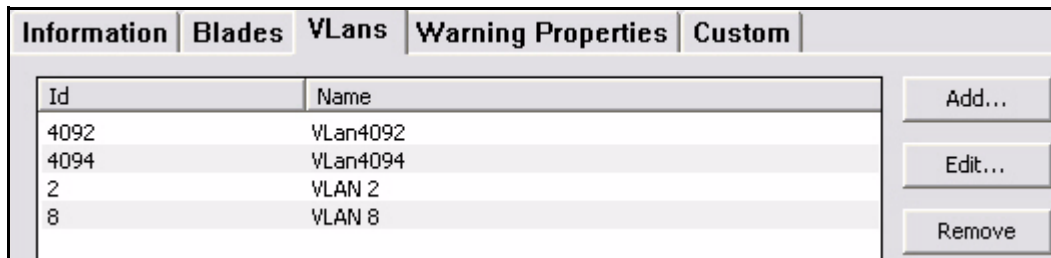
To add a VLAN:

- Step 1 Right-click the **Protocol Processor** in the Tree and select **Modify** → **Item**.

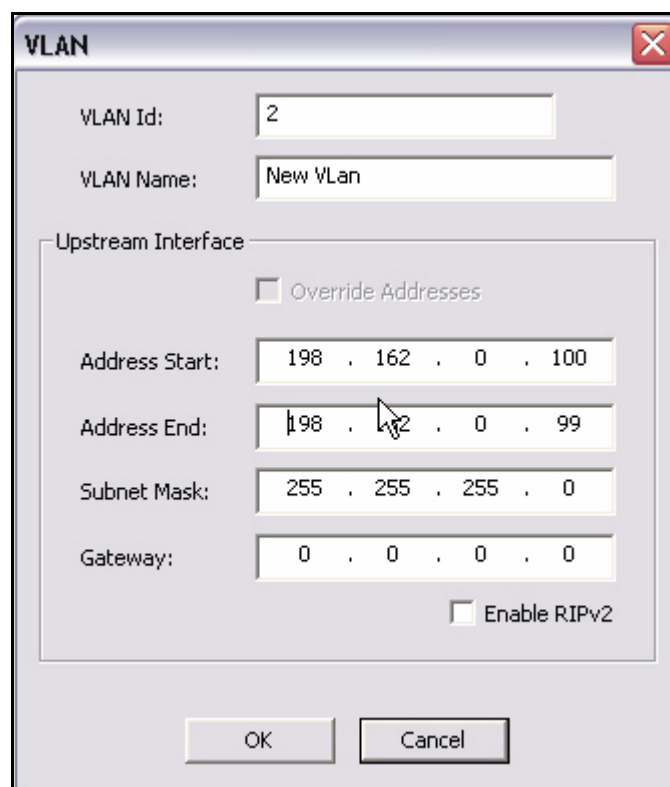




Step 2 Select the **VLANS** tab in the Protocol Processor dialog box.



Step 3 Click **Add** to display the **VLAN** dialog box.



Step 4 Enter a **VLAN ID** and **VLAN Name**. VLAN IDs can range from 2 to 4094.

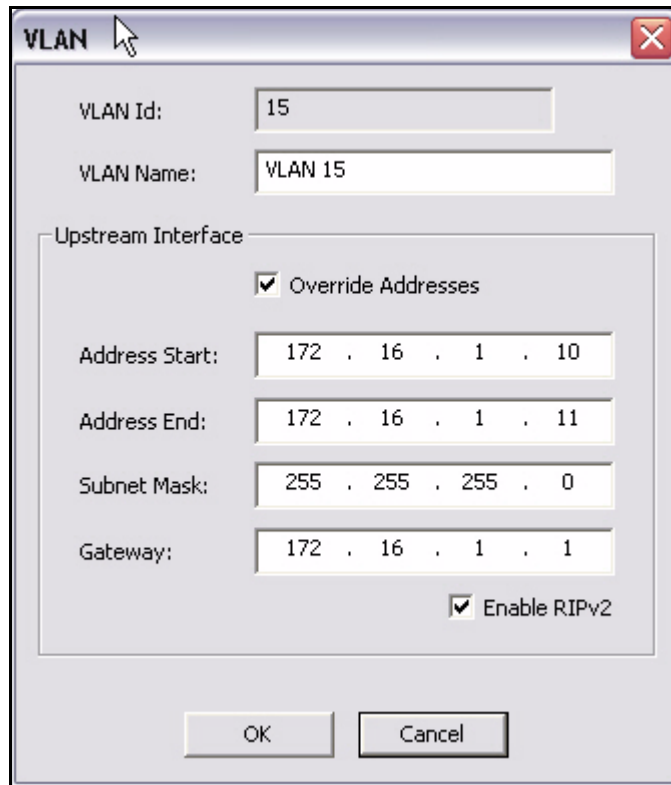
Step 5 Select **Enable RIPv2** to advertise remote routes to your upstream router using the protocol RIPv2.

Step 6 In the **Address Start** field, specify the Upstream Interface IP Address to be used by the first blade. iBuilder automatically enters the remaining IP addresses

Step 7 Click **OK**. A new Upstream VLAN Interface is now defined.

You can modify the automatically-assigned addresses as follows:

- Step 1 On the **VLAN** tab, select the row containing the **ID** and **Name** of the interface you want to modify and click **Edit**.



- Step 2 Select the **Override Addresses** check box.

- Step 3 Enter the IP addressing information as desired.

If a new blade is subsequently added for scalability, all VLAN end addresses will be automatically updated to give the new blade the appropriate upstream interfaces, and the VLANs will be added to the new blade.

### **Special VLAN Configuration**

VLAN support requires one special configuration task, which must be done at the Linux level on the Protocol Processor. To support VLAN, the upstream Ethernet port (eth0) of the Protocol Processor must be configured with an MTU of 1504. This is done by typing **"MTU = 1504"** (without quotation marks) in the file `/etc/sysconfig/network-scripts/ifcfg-eth0`. Once this is done, save the file. After saving the file, the network services must be restarted with the following command: **service network restart**.



### **NOTE**

If a line like this is already present for eth0, but contains a different value (e.g. 1500), then edit the line to the above value. The MTU value can also be checked by typing **ifconfig** at the prompt to display the MTU size.



**WARNING** Do not change the default MTU (1500) on the tunnel interface (eth1).



## 6 Defining Networks, Line Cards, and Inroute Groups

The network child elements include the line cards or 10000 series satellite hub, the inroute groups, and the remotes. Before you add a Network, you must have already added a Protocol Processor.

This chapter contains the following sections:

- [“iDirect Line Card and Hub Models” on page 93](#)
- [“Adding a Network” on page 93](#)
- [“Adding a Tx Line Card, a Tx/Rx Line Card, or a 10000 Series Hub” on page 94](#)
- [“Setting Warning Properties for Line Cards” on page 97](#)
- [“Adding Receive \(Rx\) Line Cards” on page 97](#)
- [“Adding an iSCPC Line Card” on page 99](#)
- [“Defining a Standby Line Card” on page 101](#)
- [“Adding Inroute Groups” on page 107](#)

### 6.1 iDirect Line Card and Hub Models

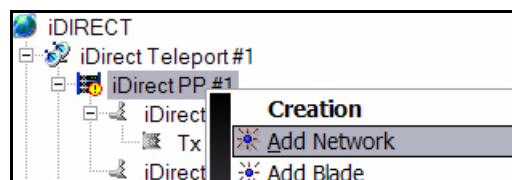
iBuilder supports all of the following line card and hub models:

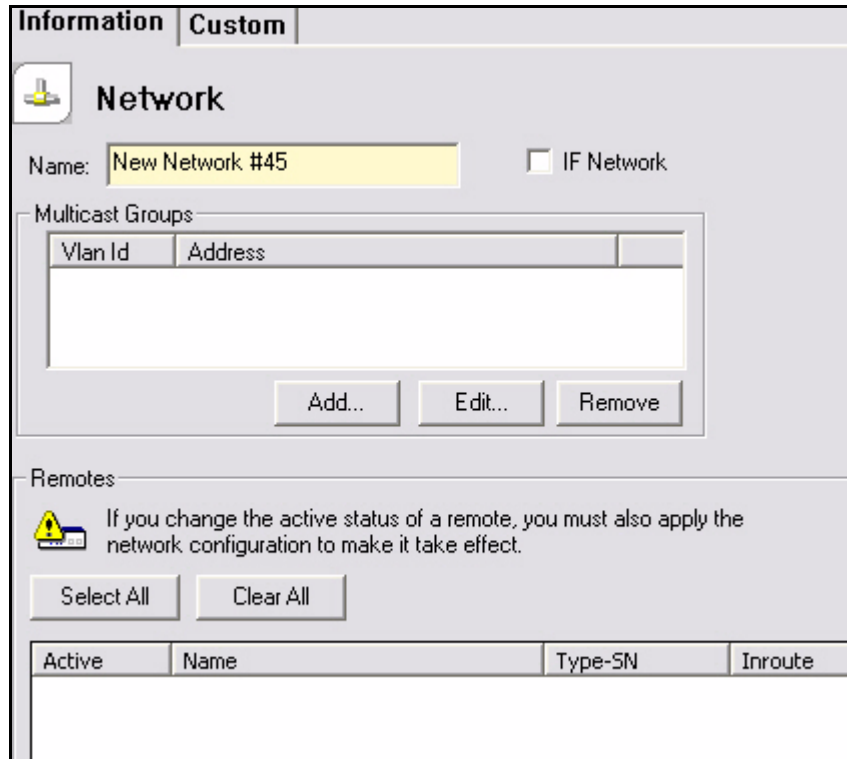
- NetModem II and NetModem II-Plus line cards
- iNFINITI M1D1 line card
- iNFINITI M0D1 line card (receive-only)
- iNFINITI M0D1-NB line card (narrow-band, receive-only)
- iSCPC M1D1 line card (for point-to-point, SCPC connections)
- iNFINITi 10000 series Private Hub
- iNFINITI 10000 series Mini Hub

### 6.2 Adding a Network

To create the network, follow the procedure below:

- Step 1 Right-click the **Protocol Processor (PP)**, and select **Add Network**. The new network appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.





**Information** Custom

**Network**


Name:   IF Network

Multicast Groups

Vlan Id	Address

Add... Edit... Remove

Remotes

 If you change the active status of a remote, you must also apply the network configuration to make it take effect.

Select All Clear All

Active	Name	Type-SN	Inroute

Step 2 Enter a name for the Network.

Step 3 Click the **IF Network** check box *only* if you are creating an L-Band/Bench Test network. This will disable the Geo Location entry for all remotes on this network.

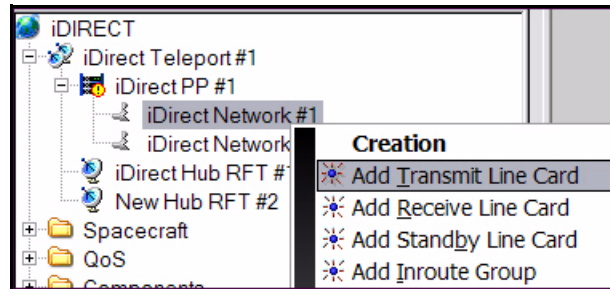
### 6.3 Adding a Tx Line Card, a Tx/Rx Line Card, or a 10000 Series Hub

After creating the Network, you must add either a transmit (Tx) line card, a transmit/receive (Tx/Rx) line card, or a 10000 series hub. A 10000 series Satellite Hub is configured by selecting the correct hub model (Private Hub or Mini-Hub) in the drop-down menu. Only one line card in each network may have transmit capabilities. You should have already created a carrier. If you have not, the line card will have an *Incomplete* status until a carrier is created and assigned to it.

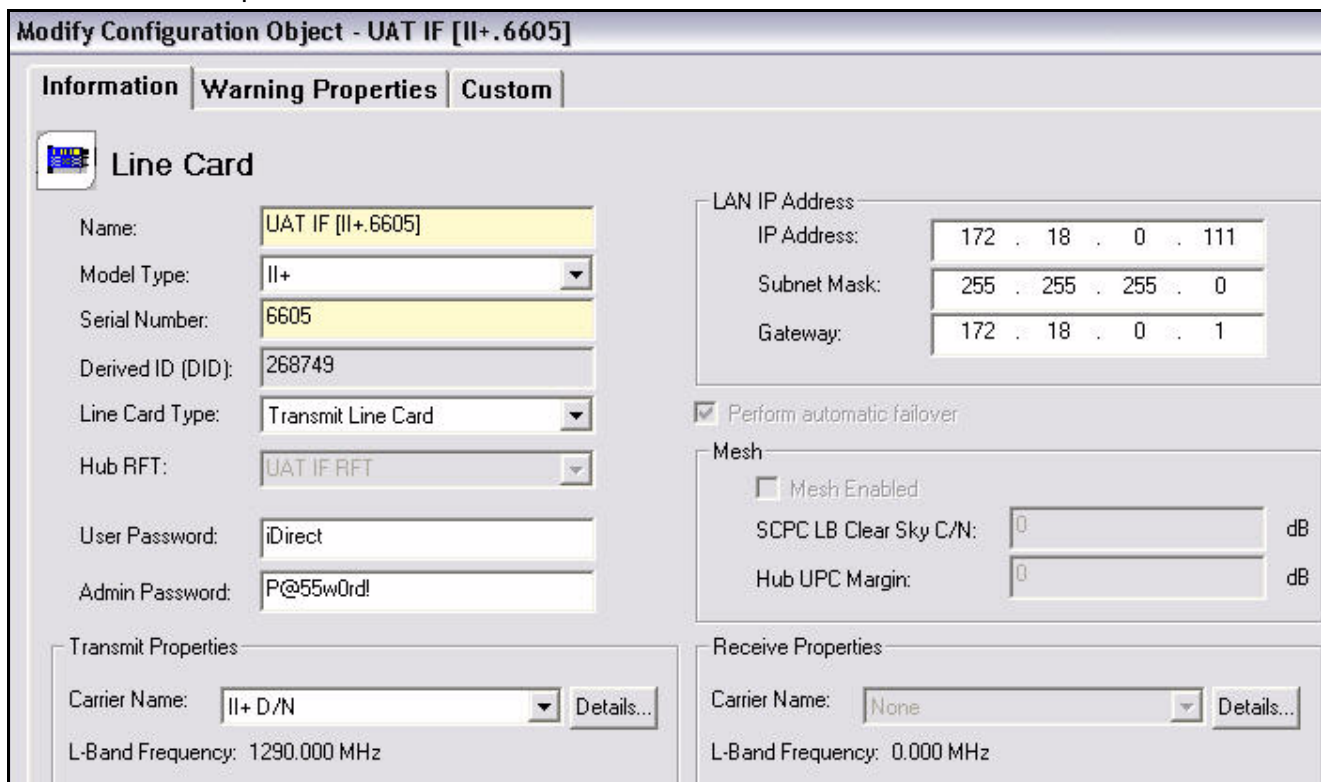
If you are adding mesh capabilities to your network, you must use an M1D1 line card or a Private Hub for your mesh downstream carrier. Mini hubs and Private Hub-S models are not supported. Selecting mesh-enabled will configure your line card or hub to monitor the downstream carrier. For more details on adding mesh communications to your iDirect network see [chapter 3, "Mesh Technical Description,"](#) of the [iDirect Technical Reference Guide](#).

To add a transmit line card, follow the procedure below:

Step 1 Right-click **Network** and select **Add Transmit Line Card**. The new line card appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define their basic parameters.



Step 2 Enter a name for the line card.



**Modify Configuration Object - UAT IF [II+.6605]**

Information | Warning Properties | Custom

**Line Card**

Name: UAT IF [II+.6605]

Model Type: II+

Serial Number: 6605

Derived ID (DID): 268749

Line Card Type: Transmit Line Card

Hub RFT: UAT IF RFT

User Password: iDirect

Admin Password: P@55w0rd!

LAN IP Address

IP Address: 172 . 18 . 0 . 111

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 172 . 18 . 0 . 1

Perform automatic failover

Mesh

Mesh Enabled

SCPC LB Clear Sky C/N: 0 dB

Hub UPC Margin: 0 dB

Transmit Properties

Carrier Name: II+ D/N Details...

L-Band Frequency: 1290.000 MHz

Receive Properties

Carrier Name: None Details...

L-Band Frequency: 0.000 MHz

Step 3 Select a **Model Type**. The model type you select must match the installed line card or 10000 series hub. If you are configuring a **Mesh Enabled** line card, you must select either **PrivateHub** or **M1D1** as the **Model Type**.

Step 4 Enter a **Serial Number**. A system-generated DID is displayed in the **Derived ID** box.

- a With the introduction of the iDirect iFINITI series™ platform, serial numbers are no longer sufficient to uniquely identify remotes and line cards. Serial numbers are guaranteed to be unique within a particular model type, but could be duplicated from one model type to another. To avoid potential duplicates and the problems they would cause, iDS 6.0 introduces the

concept of a *Derived ID*, or DID. The DID is a 32-bit integer formed by joining a model type code with a unit's serial number. Each remote and line card will have a unique DID value.

- b In the NMS, the DID is typically formatted as **<Model Type Name>.<Serial Number>**, for example **II+.10045** or **5150.1492**. Occasionally you may see the raw DID, however, especially when viewing server log files or console output. You may also select the raw DID as a column to view in iBuilder's Details View. Note: the model type code for NetModem II remotes is zero, so the raw DID for these units is equal to the serial number.

Step 5 Select the **Line Card Type** from the drop-down box. You may select a transmit or transmit/receive line card. See [chapter 4, "iDirect Modulation Modes and FEC Rates,"](#) of the [iDirect Technical Reference Guide](#).

Step 6 Select the **Hub RFT** that is associated with this network. This selection gives you a list of carriers.

Step 7 Enter the IP Address, Subnet Mask, and Gateway.

Step 8 If you are adding a mesh-enabled line card:

- a Select **Mesh Enabled**.
- b When you commission the line card, you must specify the following **Uplink Control Parameters** for a transmit line card if it is going to be used in a mesh network:
  - **SCPC LB Clear Sky C/N** is the C/N of the loopback SCPC carrier as measured by the line card modem under clear sky conditions. This value is typically set during hub commissioning.
  - **Hub UPC Margin** is the maximum amount of uplink power control available at the hub through an external device.

For more information on setting these parameters, see ["Set the Clear Sky C/N Parameter for a Mesh Outroute" on page 247](#) and ["Set the UPC Margin for a Mesh Outroute" on page 248](#).

Step 9 By default, the **User Password** is set to *iDirect* and the admin password is set to *P@55w0rd!*. You may specify alternate passwords.

Step 10 Select the **Transmit Carrier** associated with this line card. If this is a transmit/receive line card, also select the **Receive Carrier**.

Step 11 The line card appears in the Tree under the Network.



## WARNING

You must correctly specify both the serial number and the model type for a line card or 10000 series hub to function properly. If you configure an M1D1 card as an M0D1 card, for example, the line card will not operate in a network.



## 6.4 Setting Warning Properties for Line Cards

You can use iBuilder to modify both global properties of line card warnings and warning properties for individual line cards. To change global warning properties for line cards, select **Global Warnings for Linecards** from the **Edit** menu. To change warning properties for individual line cards, click the **Warning Properties** tab for the line card you want to modify.

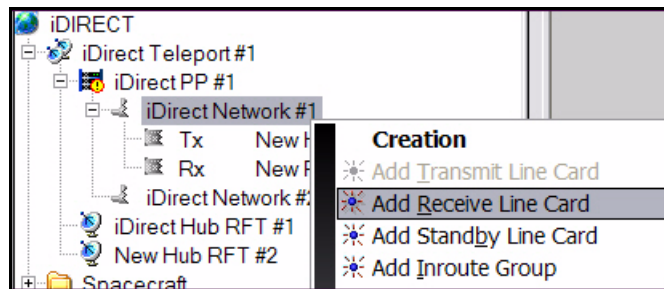
For details on configuring warning properties for line cards, remotes and protocol processor blades, please see [“Configuring Warning Properties” on page 55](#).

## 6.5 Adding Receive (Rx) Line Cards

Configure the desired number of receive line cards for this network, configuring only one per inroute. You may have up to 19 receive line cards per chassis. Before adding the line card, you must have defined a carrier.

To add a receive line card, follow the procedure below:

- Step 1 Right-click **Network** and select **Add Receive Line Card**. The new line card appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.



**Modify Configuration Object - New Hub #5146 [Modified]**

Information | Warning Properties | Custom

**Line Card**

Name:

Model Type:

Serial Number:

Derived ID (DID):

Line Card Type:

Hub RFT:

User Password:

Admin Password:

LAN IP Address

IP Address:

Subnet Mask:

Gateway:

Perform automatic failover

Mesh

Mesh Enabled

SCPC LB Clear Sky C/N:  dB

Hub UPC Margin:  dB

Transmit Properties

Carrier Name:  Details...

L-Band Frequency: 0.000 MHz

Receive Properties

Carrier Name:  Details...

L-Band Frequency: 0.000 MHz

- Step 2 You may use the system-generated generic name or enter a new name for the card.
- Step 3 Select the **Model Type** of the line card.
- Step 4 Enter a **Serial Number**. A system-generated DID is displayed in the **DID** box.
- Step 5 Enter the IP Address, Subnet Mask, and Gateway.
- Step 6 By default, the **User Password** is set to *iDirect* and the admin password is set to *P@55w0rd!*. You may specify alternate passwords.
- Step 7 In **Receive Properties**, select the **Carrier** associated with this line card.
- Step 8 The receive line card appears in the Tree under the Network.



**NOTE**

Since a receive line card requires no special configuration to be used for mesh, you cannot select **Mesh Enabled** when adding a receive line card for a mesh inroute group. Any receive line card becomes “mesh-enabled” by virtue of adding it to a mesh-enabled inroute group. See [“Adding Inroute Groups” on page 107](#).

## 6.6 Adding an iSCPC Line Card

An iSCPC line card is the hub equipment that transmits and receives the SCPC carriers used in a point-to-point connection with an iSCPC remote. You can configure the following iDirect **Model Type** as an iSCPC “line card:”

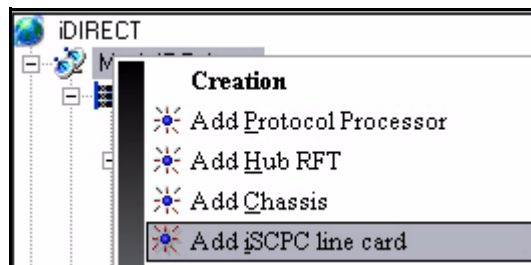
- iSCPC M1D1 Line Card

For the most part, iSCPC line cards, iSCPC remotes, and other iDirect remotes share a common set of parameters and are defined using similar dialog boxes. This section only discusses how to add an iSCPC line card to the network tree and select a hub RFT. The instructions for defining parameters common to iSCPC line cards and remotes are contained in [chapter 7, “Configuring Remotes,”](#) on [page 93](#).

As with TDMA networks, you must configure a Hub RFT record for the hub end point of an iSCPC link, and a set of VSAT components for the remote end point. You may use traditional VSAT components in your Hub RFT, such as iDirect-supported BUCs and LNBS, by defining these components in the “HubRFT Components” folder in iBuilder’s network tree. You may also use an existing Hub RFT definition in iBuilder.

To add an iSCPC line card, follow the procedure below:

- Step 1 Right-click your Teleport and select **Add iSCPC Line Card**. The new line card appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define its basic parameters.



Information	IP Config	QoS	VSAT	Warning Properties	Custom
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <h3>Remote</h3> <p>Name: <input type="text" value="New iSCPC Line Card #126"/></p> <p>Model Type: <input type="text" value="M1D1-iSCPC"/></p> <p>Serial Number: <input type="text" value="0"/></p> <p>Derived ID (DID): <input type="text" value="9699328"/></p> <p>Hub RFT: <input type="text" value="None"/></p> <p>User Password: <input type="text" value="iDirect"/></p> <p>Admin Password: <input type="text" value="P@55w0rd!"/></p> <p> <input type="checkbox"/> Active      <input type="checkbox"/> MUSiC Box  <input type="checkbox"/> Link Encryption      <input type="checkbox"/> Disable Tx P/W/M         </p> <div style="display: flex;"> <div style="width: 45%;"> <p>Compression</p> <p><input type="checkbox"/> TCP payload</p> <p><input type="checkbox"/> UDP header</p> <p><input type="checkbox"/> UDP payload</p> </div> <div style="width: 55%;"> <p>Mesh</p> <p><input type="checkbox"/> Enabled</p> <p>SCPC Clear Sky C/N: <input type="text" value="0"/> dB</p> <p>TDMA LB Clear Sky C/N: <input type="text" value="0"/> dB</p> </div> </div> </div> <div style="width: 50%;"> <p>Customer</p> <p>Name: <input type="text"/></p> <p>Phone Number: <input type="text"/></p> <p>Commission Date: <input type="text"/></p> <p>Contract Number: <input type="text"/></p> <p>Site Notes: <div style="border: 1px solid gray; height: 100px;"></div></p> <p>Distributor</p> <p>Name: <input type="text"/></p> <p>Phone Number: <input type="text"/></p> <p>Fax Number: <input type="text"/></p> </div> </div>					
<p>Transmit Properties</p> <p>Carrier Name: <input type="text" value="Upstream Carrier #75"/> <input type="button" value="Details..."/></p> <p>L-Band Frequency: 0.000 MHz</p> <p>Initial Power: <input type="text" value="-25"/> dBm</p> <p>Max Power: <input type="text" value="0"/> dBm</p>			<p>Receive Properties</p> <p>Carrier Name: <input type="text" value="Downstream Carrier #76"/> <input type="button" value="Details..."/></p> <p>L-Band Frequency: 0.000 MHz</p>		

- Step 2 Enter a **Name** for the line card.
- Step 3 Select the **Model Type** of the line card or remote you are using to terminate your SCPC connection at the hub.
- Step 4 Enter a **Serial Number**. A system-generated DID is displayed in the **DID** box.
- Step 5 Select the **Hub RFT** that is associated with your iSCPC line card.
- Step 6 At this point, the procedure for configuring the iSCPC line card is similar to the procedure for configuring a remote. To complete the configuration of the line card, follow the instructions in [chapter 7, "Configuring Remotes,"](#) beginning with the section titled "[Information Tab](#)" on page 116. Special considerations related to iSCPC line cards are noted in those instructions.

## 6.7 Defining a Standby Line Card

Only one standby line card may be defined for any one network. Standby line cards are configured similarly to transmit and receive line cards, by right-clicking **Network** and selecting **Add Standby Line Card**, or by selecting **Standby** in the **Line Card Type** drop-down box in the Modify Configuration dialog box.

When a standby line card is defined, the NMS can automatically detect the failure of an operational line card in a network and will swap that card with the standby line card. It is not required that a standby line card be configured for a network. If there is no standby configured, the NMS servers will not attempt to initiate the failover operation.



### NOTE

When configuring a line card for Tx standby or Tx/Rx standby, ensure that the Tx IFL cable is connected.

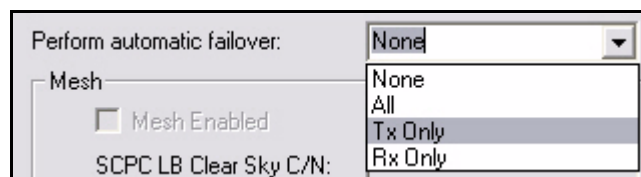
### 6.7.1 Selecting Automatic Failover

By default, a standby line card backs up all other line cards in a network. To improve failover time for the most critical line card (the transmit line card), the standby is pre-loaded with the transmit line card's configuration parameters. In the event that the transmit line card fails, the standby can assume its role within a matter of seconds. (The phrase "transmit line card" as used here refers to both transmit and transmit/receive line cards.) Failover of receive line cards takes longer, requiring the NMS to send the failed card's configuration to the standby and then to reset it for the failover to complete.

The option to command a standby line card to back up only the transmit line card allows you to favor the card that is the most critical to the network. In a multi-inroute, frequency-hopping network, the failure of a receive-only line card results in diminished upstream bandwidth only; remotes will automatically load-balance across the remaining receive line card(s) without dropping out of the network. If the transmit line card fails, however, the entire network will be out of service.

You can guard against a double failure by setting the standby line card to back up the transmit line card only. This ensures that the standby line card will be available to take over for a failed transmit line card even in the case of a prior receive line card failover.

You can control the line card's behavior during failover by selecting the desired option in the **Perform Automatic Failover** drop-down list on the standby line card's Modify dialog. Four selections are available in the menu:



- Select **None** to disable automatic failover. In the case of a line card failure, you must initiate the failover operation from iBuilder by selecting the **Swap Line Card** option from any non-standby line card in the network.
- Select **All** to configure the standby line card to backup all transmit and receive line cards. (This is the default selection.)
- Select **Tx Only** to configure the standby line card to backup only your transmit line card.
- Select **Rx Only** to configure the standby line card to backup only your receive line cards.

Automatic failover will occur only when the NMS fails to receive the expected heartbeat message from the line card. This message will be lost if the line card fails, or if any component in the communication path between the NMS and the line card fails.

## 6.7.2 Failover Prerequisites

The following prerequisite conditions must be met in order for the failover operation to proceed:

1. A standby line card must be defined in iBuilder for the network.
2. The standby line card must be in the **OK** state (and accessible from the NMS) as determined by the NMS event server.
3. The chassis must be currently accessible through the EDAS TCP interface.

If conditions two or three cannot be met during normal operation, the standby line card will enter the **WARNING** state in iMonitor and the event server. The text of this warning is:

```
"Cannot perform failover operation: <reason>"
```

If the standby line card itself is down, both this warning and the down alarm will be active in iMonitor and the event server.

## 6.7.3 Basic Failover Concepts

Each second, every line card sends a diagnostic message to the NMS. This message contains the status of various onboard components. If the NMS fails to receive any diagnostic messages from a line card in a five-second time period, and all failover prerequisites are met, it begins the failover process.

For Tx(Rx) line cards, the standby assumes the failed card's role immediately. For Rx line cards, the standby needs to flash a new options file and reset. The estimated time to complete a Tx(Rx) line card failover is less than 10 seconds; the estimated time to complete a Rx-only line card is less than 1 minute.



### NOTE

If your Tx line card fails, or you only have a single Rx line card and it fails, all remotes must re-acquire into the network after failover is complete.

## 6.7.4 Tx(Rx) versus Rx-Only Line Card Failover

The most important line card in a network is the Tx(Rx) line card; if this card fails, all remotes drop out of the network. When an Rx-only card in a frequency-hopping inroute group fails, all remotes automatically begin sharing the other inroutes. While this may result in diminished bandwidth, remotes do not drop out of the network.

iDirect's failover method guarantees the fastest failover possible for the Tx(Rx) line cards. The standby line card in each network is pre-configured with the parameters of the Tx card for that network, and has those parameters loaded into memory. The only difference between the active Tx(Rx) card and the standby is that the standby mutes its transmitter (and receiver). When the NMS detects a Tx(Rx) line card failure, it sends a command to the standby to un-mute its transmitter (and receiver), and the standby immediately assumes the role of the Tx(Rx) card.

Rx-only line cards take longer to failover than Tx(Rx) cards because they need to receive a new options file, flash it, and reset.

## 6.7.5 Failover Sequence of Events

The flow chart below shows the sequence of events performed on the NMS server to execute a complete failover.

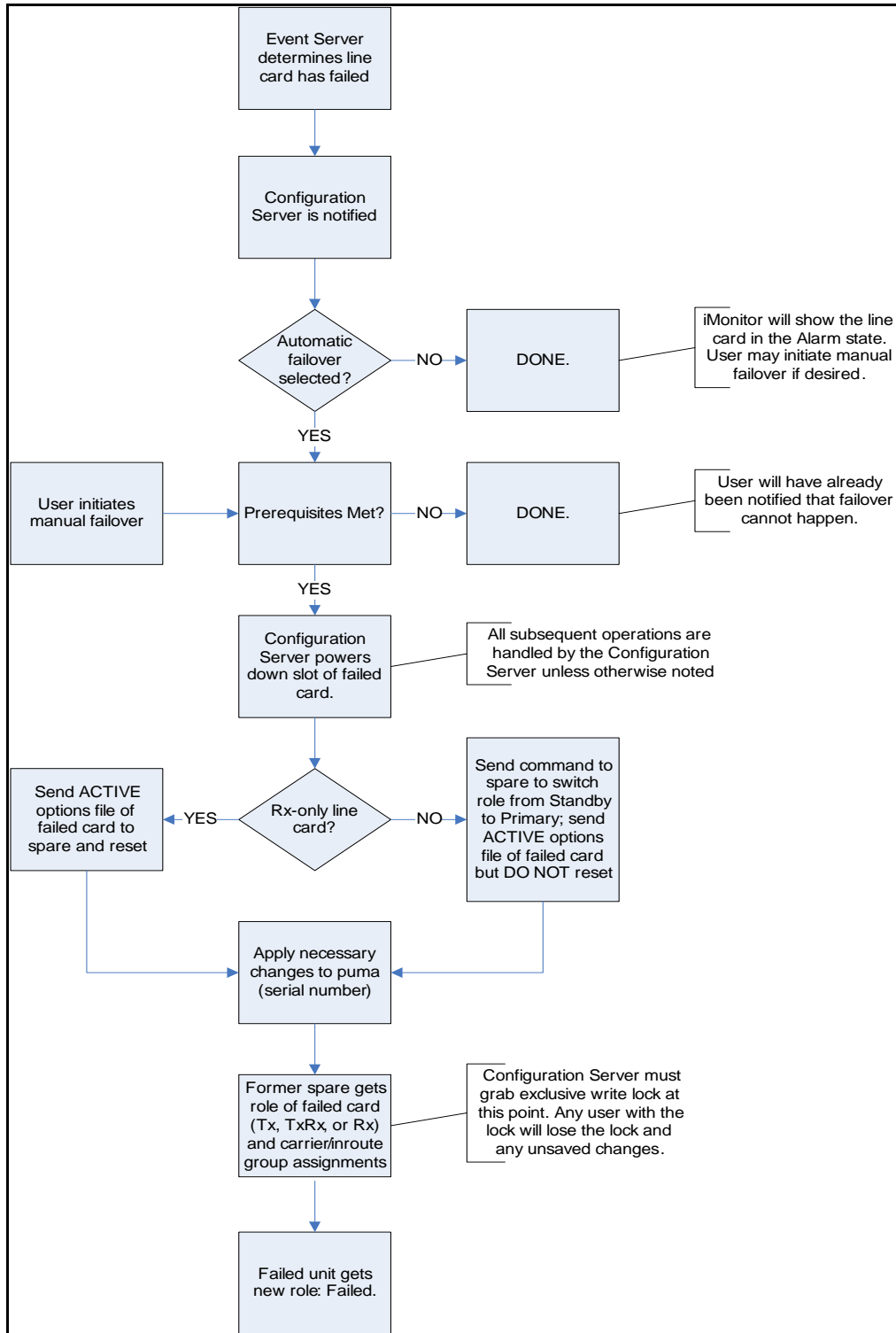


Figure 6-1: Failover Sequence of Events, NMS Server Perspective



## 6.7.6 Failover Operation: User's Perspective

Portions of the failover sequence of events are revealed in real-time. You may perform a historical condition query at any time to see the alarms and warnings that are generated and archived during the failover operation. The flow chart in [Figure 6-2, p. 105](#) shows the sequence of events you will see on the screen in real-time during a failover operation.

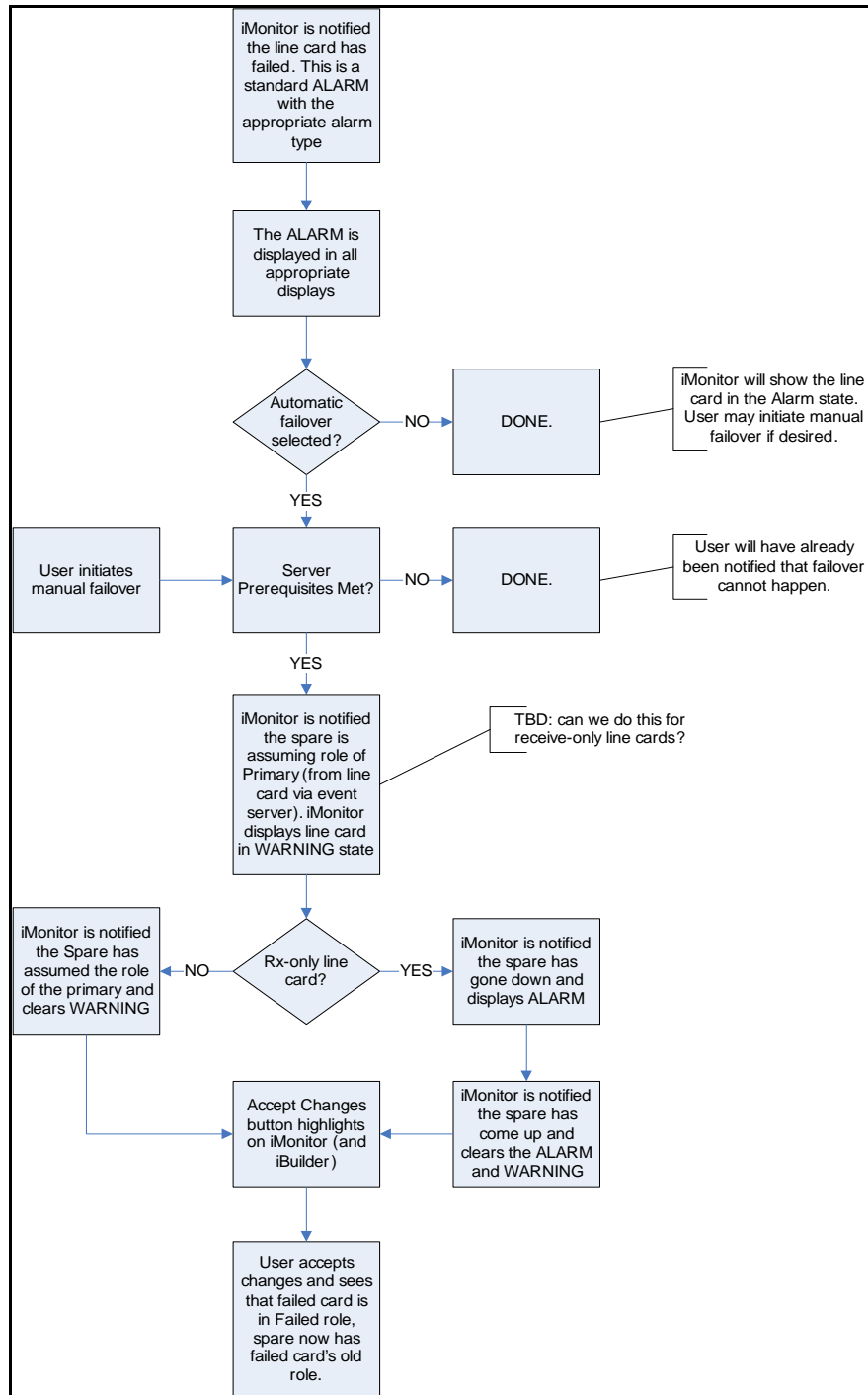


Figure 6-2: Failover Sequence of Events, NMS User Perspective

## 6.7.7 Recovering from a Line Card Failover

After line card failover, the system will be operational, but will be in an interim state requiring recovery. This recovery involves the following procedure:

- Step 1 *IMPORTANT:* First, unplug the I/F Tx (and Rx) cables from the front of the failed unit.
- Step 2 *IMPORTANT:* Next, remove the Ethernet cable from the front of the failed unit.
- Step 3 It is now safe to power on the chassis slot of the failed unit for further examination.
- Step 4 Analyze the failure by connecting a console cable and examining the unit. If the card experienced a hard failure or internal component failure, the user must remove the failed card from the chassis and return it to iDirect for repair. Some failures, such as those listed below, may be repaired on-site.
  - Switch port failure
  - LAN cable failure.
  - FPGA image load failure or runtime flash corruption.

## 6.7.8 Recovering from a Repairable Line Card Failure On-site

This type of recovery turns the failed line card back into an operational standby line card. To do this, follow the procedure below:

- Step 1 Log onto the failed unit's console.
- Step 2 In iBuilder, switch "Line Card Type" from Failed to Standby.
- Step 3 Using iBuilder, power on the line card's chassis slot.
- Step 4 Using the console, change the unit's role from Tx(Rx) to Standby using the following console command: `options set OPTIONS_FILE is_standby 1`.
- Step 5 Save the options file to flash: `options flash`.
- Step 6 Reset the line card.
- Step 7 Re-connect the line card's Ethernet port.

You may now connect to the line card using iSite or the telnet console and proceed with further debugging, if necessary.

## 6.8 Adding Inroute Groups

Inroute Groups are groups of receive line cards, or Inroutes. If you have used a transmit/receive line card, you may add this card to the Inroute Group also. However, transmit-only line cards may not be included. The purpose for bundling several receive line cards together into Inroute Groups is to allow for load balancing among the individual line cards. You must have created Inroute Groups in order to add remotes to the network.

The relationship between carriers, line cards, and inroute groups is shown in [Figure 6-3, p. 107](#). There are specific rules regarding the assignment of line cards to inroute groups.

1. You cannot assign a line card to an inroute group unless its assigned carrier is identical in data rate and FEC block size to the other line card(s) in that inroute group.
2. You cannot assign a line card to an inroute group if it is already assigned to another inroute group. In this case, if rule 1 is true, you can un-assign the line card from its current inroute group and re-assign it to the desired inroute group.
3. You may not change a line card's carrier assignment if the line card is assigned to an inroute group. However, you may modify the characteristics of the current carrier (see rule 4 below).
4. If you modify either the FEC block size or data rate of a carrier that belongs to a line card in an inroute group, iBuilder will automatically change all other carriers that belong to the other line cards in that inroute group. It will prompt you first and allow you to cancel the modify operation.

To assign a line card to an inroute group, modify the Inroute Group and click **Add**. iBuilder will only show you line cards that are valid to be assigned to that inroute group. If you don't see line cards you expect to see, review the rules above.

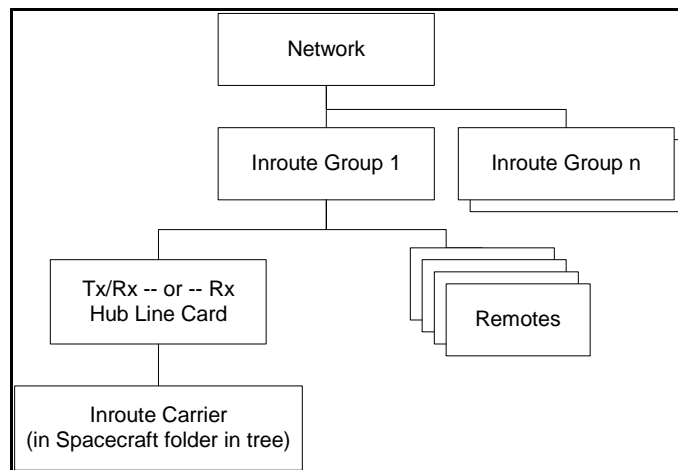


Figure 6-3: Inroute Group Relationships

### **Carrier Grooming**

Carrier Grooming mode is an option in which remotes dynamically acquire into the inroute with the fewest number of remotes (assuming multiple inroutes in the group). Once acquired into an

inroute, the remote will remain in that inroute until it passes through acquisition again. iMonitor's Inroute Distribution screen provides an "ACQ Bounce" function that forces a remote to re-acquire without resetting. An RCM is required for Carrier Grooming.

### **Frequency Hopping**

Users may also select Frequency Hopping mode when defining inroute groups. Frequency Hopping requires that you upgrade your Hub Chassis with redundant Reference Clock Modules (RCMs). Frequency Hopping mode provides true run-time load balancing across all the inroutes within an inroute group. In Frequency Hopping mode, remotes will dynamically load-balance across all inroutes in the group based on inroute demand. The Protocol Processor analyzes upstream demand from all remotes and automatically allocates timeplan slot assignments to achieve an equal balance of remote demand across all the inroutes. Remotes will hop from one inroute to another either on a frame boundary or within the same frame depending on the nature of the demand.

Both Carrier Grooming and Frequency Hopping provide an added level of inroute redundancy as well as improved performance. When line cards are added to or removed from a network, remotes respond dynamically, either by reacquiring into another inroute when a line card is removed or fails, or by moving to a newly added inroute. The use of inroute groups is mandatory with release 4.0 and above. However, you may continue to operate your networks exactly as before by configuring a single inroute in each of your inroute groups. (This will be the default configuration immediately after you upgrade to release 5.0 from any release prior to 4.0.)

### **Mesh-Enabled Inroute Groups**

A mesh-enabled Inroute Group contains inroutes that are received both by the hub and by mesh-enabled remotes. This allows direct remote-to-remote communications for real-time traffic, eliminating the double satellite hop and extra bandwidth required for star traffic. To indicate that an inroute group will be used by mesh remotes, you must select **Mesh Enabled** for the group on the **Information** tab of the **Inroute Group** dialog box. Because all remotes in a mesh Inroute Group receive the mesh inroute, you must be careful to correctly set the values on the **Acquisition and Uplink Control Parameters** tab. For general details on iDirect's mesh implementation, see [chapter 3, "Mesh Technical Description,"](#) of the [iDirect Technical Reference Guide](#).



#### **NOTE**

Beginning with iDirect release 7.0, acquisition and uplink control parameters are configured for each Inroute Group. These parameters are no longer configured at the network level.



#### **NOTE**

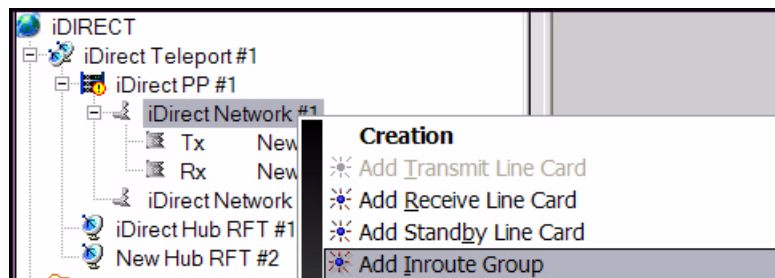
iDirect release 7.0 limits each mesh Inroute Group to a single mesh inroute. For a list of mesh limitations in release 7.0, see [chapter 3, "Mesh Technical Description,"](#) of the [iDirect Technical Reference Guide](#).

**NOTE**

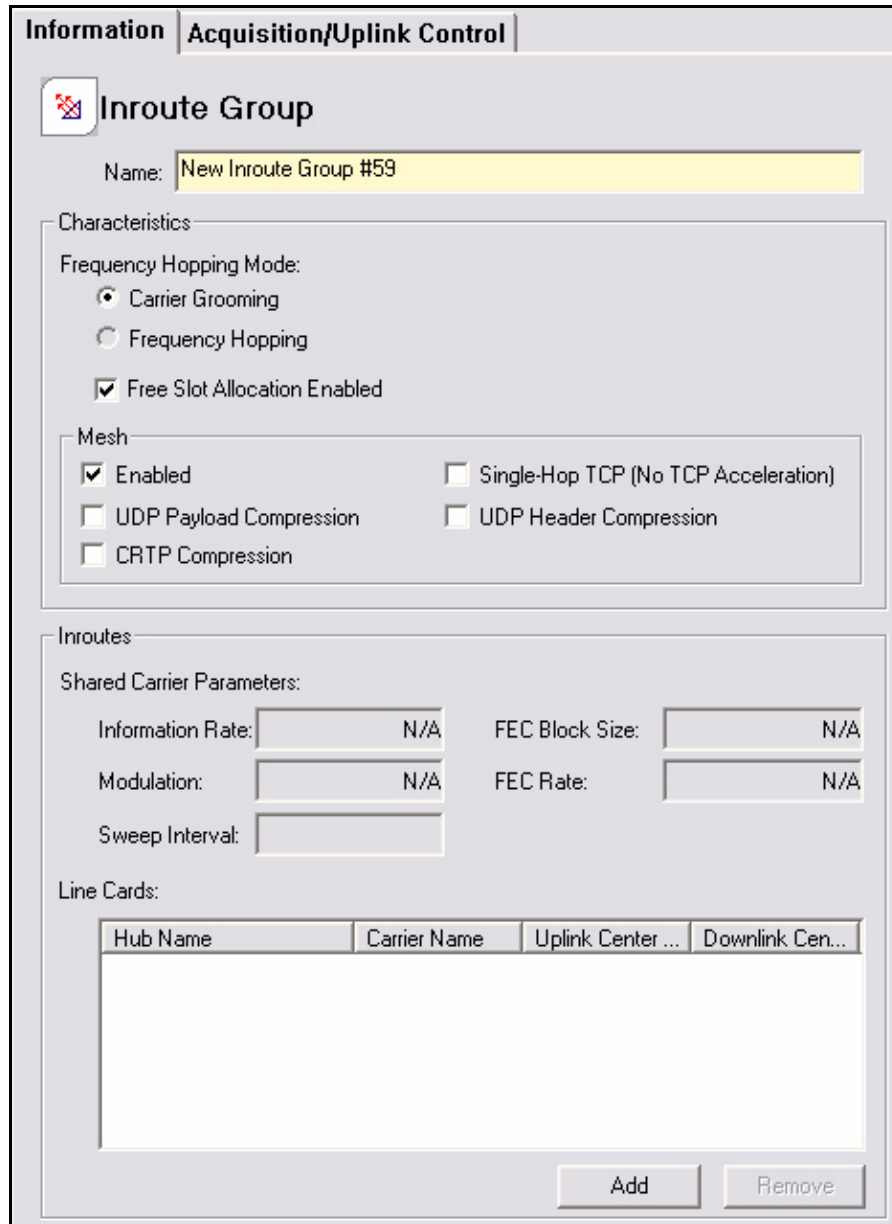
Only iINFINITI 5300 and 7300 series remotes can be added to a mesh inroute group.

**Adding an Inroute Group**

- Step 1 Right-click **Network** and select **Add Inroute Group**. The new inroute group appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define the basic parameters.



Step 2 Enter a name for the Inroute Group. We suggest selecting a name that allows you to associate it with its corresponding Hub.



**Information** | **Acquisition/Uplink Control**

**Inroute Group**

Name:

Characteristics:

Frequency Hopping Mode:

- Carrier Grooming
- Frequency Hopping

Free Slot Allocation Enabled

Mesh:

- Enabled
- Single-Hop TCP (No TCP Acceleration)
- UDP Payload Compression
- UDP Header Compression
- CRTP Compression

Inroutes:

Shared Carrier Parameters:

Information Rate:       FEC Block Size:

Modulation:       FEC Rate:

Sweep Interval:

Line Cards:

Hub Name	Carrier Name	Uplink Center ...	Downlink Cen...

Step 3 **Free Slot Allocation Enabled** and **Carrier Grooming** are selected by default. See [“Carrier Grooming” on page 107](#) and [“Frequency Hopping” on page 108](#) above. For more information about Free Slot Allocation Enabled, see [chapter 5, “QoS Implementation Principles,”](#) of the [iDirect Technical Reference Guide](#).

Step 4 In the **Mesh** area of the dialog box:

- a Select **Enabled** if you are adding a mesh inroute group.
- b Select **UDP Payload Compression** if you want to enable payload compression for UDP packets for all remotes in your mesh inroute group.

- c Select **CRTP Compression** if you want to enable CRTP for RTP packets for all remotes in your mesh inroute group.
- d Select **UDP Header Compression** if you want to enable header compression for UDP packets for all remotes in your mesh inroute group.
- e Select **Single Hop (No TCP Acceleration)** if you want TCP traffic to be sent as single-hop, mesh traffic. If this check box is cleared, only UDP packets will be sent as single-hop, mesh traffic.

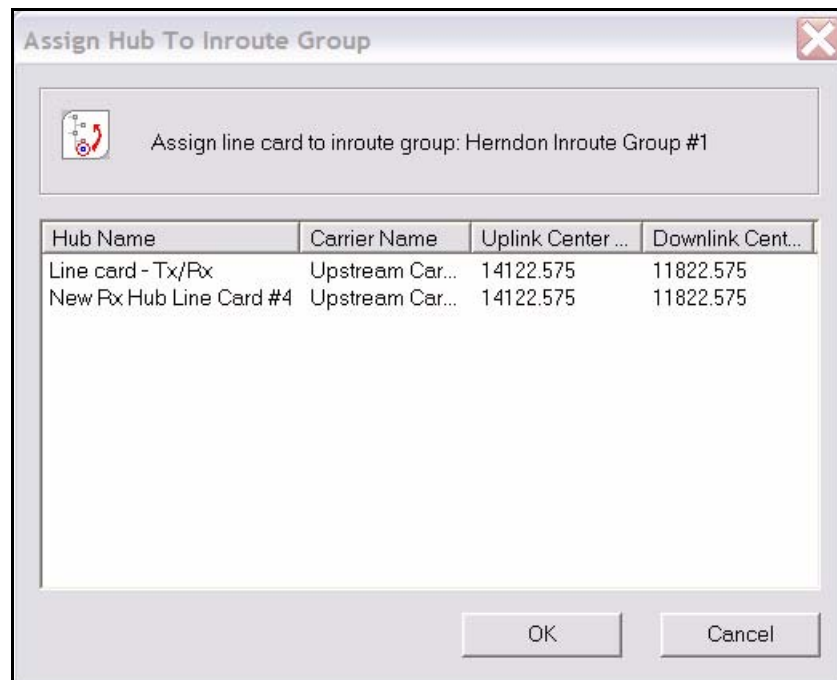


**WARNING** If you select **Single Hop (No TCP Acceleration)** for your mesh inroute group, TCP traffic to or from remotes in the inroute group will *not* be accelerated. This is true for both star and mesh traffic.



**NOTE** If **Mesh is Enabled**, the mesh settings for compression and single-hop TCP configured for the inroute group apply to all remotes in that group, overriding any individual remote settings that may have been configured. For a discussion of the various compression types, see [“Enabling IP Packet Compression Types” on page 153.](#)

- Step 5 Click **Add** to add line cards (with the same Information Rate, FEC Rate, and Modulation) to this Inroute Group. All line cards in an Inroute Group must have the same parameters.
- Step 6 In the **Assign Hub To Inroute Group** dialog box, select the line cards that you wish to add. Click **OK**. You are returned to the **Inroute Group** dialog box.



Step 7 The **Shared Carrier Parameters** area displays the shared values of all selected line cards.

Inroutes

Shared Carrier Parameters:

Information Rate:  FEC Block Size:

Modulation:  FEC Rate:

Sweep Interval:

Line Cards:

Hub Name	Carrier Name	Uplink Center ...	Downlink Cen...
TAC Rx 6677	Bench Test In...	1400.000	1400.000

Step 8 Click the **Acquisition/Uplink Control** tab.

**Information** **Acquisition/Uplink Control**


Acquisition Parameters

Frequency Range:  Hz

Frequency Interval:  Hz

Uplink Control Parameters

**C/N Relative to Nominal:** -3.0 -1.0 1.0 3.0



**Power Adjust:** +2.0 +0.5 +/-0.0 -0.5 -2.0

TDMA Nominal C/N:  dB

TDMA Clear-Sky C/N:  dB

**Fine Adjust**

Below Nominal C/N:  dB

After Nominal C/N:  dB

Power Adjust:  dBm

**Coarse Adjust**

Below Nominal C/N:  dB

After Nominal C/N:  dB

Power Adjust:  dBm



Step 9 You can specify the following **Uplink Control Parameters** for your inroute group:

- **Frequency Range** is a read-only field showing the total range of the frequency band “swept” during acquisition, one half on either side of the target frequency. This value reflects the stability entered in the hub downconverter (LNB) configuration.
- **Frequency Interval** is the read-only step size for the sweep across the **Frequency Range**.
- The **Fine Adjust** and **Coarse Adjust** parameters define the ranges and increments used when applying uplink power control adjustments to the upstream carriers for this inroute group.
- **TDMA C/N Nominal** is the target C/N value of the upstream TDMA carriers in this inroute group as measured by the line card modem. **TDMA C/N Nominal** should be set during hub commissioning.

For a mesh inroute group, **TDMA C/N Nominal** is used as a backup reference in the event of a failure of the SCPC loopback, allowing the network to continue to operate as a star network from the perspective of uplink power control.

**TDMA C/N Nominal** is determined based on the link budget analysis for your network, which takes into consideration the modulation and FEC rate. The fine adjustment is typically set to +/-1 dB.

For networks that migrate from iDirect release 6.0 to release 7.0, this value will be set to:

$$(Fine\ Adjust\ Upper\ C/N - Fine\ Adjust\ Lower\ C/N) / 2$$

- **TDMA Clear Sky C/N** applies to mesh inroute groups only. It is the C/N of the upstream TDMA carrier as measured by the line card modem under clear sky conditions. This value is typically set during commissioning. (For details, see [“Set the Clear Sky C/N Parameters for a Mesh Inroute Group” on page 248.](#))

Step 10 Click **OK** and the Inroute Group appears in the Tree under the Network.



## 7 Configuring Remotes

The most important components of your network are the remotes. This chapter discusses the various aspects of their functionality; provides instructions on how to create and configure them; and provides details about their parameters. It contains the following sections:

- [“iDirect Remote Satellite Router Models” on page 115](#)
- [“Before You Start” on page 115](#)
- [“Adding Remotes” on page 115](#)
- [“Setting Warning Properties for Remotes” on page 145](#)
- [“Adding a Remote by Cloning an Existing Remote” on page 145](#)
- [“Roaming Remotes” on page 145](#)
- [“Enabling IP Packet Compression Types” on page 153](#)

### 7.1 iDirect Remote Satellite Router Models

As of release 6.0.9, iBuilder supports all of the following remote satellite router models:

- NetModem II and NetModem II Plus
- iNFINITI 3100
- iNFINITI 5100 and 5150
- iNFINITI 5300 and 5350
- iNFINITI 7300 and 7350
- iConnex-H and iConnex-R

### 7.2 Before You Start

Configuring remotes is a complex procedure. Before you start, you must know the IP addressing scheme of your network, the specifications of all outdoor components, and the geographic location and hemisphere of your satellite. You must also have performed the following functions before configuring a remote:

- Configured the network in which the remote will reside
- Configured all of that network’s parent elements
- Configured one or more Inroute Groups within the network where the remotes will reside

### 7.3 Adding Remotes

All iDirect remotes that transmit on an upstream TDMA carrier must be associated with an Inroute Group. This allows all remotes assigned to an inroute group to share all carriers (line cards)

currently being serviced by the inroute group. You will probably have a multitude of remotes associated with a given Inroute Group.

An iSCPC remote is used to establish point-to-point communications with an iSCPC line card. Only one line card and one remote participate in any iSCPC connection. Therefore, an iSCPC remote is not a member of an inroute group. Instead, an iSCPC remote is associated with its peer line card. Before you can add an iSCPC remote, you must first add the iSCPC line card as described in [“Adding an iSCPC Line Card” on page 99](#).

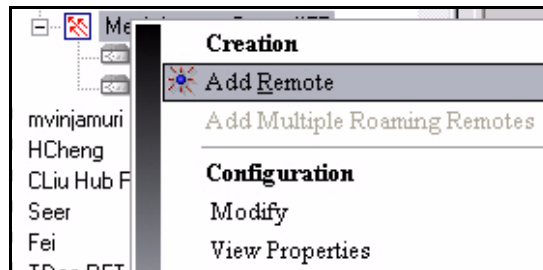


## NOTE

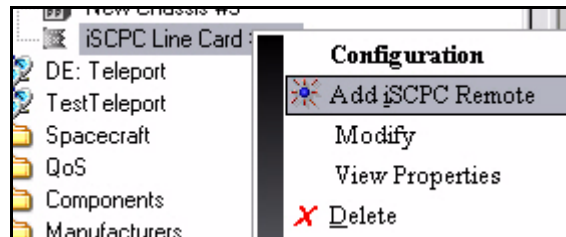
Only iNFINITI 7000 Series remotes and iNFINITI 5000 Series remotes can be configured as iSCPC remotes in iBuilder. However, iSite continues to support iSCPC links using NetModem II Plus remotes.

To add and configure remotes, follow the procedure below:

- Step 1 If you are adding a remote to an inroute group, right-click the **Inroute Group** and select **Add Remote**.



If you are adding an iSCPC remote, right-click the peer iSCPC line card and select **Add iSCPC Remote** from the menu.



## 7.4 Information Tab

The new remote appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to define this remote’s configuration parameters. The **Remote** dialog box has

a number of user-selectable tabs across the top. The **Information** tab is visible when the dialog box opens.



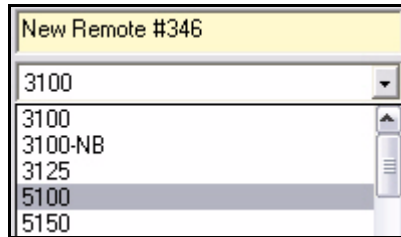
**NOTE**

Many of the steps described in the remaining sections for configuring remotes also apply to configuring iSCPC line cards. For instructions on adding an iSCPC line card to the network tree and selecting a Hub RFT for the line card, see [“Adding an iSCPC Line Card” on page 99.](#)

Information	IP Config	Switch	QoS	Geo Location	VSAT	Warning Properties	Custom
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <h3>Remote</h3> <p>Name: <input type="text" value="INFINITI [468]"/></p> <p>Model Type: <input type="text" value="5350"/></p> <p>Serial Number: <input type="text" value="468"/></p> <p>Derived ID (DID): <input type="text" value="6816212"/></p> <p>Inroute Group: <input type="text" value="Mesh-IF Inroute Group 1"/></p> <p>User Password: <input type="text" value="iDirect"/></p> <p>Admin Password: <input type="text" value="iDirect"/></p> <p><input checked="" type="checkbox"/> Active      <input type="checkbox"/> MUSIC Box</p> <p><input type="checkbox"/> Link Encryption      <input type="checkbox"/> Disable Tx PWM</p> <div style="display: flex;"> <div style="width: 50%;"> <p>Compression</p> <p><input type="checkbox"/> TCP payload</p> <p><input type="checkbox"/> UDP header</p> <p><input type="checkbox"/> UDP payload</p> <p><input type="checkbox"/> CRTP</p> </div> <div style="width: 50%;"> <p>Mesh</p> <p><input type="checkbox"/> Enabled</p> <p>SCPC Clear Sky C/N: <input type="text" value="0"/> dB</p> <p>TDMA LB Clear Sky C/N: <input type="text" value="0"/> dB</p> </div> </div> </div> <div style="width: 50%;"> <p>Customer</p> <p>Name: <input type="text"/></p> <p>Phone Number: <input type="text"/></p> <p>Commission Date: <input type="text"/></p> <p>Contract Number: <input type="text"/></p> <p>Site Notes: <div style="border: 1px solid gray; height: 100px;"></div></p> <p>Distributor</p> <p>Name: <input type="text"/></p> <p>Phone Number: <input type="text"/></p> <p>Fax Number: <input type="text"/></p> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;"> <p>Transmit Properties</p> <p>Carrier Name: <input type="text" value="None"/> <input type="button" value="Details..."/></p> <p>L-Band Frequency: 0.000 MHz</p> <p>Initial Power: <input type="text" value="-6"/> dBm</p> <p>Max Power: <input type="text" value="0"/> dBm</p> </div> <div style="width: 45%;"> <p>Receive Properties</p> <p>Carrier Name: <input type="text" value="Mesh-IF Downstream Carrier"/> <input type="button" value="Details..."/></p> <p>L-Band Frequency: 0.000 MHz</p> </div> </div>							

Step 2 On the **Remote Information** tab, enter a name for this remote.

- Step 3 Select the **Model Type** of the remote from the drop-down list. The model type you select must match the actual hardware model.



- Step 4 Enter the unique serial number for the remote.
- Step 5 A system-generated DID automatically appears in the **Derived ID** box.
- With the introduction of the iDirect iNFINITI series™ platform, serial numbers are no longer sufficient to uniquely identify remotes and line cards. Serial numbers are guaranteed to be unique within a particular model type, but could be duplicated from one model type to another. To avoid potential duplicates and the problems they would cause, iDS 6.0 introduces the concept of a *Derived ID*, or DID. The DID is a 32-bit integer formed by joining a model type code with a unit's serial number. Each remote and line card will have a unique DID value.
  - In the NMS, the DID is typically formatted as **<Model Type Name>.<Serial Number>**, for example **II+.10045** or **5150.1492**. Occasionally you may see the raw DID, however, especially when viewing server log files or console output. You may also select the raw DID as a column to view in iBuilder's Details View (this view is discussed in more detail later in this document). Note: the model type code for NM II remotes is zero, so the raw DID for these units is equal to the serial number.
- Step 6 The name of the Inroute Group with which this remote is associated automatically appears in the **Inroute Group** box.
- Step 7 By default, the **User Password** is set to *iDirect* and the **Admin Password** is set to *P@55w0rd!*. You may specify alternate passwords. The User Password provides users with access to basic commands and the Admin password provides administrator-level access to all commands. For security reasons, network operators should change the telnet console and iSite User and Admin passwords from the defaults.
- Step 8 Select **Active** to enable the Protocol Processor to become aware of the remote site in the network, which it will do once you apply changes at the network level. If the remote is Active, the remote is available for access to the network.

Network operators can define the remote parameters before actually activating the remote when it is commissioned. This option also allows you to deactivate remotes, which removes them from the Protocol Processor's current network configuration, but leaves the configured parameters intact.

- Step 9 Select **MUSIC Box, Disable Tx PWM, or Link Encryption**.
- a Select **MUSIC Box** if this site will use a Multi User Summing Chassis at the remote site. The iDirect MUSIC Box allows a common antenna/electronics platform to be shared across multiple remotes that are at the same physical location. Selecting MUSIC Box overwrites VSAT ODU settings that turn on the DC/10 MHz timing; instead, the MUSIC Box provides the DC/10 MHz timing.
  - b Select the Disable Tx PWM to disable the Transmit Pulse Width Modulation on the remote and enable console pointing mode. (With this box selected, installers don't have to remove the transmit cable during pointing.)
  - c If you are commissioning a NetModem II Plus and have purchased the **Link Encryption** option, installation of special hardware and software on the Protocol Processor is required. **Link Encryption** must be enabled via the NMS before the check box is visible.
- Step 10 In the **Compression** area of the dialog box, select any IP compression types you want to enable for this remote. For details on the different types of compression available, see ["Enabling IP Packet Compression Types" on page 153](#).



## NOTE

**UDP Header Compression, UDP Payload Compression and CRTP** cannot be selected for individual **Mesh** remotes in mesh-enabled inroute groups. Instead, all mesh remotes in the inroute group use the settings for these parameters that are configured for that inroute group. For details on configuring mesh parameters for inroute groups, see ["Adding Inroute Groups" on page 107](#).

- Step 11 If this remote will be commissioned to send and receive mesh traffic on the inbound carriers, enter the following parameters in the **Mesh** section of the dialog box:
- a Select **Enabled**.
  - b Enter a value for **SCPC Clear Sky C/N**. **SCPC Clear Sky C/N** is the C/N of the downstream SCPC carrier as measured by the remote modem under clear sky conditions. This value is typically set during remote commissioning.
  - c Enter a value for **TDMA Loopback Clear Sky C/N**. This represents the C/N of the loopback TDMA carrier as measured by the remote modem under clear sky conditions. This value is typically set during remote commissioning.

See [Section 13.3 “Set the Clear Sky C/N Parameters for a Mesh Remote”](#) of the [Installation and Commissioning Guide for iDirect iNFINITI Series Satellite Routers](#) for details on setting these parameters.



**NOTE** Only iNFINITI 5300 and 7300 series remotes can be configured to carry mesh traffic.

## 7.4.1 Transmit and Receive Properties

This section discusses the transmit and receive parameters on the **Information** tab.

Transmit Properties	Receive Properties
Carrier Name: <input type="text" value="Upstream Carrier #4"/> Details...	Carrier Name: <input type="text" value="Downstream Carrier #3"/> Details...
L-Band Frequency: 0.000 MHz	L-Band Frequency: 0.000 MHz
Initial Power: <input type="text" value="-25"/> dBm	
Max Power: <input type="text" value="0"/> dBm	

Step 1 In the **Information** tab's **Transmit Properties** and **Receive Properties** panes, the **Details** buttons allow you to view the details about the carriers.



**NOTE** If you are configuring an iSCPC remote or line card, you can only select the transmit and receive carriers when defining the line card. iBuilder will automatically assign the transmit carrier of the line card to be the receive carrier of the remote. iBuilder will also assign the receive carrier of the line card to be the transmit carrier of the remote. If you have not yet defined your iSCPC carriers, see [“Adding Carriers” on page 69](#).

Step 2 In **Transmit Properties**, the L-Band Frequency is calculated and displayed for you once the BUC is assigned on the **VSAT** tab. See [“VSAT Tab” on page 143](#).

Step 3 Enter the **Initial Power** level in dBm, based on the commissioning results. The default is -25.

Step 4 In **Max Power**, enter the maximum Tx power level in dBm based on commissioning results. The default is zero. The range for both Initial and Max power is -35 to +7 for a NetModem II Plus or iNFINITI remote. (The range for a NetModem II is -25 to +7.)

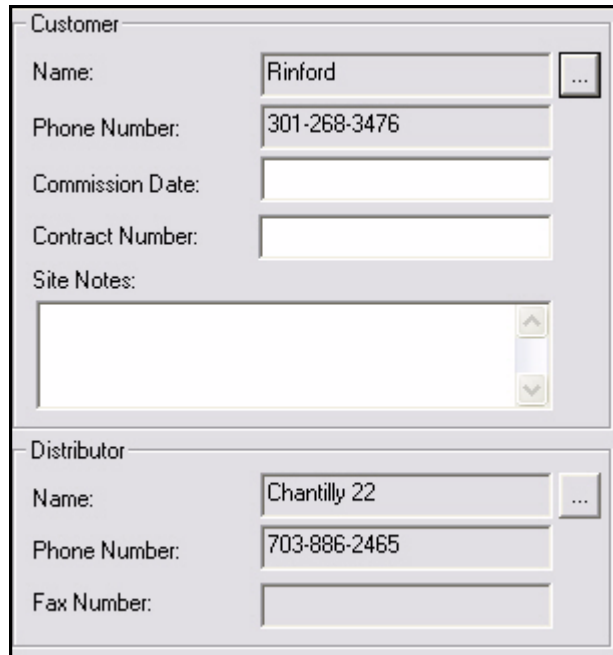
Step 5 In the **Receive Properties** pane, you cannot select the **Carrier Name**, although you can view the details regarding it. This is the downstream SCPC carrier for the network.



Step 6 The L-Band Frequency is calculated for you once the LNB is assigned on the **VSAT** tab. See [“VSAT Tab” on page 143](#).

## 7.4.2 Customers and Distributors

This section discusses the Customer and Distributor parameters on the **Information** tab. It is completely optional whether or not you want to enter customers or distributors. The following procedures show a customer being added; however, the procedure for adding customers and distributors is the same.



<b>Customer</b>	
Name:	Rinford
Phone Number:	301-268-3476
Commission Date:	
Contract Number:	
Site Notes:	
<b>Distributor</b>	
Name:	Chantilly 22
Phone Number:	703-886-2465
Fax Number:	

Step 1 To add a Customer or a Distributor associated with the remote, click the **List** button to the right of the **Name** box. The **Customers** or **Distributors** dialog box appears.

If any customers or distributors have already been added to the NMS database, the names appear in the list, as shown below.

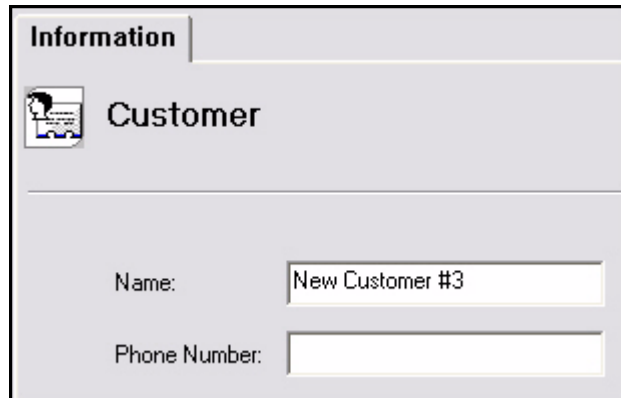


Customers	
Customers	
Name	
None	
Morgan	
Rinford	

Step 2 To the right of the dialog box, you can click **Add** to add another customer or distributor.



Step 3 The **Information** tab's **Customers** (or **Distributors**) dialog box appears.

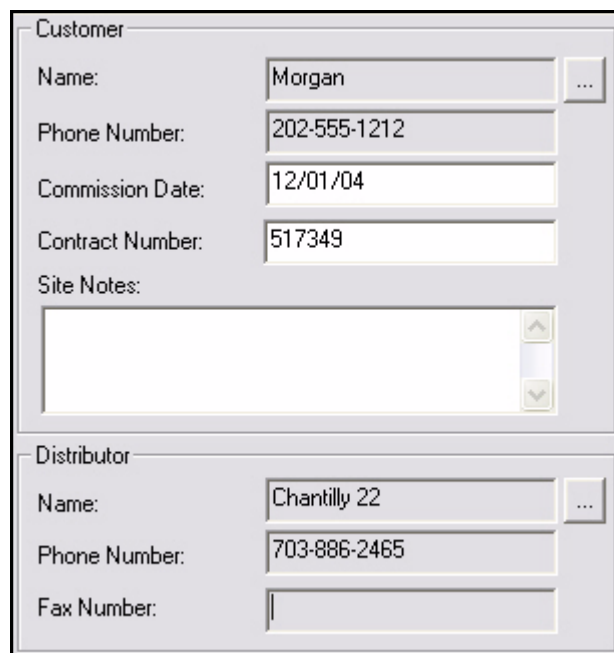
A dialog box titled 'Information' with a sub-tab 'Customer'. It contains a small icon of a person and the word 'Customer'. Below this, there are two input fields: 'Name:' with the text 'New Customer #3' and 'Phone Number:' with an empty field.

Step 4 Enter the Customer's or Distributor's Name and phone number.

Step 5 Click **OK**. You are returned to the **Customers** (or **Distributors**) dialog box

Step 6 To add more customers or distributors, follow this procedure again. Click **OK**. You are returned to the **Remote** dialog box's **Information** tab.

Step 7 The new customer or distributor appears in the boxes, as shown below.

A screenshot of a software interface showing two sections. The top section is titled 'Customer' and contains fields for Name (Morgan), Phone Number (202-555-1212), Commission Date (12/01/04), and Contract Number (517349). Below these is a 'Site Notes' field with a scrollable area. The bottom section is titled 'Distributor' and contains fields for Name (Chantilly 22), Phone Number (703-886-2465), and Fax Number (empty).

- Step 8 For customers, you can enter a **Commission Date**, **Contract Number**, and additional information in the **Site Notes** box, such as keeping a log of commissioning or operational events.
- Step 9 If you click **OK**, the dialog box will close, but your changes will be saved. Instead, click the **IP** tab to continue configuring the remote. See [“IP Config Tab” on page 123](#).

## 7.5 IP Config Tab

The **IP Config** tab consists of several individual panes, each of which is displayed and discussed below.

### 7.5.1 VLAN and LAN Information

iBuilder provides a wide range of IP configurations for remotes accessible from the **IP** tab. All configurable IP parameters and all VLANs are collected onto a single tab for quick reference.

iDirect Software supports end-to-end VLAN tagging. To implement this feature, the router or switch that is upstream from the Protocol Processor must support IEEE 802.1Q (VLAN) tagging. When multiple VLANs are present on the remote, a similar switch that is downstream from the remote is also required.

A detailed, two-VLAN, multiple-remote example is shown in the figure below. Management traffic between the NMS and remote must be untagged and each remote must have a unique Management IP address. Networks may contain a mixture of remote VLAN and traditional IP-based remotes. Each remote must be configured to work in either traditional IP or VLAN mode.

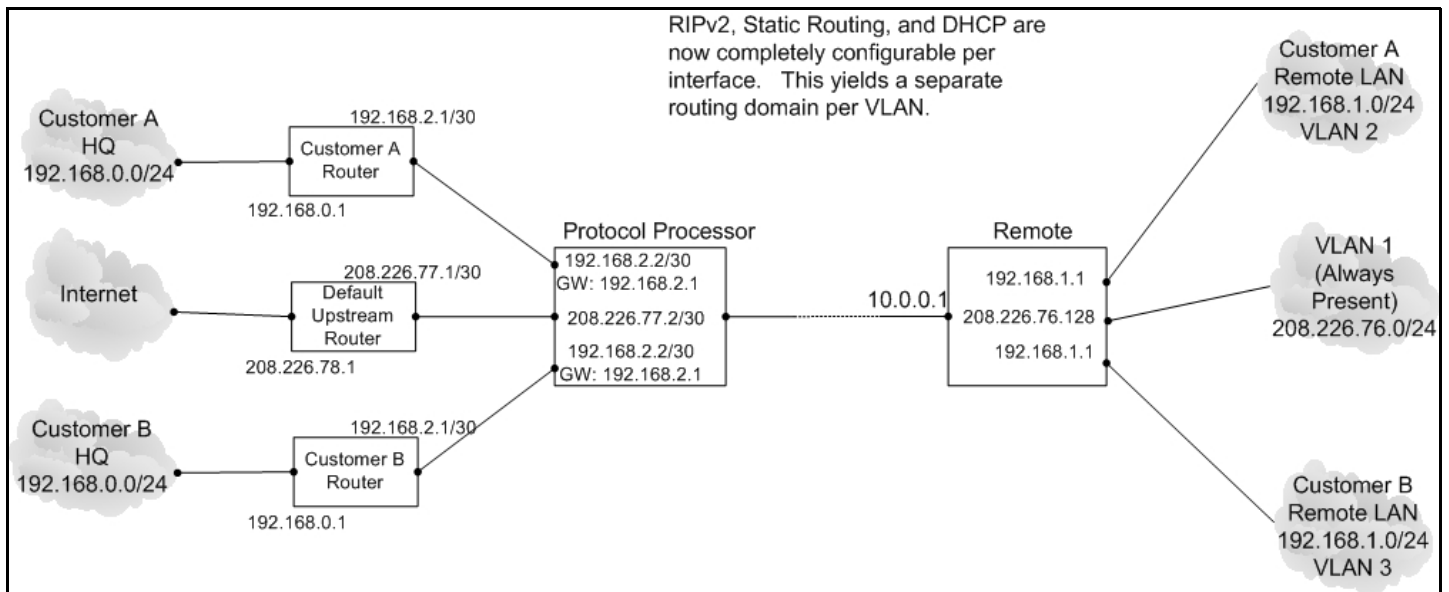


Figure 7-1: Sample VLAN Network Layout

The iDirect VLAN capability allows customers to use their existing IP addressing schemes. Since all routing options (RIPv2 and static routing) are configurable per VLAN interface, the end-to-end VLAN feature allows each end customer to have their own routing architecture independent of other customers sharing the same physical network components.

All traffic on a mesh inroute must have VLAN tagging enabled. This applies to packets sent on user-defined VLANs as well as to packets sent on the default VLAN. Remotes on the same VLAN can communicate on the mesh inroute over that VLAN. All mesh remotes on a mesh inroute can communicate over the default VLAN.

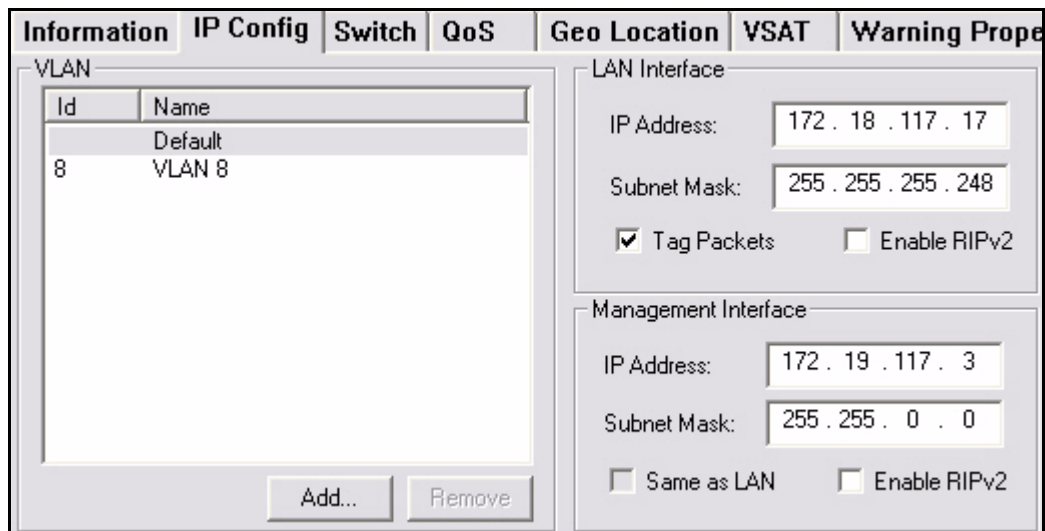
There are two check boxes for configuration of the Routing Information Protocol (RIPv2) on the remote: one for the LAN interface (eth0) and one for the for satellite interface (sat0). (The sat0 interface is called the management interface when referring to the default VLAN.) You can enable or disable RIPv2 independently on the two interfaces. Depending on the RIPv2 options selected, the remote behaves as follows:

- When RIPv2 is not enabled on either interface, RIP is completely disabled on the remote. It does not send or receive any RIP updates.
- When RIPv2 is enabled on the LAN interface, the remote sends and receives RIP updates over the LAN, updating its own IP routing table when new routing information is received.
- When RIPv2 is enabled on the satellite (or management) interface, the remote sends and receives RIP updates over the satellite, updating its IP own routing table when new routing information is received.

The remote does not relay RIP messages to other routers. Instead, it generates RIP messages based on its own IP routing table.

### **Configuring LAN and Management Interfaces**

This section discusses only the portion of the IP tab shown below.



The screenshot shows the 'IP Config' tab in the iBuilder interface. It is divided into two main sections: 'VLAN' and 'Interface Configuration'.

**VLAN Section:** A table lists VLANs with columns for 'Id' and 'Name'. The table contains two entries: 'Default' and '8 VLAN 8'. Below the table are 'Add...' and 'Remove' buttons.

Id	Name
	Default
8	VLAN 8

**Interface Configuration Section:** This section is split into two sub-sections: 'LAN Interface' and 'Management Interface'.

**LAN Interface:**

- IP Address: 172 . 18 . 117 . 17
- Subnet Mask: 255 . 255 . 255 . 248
- Tag Packets
- Enable RIPv2

**Management Interface:**

- IP Address: 172 . 19 . 117 . 3
- Subnet Mask: 255 . 255 . 0 . 0
- Same as LAN
- Enable RIPv2

The IP information for a remote is configurable per VLAN. Once you have selected a VLAN in the left pane of the dialog box, you can configure its IP addressing information in the right pane.

- Step 1 The **LAN Interface** IP address represents the remote's IP address on the selected VLAN.
- a Enter the IP Address and Subnet Mask.
  - b Select **Tag Packets** if you want to tag packets with the VLAN ID according to the IEEE 802.1Q VLAN Tagging specification.



**NOTE** VLAN tagging is required for mesh-enabled remotes all VLANs. You cannot clear the **Tag Packets** check box if the remote is enabled for mesh on the **Information** tab.

- c Selecting **Enable RIPv2** enables RIPv2 over the LAN link for the selected VLAN. RIPv2 is configurable per interface.

- Step 2 The remote's **Management Interface** (Sat) IP address represents the remote's virtual interface on the default VLAN. The NMS always communicates with the remotes using this address. This address should not conflict with the LAN Interface addresses.
- a Selecting **Same as LAN** sets the Management Interface IP address to the LAN Interface IP address. (The Gateway is always set to 0 and cannot be changed.) This option is not available on the iNFINITI Series 3000, 5000, or 7000 remotes.
  - b Selecting **Enable RIPv2** enables RIPv2 over the satellite link for the selected VLAN. RIPv2 is configurable per interface.



**NOTE** When you select a VLAN other than the default VLAN, the interface names change. **LAN Interface** changes to **ETH0 Interface**. **Management Interface** changes to **SAT0 Interface**.

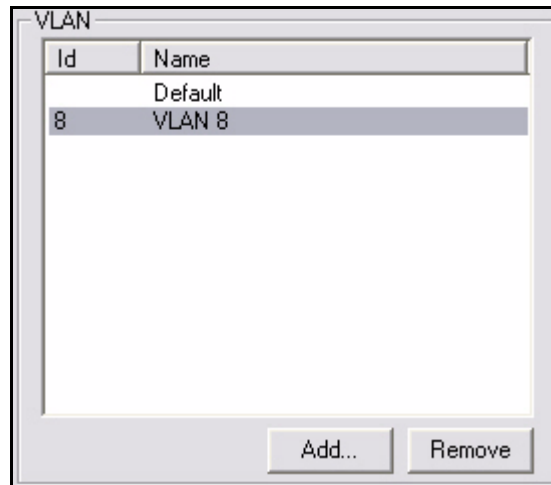
### **Adding VLANs to a Remote**

This section only discusses adding the VLAN configuration to Remotes. You must first define the VLAN Upstream Interface on the **VLANS** tab of the Protocol Processor. See [chapter 5, "Defining Network Components,"](#) section ["Adding a VLAN" on page 88](#) for details.

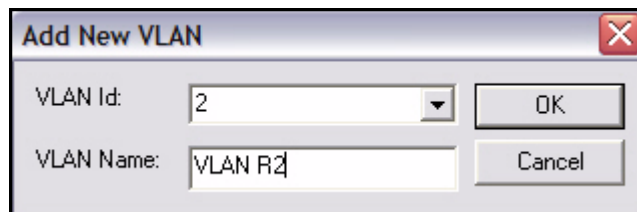
Additional VLANs can be added and removed from a remote using the appropriate buttons located in the VLAN area of the **IP Config** tab. The default **VLAN** is VLAN 1 (native VLAN) and is based on the LAN Interface address.

To add a VLAN to a remote:

Step 1 Click the **Add** button at the bottom of the VLAN area of the **IP Config** tab.



Step 2 In the **Add New VLAN** dialog box, select a **VLAN Id** and **Name**, and click **OK**. Once a VLAN is added to the remote, it appears in the VLAN list, and the LAN and Management Interfaces change to ETH0 and SAT0 Interface for the VLAN.

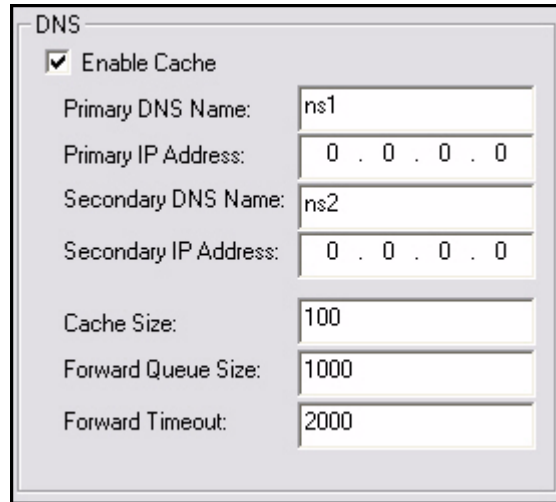


Step 3 If you click the Remove button, a warning message is displayed, asking you to confirm the deletion. VLAN 1 is the default VLAN; you cannot remove it.

The VLAN ID is also considered in QoS Traffic Profiles. See [chapter 8, “Creating and Managing QoS Profiles,”](#) section [“Adding a Service Level”](#) on page 160.

## 7.5.2 Domain Name Service (DNS)

This section discusses only the DNS portion of the **IP** tab.



DNS

Enable Cache

Primary DNS Name: ns1

Primary IP Address: 0 . 0 . 0 . 0

Secondary DNS Name: ns2

Secondary IP Address: 0 . 0 . 0 . 0

Cache Size: 100

Forward Queue Size: 1000

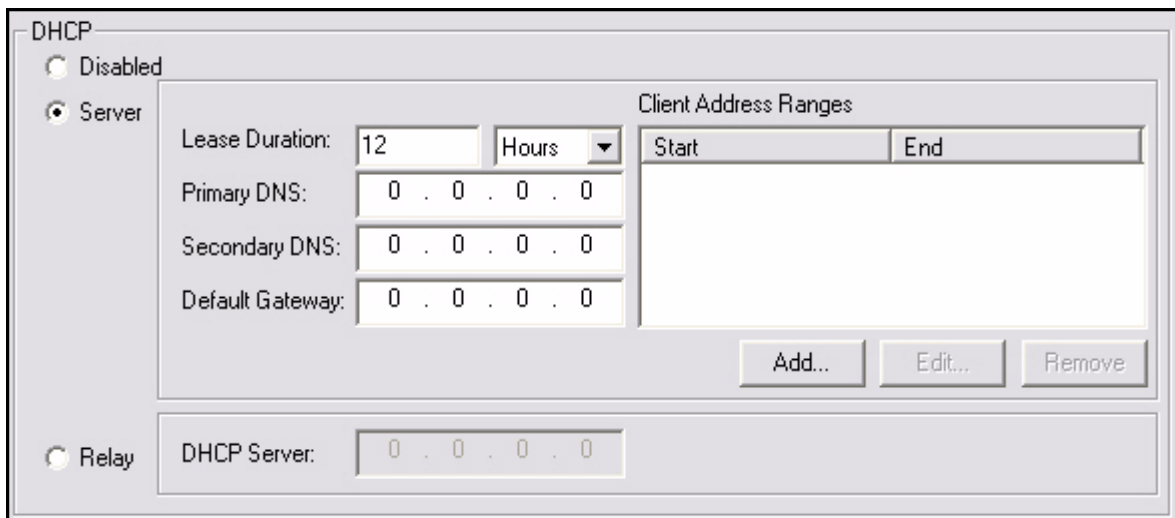
Forward Timeout: 2000

The local **DNS** cache capability, which is checked by default, is available only for the default VLAN 1 interface set.

- Step 1 If you want to configure DNS, you must specify both primary and secondary IP addresses. Assigning DNS names is optional.
- Step 2 The Cache size, Forward Queue size and Forward Timeout size shown are default values. Modifications may be made in this pane if desired.

## 7.5.3 Dynamic Host Configuration Protocol (DHCP)

This section discusses only the portion of the **IP** tab shown below.



DHCP

Disabled

Server

Lease Duration: 12 Hours

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

Client Address Ranges

Start	End

Add... Edit... Remove

Relay

DHCP Server: 0 . 0 . 0 . 0

DHCP, including DHCP relay, is configurable on a per VLAN basis. In iBuilder, DHCP is disabled by default.

Select **Relay** if you want to utilize an existing or separate DHCP server at your hub location. The remote will pass through the DHCP request and return the provided address from the server.

To enable the remote to act as the DHCP server, follow the procedure below:

- Step 1 Select **Server** to enable DHCP configuration entries.
- Step 2 Enter the **Lease Duration** or the amount of time before the address must be renewed.
- Step 3 Enter the **Primary** and **Secondary DNS** server addresses, and the **Default Gateway**.
- Step 4 Click the **Add** button to enter **Client Address Ranges**, which are the ranges of assignable addresses. Multiple unique ranges may be assigned as desired.

To edit a range, follow the procedure below:

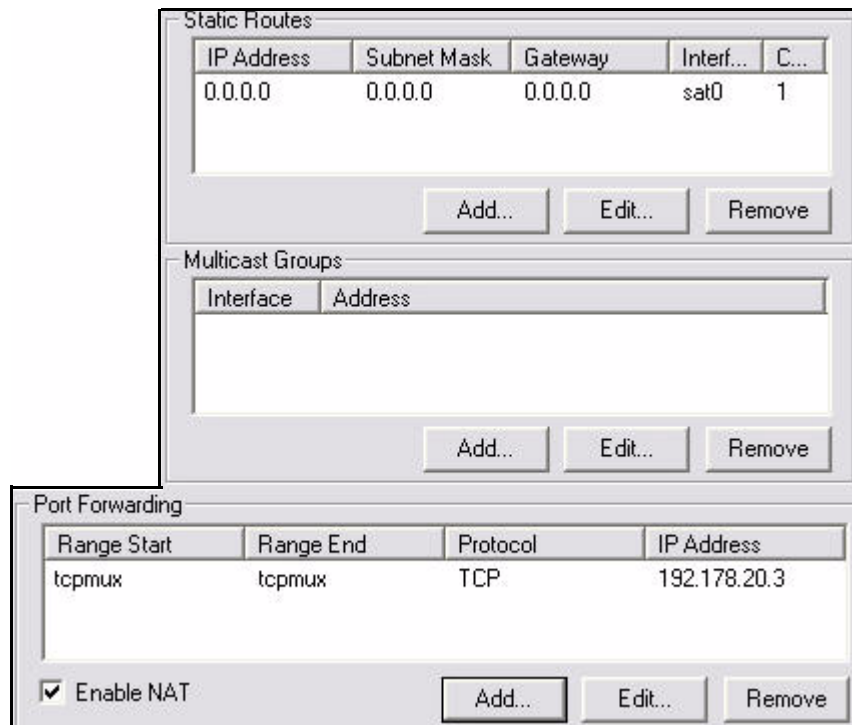
- Step 1 Click the range in the table to highlight the range you want to change.
- Step 2 Select **Edit**.
- Step 3 Edit the range and click **OK** to save your changes.
- Step 4 If you select a range in the table and click the **Remove** button, a warning message is displayed, asking you to confirm the deletion.
- Step 5 Click **OK** to delete the range.



## 7.5.4 Static Routes, NAT, Multicast Groups, and Port Forwarding

This section discusses only the portion of the IP tab shown below.

The default route across the **sat 0** interface is added by default when you create a new remote. Do not delete this route unless your remote routing scheme requires it.

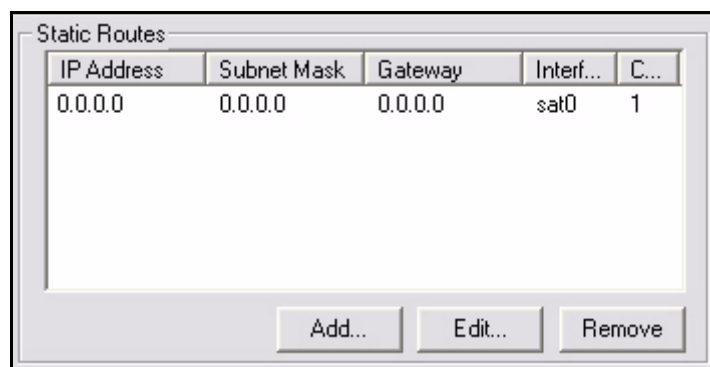


The screenshot shows a configuration window with three main sections:

- Static Routes:** A table with columns: IP Address, Subnet Mask, Gateway, Interf..., and C... The first row contains: 0.0.0.0, 0.0.0.0, 0.0.0.0, sat0, 1. Below the table are buttons: Add..., Edit..., and Remove.
- Multicast Groups:** A table with columns: Interface and Address. Below the table are buttons: Add..., Edit..., and Remove.
- Port Forwarding:** A table with columns: Range Start, Range End, Protocol, and IP Address. The first row contains: tcpmux, tcpmux, TCP, 192.178.20.3. Below the table is a checkbox labeled "Enable NAT" which is checked, and buttons: Add..., Edit..., and Remove.

### Static Routes

You can define Static Routes by selecting the **Add** button.

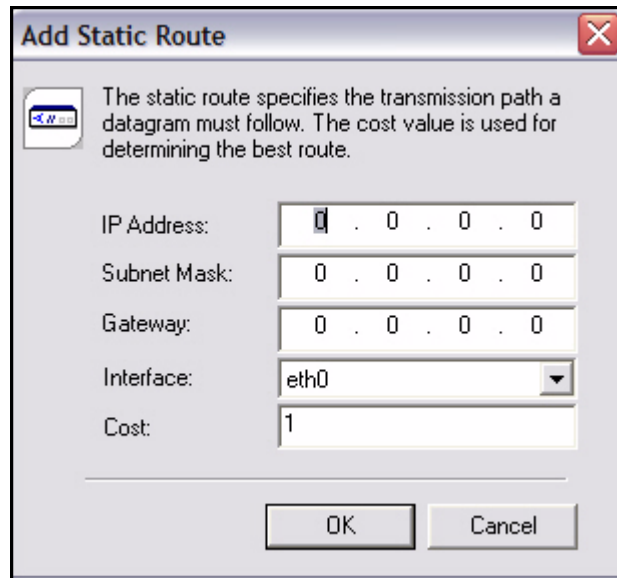


This is a close-up of the Static Routes section from the previous screenshot. It shows a table with the following data:

IP Address	Subnet Mask	Gateway	Interf...	C...
0.0.0.0	0.0.0.0	0.0.0.0	sat0	1

Below the table are three buttons: Add..., Edit..., and Remove.

The **Add Static Route** dialog box appears. You must specify the IP address, subnet mask, gateway, interface and cost value for each static route, and click **OK**.



To edit a range, follow the procedure below:

- Step 1 Click the entry in the table to highlight the range you want to change.
- Step 2 Select **Edit**, edit the entry, and click **OK** to save your changes.
- Step 3 If you select an entry in the table and click the **Remove** button, a warning message is displayed, asking you to confirm the deletion.
- Step 4 Click **OK** to delete the range.

### **Using Static Routes with Multiple Protocol Processor Blades**

You may use static routes between an upstream router and a multiple-blade Protocol Processor; this removes the need for RIPv2 on the upstream LAN. In order to ensure correct routes, you must “clamp” remotes to one specific blade using a custom key. You must also add all static routes to your upstream router.



### **WARNING**

When you clamp a remote to a specific blade, it will NOT re-acquire if that blade fails. The remote will remain out-of-network until the blade is back up, or the specific blade assignment is changed or removed using iBuilder.

Use the following procedure to clamp a remote to a specific blade:

1. Bring up the remote’s Modify Dialog in iBuilder
2. Click on the “Custom Key” tab

3. Add the following entry to the “Hub-Side” section:

```
[BLADE]
blade_id = <ID>
```

4. Click OK to close the dialog.
5. Apply the modified configuration.

To determine a blade’s ID, select **View→Details** from iBuilder’s main menu bar, and click on the PP record in the network tree view.

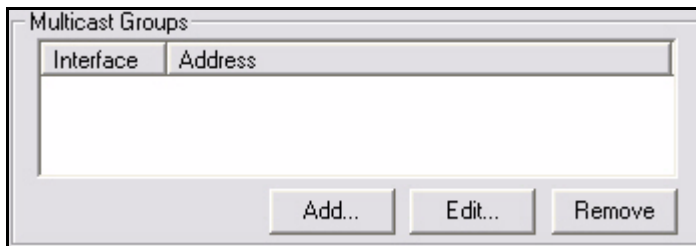
Use the following procedure to turn RIPv2 off for a Protocol Processor:

1. Bring up the Protocol Processor’s Modify Dialog in iBuilder.
2. Clear the box labeled “RIP Enabled”
3. Click OK to close the dialog and apply the modified configuration.

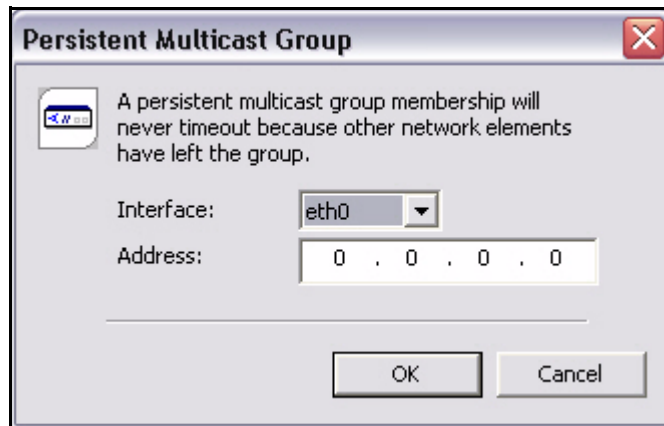
### **Multicast Groups**

To configure the remote to be a member of a persistent Multicast Group, follow these steps:

- Step 1 Click the **Add** button in the **Multicast Group** section of the screen.



The **Add Static Route** dialog box appears.

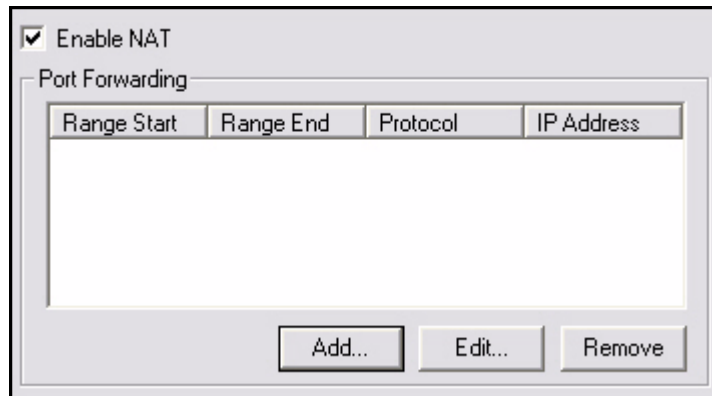


- Step 2 Select the **Interface: eth0** or **sat0**.
- Step 3 Enter an IP **Address** of the multicast group.

Step 4 Click **OK**.

### **NAT and Port Forwarding**

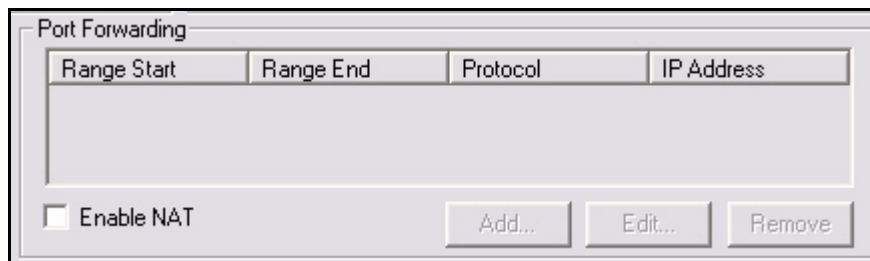
NAT and Port Forwarding can be configured on a per-VLAN basis. NAT enables you to make the Management Interface public and the LAN interface private on the remote, providing a way to have multiple private addresses represented by one public address.



To enable port forwarding, select the **Enable NAT** (Network Address Translation) check box.

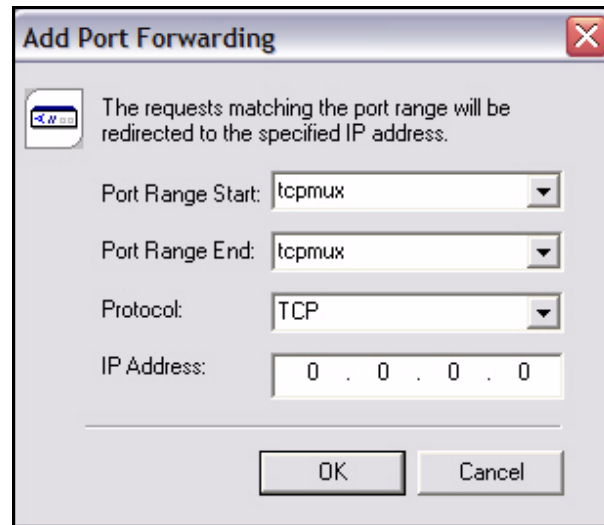
Port forwarding allows you to specify that IP packets with certain port numbers are forwarded to private IP addresses behind the remote. For example, if you wanted to run a web server on a PC with a private IP address, you could specify http as the port start and port end, with TCP as the protocol, and then add the PC's IP address in the IP address field.

Step 1 Click **Add** to access the **Add Port Forwarding** dialog box.



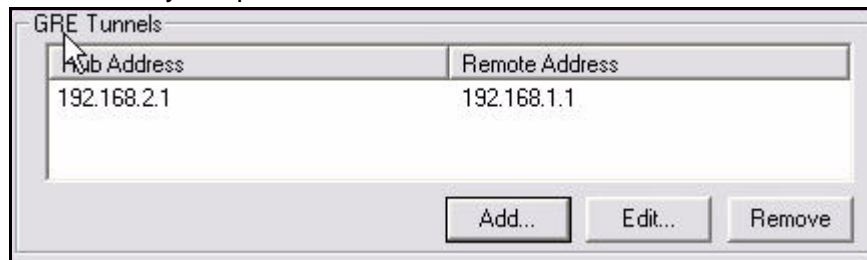
Step 2 Select a start and end port range for port forwarding. Select a protocol and specify an IP address.

Step 3 Click **OK** to save your changes.



## 7.5.5 Accelerated GRE Tunnels

This section discusses only the portion of the **IP** tab shown below.

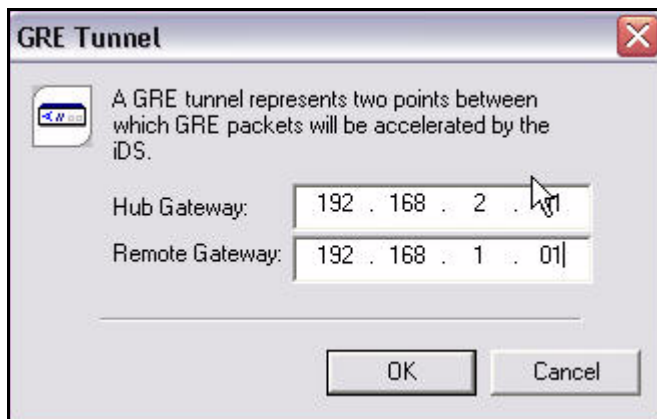


Beginning with release 6.0.5, you may send GRE-tunneled data with TCP acceleration across an iDS network.

Use the following procedure to define a GRE Tunnel:

- Step 1 Click **Add** to access the GRE Tunnel dialog box.
- Step 2 Specify the hub and remote endpoints for the tunnel.

Step 3 Click **OK** to save your changes.



## NOTE

This procedure only sets up the GRE tunnel within the iDS system. You must still establish the actual GRE endpoints on both sides of the link for a GRE tunnel to work. GRE endpoints must be configured upstream from the Protocol Processor and downstream from the remote.

## 7.6 Switch Tab

Using the **Switch** tab, you can associate each of the eight RJ45 Lan B Ethernet ports located on the back panel of some iDirect remote modems with a specific VLAN. For a VLAN to appear on the **Switch** tab, it must first be added to the remote on the Remote **Information** tab. (See [“Adding VLANs to a Remote” on page 125](#)). Note that the **Switch** tab is only displayed for remote **Model Types** with an eight port switch. These **Model Types** include:

- iNFINITI 5000 Series remotes
- iNFINITI 7000 Series remotes

By default, all VLAN ports are defined as trunks. When a port is defined as a trunk, all traffic on any VLAN (including both user-defined VLANs and the default VLAN) can pass through the port. All user-defined VLAN frames on trunk ports are tagged to explicitly identify the VLAN. Default VLAN traffic passing through a trunk port is not tagged.

As an alternative to allowing a port to act as a trunk, you can define a port to be dedicated to a single, specific VLAN. You can dedicate a port to any user-defined VLAN or to the default VLAN. When a port is dedicated to a VLAN, only traffic for that VLAN passes through the port. There is no VLAN tagging on a port dedicated to a single VLAN, regardless of whether the port is dedicated to the default VLAN or to a user-defined VLAN.

The **Switch** tab allows you to perform the following operations:

- Dedicate a port to a specific VLAN
- Configure a port as a trunk (allow traffic on all VLANs to pass through the trunk)

- Specify the port speed and mode (full duplex or half duplex)
- Copy the table of switch settings to an external application such as a spreadsheet

To configure the eight port switch follow these steps:

- Step 1 Click the **Switch** tab to view the current assignment of VLANs to ports. The **Switch** tab contains two panes: the **Port View** (on the left), and the **VLAN View** (on the right). Only VLANs that have already been added to this remote appear in the display.

By default, all ports are defined as trunks. Trunk ports display the word **Yes** in the **All VLANs** row of the **VLAN View**. Trunk ports also display **All VLANs** to the right of the port in the **Port View**. This default configuration is illustrated below.

Information	IP Config	Switch	QoS	Geo Location	VSAT	Warning Properties	Custom																																													
Port View		VLAN View																																																		
Switch Port 1 All VLANs Port 2 All VLANs Port 3 All VLANs Port 4 All VLANs Port 5 All VLANs Port 6 All VLANs Port 7 All VLANs Port 8 All VLANs		<table border="1"> <thead> <tr> <th>VLAN</th> <th>Port1</th> <th>Port2</th> <th>Port3</th> <th>Port4</th> <th>Port5</th> <th>Port6</th> <th>Port7</th> <th>Port8</th> </tr> </thead> <tbody> <tr> <td>All VLANs</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> </tr> <tr> <td>Default</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Vlan4092</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Vlan4094</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>						VLAN	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	All VLANs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Default									Vlan4092									Vlan4094								
VLAN	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8																																												
All VLANs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes																																												
Default																																																				
Vlan4092																																																				
Vlan4094																																																				

- Step 2 You can use either the **Port View** or the **VLAN View** to dedicate a port to a single VLAN. Both methods are described here:

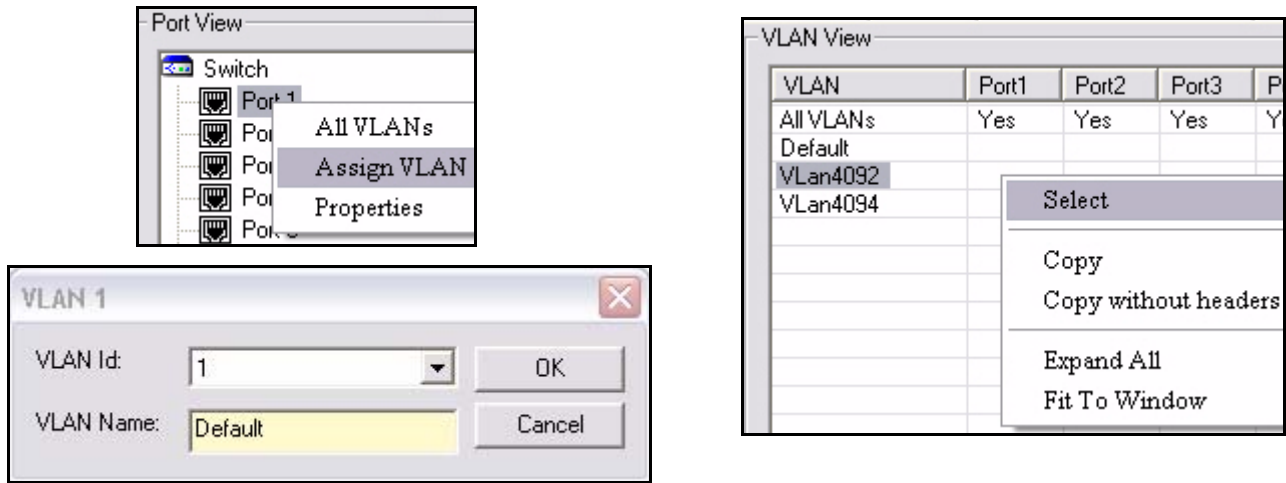
To use the **Port View** to dedicate a port to a single VLAN:

- In the **Port View**, right-click the port that you want to configure and select **Assign VLAN** from the menu to display the dialog box. (Note: you can also select the port and click the **Assign VLAN** button at the bottom of the screen.)
- In the dialog box, select the **VLAN ID** of the VLAN you want to assign to the port. (The **VLAN Name** will be displayed automatically when you select the **VLAN ID**.)
- Click **OK**.

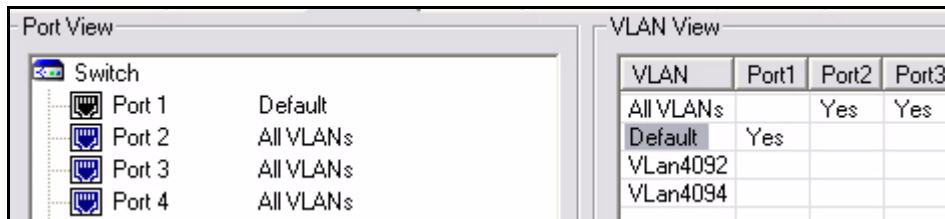
To use **VLAN View** to dedicate a port to a single VLAN:

- In the **VLAN View**, right-click in the table cell representing the port of the VLAN you want to configure.
- Choose **Select** from the menu.

Both methods of dedicating a port to a VLAN are illustrated below.



In the **VLAN View**, the word **Yes** will be displayed for the VLAN in the column for the selected port, and the **Port View** will display the new selection.

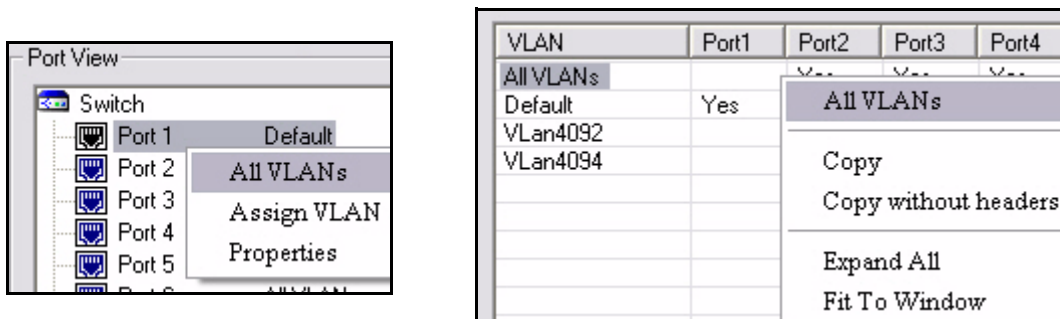


## NOTE

You can double-click in any empty cell in the **VLAN view** to select that cell. Double-clicking in an empty cell will select that cell, causing the word **Yes** to be displayed. The cell that was previously selected will be cleared.

Step 3 To reconfigure a dedicated port to be a trunk, do one of the following

- In the **Port View**, right-click the port and select **All VLANs** from the menu.
- Or, in the **VLAN View**, right-click in the column of the port in the **All VLANs** row and select **All VLANs** from the menu.



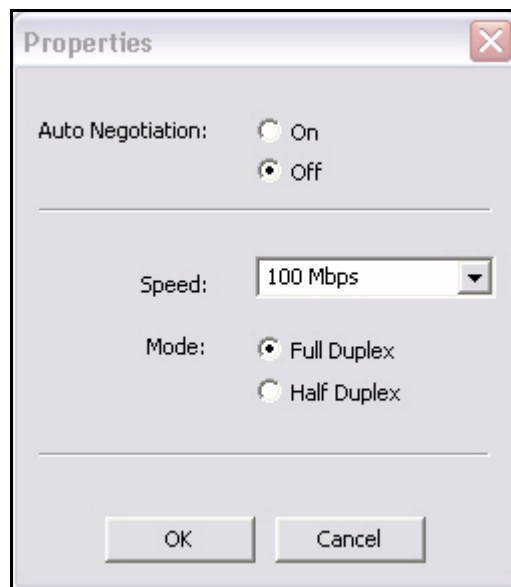


Step 4 You can select the same setting for all ports by clicking your choice in the **VLAN** column of the **VLAN View** and clicking **Select All** in the menu. The word **Yes** will appear in all columns of the selected row. In this example, **Select All** was used to dedicate all ports to the default VLAN.

VLAN View								
VLAN	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8
All VLANs								
Default	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Vlan4092								
Vlan4094								

Step 5 By default, the port speed and port mode are automatically negotiated. Follow these steps if you want to disable auto-negotiation and select a port speed and port mode:

- a In the **Port View**, right-click the port you want to configure and select **Properties** from the menu to display the **Properties** dialog box.



- b In the **Properties** dialog box, select **Off** for **Auto Negotiation**.
- c Select a **Speed** for the port: **10 Mbps** or **100 Mbps**.
- d Select a **Mode** for the port: **Full Duplex** or **Half Duplex**.



**WARNING** The port settings must match the attached equipment. Mismatches in either port speed or port mode will result in packet loss.

Step 6 To copy a row (or all rows) from the **VLAN View** so that you can paste the information into a separate application such as a spreadsheet, follow these steps:

- a In the **VLAN** column, click the VLAN name (or click **All VLANs**) in the first column of the row you want to select. This will highlight the name in the VLAN column. (Or press **Ctrl + A** to select all rows in the table.)
- b Right-click on any of the selected entries in the first column; then select **Copy** or **Copy without headers** from the menu.

VLAN	Port1	Port2
All VLANs		
Default		Yes
Vlan4092	Yes	
Vlan4094		

Select All
Copy
Copy without headers

- c You can now paste the row or rows you copied into your target application.

## 7.7 QoS Tab

The following sections provide an overview of how Quality of Service (QoS) is configured on iDirect's remotes.

### 7.7.1 QoS Profiles

You can assign both upstream and downstream Filter Profiles and Traffic Profiles to any remote. Simply select the desired profile from the four drop-down lists at the top of the **QoS** tab. When you click **Details**, iBuilder automatically displays a read-only summary of that profile for quick reference. For more information on assigning QoS Profiles, see [chapter 8, "Creating and Managing QoS Profiles."](#) For an in-depth discussion on how QoS is implemented in iDirect's system, see [chapter 5, "QoS Implementation Principles,"](#) of the [iDirect Technical Reference Guide](#). The **QoS** tab is shown below.

<b>Information</b>	<b>IP Config</b>	<b>Switch</b>	<b>QoS</b>	<b>Geo Location</b>	<b>VSAT</b>	<b>Warning Properties</b>	<b>Custom</b>
--------------------	------------------	---------------	------------	---------------------	-------------	---------------------------	---------------

**Downstream QoS**

Filter Profile:

Traffic Profile:

**Upstream QoS**

Filter Profile:

Traffic Profile:

**Downstream SAR**

Enable Segment Size:  bytes

**Upstream SAR**

Enable Segment Size:  bytes

**Downstream Rate Shaping**

Maximum Information Rate:

Enable  kbps

Committed Information Rate (CIR):

Enable  kbps

**Upstream Rate Shaping**

Maximum Information Rate:

Enable  kbps

Committed Information Rate (CIR):

Enable  kbps

Minimum Information Rate:

Enable  kbps

**PAD**

Optimize for:  Maximum channel efficiency  Minimum latency

## 7.7.2 Upstream and Downstream SAR

This section discusses only the parameters of the **QoS** tab shown below. For information about SAR, including recommended segment sizes for **Upstream SAR** and **Downstream SAR**, see [chapter 5, “QoS Implementation Principles,”](#) of the [iDirect Technical Reference Guide](#).

<p><b>Downstream SAR</b></p> <p><input type="checkbox"/> Enable Segment Size: <input type="text" value="70"/> bytes</p>	<p><b>Upstream SAR</b></p> <p><input checked="" type="checkbox"/> Enable Segment Size: <input type="text" value="70"/> bytes</p>
---	--

Step 1 Either Downstream and Upstream Segmentation and Reassembly (SAR). Downstream defaults to “off” (unchecked), whereas upstream defaults to “on” (checked).

Step 2 Enter the **Segment Size** for each.



**NOTE**

Upstream SAR is always enabled on all mesh-enabled remotes. You must ensure that the upstream SAR segment size is set to the same value for all mesh remotes in an Inroute Group. iDirect recommends that you use the default SAR segment size.

### 7.7.3 Upstream and Downstream Rate Shaping

This section discusses only the parameters of the **QoS** tab shown below.

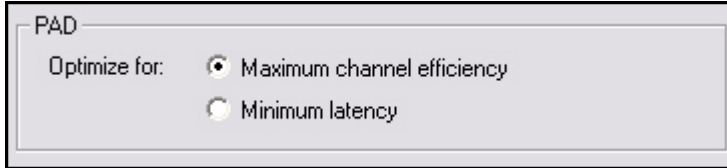
<p>Downstream Rate Shaping</p> <p>Maximum Information Rate:</p> <p><input type="checkbox"/> Enable <input type="text" value="0.001"/> kbps</p> <p>Committed Information Rate (CIR):</p> <p><input type="checkbox"/> Enable <input type="text" value="0.001"/> kbps</p>	<p>Upstream Rate Shaping</p> <p>Maximum Information Rate:</p> <p><input type="checkbox"/> Enable <input type="text" value="4.532"/> kbps</p> <p>Committed Information Rate (CIR):</p> <p><input type="checkbox"/> Enable <input type="text" value="4.532"/> kbps</p> <p>Minimum Information Rate:</p> <p><input type="checkbox"/> Enable <input type="text" value="0.28"/> kbps</p>
<p>PAD</p> <p>Optimize for: <input checked="" type="radio"/> Maximum channel efficiency <input type="radio"/> Minimum latency</p>	

For information about rate shaping for QoS, see [chapter 5, “QoS Implementation Principles,”](#) of the *iDirect Technical Reference Guide*.

- Step 1 Either select or clear **Enable** on **Downstream** and **Upstream Rate Shaping** check boxes.
- Step 2 If you enable **Downstream Rate Shaping**, you may enter a value for **Maximum** or **Committed Information Rate**.
- Step 3 If you enable **Upstream Rate Shaping**, you may enter a value for **Maximum**, **Committed**, or **Minimum Information Rate**.

## 7.7.4 PAD

This section discusses only the parameters of the **QoS** tab shown below. For information about PAD, see [chapter 5, “QoS Implementation Principles,”](#) of the [iDirect Technical Reference Guide](#).



The screenshot shows a window titled "PAD" with a "Optimize for:" label. There are two radio button options: "Maximum channel efficiency" (which is selected) and "Minimum latency".

Select either **Optimize for: Maximum channel efficiency** or **Minimum latency**.

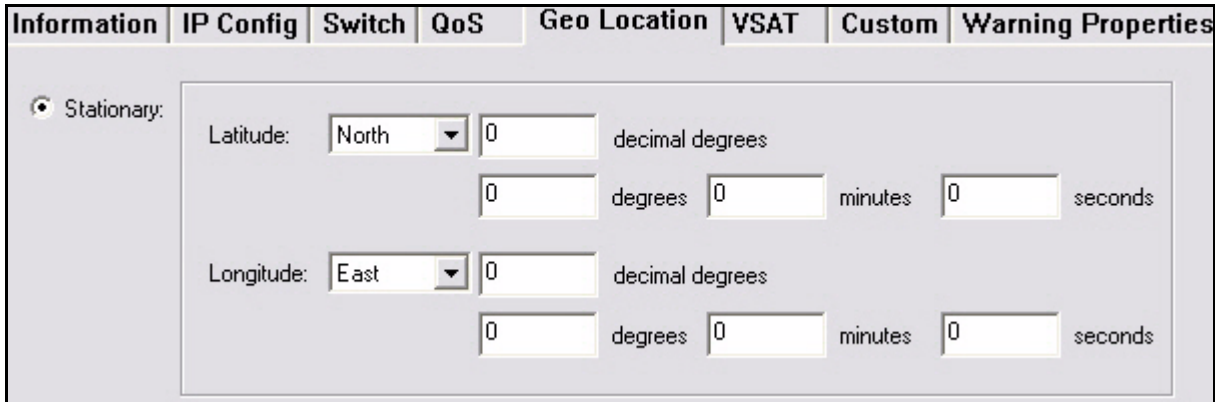


### Warning

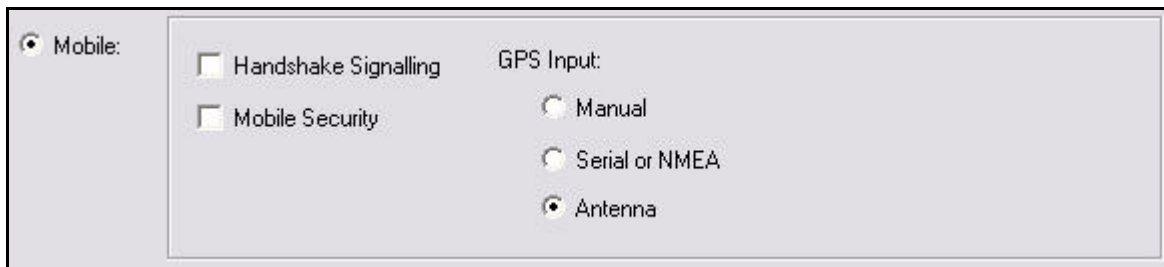
Selecting **Minimum Latency** instructs the PAD layer not to hold onto partially filled TDMA bursts but to release them immediately. This can result in an increased number of unused bytes per burst, significantly decreasing the upstream throughput for remotes with this setting. Do not select **Minimum Latency** unless you are certain that your application requires it.

## 7.8 Geo Location Tab

If you are commissioning a stationary remote, use the **Geo Location** tab to specify the geographic location of the installation site. Geo location can be determined by using a GPS.



If you are commissioning a mobile remote, use the **Geo Location** tab to specify the remote's mobile settings.



Follow these steps if you are commissioning a mobile remote:

- Step 1 Select **Mobile**.
- Step 2 Selecting **Handshake Signaling** provides an input and output signal to the stabilizing antenna through the serial console port. (See the following section on **Mobile State**.)
- Step 3 Selecting **Mobile Security** prevents the remote's latitude and longitude location from being sent over the air to the NMS. If this is selected, it will not be possible to determine the remote's location from the hub. (See the following section on **Mobile State**.)
- Step 4 Select the correct type of GPS input for your mobile remote.

### **Mobile State**

When the remote is configured as Mobile, it looks for a GPS string on the serial console port to provide its latitude and longitude information in the form of an NMEA string. It uses this information to compute the FSD and acquire into the network.

Once a remote has been acquired into the network, the remote automatically sends its latitude and longitude to the hub every 30 seconds. However, when Mobile Security is selected, the remote will not send its current geographic location to the hub. Since the hub requires this information to communicate with the remote, mobile remote users must determine it and communicate it to the remote, enabling the remote to compute the FSD.

In the absence of a GPS receiver interface to the modem, the latitude and longitude information can be supplied through the serial console interface. The console interface for a mobile remote runs at 4800 baud. This baud rate is a requirement of the NMEA protocol used by GPS to communicate with the remote. (Note that the console interface for NetModems not in Mobile Mode is 9600 baud). Customers can also provide the geographic location information for the hub through the iSite GUI. (The hub geographic location is always sent as a broadcast message from the hub.)

Handshake signaling requires a stabilizing antenna and requires customers to build their own electrical interface (converter) to communicate with the antenna. When modem handshaking is enabled at the NMS, the mobile remote provides an input and output signal to the stabilizing antenna through the serial console port. The output signal, or lock signal, indicates the frame lock status of the receiver on the remote. The input signal TxMute is used to mute the transmitter until the antenna pointing is completed.

The remote sends an RS-232 active signal on the console port DTR output (pin 2) while the modem is trying to acquire the downstream carrier. Once the remote achieves TDM frame lock, the DTR signal becomes inactive. This signal is intended to indicate to the auto-point antenna equipment when to switch from coarse-tune to fine-tune mode.

The DSR input on the console port (pin 7) can be used as a “mute” function and will allow the auto-point antenna equipment to delay acquisition transmit until the antenna has finished pointing. Without this function, the modem may transmit as soon as it detects TDM frame lock, before the antenna is properly pointed and polarized. Sending an RS-232 active level to the DSR input enables the mute function.






**NOTE** Mesh remotes cannot be deployed as mobile remotes.

## 7.9 VSAT Tab

The **VSAT** tab contains two sets of inter-related VSAT tabs. The top contains tabs and drop-down list boxes for selecting the previously defined IFL, BUC, Reflector Mount, Reflector, and LNB. The tabs on the bottom display configuration details for the currently selected subcomponent. Switching between tabs enables users to review the configuration of selected subcomponents on

one screen. To add these subcomponents entries to the NMS database, see [chapter 3, “Overview of the Network Management System for iBuilder,”](#) section [“Adding Entries to Folders”](#) on page 22.

Information	IP Config	Switch	QoS	Geo Location	VSAT	Custom	Warning Properties																																			
<h3>Remote Antenna</h3>																																										
IFL:	TDoc IFL																																									
BUC:	TDoc BUC																																									
Reflector Mount:	TDoc Reflector Mount																																									
Reflector:	TDoc Reflector	Hunt Frequency:	0	MHz																																						
LNB:	TDoc LNB	Hunt Polarity:	Horizontal																																							
Approx. Cable Length:	30	meters	Noise Reference Frequency:	0	MHz																																					
<table border="1"> <thead> <tr> <th>IFL</th> <th>BUC</th> <th>Reflector Mount</th> <th>Reflector</th> <th>LNB</th> </tr> </thead> <tbody> <tr> <td colspan="5">  <h3>IFL</h3> </td> </tr> <tr> <td>Manufacturer:</td> <td colspan="4">None</td> </tr> <tr> <td>Manufacturer Part Number:</td> <td colspan="4">TDoc IFL</td> </tr> <tr> <td>iDIRECT Part Number:</td> <td colspan="4"></td> </tr> <tr> <td>Loss:</td> <td>0</td> <td colspan="3">dB</td> </tr> <tr> <td>DC Resistance:</td> <td>0</td> <td colspan="3">Ohm</td> </tr> </tbody> </table>								IFL	BUC	Reflector Mount	Reflector	LNB	 <h3>IFL</h3>					Manufacturer:	None				Manufacturer Part Number:	TDoc IFL				iDIRECT Part Number:					Loss:	0	dB			DC Resistance:	0	Ohm		
IFL	BUC	Reflector Mount	Reflector	LNB																																						
 <h3>IFL</h3>																																										
Manufacturer:	None																																									
Manufacturer Part Number:	TDoc IFL																																									
iDIRECT Part Number:																																										
Loss:	0	dB																																								
DC Resistance:	0	Ohm																																								

- Step 1 In the **Remote Antenna** area, select a BUC from the **BUC** drop-down box.
- Step 2 Select the LNB you are using for this remote from the LNB drop-down box.
- Step 3 Selecting an IFL, Reflector Mount, and/or Reflector is optional.
- Step 4 Approximate cable length should be set during the commissioning process.
- Step 5 The tabs on the lower half of the dialog box display the details of the components that you have selected. Click **OK** to save your settings. The new remote appears in the Tree under the Inroute Group to which you assigned it.



## 7.10 Setting Warning Properties for Remotes

You can use iBuilder to modify both global properties of remote warnings and warning properties for individual remotes. To change global warning properties for remotes, select **Global Warnings for Remotes** from the **Edit** menu. To change warning properties for individual remotes, click the **Warning Properties** tab for the remote you want to modify.

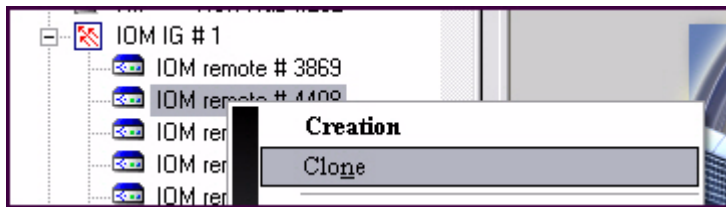
For details on configuring warning properties for line cards, remotes and protocol processor blades, please see [“Configuring Warning Properties” on page 55](#).

## 7.11 Adding a Remote by Cloning an Existing Remote

You can either add a new remote by using the procedures in [“Adding Remotes” on page 115](#) or you can *clone* an existing remote to create another remote with a new name but the same definition. The cloning feature is a quick and easy way to create several remotes with minor differences, without having to configure each one from a blank configuration screen.

To clone an existing remote, follow the procedure below:

- Step 1 Right-click a **Remote** and select **Clone**. In the example below, the remote named “IOM Remote 4408” is being cloned. A new remote named “Copy of IOM Remote 4048” appears in the Tree and the remote configuration dialog box is displayed.



- Step 2 Enter a new name for the remote.
- Step 3 Modify any fields you want to change for the new remote.
- Step 4 Click **OK** to save your changes.

## 7.12 Roaming Remotes

iDirect release 7.0 allows you to define mobile remotes that “roam” from network to network around the globe. Roaming remotes are not constrained to a single location or limited to any geographic region. Instead, by using the capabilities provided by the iDirect “Global NMS” feature, you can configure your remote terminals to have true global IP access.



### NOTE

Global NMS is a licensed feature. If you plan to define and track roaming remotes in your network, please contact the iDirect Technical Assistance Center (TAC).

The Global NMS feature allows remotes to move among networks on various transponders and satellites, controlled from various hubs. To accomplish this, you must define the remote in all of the networks in which it will be visible. For more information of the Global NMS feature, see [chapter 7, “Global NMS Architecture”](#) of the [iDirect Technical Reference Guide](#).

The set of parameters that defines a roaming remote falls into three categories:

- Parameters that must be the same in all networks: DID, telnet passwords, and remote name. iBuilder will not allow you to define these parameters inconsistently across networks for the same remote.
- Parameters that must be different in each network. These consist mostly of internal database IDs and references that are automatically established by iBuilder when the remote is defined in multiple networks.
- Parameters that may be the same or different from network to network. These “don’t care” parameters include everything not in the lists above. Examples are IP configuration, QoS settings, initial transmit power values.

Once you define a roaming remote and add it to multiple networks, the “don’t care” parameters will be identical in all networks. At that time, you can modify these parameters in the different networks as desired. (See [“Managing “Don’t Care” Parameters” on page 150](#)).

**NOTE**

The Global NMS feature is available only on iNFINITI remotes. NetModem II Plus remotes cannot roam from network to network.

**NOTE**

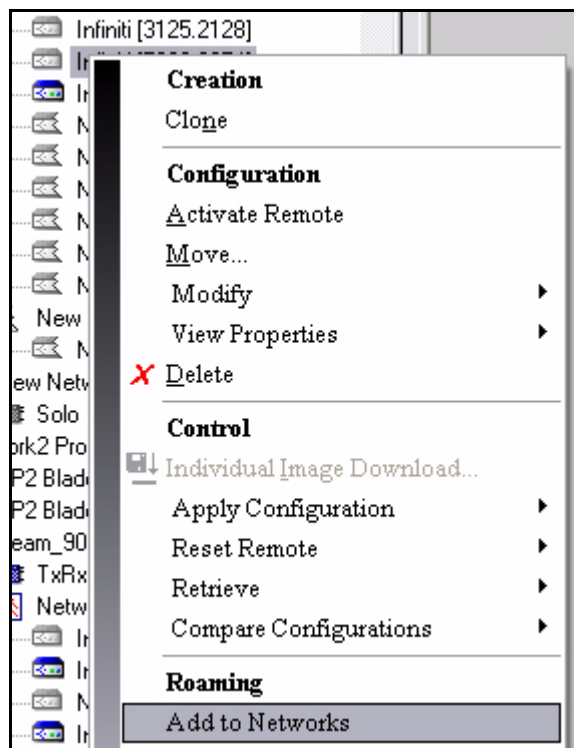
Mesh remotes cannot act as roaming remotes.

## 7.12.1 Adding a Roaming Remote

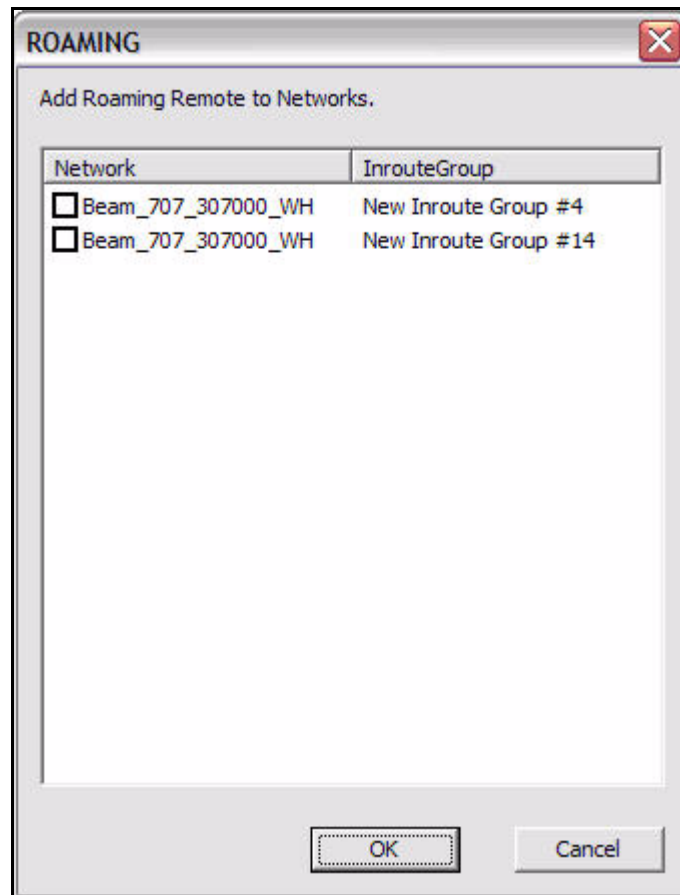
To define a roaming remote, first create the remote in one of the target networks using the procedure in [“Adding Remotes” on page 115](#). Define this remote in the normal way for that network, including setting IP parameters and features, VSAT components, rate limits, and other settings.

Once you have added the remote to one network, follow the steps below to add it to the remaining networks:

- Step 1 Right-click the Remote in the Tree and select **Add to Networks** in the **Roaming** section of the remote menu.



Step 2 Select the appropriate check boxes to add the remote to one or more additional networks.



Step 3 Click **OK** to save your changes and close the dialog box. iBuilder automatically adds the remote to the selected networks, copying the “don’t care” configuration items to the new networks. You are free to modify the remote’s configuration in the other networks as desired.



**NOTE**

When adding roaming remotes to networks, only networks in which the remote is not currently configured are displayed in the dialog box.

## 7.12.2 Managing Roaming Remote Configuration

There are two primary ways to manage a roaming remote's configuration across all of its network instances. Each is described in the sections that follow.

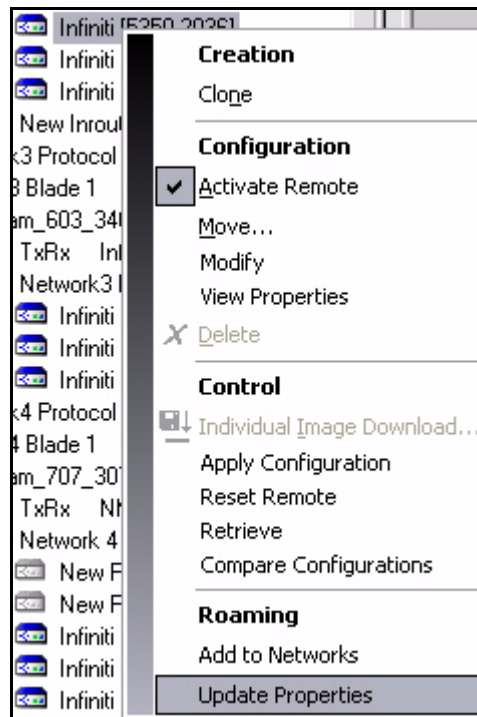
The Revision Server is completely compatible with roaming remotes. You may upgrade a network even if a roaming remote is in another network. As long as IP connectivity is available from the NMS to the remote, the remote will receive the download package (image and options file), write it to flash memory, and reset. For details, see [“Downloading Remotes Using Revision Server” on page 207](#).

### **Managing “Must be the Same” Parameters**

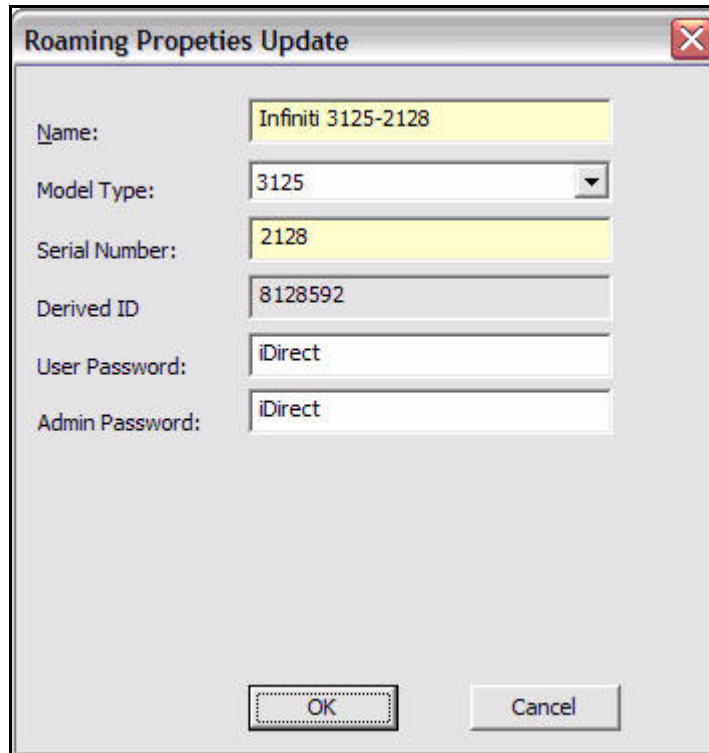
You can modify the parameters that must be the same across all network instances of a roaming remote by selecting **Update Properties** in the Tree for that remote. When you change a parameter in one network using the remote's **Update Properties** dialog box, iBuilder makes the same change to that remote in all of its networks.

Use the following procedure to change roaming remote parameters that must be the same in all networks:

- Step 1 Right-click the Remote in the Tree and select **Update Properties** in the **Roaming** section of the remote menu.



Step 2 Update the values in the **Roaming Properties Update** dialog box as desired.



The image shows a dialog box titled "Roaming Properties Update" with a close button (X) in the top right corner. The dialog contains several input fields:

- Name:** A text box containing "Infiniti 3125-2128".
- Model Type:** A dropdown menu with "3125" selected.
- Serial Number:** A text box containing "2128".
- Derived ID:** A text box containing "8128592".
- User Password:** A text box containing "iDirect".
- Admin Password:** A text box containing "iDirect".

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Step 3 Click **OK** to save your changes and close the dialog box. iBuilder updates the remote in all of its networks.

### **Managing “Don’t Care” Parameters**

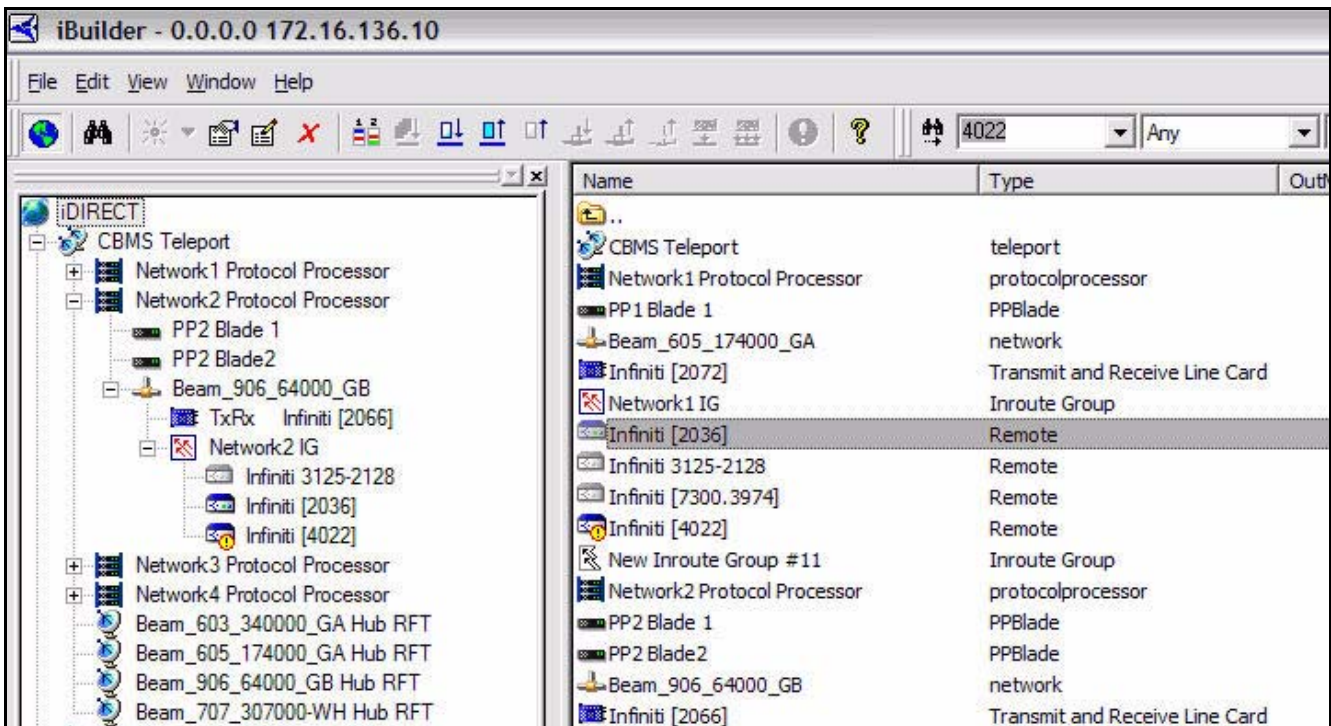
You can change the value for a “don’t care” parameter on a roaming remote in a single network by following the usual procedure: right-click the remote in the Tree for the desired network and selecting **Modify**. This allows you to modify the remote’s parameters in one network while leaving them unchanged in the others.

However, it is likely that many of a roaming remote’s “don’t care” parameters will be the same from network to network. In those instances, iDirect recommends that you use iBuilder’s Group Edit feature to modify the remote. Since this method allows you to modify shared parameters on all instances of the remote at the same time, it is both easier and less error-prone than making the changes one by one. For a general discussion of this feature, see [“Working with Multiple Elements Simultaneously” on page 47](#).

Follow these steps to modify multiple instances of the same remote:

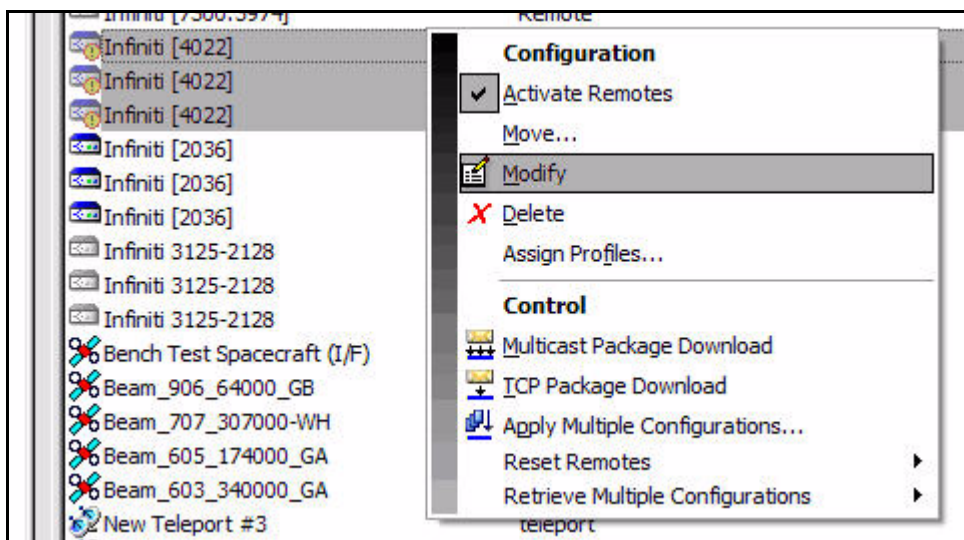
- Step 1 Select **View → Details** from the iBuilder main menu to display the **Details** pane. The **Details** pane is displayed to the right of the Tree.
- Step 2 Select the top-level node in the Network Tree view.

- Step 3 Select **View → Collapse Details Hierarchy** from the iBuilder main menu. This option removes the hierarchical structure of the network elements and components so they can all be shown in a single window.



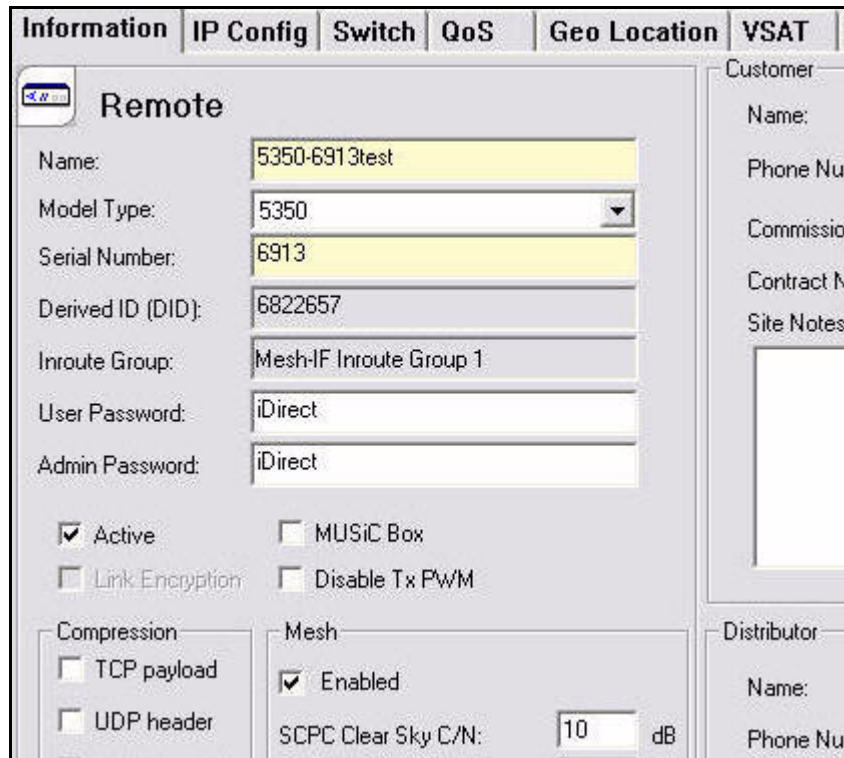
- Step 4 In the **Details View**, select the **Type** column header to sort by element type. This will group together all remotes, regardless of their networks.

- Step 5 If desired, select the **Name** column header to further sort by element name. This will group together all instances of a roaming remote, since the remote has the same name in all networks.





- Step 6 Select all desired instances of the Roaming Remote in the **Details** pane. Then right-click the selected group and choose **Modify** from the menu. You may now modify any of the remote's parameters that are shared across all network instances.



### 7.12.3 Beam Switching for Roaming Remotes

The decision of which network a particular roaming remote joins is made by the remote. There are currently three beam selection methods supported by iDirect.

#### Automatic Beam Selection

Automatic beam selection is the most powerful and flexible way for remotes to roam from network to network. It requires an auto-pointing antenna at the remote site, and a *map server* process on the NMS.

The map server contains footprint information for all beams on all satellites in the global network. It parcels out pieces of the map to remotes based on their current geographic location. Depending on signal quality and location, the remote will either remain in the current network or automatically switch to a higher-quality network.



#### **NOTE**

For more information on this feature, see the iDirect Technical Note titled "Automatic Beam Selection."



## **Manual Beam Selection**

Users at a remote terminal can command the remote to join a particular network using the **beamselector** command, available from the remote's console. The following figure shows the command format and the output of the "list" option.

```
[RMT:2036] admin@telnet:10.0.150.7;1084
> beamselector
control      Beam selector control command
list         list known beams
mapsize      print or change the map size request params
params       stats | params | debug
switch       switch to new beam

[RMT:2036] admin@telnet:10.0.150.7;1084
> beamselector list
3 is currently selected
3 = Beam_603_340000_GA
2 = Beam_906_64000_GB
1 = Beam_605_174000_GA
```

Figure 7-2: Figure: Using the Console's beamselector Command

## **"Round Robin" Beam Selection**

In the absence of both a map server and a **beamselector** command from the console, remotes default to a round-robin selection algorithm. Using this method, a remote will attempt to join each network in turn for five minutes until the remote is acquired. The order in which the remote tries each network is based on the perceived quality of the network's downstream carrier, as determined by the remote's geographic location relative to the satellite longitude.

## **7.13 Enabling IP Packet Compression Types**

Four types of IP packet compression are supported in iDirect:

- TCP payload compression
- UDP header compression
- UDP payload compression
- CRTP (RTP header compression)

The following sections discuss these compression type.

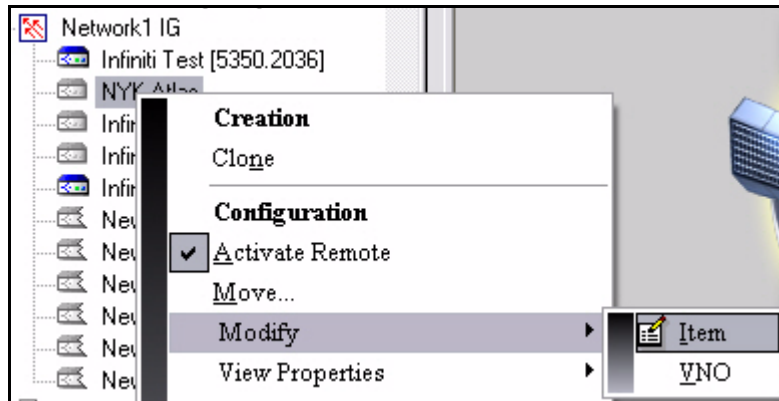


### **NOTE**

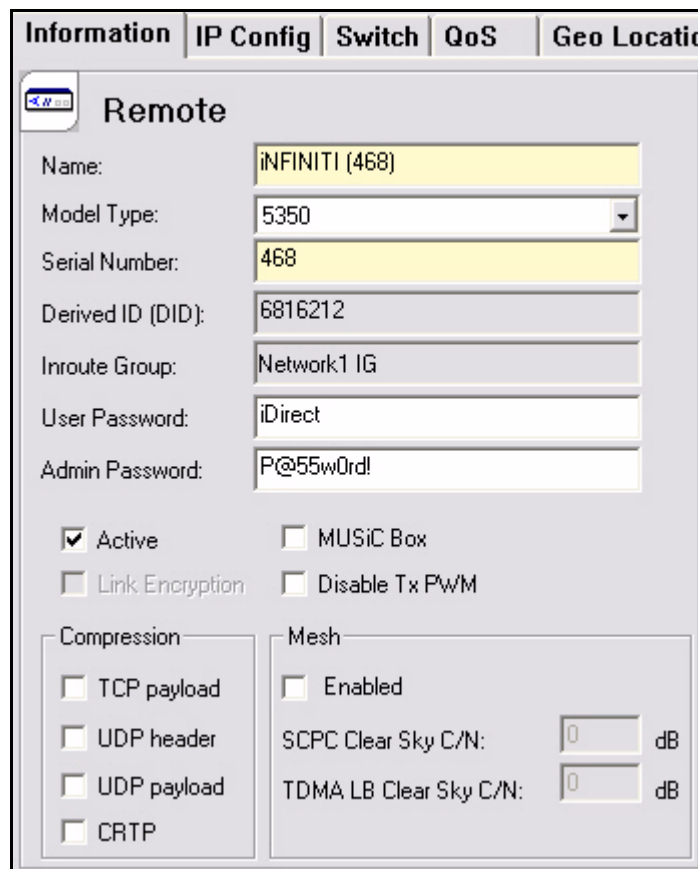
For remotes in a mesh inroute group, you must enable and disable the various compression types at the inroute group level. The inroute group compression settings override individual remote settings. See ["Adding Inroute Groups" on page 107](#) for details.

You can enable each compression type per remote on the remote's **Information** tab by following these steps:

Step 1 Right-click the **Remote** and select **Modify** → **Item**.



Step 2 In the **Compression** area of the **Information Tab**, select each compression type that you want to enable for the remote.



Step 3 Click **OK** to save your changes.

### 7.13.1 TCP Payload Compression

You can enable TCP payload compression on your iNFINITI 5000 and 7000 series remotes to increase the available bandwidth for TCP streams during periods of channel congestion. When enabled, the TCP streams are compressed on both the downstream and upstream channels simultaneously. By default, TCP payload compression is turned off.

TCP payload compression is activated only during times of congestion. If no congestion is present, data passes through the compression layer unchanged. The compression ratio varies depending on the amount of congestion and the nature of the TCP payload data.

Even during channel congestion, compression is *not* enabled under all circumstances. If a remote's CPU utilization is above 50 percent, TCP payload compression is automatically disabled for all sessions. If CPU utilization is below 50 percent, a maximum of five TCP sessions are compressed. If the number of sessions exceeds five, the additional sessions are not compressed.



#### NOTE

TCP payload compression is available only on iNFINITI 5000 series and iNFINITI 7000 series remotes. It is not available on iNFINITI 3000 series or NetModem II Plus units.

### 7.13.2 UDP Header Compression

UDP header compression is performed on per-packet basis using zlib. Unlike TCP Payload compression, it is not stream-based. UDP header compression is available for all iDirect remote model types.

iDirect UDP header compression follows the specification in RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*. This RFC defines both CRTP (header compression for RTP packets) and UDP header compression (for other UDP packets). When you enable UDP header compression in iBuilder, only non-RTP headers are compressed for UDP packets. If you want header compression to be applied to RTP packets, you must enable CRTP. (See [“CRTP” on page 156.](#))

The iDirect UDP header compression implementation is a simplex-based compression scheme with the periodic retransmission of full headers to restore the compression state in the event of error.

#### **UDP Header Compression Performance Characteristics**

You can expect the following performance characteristics for UDP header compression in iDirect networks:

- The 28-byte header is typically reduced 8 bytes.
- The average compressed header size is 9.25 bytes.
- The reduction in header size is approximately 67 percent.

### 7.13.3 CRTP

Compression of RTP packet headers (CRTP) is performed on per-packet basis using zlib. Unlike TCP Payload compression, it is not stream-based. CRTP is available for all iDirect remote model types.

iDirect's implementation of the CRTP algorithm follows the specification in RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*. This RFC defines both CRTP (header compression for RTP packets) and UDP header compression (for other UDP packets). When you enable CRTP in iBuilder, only RTP packet headers are compressed. If you want header compression to be applied to other UDP packets, you must enable UDP header compression. (See ["UDP Header Compression" on page 155.](#))

The iDirect CRTP implementation is a simplex-based compression scheme with the periodic retransmission of full headers to restore the compression state in the event of error. Correct functionality of the CRTP implementation has been field-proven in multiple iDS releases.

#### **RTP Header Compression Performance Characteristics**

You can expect the following performance characteristics for RTP header compression in iDirect networks:

- The 40-byte header is typically reduced to 10 bytes.
- The average header size is 11.875 bytes.

The reduction in header size is approximately 70 percent.

### 7.13.4 UDP Payload Compression

iDirect's UDP payload compression algorithm is similar to the algorithm used by iDirect for TCP payload compression. (See [Section 7.13.1 "TCP Payload Compression"](#) for details.) However, the implementation differs in the following significant areas:

- UDP payload compression is packet-based rather than session-based.
- The UDP payload compression algorithm always attempts to compress UDP packets prior to transmission. Unlike TCP payload compression, it does not make dynamic decisions based on congestion, system load, etc.

UDP payload compression is designed specifically for the GSM backhaul market. It is unlikely that enabling UDP payload compression will have any noticeable benefit for standard voice traffic, since this type of traffic normally cannot be compressed. iDirect does not recommend enabling this compression feature for typical VoIP traffic; it will not increase channel capacity and it will put unnecessary strain on the remote's processor.

## 8 Creating and Managing QoS Profiles

This section discusses the concept of QoS profiles in detail, and what it means for your networks. It contains the following sections:

- [“What is a QoS Profile?” on page 157](#)
- [“Storage of QoS Profile” on page 158](#)
- [“Adding and Modifying Upstream and Downstream Profiles” on page 159](#)
- [“Cloning a Profile” on page 160](#)
- [“Adding a Service Level” on page 160](#)
- [“Adding a Filter” on page 163](#)
- [“Assigning a Profile to a Remote” on page 166](#)
- [“Assigning QoS Profiles to Individual and Multiple Elements” on page 167](#)
- [“Icon Color Indicators for Profiles” on page 169](#)

### 8.1 What is a QoS Profile?

iBuilder supports two types of QoS profiles: Traffic Profiles and Filter Profiles. A QoS Traffic Profile is a group of service levels, collected together and given a name of your choice. A QoS Filter Profile encapsulates a single filter definition, and contains a group of rules instead of service levels. Both Traffic Profiles and Filter Profiles are separated into downstream and upstream subtypes; this gives you even more flexibility to shape your upstream and downstream traffic. The QoS Profiles in iBuilder make it easy for you to manage groups of QoS settings across medium-to-large networks. [Figure 8-1](#) on [page 158](#) shows the relationship between remotes and QoS profiles.

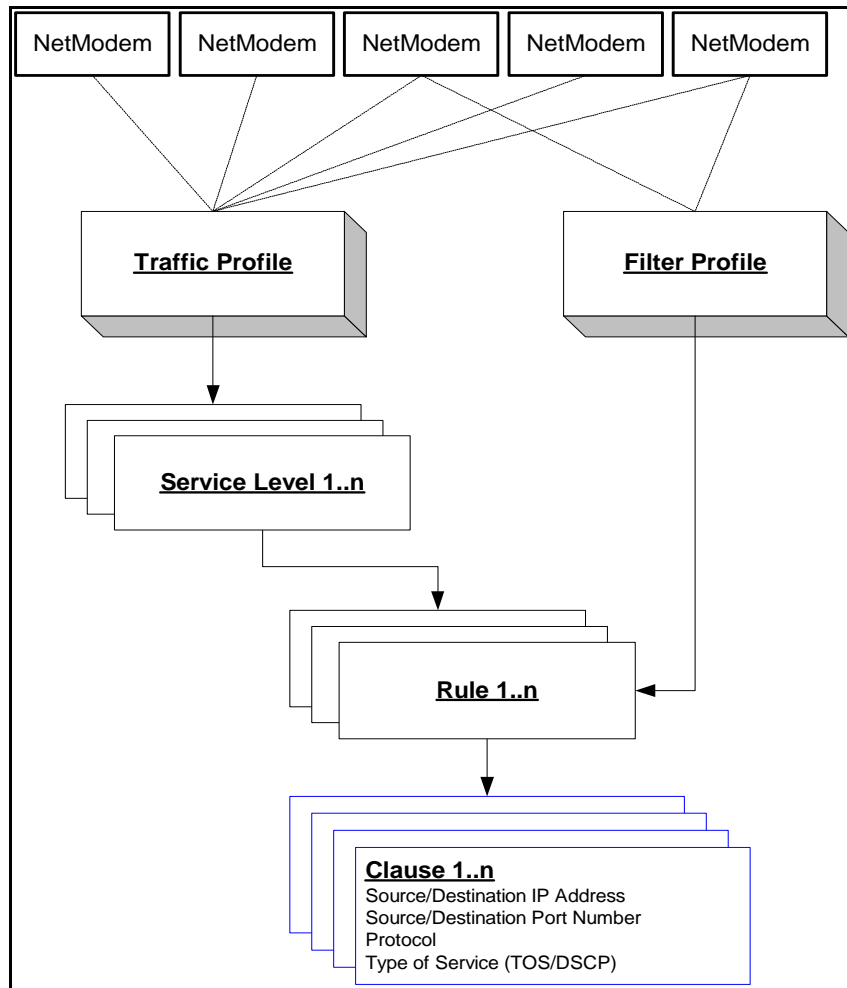
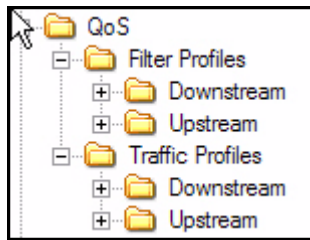


Figure 8-1: Remotes Associated with Profiles

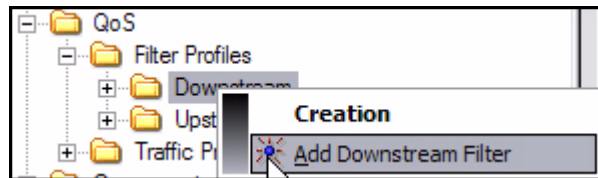
## 8.2 Storage of QoS Profile

QoS Traffic and Filter Profiles are stored in separate folders in iBuilder's Network Tree. They are not associated with a teleport; instead they are independent of any network hierarchy, similar to spacecraft and antenna components.



### 8.3 Adding and Modifying Upstream and Downstream Profiles

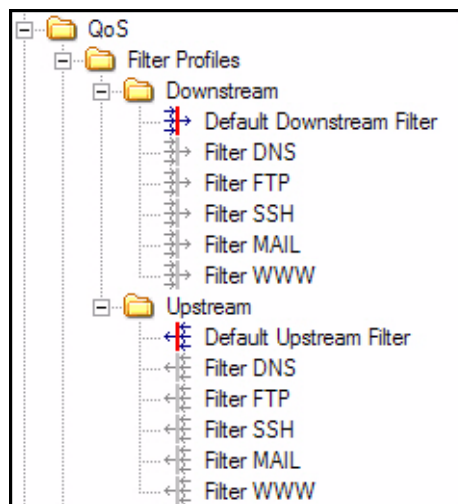
To add a new profile, point to an upstream or downstream folder under Filter or Traffic Profiles; right-click to open it; and select the **Add** option. The title of the Add option will be different depending on what type of profile you are adding. The example below shows a Downstream Filter being added.

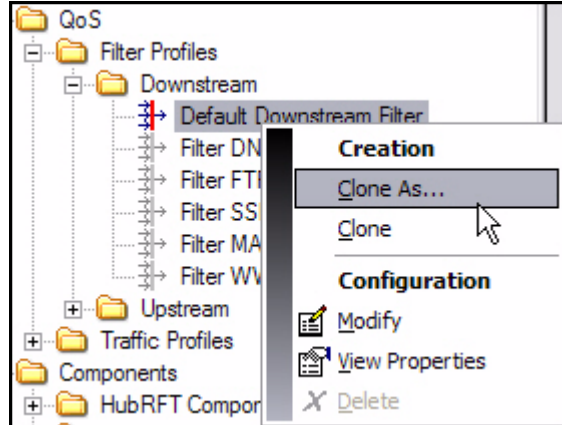


A **Modify Configuration** dialog box opens to allow you to configure the profile you are adding. You can assign it a name, and click Add to display either the **Add Filter** dialog box or the **Add Service Level** dialog box. These are discussed further in:

- [“Adding a Service Level” on page 160](#)
- [“Adding a Filter” on page 163.](#)

Once a filter or service level is configured and saved, it appears in the list within its respective folder, as shown below.





## 8.4 Cloning a Profile

You can then right-click to select a profile and then select **Clone** or **Clone As** to create another profile with a new name, but that has the same definition. The cloning feature is a quick and easy way to create several profiles with minor differences, without having to configure each one from a blank configuration screen.

- If you select **Clone**, a copy of the selected profile is created in the same folder. You can then edit the new profile to make a few minor changes.
- If you select **Clone As**, the selected profile will automatically be copied to the folder that houses profiles of the opposite direction. For example, if you select Clone As on an Upstream Traffic Profile, it will create a duplicate Traffic Profile and place it in the Downstream folder.

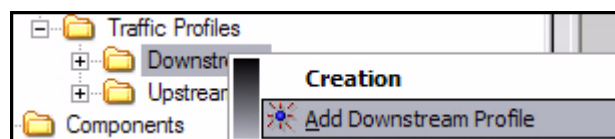
For traffic profiles, you create multiple service levels, each with its own set of rules. For filter profiles, you create a list of rules.

## 8.5 Adding a Service Level

You will normally create multiple service levels, each with its own set of rules. Each service level has a set of rules that determine which packets match. The service level type is chosen based on the type of traffic that is matched by the service level.

To add a service level, follow the procedure below:

- Step 1 Right-click an Upstream or Downstream Traffic Profiles folder. The **Traffic Profile** dialog box opens.








**Information**

**Downstream Traffic Profile**

Profile Name:

Service Levels ↑ ↓

	Service Level	Type	Scheduling	Depth ms	Drop	TOS Mark	Realtime	Trigger CIR
	UDP	U	cost_based (0.50)	250	OLDEST	N/A	Normal	Y
	TCP	R	cost_based (0.50)	250	OLDEST	N/A	Normal	Y
	DEFAULT	U	cost_based (0.50)	250	OLDEST	N/A	Normal	Y

Add... Edit... Delete

Rules

```
SERVICE LEVEL :: UDP
PROTOCOL = UDP
```

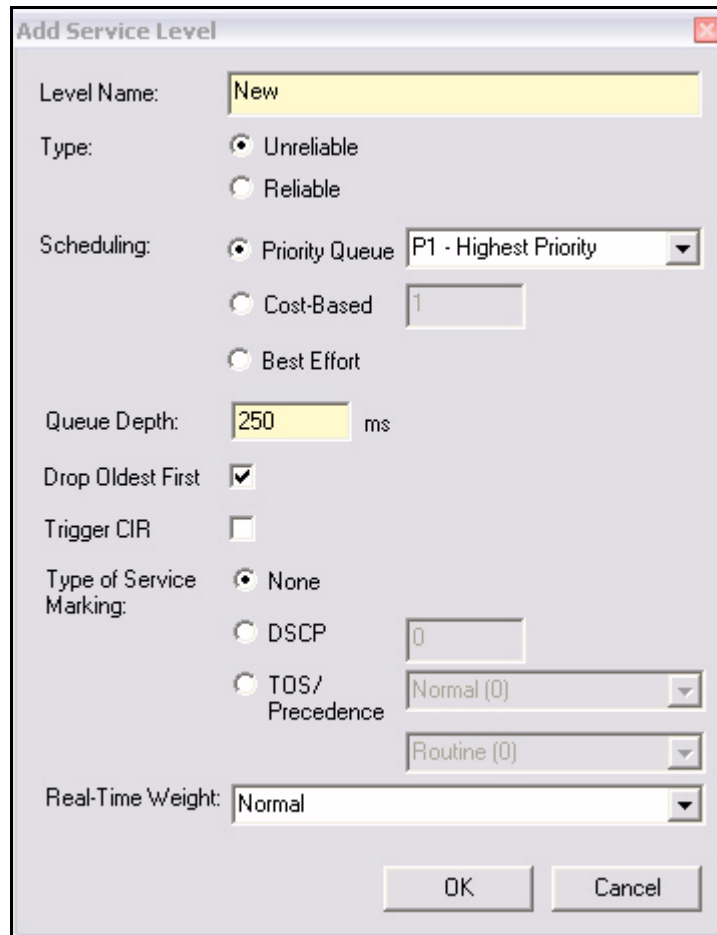
Add... Edit... Delete

Used by:

Remote	Network
7350-4595	SQA Network
SRAO Remote [2012]	SRAO Network

Show Protocol Names

Step 2 Click the **Add** button. The **Add Service Level** dialog box opens.



Step 3 Enter a name for the service level.

Step 4 Choose **Reliable** or **Unreliable**. If the service level is intended to match TCP traffic, you should choose **Reliable**. All other traffic must have an **Unreliable** designation.

Step 5 Select the method of **Scheduling** to be used for this service level: **Priority Queue**, **Cost-Based**, or **Best Effort**. If you select **Priority Queue**, then select the priority level from the menu. If you select **Cost-Based**, then enter a cost level.

For details on each scheduling method, see the discussion of packet scheduling in [chapter 5, “QoS Implementation Principles,”](#) of the [iDirect Technical Reference Guide](#).

Step 6 Enter the **Queue Depth**.

Step 7 Select or clear the **Drop Oldest First**.

Step 8 Select the **Trigger CIR** (Committed Information Rate) check box to enable Dynamic CIR for this service level only.

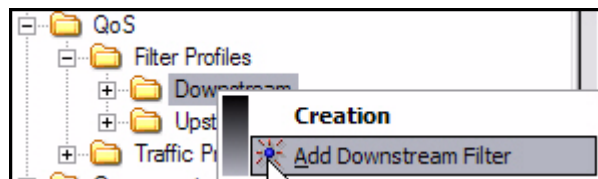
- Step 9 To create a service level traffic profile with Static CIR, ensure that this check box is cleared and that you have configured the **Upstream Rate Shaping** parameters. See [chapter 7, “Configuring Remotes,”](#) section [“Upstream and Downstream Rate Shaping”](#) on page 140.
- Step 10 Choose the **Type of Service Marking** you want.
- Step 11 Select the **Real-Time Weight**. For information about this parameter, see the discussion of network QoS (real-time demand) in [chapter 5, “QoS Implementation Principles,”](#) of the [iDirect Technical Reference Guide](#).
- Step 12 Click **OK** to save this service level.
- Step 13 If you need to edit anything later, simply click the **Edit** button on the **Traffic Profile** dialog box shown above. An **Edit Service Level** dialog box opens, which is exactly the same as the **Add** dialog box. Make any necessary changes and click **OK**.

## 8.6 Adding a Filter


You might find it desirable to create multiple filter profiles, each with a list of rules.

To add a Filter Profile, follow the procedure below:

- Step 1 Right-click an Upstream or Downstream Filter Profiles folder. The **Filter Profile** dialog box opens.



**Information**

 **Downstream Filter Profile**

Name:

Filter

Rules

```
protocol = 3pc AND source_ip_address <> 192.178.24.12 255.255.255.0 AND destination_ip_address <> 192.178.42.44 255.255.255.0
```

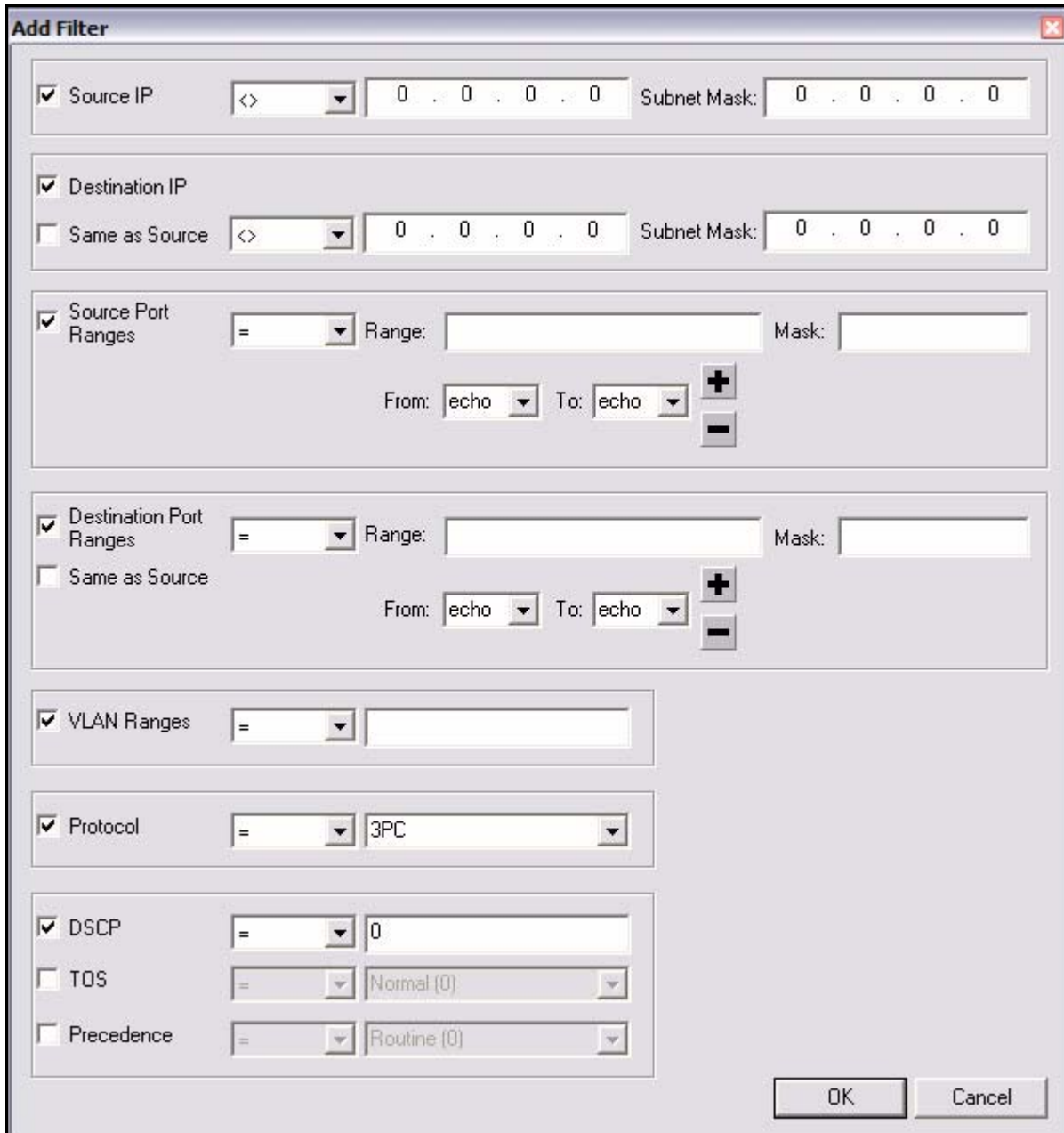
Used by:

Remote	Network

Show Protocol Names

- Step 2 Click the **Add** button. The **Add Filter** dialog box opens, allowing you to enter a filtering rule. Note that *all* comparisons specified (as indicated by the check boxes on the left-hand side) must match for the rule to be considered matched.

Each filter profile has one or more rules. For a packet to be further classified at a given traffic profile, it must match **at least one** of that filter profile's rules. A rule is made up of one or more comparisons between IP header fields and a known constant value specified by the user. The system compares each rule of each traffic profile in the order specified, and classifies the packet according to the first service level that matches.



- Step 1 Enter a **Source** and **Destination IP** address and their corresponding **Subnet Masks** and select the = or <> designations. **Source** and **Destination IP** addresses may be supplied as a constant along with a **Subnet Mask**. The IP header may be **equal to (=)** or **not-equal to (<>)** the known constant. The subnet mask is first applied to the IP address in the packet, and then compared against the user-supplied address. This way, **Source** and **Destination Ranges** of subnet masks may be made to match the rule.
- Step 2 Enter the **Source** and **Destination Port Ranges** and select the desired protocols, which may be **equal to (=)** or **not-equal to (<>)** the constant.

- Step 3 Enter the **VLAN Ranges**, which may be **equal to (=)** or **not-equal to (<>)** the constant.
- Step 4 Enter the **Protocol**, which may be **equal to (=)** or **not-equal to (<>)** the constant.
- Step 5 Select either DiffServ **DSCP**, in which case you cannot select TOS or Precedence, or select **TOS** or **Precedence**, in which case you cannot select **DSCP**.
- Step 6 Click **OK** to save the filter profile.
- Step 7 If you need to edit anything later, simply click the **Edit** button on the **Filter Profile** dialog box shown above. An **Edit Filter Profile** dialog box opens, which is exactly the same as the **Add** dialog box. Make any necessary changes and click **OK**.

## 8.7 Assigning a Profile to a Remote

The QoS tab on each remote's properties window shows both upstream and downstream filter profiles and traffic profiles side-by-side. There are four drop-down lists that allow you to select the appropriate profile.

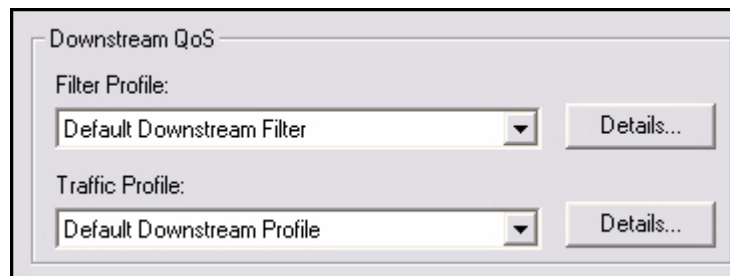


Figure 8-2: Downstream QoS (Left side of QoS pane)

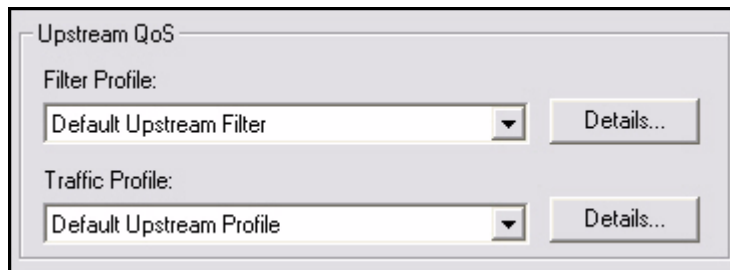


Figure 8-3: Upstream QoS (Right side of QoS pane)

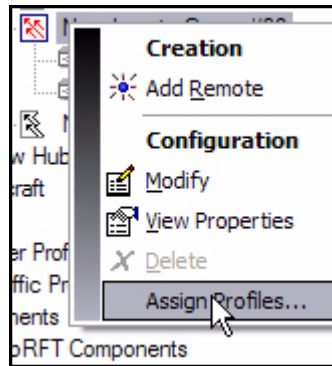
For each type of profile (upstream, downstream, filter profile, traffic profile), simply select the desired profile from the drop-down list. iBuilder automatically displays a read-only summary of the profile for quick reference. You can also manage assignment for multiple modems at once using the Profile Assignment Editor. See [“Assigning QoS Profiles to Individual and Multiple Elements” on page 167](#) for more information.

## 8.8 Assigning QoS Profiles to Individual and Multiple Elements

You can assign profiles to remotes, networks, and teleports.

To assign a profile to an element, follow the procedure below:

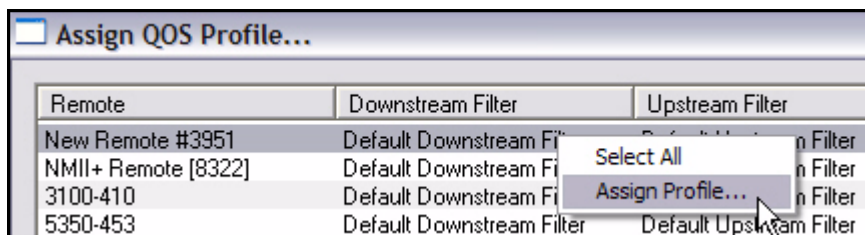
- Step 1 Right-click the element in the Tree and select **Assign Profiles**. The **Assign QoS Profile** dialog box opens. In this example, a network is having profiles assigned to its remotes.



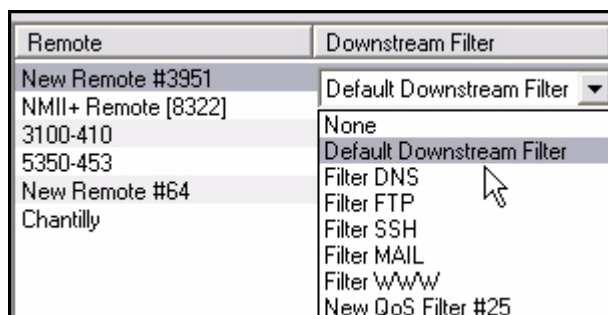
The **Assign QoS Profile** dialog box lists all of the upstream and downstream Traffic (Service Level) Profiles and Filter Profiles (which filter based on IP addressing, VLANs and protocols). The title row specifies the filters and traffic profiles, and the far left column lists the remotes in the network to which we are assigning profiles.

Remote	Downstream Filter	Upstream Filter	Downstream Traffic	Upstream Traffic
New Remote #3951	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
NMII+ Remote [8322]	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
3100-410	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
5350-453	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
New Remote #64	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
Chantilly	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile

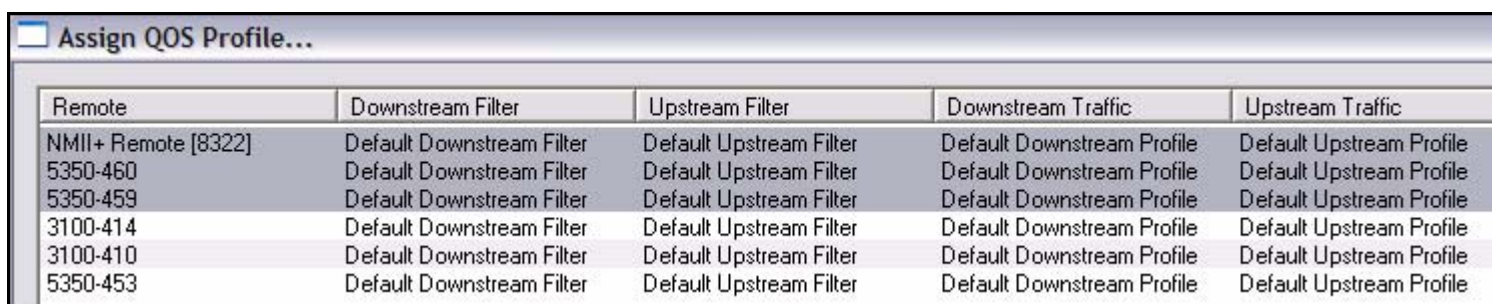
Step 2 To assign a different profile to a remote, select the row that the remote is in, and right-click in the column of the profile you want to change. In the example below, we clicked in the Downstream Filter column for New Remote #3951.



Step 3 Select **Assign Profile**. A drop-down list of all available profiles of that type appears. For example, in this case, a list of all available Downstream Filters would appear, as shown below.



Step 4 You can also change multiple assignments at the same time. Select all of the remotes that you want to change, using the standard Windows multiple-select keys (Ctrl or Shift), then right-click in the column for the type of profile you want to change (upstream, downstream, filter or traffic). The assignment you make is applied to all modems that are currently selected. The example below shows the first three remotes selected.





Step 5 Click a filter and select **Assign Profile** as you do with a single entry.

Remote	Downstream Filter	Upstream Filter	Downstream Traffic	Upstream Traffic
NMII+ Remote [8322]	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
5350-460	Default [ Select All	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
5350-459	Default [ Assign Profile...	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
3100-414	Default [	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
3100-410	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
5350-453	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile

Step 6 Select a profile from the drop-down list. It will be assigned to all of the selected remotes.

Remote	Downstream Filter	Upstream Filter	Downstream Traffic	Upstream Traffic
NMII+ Remote [8322]	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
5350-460	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
5350-459	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
3100-414	None	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
3100-410	Default Downstream Filter	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
5350-453	Filter DNS	Default Upstream Filter	Default Downstream Profile	Default Upstream Profile
	Filter FTP			
	Filter SSH			
	Filter MAIL			
	Filter WWW			
	New QoS Filter #25			
	New QoS Filter #26			
	New QoS Filter #28			
	New QoS Filter #30			
	New QoS Filter #31			
	New QoS Filter #32			

### **How do I Tell What Remotes are Using a Given Profile?**

The **Assign QoS Profile** dialog box lists all the remotes using a given profile. It also shows all modems and their current profile assignments in tabular format.

## **8.9 Icon Color Indicators for Profiles**

When a profile is being used, the icon in the network Tree appears in color (notice the red side bar on the first entry in the above figure). When it is not being used, its icon is displayed in gray. This allows you to quickly determine which profiles are assigned to at least one modem and which ones are not being used.

When you initially upgrade your system, the default profiles for each type is displayed in gray because no modems are currently using the default profiles.



## 9 Configuring the Initial Hub Chassis

The connection between the Hub Chassis and the NMS is encapsulated in a third-party IP-addressable controller card called the EDAS board, designed and manufactured by Intelligent Instruments, Inc. Using the EDAS board, the NMS servers are able to control slot power and jumper settings, and monitor the status of the power supplies and fans.

The only way to configure the IP address of the EDAS board is via the 9-pin serial port on the back of the Hub Chassis, labeled “Config Port”, using a null-modem serial cable and the iDirect-supplied Windows GUI, “EDAS SYSCHECK”. (See the Technical Note titled *Upgrading to Release 3.1.x* for instructions on installing this utility.)

This chapter includes the following sections:

- [“Configuring the Chassis IP Address”](#)
- [“Configuring and Controlling the Hub Chassis from iBuilder”](#)

### 9.1 Configuring the Chassis IP Address

Use the following procedure to configure the Hub Chassis IP address.

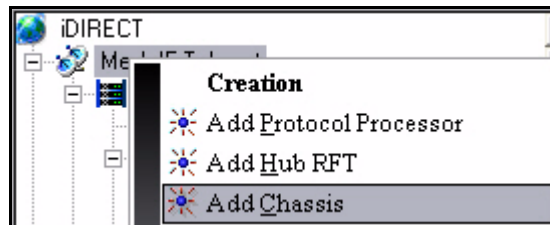
- Step 1 Ensure that you have a standard null modem serial cable.
- Step 2 Connect your PC to the Hub Chassis Config Port using the serial cable.
- Step 3 Run EDAS SYSCHECK on the PC.
- Step 4 Select the **Program** tab.
- Step 5 Select the correct COM port.
- Step 6 Click the **Attach to EDAS** button. After connection, the current IP settings of the EDAS board will be displayed.
- Step 7 Select the **Configuration** tab.
- Step 8 Set the appropriate IP address, subnet mask and default gateway values. The default gateway should be your upstream router.
- Step 9 Re-select the **Program** tab.
- Step 10 Write each IP address value to the board by pressing the appropriate buttons.
- Step 11 Reset the EDAS board by powering the Hub Chassis down and back up, or by resetting just the EDAS board. (For the latter option, you will have to remove the EDAS board cover and reset the power connector to the board itself.)

Note: The “Ethernet Address” field should never be modified.

## 9.2 Configuring and Controlling the Hub Chassis from iBuilder

The Hub Chassis includes the line cards, power supplies, and fans.


- Step 1 iBuilder's Chassis Configuration screen is an enhanced Windows list control, with one row for each slot and jumper. Rows are arranged from top to bottom to mirror the chassis slots from right to left. To create a Chassis in iBuilder, right-click the **Teleport**, select **Add Chassis**. The new chassis appears in the Tree with a system-generated generic name, and a dialog box appears allowing you to assign its line cards.



Step 2 Enter a name for the chassis.

**Modify Configuration Object - Chantilly [Modified]**

**Information**

 **Chassis**

Name:

IP Address:

RCM Installed

State	Jumpers	Slots	Hub Assignment
<input checked="" type="checkbox"/> On		Slot 1	Free
<input checked="" type="checkbox"/> On		Slot 2	Free
<input checked="" type="checkbox"/> On		Slot 3	Free
<input checked="" type="checkbox"/> On		Slot 4	Free
<input checked="" type="checkbox"/> On	Jumper 1		
<input checked="" type="checkbox"/> On		Slot 5	Free
<input type="checkbox"/> Off		Slot 6	Free
<input type="checkbox"/> Off		Slot 7	Free

Step 3 Enter the **IP Address**.

Step 4 To turn power on for a particular slot, or to set a jumper, click the check boxes beside the slots in which you have installed line cards. After each group four slot rows, you will see a jumper row. Do not select the jumper boxes unless your network spans virtual backplanes.

Step 5 To associate configured line cards with specific slots, click the slot row you want to assign, and right-click. A box opens enabling you to select either Assign Hub or Free.

<input checked="" type="checkbox"/> On		Slot 7	Free
<input type="checkbox"/> Off		Slot 8	Free
<input type="checkbox"/> Off	Jumper 2		
<input type="checkbox"/> Off		Slot 9	Free
<input type="checkbox"/> Off		Slot 10	Free
<input type="checkbox"/> Off		Slot 11	Free

**Assign Hub**  
Free

Step 6 Select **Assign Hub**.

You can also select **Free** to indicate that no modems are installed in that slot. The associations you make must reflect the actual physical layout of your chassis; iBuilder cannot map logical associations to physical line card locations.

**Step 7** When you select Assign Hub, a drop-down list appears in the row, listing of all the hub modems that can be assigned to that line card.

Slot 5	Free
Slot 6	Free
Slot 7	NMII+ TxRx [3162] (TxRx) NM Network
Slot 8	NMII+ Standby [3083] (Stdby) NM Network
	Phoenix HLC 442 (TxRx) Phoenix Network
	Transmit Chantilly Hub 1 (Tx) Chantilly Network
Slot 9	Receive Chantilly Hub 1 (Rx) Chantilly Network
Slot 10	Receive Chantilly Hub 2 (Rx) Chantilly Network
Slot 11	Free

**Step 8** Click the drop-down list to select the modem you want to link to that line card.

**Step 9** Click **OK**. When you save your changes, iBuilder displays the *Changes Pending* icon for the Chassis in the network Tree.

**Step 10** To make your changes active, you must right-click the **Chassis** and select **Apply Configuration**.

iBuilder uses the following rules when making line card assignments:

- If no line cards have been associated with slots, the drop-down choice list will contain all the hubs you currently have defined.
- After you make the first association, the following rules apply:
  - That line card no longer appears in any drop-down list.
  - Only line cards from the same network appear in drop-down lists for other slots in the same virtual backplane. If you have unassigned Solo line cards, they also appear.
  - Drop down lists for other virtual backplanes will not contain any line cards from the network already assigned.
- If you have two networks in adjacent virtual backplanes, iBuilder will not let you set the jumper between those two backplanes.
- To assign line cards from a single network across a jumper, you must first set that jumper.
- If you have a large network that spans a jumper, iBuilder will not let you clear the jumper.

Although the EDAS controller allows you to set jumpers and control slot power, it doesn't allow real-time queries for its current state. Additionally, all slots are powered on by default when the chassis is powered on. For this reason, the configuration database is the sole keeper of slot power and jumper settings. When the configuration server starts up, or after a reconnection to the EDAS, it automatically applies the settings stored in the database to the EDAS, thus restoring the desired Chassis state.





## 10 Controlling Remotes

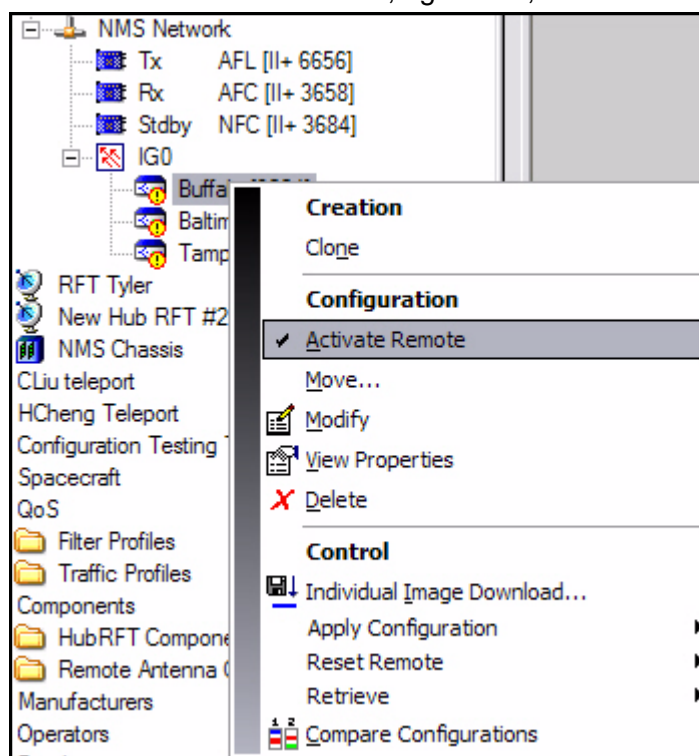
This chapter discusses the following topics:

- [“Activating and Deactivating Remotes”](#)
- [“Moving Remotes”](#)

### 10.1 Activating and Deactivating Remotes

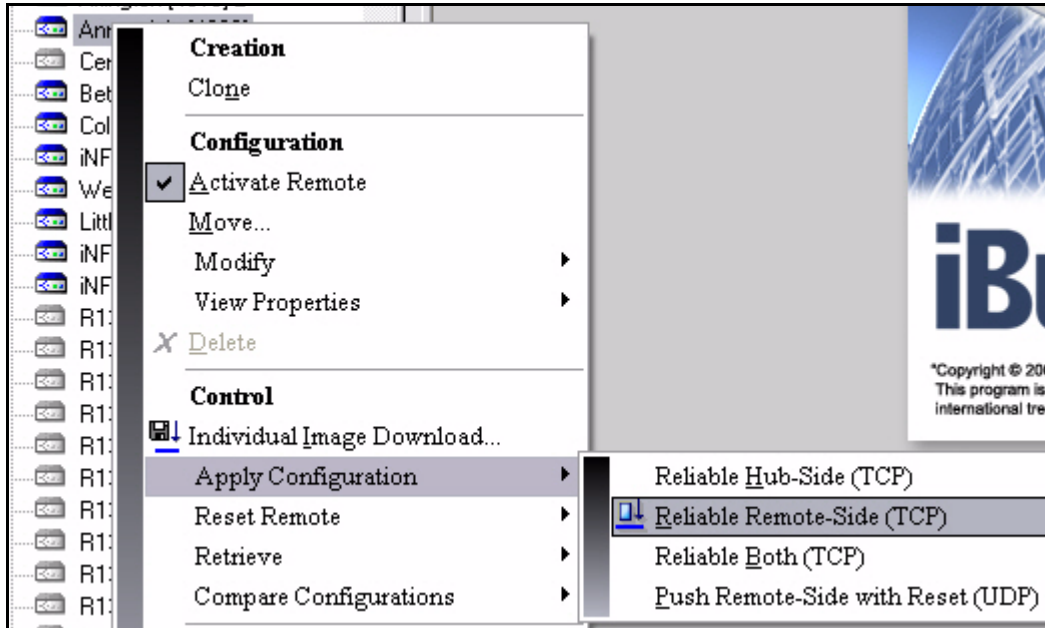
Remotes may be activated and deactivated by selecting the remote you want to activate, right-clicking on it, and selecting **Activate Remote**.

Step 1 Select a deactivated remote, right-click, and then select **Activate Remote**.

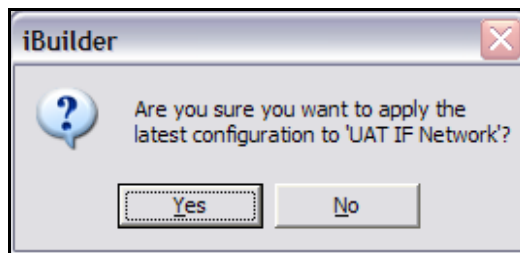


The term **Activation Pending** appears in red text to the right of the remote you are activating. The term **Changes Pending** appears in red text to the right of its corresponding network. For other states, see [Step 4, p. 178](#).

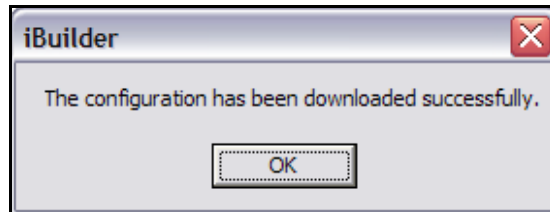
Step 2 Select the network in which the remote resides, right-click the network, and then select **Apply Configuration**.



Step 3 Click **Yes** to confirm the action.



Step 4 Click **OK** to acknowledge that the configuration has been downloaded successfully.



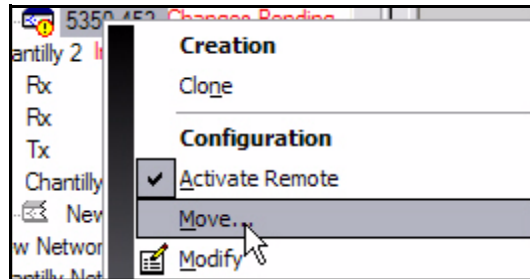
If the remote has been acquired into the network, the term **Nominal** appears in blue text to the right of both the remote and the network. If it has not been commissioned and acquired into the network for the first time, the term **Never Applied** appears to the right of the remote.

- Step 5 To deactivate an active remote, select an activated remote, right-click it, and select **Activate Remote**. The check mark will be removed and the remote will become inactive.

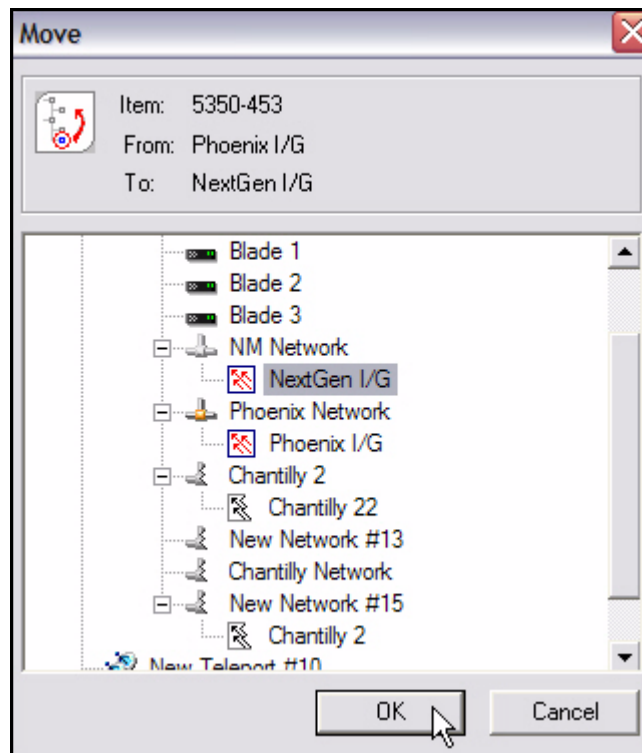
## 10.2 Moving Remotes

In iBuilder you can easily move remotes from one Inroute Group or Network to another.

- Step 1 Right-click the remote to be moved, and select **Move**.



- Step 2 In the **Move** dialog box, highlight the destination Inroute Group and click **OK**.



The remote now appears under the selected Inroute Group in the **Tree**.



## 11 Retrieving and Applying Saved and Active Configurations

Once you have configured your network elements, you might add more elements which will need to be configured, or you might simply modify the configuration of one or more elements in your network. This chapter includes:

- [“Configuration Options Files” on page 181](#)
- [“Hub-side and Remote-side Options Files” on page 181](#)
- [“Modifying, Deleting, and Viewing Configurations” on page 182](#)
- [“Retrieving Configurations” on page 183](#)
- [“Comparing Configuration Changes” on page 188](#)
- [“Applying Configuration Changes” on page 190](#)
- [“Configuration Changes on Roaming Remotes” on page 198](#)

### 11.1 Configuration Options Files

You can retrieve current configurations and save them on your PC as “Options” files. You can also download (or **apply**) the Options files to other elements of the same type or to elements that will be affected by a modified element’s new configuration. In addition, you can compare an element’s “Saved” configuration its “Active” configuration.

Network elements such as remotes and Protocol Processors have both Active and Saved configurations. The Saved configuration is the configuration that is stored in the NMS database. The Active configuration is resident on the network element itself. When you modify the configuration of an element, the Saved configuration is updated. When you **Apply** the changes, the Saved configuration is sent to the element and loaded as the Active configuration.

The iDirect NMS system knows which elements are dependent upon one another, so that if you download an Options file to one element that affects the configuration of other elements in the network, the system will automatically update those elements as well.

You can retrieve the configurations of the following elements:

- Protocol Processors (Active and Saved configurations)
- Chassis (Saved configuration only)
- Networks (Active and Saved configurations)
- Line Cards (Saved configuration only)
- Remotes (Active and Saved configurations)

### 11.2 Hub-side and Remote-side Options Files

Each remote has two separate Options files, each with Saved and Active versions. One remote Options file, called the “remote-side” Options file, is sent to the remote. The other remote Options file, called the “hub-side” Options file, is sent to the Protocol Processor to configure the remote on

the PP. When you modify a remote using iBuilder, the changes may affect the remote-side Options file, the hub-side Options file, or both.

You can perform the following control operations on both types of remote Options files from the remote level of the Network Tree:

- Apply configuration changes
- Retrieve the active and saved configurations
- Compare the active configuration to the saved configuration

Separate versions of the “Changes Pending” icon indicate which of the remote Options files has been affected by a change. There are three icon variations: remote-side only, hub-side only, and both. The hub-side icon is referred to as “PP-Side” in the figure below.



The following sections describe how to modify, retrieve, compare, and apply configurations on remotes as well as on other network elements.

### 11.3 Modifying, Deleting, and Viewing Configurations

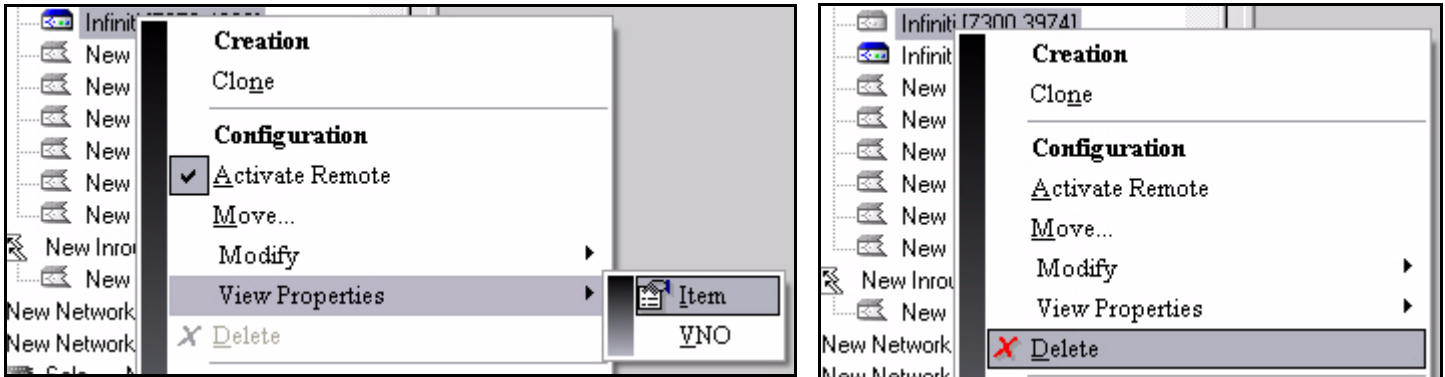
You can modify your network configuration by right-clicking on the element in the Tree that you want to modify and selecting **Modify** from the menu. In cases where you can also modify the VNO properties for an element, select **Modify → Item** to modify the element’s configuration; select **Modify → VNO** to modify the VNO properties. Similarly, you can delete or view the configuration of an element by selecting either **Delete**, **View Properties**, **View Properties → Item**, or **View Properties → VNO**.



#### NOTE

You must deactivate a remote before you can delete it. When a remote is activated, a check mark is shown next to the **Activate Remote** selection in the network tree for the remote. To deactivate a remote, right click the remote in the Network Tree and select **Activate Remote** to remove the check mark.

The Network Tree menu selections for viewing and deleting a remote are shown below. Notice that you cannot select **Delete** until a remote is deactivated.



## 11.4 Retrieving Configurations

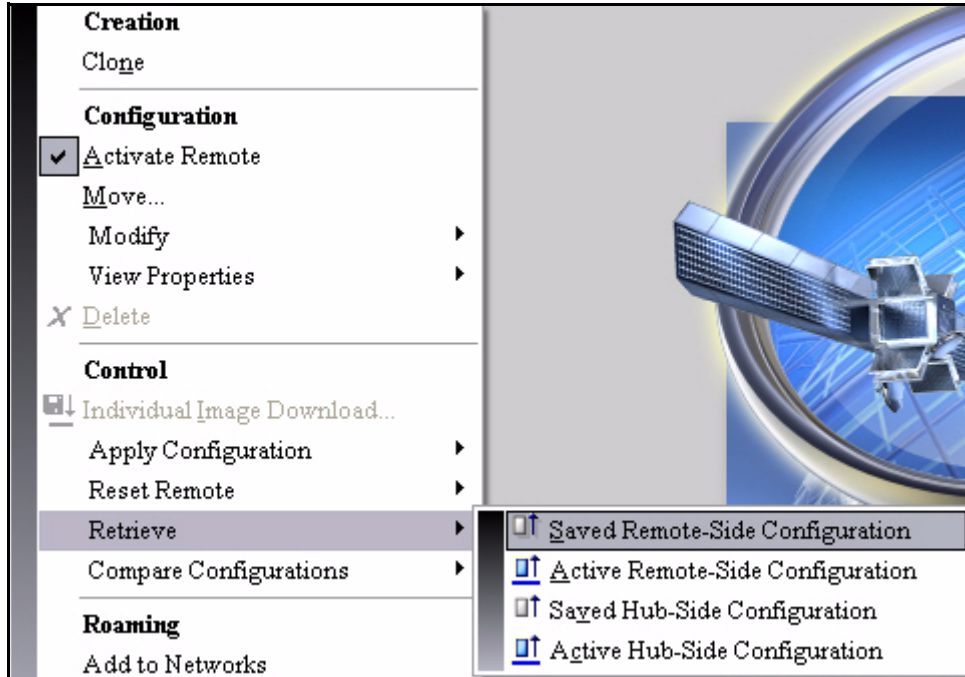
When you make modifications to any element, iBuilder saves the modified configuration at the NMS in the Saved Options file. To retrieve this latest version of the Options file and apply it to one or more elements, you must use the “Retrieve Saved Configuration” function.

An Active Configuration is the configuration that is currently running on the element. By retrieving it, you are creating an Options file with that current configuration and saving it on your PC as an “.opt” file. You can then download, or *apply*, this Options file to one or more elements of the same type. For example, if you retrieve and save the current configuration of a particular remote, you can then apply that configuration to one or more other remotes.

### 11.4.1 Retrieving a Single Saved or Active Configuration

To retrieve a saved configuration, follow the procedure below:

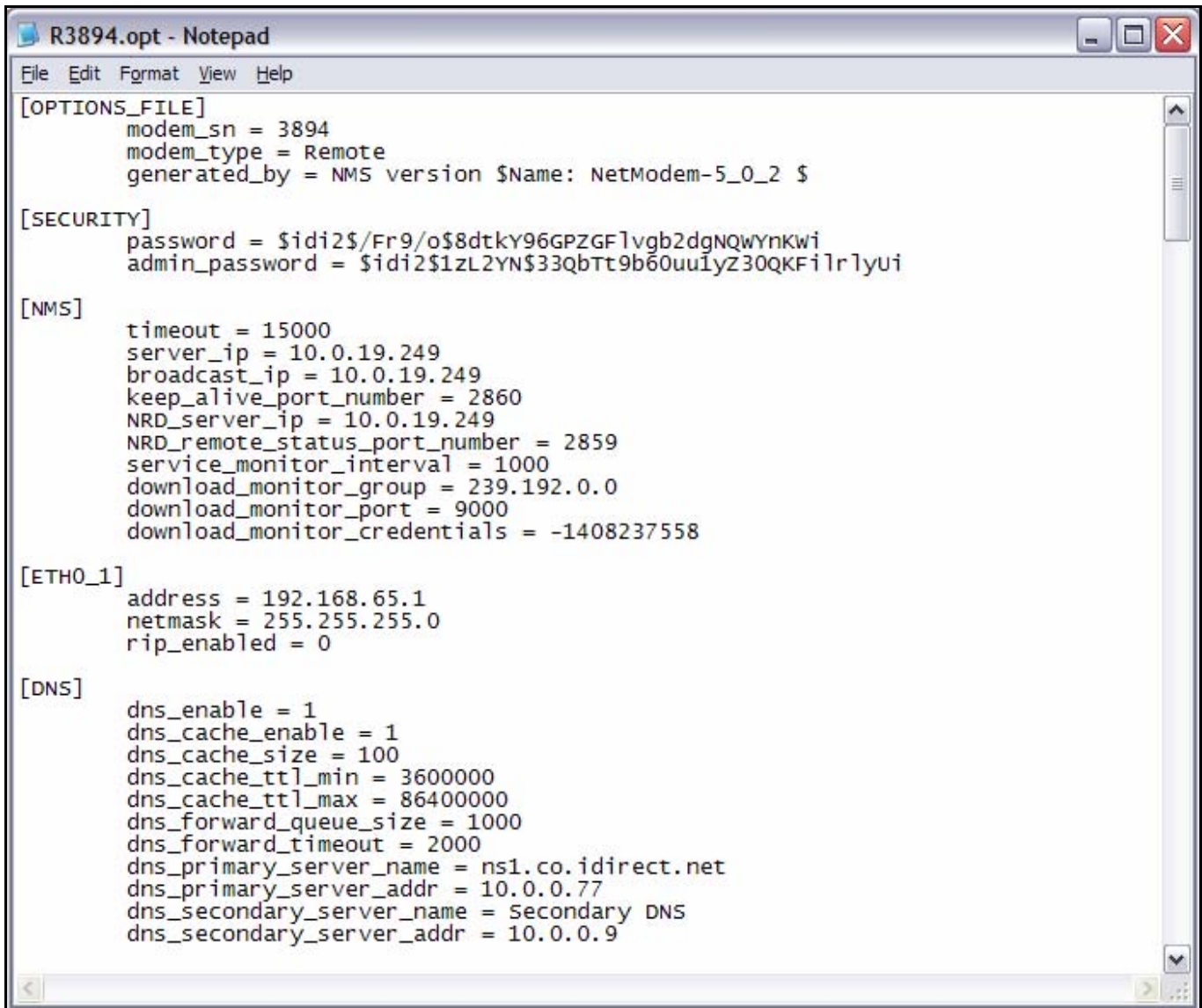
- Step 1 Right-click the element whose configuration you want to retrieve, select **Retrieve**, and then select **Active Configuration** or **Saved Configuration**. In the case of remotes, the menu allows you to select either the hub-side or the remote-side configuration for retrieval. The example below shows Saved Configurations being selected. However, the procedure for both are the same.



Step 2    Navigate to the saved configuration file on your PC and click **OK**. Placing it in your My Documents folder will make it easier to find later.



- Step 3 The options file opens in Notepad allowing you to review your configuration parameters before you apply them.



```
R3894.opt - Notepad
File Edit Format View Help
[OPTIONS_FILE]
modem_sn = 3894
modem_type = Remote
generated_by = NMS version $Name: NetModem-5_0_2 $

[SECURITY]
password = $idi2$/Fr9/o$8dtkY96GPZGF1vgb2dgNQWYNKwi
admin_password = $idi2$1zL2YN$33QbTt9b60uuIyZ30QKFiRlyui

[NMS]
timeout = 15000
server_ip = 10.0.19.249
broadcast_ip = 10.0.19.249
keep_alive_port_number = 2860
NRD_server_ip = 10.0.19.249
NRD_remote_status_port_number = 2859
service_monitor_interval = 1000
download_monitor_group = 239.192.0.0
download_monitor_port = 9000
download_monitor_credentials = -1408237558

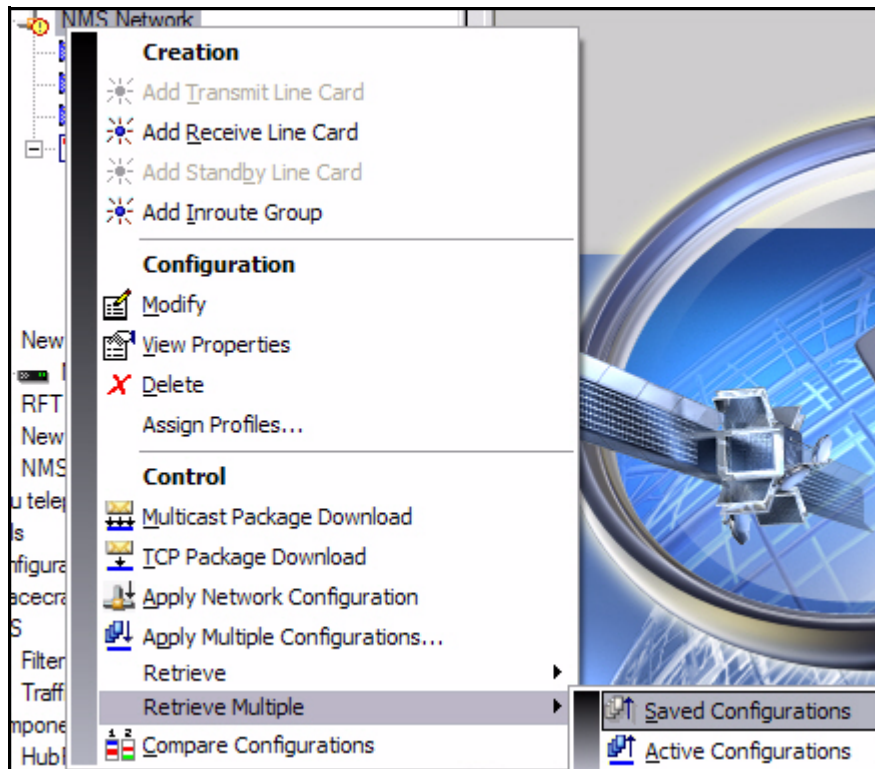
[ETH0_1]
address = 192.168.65.1
netmask = 255.255.255.0
rip_enabled = 0

[DNS]
dns_enable = 1
dns_cache_enable = 1
dns_cache_size = 100
dns_cache_ttl_min = 3600000
dns_cache_ttl_max = 86400000
dns_forward_queue_size = 1000
dns_forward_timeout = 2000
dns_primary_server_name = ns1.co.idirect.net
dns_primary_server_addr = 10.0.0.77
dns_secondary_server_name = Secondary DNS
dns_secondary_server_addr = 10.0.0.9
```

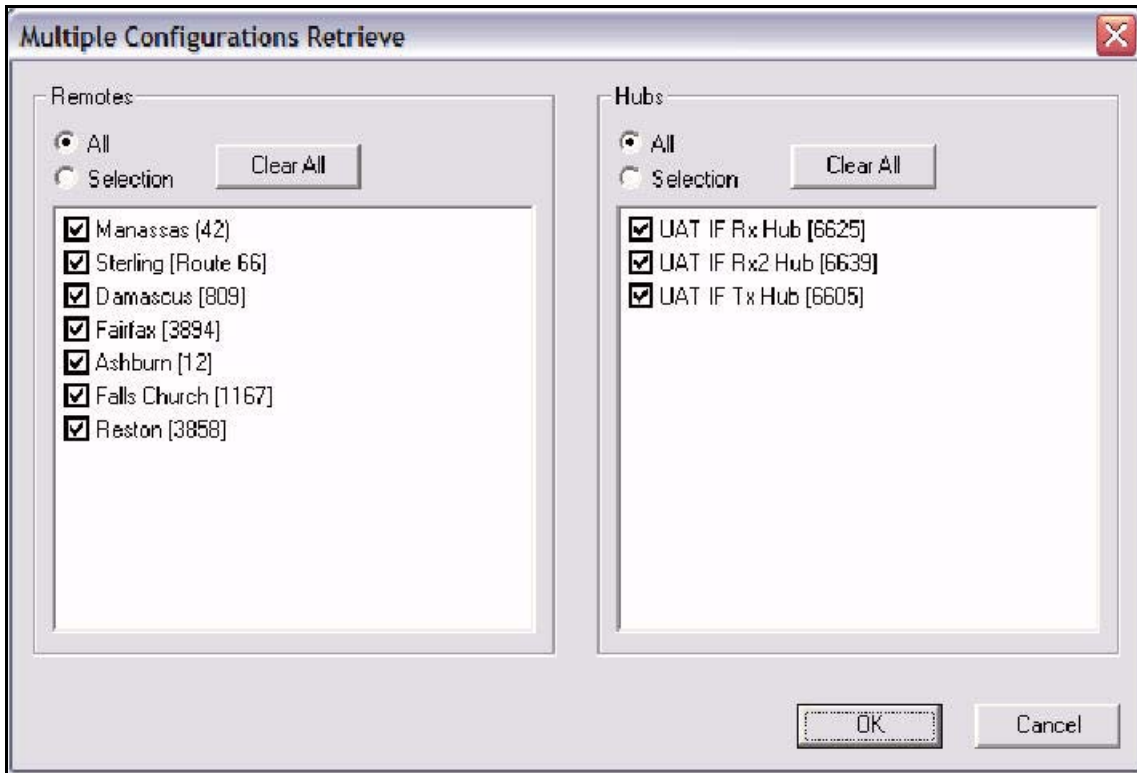
## 11.4.2 Retrieving Multiple Saved or Active Configurations

You can simultaneously retrieve multiple saved or active configurations for remotes or hubs as follows:

- Step 1 Right-click the **Network** element and select **Retrieve Multiple**. Then select either **Active Configurations** or **Saved Configurations**. (The example below shows **Saved Configurations** being selected. The procedure for retrieving multiple **Active Configurations** is identical.)

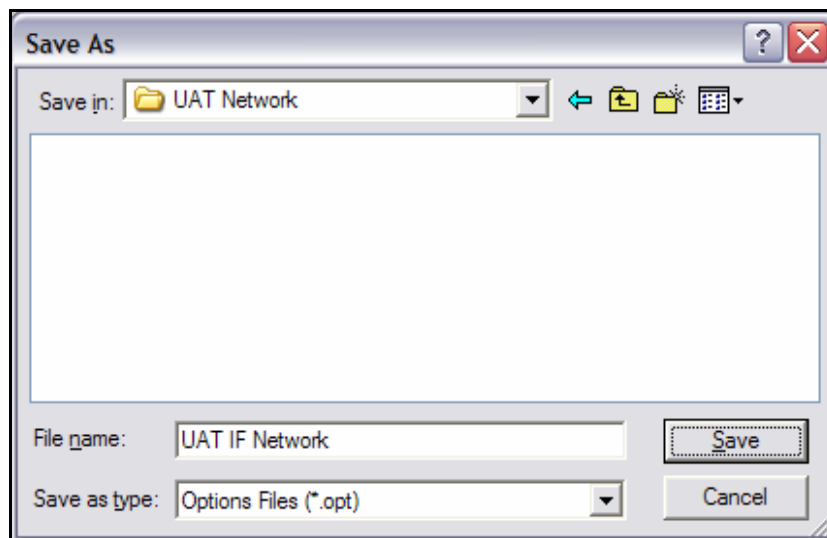


Step 2 In the **Multiple Configuration Retrieve** dialog box, select the remotes and/or the hubs for which you want to retrieve the configurations.



Step 3 In the **Save As** dialog box, navigate to the location on your PC where you want to save the configuration files.

Step 4 Click **Save**.



Step 5 iBuilder retrieves the selected configurations and copies them to the designated location. Both the remote-side and hub-side options files will be retrieved and saved for any selected remotes.



You will be able to access the files in the location to which you saved them.



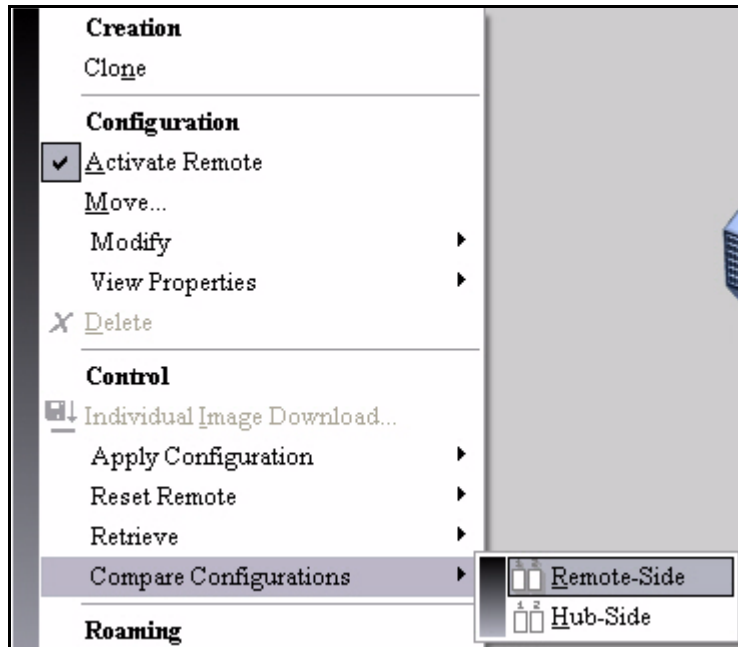
## 11.5 Comparing Configuration Changes

When you perform a **Retrieve** command, iBuilder automatically opens the Options file so you can view the configuration. In addition, if you have made changes to an element, you can compare the “Latest” configuration in iBuilder with the “Active” configuration currently applied to that element. Once you are satisfied with the results, apply the configuration using one of the methods in [“Applying Configuration Changes” on page 190](#).

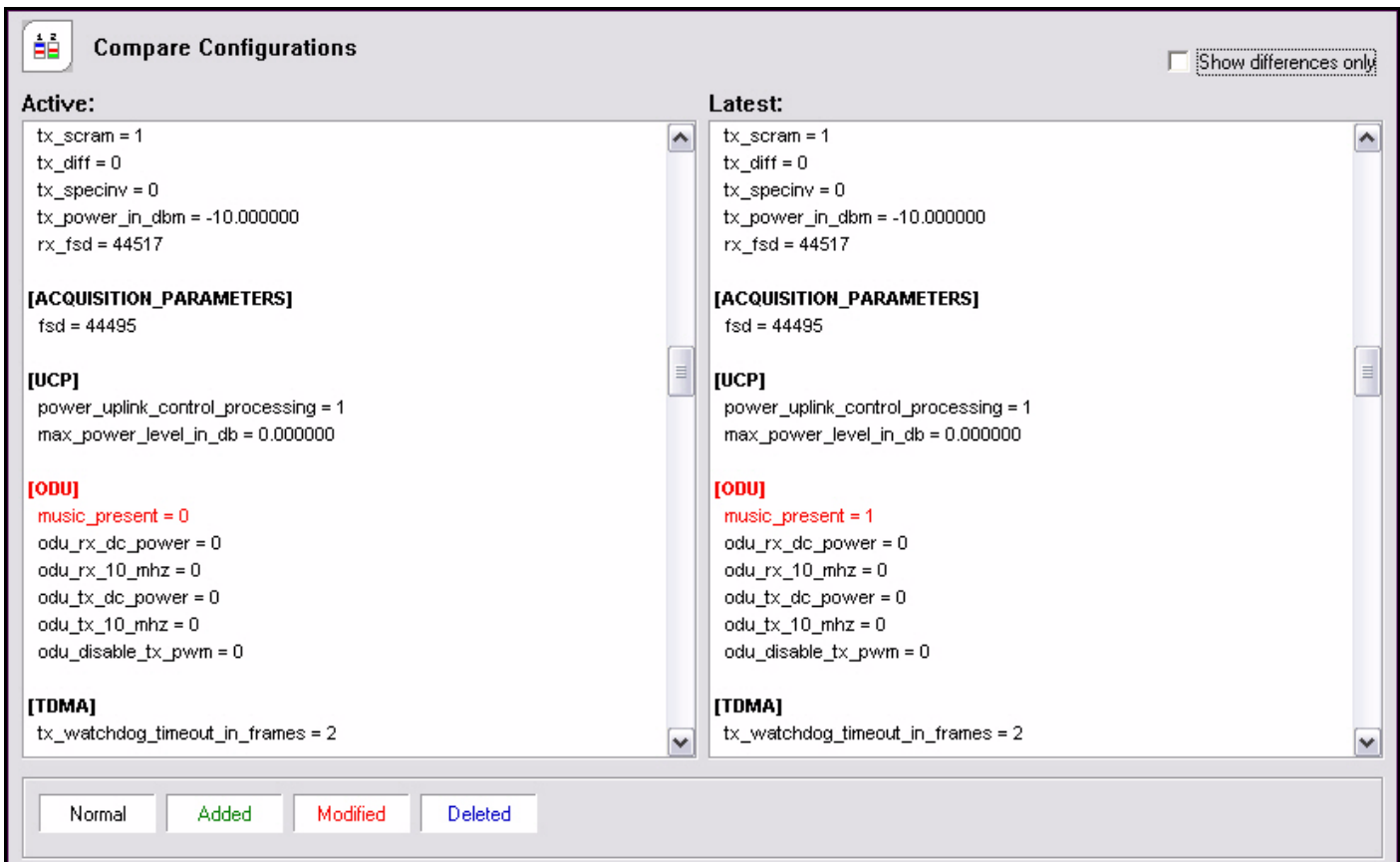
You can compare configurations for Protocol Processors, Chassis, Networks, Line Cards, and Remotes using the following method. This example compares the active configuration that was last applied to a remote with the remote’s latest configuration as stored in the NMS database. Notice that the operator has configured a MUSiC Box for this remote, but has not yet applied the changes.

To compare the active configuration of an element with its latest configuration, follow this procedure:

Step 1 Right-click the element in the Tree and select **Compare Configurations**. In the case of a remote, select **Remote-Side** or **Hub-Side**.



Step 2 To view all configuration parameters in the dialog box, clear the **Show differences only** check box. Note that differences are shown in red.



Step 3 To view only the parameters that are different, select the **Show differences only** check box.



## 11.6 Applying Configuration Changes

You can apply the latest configuration changes to multiple elements at the same time, which greatly improves the management of your networks, especially as they grow. Whether you want to download configurations to one or multiple Networks, Line Cards, or Remotes, you can do so via the **Automated Configuration Downloader** dialog box, accessed from the Network element in the Tree. You can also use the **TCP Download** feature to download Options files to multiple remotes and line cards. The TCP Download feature allows you to download Image files also. For information about this feature, see [chapter 12, “Upgrading Software and Firmware.”](#)

### **Maintenance Window Consideration**

Be aware, however, that downloading configurations or images to multiple elements can take a long time to complete and uses a lot of bandwidth. Therefore, you probably should establish a maintenance window in which to make a large number of multiple changes.

### **Sequence of Download**

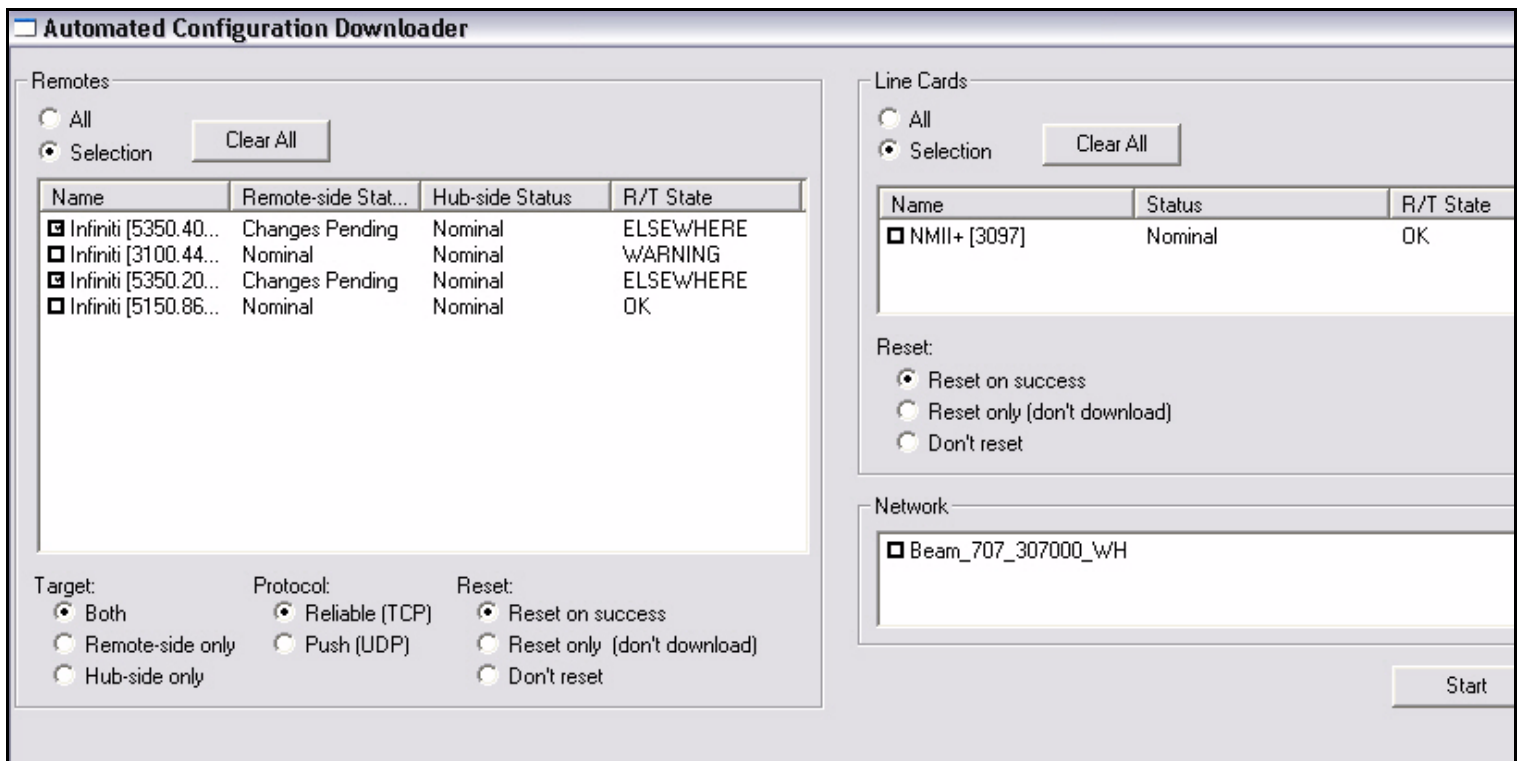
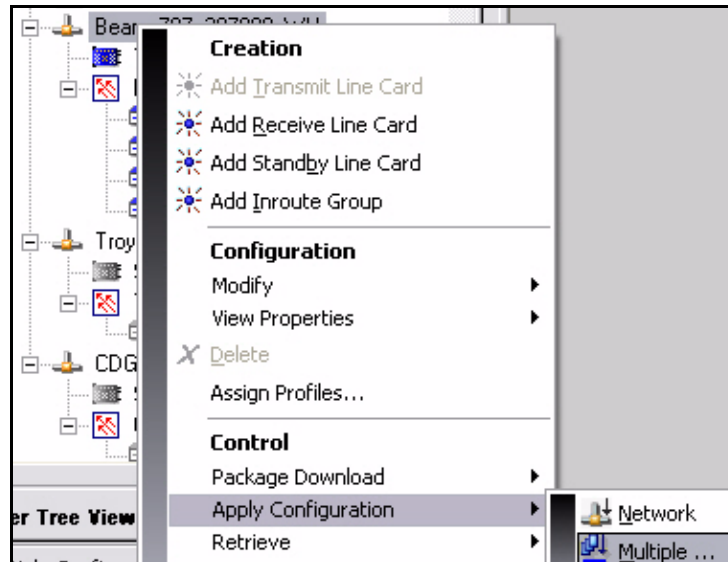
When applying configurations to multiple elements, iBuilder treats each group of elements as a batch, processing the batches in upstream order. Therefore, remotes are downloaded first, followed by hub lines cards, and finally the network itself.

All elements of a batch must complete its download successfully before iBuilder will proceed to the next batch. For example, if any remote in a given batch fails during the download process, iBuilder will stop at the end of the remote batch and wait for your next command. It will not download to any line cards or to the network. However, all elements within a single batch are processed simultaneously, so a single remote failure will not stop the other remotes from being downloaded. Also, if the reset button is selected on the dialog box, iBuilder immediately sends a reset command to any remote that downloads successfully. If this behavior is not desired, make sure you check the **Don't reset** button (you can always select “**Reset only**” at a later time).

## 11.6.1 Applying Multiple Configurations to Network Elements

To download configurations to one or several of these elements, follow the procedure below:

- Step 1 Right-click Network and select **Apply Configuration → Multiple**. This launches the Automated Configuration Downloader.





The Automated Configuration Downloader is divided into three main sections:

- Remotes
- Line Cards
- Network

Beside each entry is a check box that you can select to include that item in the download. When you first launch the Automated Configuration Downloader, all Remotes that currently have changes pending are automatically preselected. If a box is not checked, the configuration will not be downloaded to the corresponding element.

### **Remote Protocol and Reset Options**

In the Remote pane are two additional options. The Protocol option lets you choose between reliable (TCP) and push (UDP) delivery methods. If all the modems in your list are currently acquired into the network, iDirect recommends using the reliable delivery method.

### **Reset Options**

The Reset option allows you to choose a reset action after the download completes. The three choices are: Reset on success, Reset only, or Don't reset.

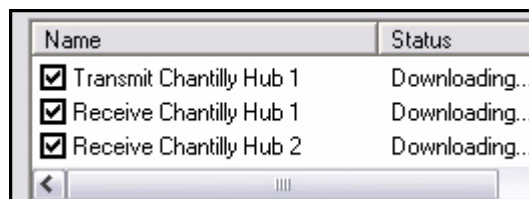
- Reset on success will automatically reset the modems after a successful download.
- Choosing "Reset only", simply resets the modems without a download being performed. This option is useful if you previously selected "Don't reset", but now you want to reset the downloaded modems.
- Don't Reset simply does not reset the modem.

### **Stopping the Download**

The stop command attempts to halt processing at the next appropriate step after its current operation. iBuilder will not stop download operations that are currently in progress, but when the current operation is finished, iBuilder will not continue to the next chosen step.

For example, assume you have selected a given remote and clicked the **Reset on Success** button. If you click **Stop** in the middle of the download, the reset command will not be sent. However, the current download will finish; iBuilder makes no attempt to halt a download in the middle or to back out a downloaded configuration.

Click **Start**. The Status column shows that the configuration is downloading.



Name	Status
<input checked="" type="checkbox"/> Transmit Chantilly Hub 1	Downloading...
<input checked="" type="checkbox"/> Receive Chantilly Hub 1	Downloading...
<input checked="" type="checkbox"/> Receive Chantilly Hub 2	Downloading...



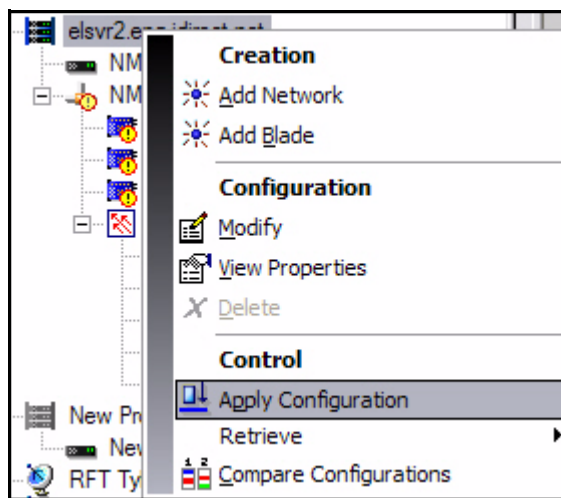
## 11.6.2 Applying Configurations to Individual Elements

You can apply configurations to individual Protocol Processors, Chassis, Networks, Remotes, and Line Cards.

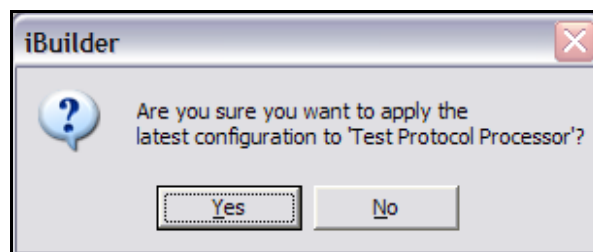
### Applying a Configuration to a Protocol Processor or Chassis

To apply configuration changes to a Protocol Processor or a Chassis, follow the procedure below. The examples show the configuration being applied to the protocol processor, but the procedure is the same for both.

- Step 1 Right-click the **Protocol Processor** or **Chassis** and select **Apply Configuration**.

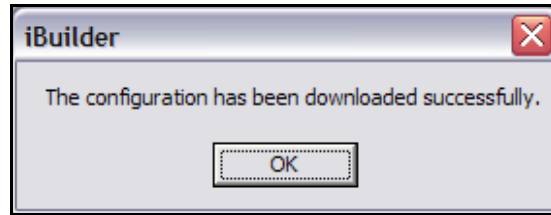


- Step 2 A message appears asking you to confirm the download. Click **Yes**.



A confirmation message appears when the configuration has been downloaded successfully.

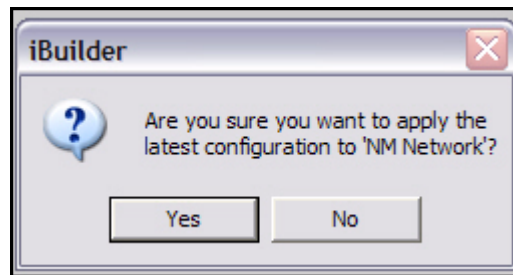
- Step 3 Click **OK**.



### **Applying a Configuration to the Network**

To apply the configuration at the Network level, follow the procedures below:

- Step 1 Right-click the **Network** and select **Apply Configuration**.
- Step 2 A message appears asking you to confirm the download. Click **Yes**.



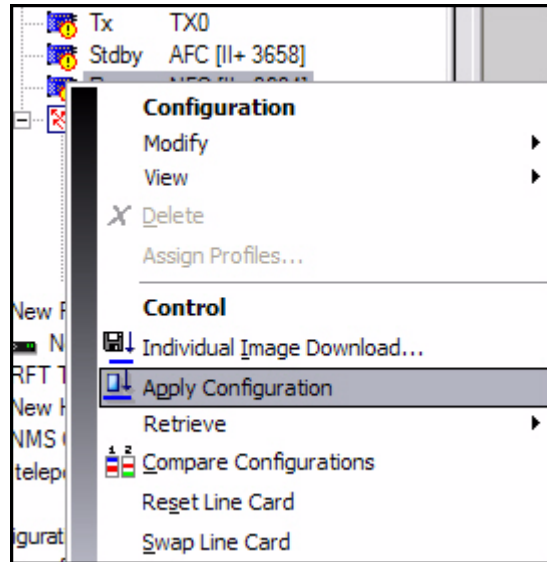
A message appears, requesting that you wait while the configuration is applied.



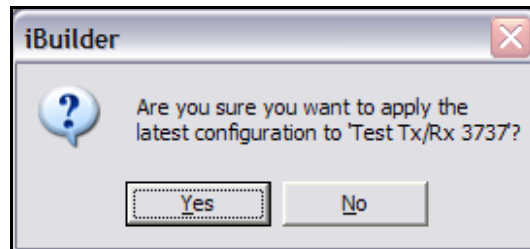
After the configuration is applied to the Network, the status of the network changes from *Changes Pending* to *Nominal*.

### **Applying a Configuration to the Line Card**

- Step 1 Right-click the any type of Line Card (Tx, Rx, Tx/Rx, Standby) and select **Apply Configuration**.



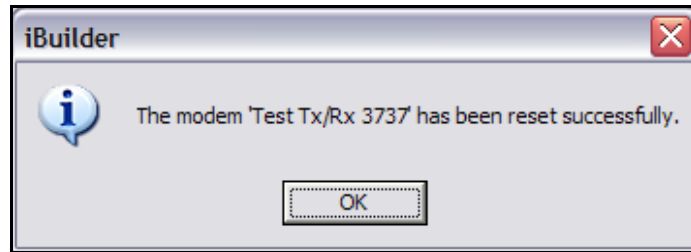
Step 2 A message appears, prompting you to confirm the download. Click **Yes**.



Step 3 When the download is complete and successful, a message appears, allowing you the option of resetting the unit now or waiting and resetting it later.



Step 4 Click **Reset Now** or **Reset Later**, depending upon your needs. If you reset the remote now, a message appears, confirming that the unit was reset successfully.

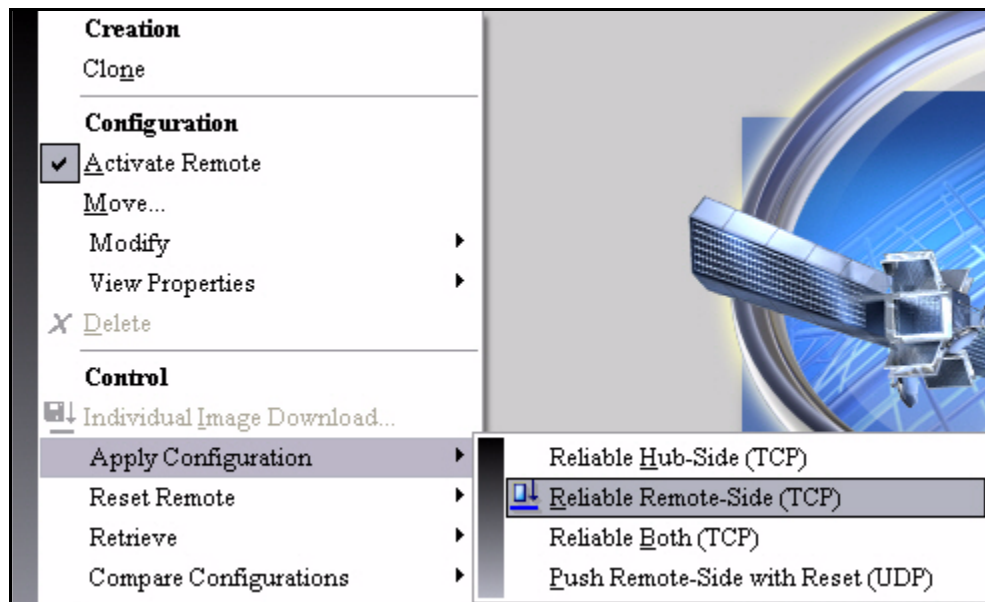


Step 5 Click **OK**.

### **Applying a TCP or UDP Configuration to a Remote**

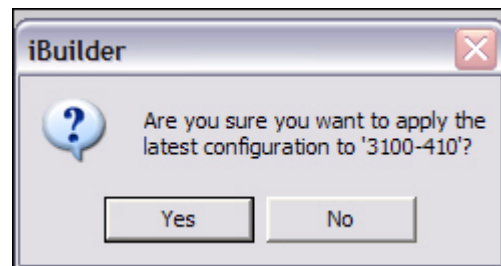
When applying remote configurations, you may choose remote-side, hub-side, or both sides. When you select both sides, iBuilder enforces the correct apply order: remote, then hub.

- Step 1 Right-click the remote whose configuration you want to be changed.
- Step 2 Select **Apply Configuration**, and then select **Reliable Hub-Side (TCP)**, **Reliable Remote-Side (TCP)**, **Reliable (Both)**, or **Push Remote-Side with Reset (UDP)**. It is recommended that you use TCP if possible.

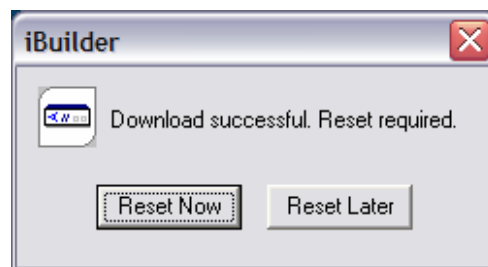


Step 3 A message appears asking you to confirm the download.

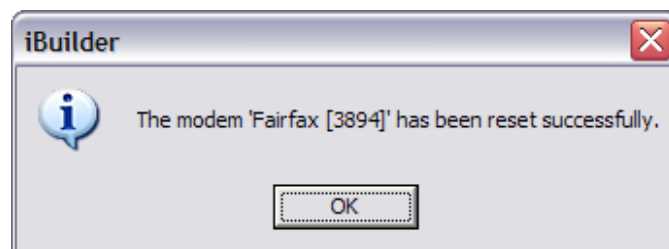
Step 4 Click **Yes**.



- Step 5 When the download is complete and successful, a dialog box appears, giving you the option of resetting the remote now or waiting and resetting it later.



- Step 6 Click **Reset Now** or **Reset Later**, depending upon your needs. If you reset the remote now, a message appears, confirming that the remote was reset successfully.



- Step 7 Click **OK**. The remote's status will return to nominal.

## 11.7 Configuration Changes on Roaming Remotes

The NMS maintains two options files for each non-roaming remote. One file resides on the Protocol Processor and the other resides on the remote itself. Together, these two files represent the configuration for a remote terminal in a single network. Roaming remotes require a different set of option files. This section describes the options files associated with roaming remotes and the implications of applying configuration changes to remotes that are configured in multiple networks.

### 11.7.1 Roaming Options File Generation

The figure below illustrates the options files generated by the NMS for both non-roaming and roaming remotes. Roaming remote options files are built as an extension to the normal two file structure.

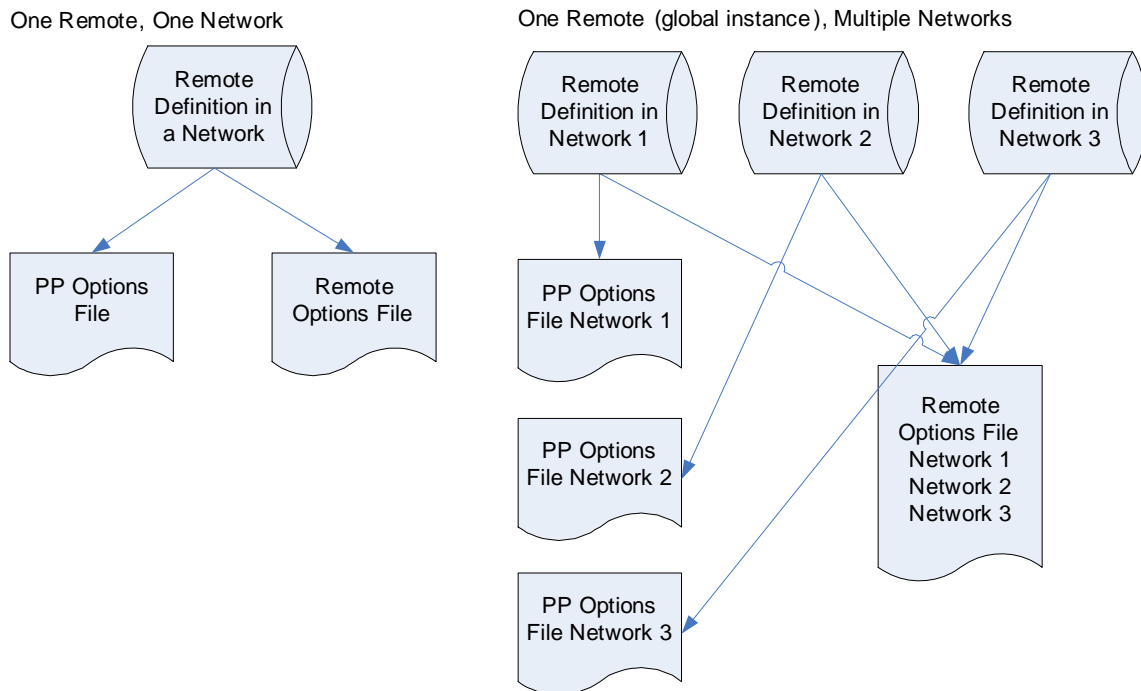


Figure 11-1: Global NMS Options Files

As with non-roaming remotes, the NMS sends a single options file to each roaming remote. However, the NMS puts all the necessary parameters for each of the member networks into a single remote options file.

The structure of the options file sent to the protocol processor has not changed. However, the NMS generates a separate PP options file for each network a roaming remote belongs to.

## 11.7.2 Pending Changes across Networks

With a single remote options file now containing elements from multiple networks, a roaming remote's configuration can now change for one, many, or all networks the remote is a member of. This leads to some differences when the NMS compares it's own configuration files to those resident on the Protocol Processor or the remote.

For changes to a single network affecting only the Protocol Processor options files for a roaming remote:

- Only that specific network instance will show the Changes Pending icon
- Only comparisons performed on that network instance will show the differences

For changes that affect multiple networks, or changes to any remote consolidated options file:

- Each network instance will show the Changes Pending icon
- Comparison operations from any of these networks will show the differences.

## 11.7.3 Applying Changes to Roaming Remotes

When you modify a roaming remote in one network, you can apply the changes to the remote regardless of which network it's in. You do not need to wait until the remote is acquired into the network with the pending changes.

As long as the NMS can route packets to the remote terminal, it will update the remote when you apply the changes. However, the remote must be acquired into some network.

For example, if a remote is a member of Networks 1, 2 and 3, and is currently in Network 1, you can make changes that affect Network 2 and apply them immediately.





## 12 Upgrading Software and Firmware

An image package is a single file that contains all the firmware images for a particular release and hardware platform. The packages contain FPGA (Field Programmable Gated Array) Images. You can download images to remotes or line cards via the Multicast Download feature, Download Image feature, or TCP Multicast feature. The TCP Multicast feature allows you to download both Option and Image files to remotes and line cards.

To upgrade from one version to another, you should schedule a maintenance window with your customers. The time required for an upgrade varies based on how many remotes you have deployed, but averages around 1 hour. The upgrade process is covered completely in the technical note, *Installing NetModem Software*. That document is specific to each release.

This chapter includes:

- [“Image Package Versions” on page 201](#)
- [“Downloading an Image to Remotes and Line Cards Concurrently” on page 201](#)
- [“Resetting Remotes” on page 206](#)
- [“Downloading an Image or Configuration File via TCP” on page 207](#)
- [“Downloading Remotes Using Revision Server” on page 207](#)

### 12.1 Image Package Versions

The iDS NMS GUIs, NMS Servers, Protocol Processor, embedded software and firmware are all released with the same version number. The NMS GUIs and NMS servers must match in version number or you will not be allowed to log in. A mixed installation (one where not all components have the same version) is not guaranteed to function properly.

The following packages are installed on the NMS server during the upgrade to release 6.0:

CpApp-remote\_NM2-5\_0\_3

- CpApp-hub\_2plus-5\_0\_3 – contains firmware images and control application for NetModem 2Plus line cards.
- CpApp-remote\_NM2-5\_0\_3 – contains firmware images and control application for NetModem 2 remote modems.
- CpApp-remote\_2plus-5\_0\_3 – contains firmware images and control application for NetModem 2plus remote modems.

The version number portion of these package names changes from release to release.

### 12.2 Downloading an Image to Remotes and Line Cards Concurrently

The Multicast Download feature allows you to download images to multiple remotes or multiple line cards in any given network. However, images can only be downloaded to a single network at a time. The Multicast Download feature uses UDP, which is explained below.

**NOTE**

Your upstream router must have multicast enabled before you can multicast images to your line cards.

## 12.2.1 Multicast via UDP

The Multicast Download operation is driven by the NMS Configuration Server, which spawns a stand-alone command that resides on the NMS server machine. The protocol for packet transmission exists entirely between the modems and the standalone command; the Protocol Processor isn't involved in any way, except to transmit multicast packets on the downstream (and ACKs/NACKs on the upstream).

A multicast download operation consists of two phases: the data transmission phase and the flash phase. During the data transmission phase, the package is broken into multicast IP packets, each of which is given a sequence number. All recipients reassemble the individual packets, in order, into the original image package. If a recipient misses a packet, it will send a NACK back to the sender, at which point the sender re-winds to the missed packet and begins re-sending. A remote will only NACK once; if it doesn't receive the missing packet it gives up and sends a final NACK when it receives the last packet.

When reassembly is complete, the flash phase begins. Each individual component of the package is extracted and written to the modem's flash memory. After flashing is complete, the modem resets automatically if the reset option was checked in iBuilder.

We refer to the protocol used for transmission as "semi-reliable". It is reliable in that recipients will NACK missing packets, but only semi-reliable in that packets are not re-sent forever. Also, the recipients only NACK missing packets; a single ACK is sent when all packets have been received, but no ACKs are sent during packet transmission.

## 12.2.2 Download Procedure

Right-click the Network and select **Multicast Download**. The **Multicast Download** dialog box is displayed. On this dialog box, you can select an image to download to multiple remotes or multiple line cards, but the images for remotes and line cards are different files, and the two files cannot be downloaded to the remotes and line cards at the same time. You must download the image to all of the remotes and then perform the procedure again to download the appropriate image to all of the line cards. You can deselect any remote or line card that you do not want to receive the new image.

### Package Section

The upper-left section of the dialog box contains a drop-down list of all available image packages (see "[Image Package Versions](#)" on page 201). When you select a particular package, the contents of the package are displayed in the **Contents** box below the drop-down list. Confirm that the control application version is correct; it is in the last row of the list.

**Multicast Download**

Package

Selected Package:

Contents:

File Na...	Checks...	Decod...	Encode...	Load A...	Jump A...
FpgaTxS...	32976	166980	100901	0x0	0x0
FpgaRx2...	65294	166980	102670	0x0	0x0
FpgaRx1...	46356	166980	107495	0x0	0x0
FpgaDqt...	12926	166980	113171	0x0	0x0
LutRxTd...	28767	65536	57002	0x0	0x0
CpApp_...	56213	1602784	714689	0x1000...	0x1000...

Download Parameters:

Download Rate:  Kb/second

Reset

Credentials:

Group Address:

Progress:

Modems

Remotes:

Name	Status

Hubs:

Name	Status
<input checked="" type="checkbox"/> TX0	Changes Pending
<input checked="" type="checkbox"/> AFC [II+ 3658]	Changes Pending
<input checked="" type="checkbox"/> NFC [II+ 3684]	Changes Pending

### **Modems and Hubs Sections**

iBuilder does not allow you to download an image package to an element that is not compatible. When you select an image package for a given element (for example, a 5100 remote, a 5150 remote, or a line card), only the elements that are compatible with that package are displayed in the list of remotes or hubs in their respective boxes on the right side of the dialog box. For example, if you select the package for 5100 remotes, only 5100 remotes are displayed in the Remotes box. Likewise, if you select the package for Receive line cards, only Receive line cards are displayed in the Hubs box. This is a safety feature that prevents you from sending a mismatched image package to the remotes and hubs. If you do not want to download the image package to a given remote or line card, clear the checkbox next to it.

### **Download Parameters Section**

The lower-left corner of the dialog box contains run-time parameters that change the behavior of the multicast. iBuilder automatically chooses an appropriate Download Rate for your network; setting this rate higher is not recommended as it may cause the download to fail.

The **Credentials** and **Group Address** fields are primarily for reference purposes, and should be left unchanged. The **Reset** check box, if selected, tells each remote to reset after the package has been processed.

When you have made your selections, click **Start** to begin the download. The **Progress** bar at the bottom of the dialog box will indicate the status of your download. The results of the download to each remote (or line card) recipient are displayed next to that recipient's name in the appropriate pane. Depending on the status of the download, you will see either "Download Complete" or "Download Incomplete". If you receive the latter message, this doesn't necessarily mean the download failed; it simply means the sending application didn't receive an ACK (acknowledgement) from that recipient. This behavior is explained in the next sections.

## **12.2.3 Downloading an Image to Out of Network Remotes**

You can download an image to remotes that are out of network. As long as the remote is locked on the downstream carrier, it will receive the packets, reassemble the package, and flash its contents. Make sure you set the reset flag if you multicast images to out-of-network remotes.

Since the remotes are out-of-network and unable to send the final acknowledgement, the iBuilder dialog box will display the "Download Incomplete" message after sending all packets.

If the remote is encrypted and out-of-network, you cannot perform a multicast download to it. This is because the required key exchange can't take place. The workaround in this situation is to temporarily turn encryption off, send the package, and turn it back on after the image has been downloaded. For more information, see the iDirect Technical Note entitled *Managing Encrypted Remotes*.

## 12.2.4 Interactions with Other iBuilder Operations

The sequence of events during a multicast download is as follows:

1. The image package is broken into separate IP multicast packets.
2. Each packet is sent in order to the recipients.
3. When all packets have been received, each recipient sends an acknowledgement to the sender
4. The contents of the package are extracted and written to flash memory (a defragment operation is performed automatically if necessary).
5. If the reset option was checked in iBuilder, each recipient resets.

After step 3, iBuilder and the NMS are “out of the loop”. iBuilder declares the download complete, and the user is free to move on to other tasks; however, the recipients are not finished – they will take up to a minute to flash the package contents. For this reason, it is wise to view recipient multicast activity in iMonitor, and wait until step 5 is complete before continuing with other tasks in iBuilder. Recipients send events into the NMS indicating the progress of the multicast operation, and these events can be viewed in an **iMonitor** events pane if the recipients are in-network.

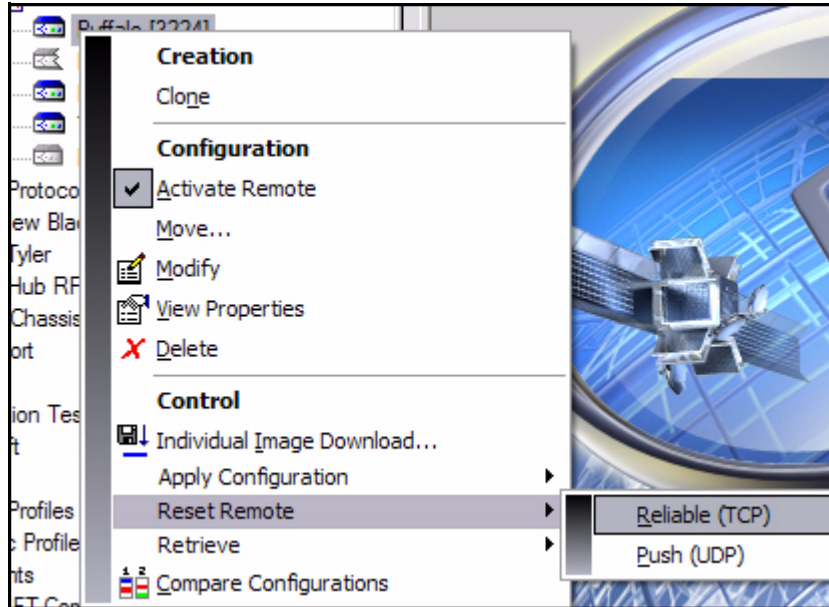
For example, consider the following sequence of events:

1. You send a package to a group of remotes.
2. When iBuilder declares the operation complete, you immediately send an options file to a particular remote.

Because options files are also stored in flash memory, and the remote may still be flashing package contents, the options file apply will “block” until the package flash is complete. iBuilder, meanwhile, is waiting for a response to the options apply, and will probably time out waiting for that response. The apply will work, but not until after iBuilder gives up waiting for a response. iDirect recommends you wait until all multicast activity is complete before performing additional tasks in iBuilder.

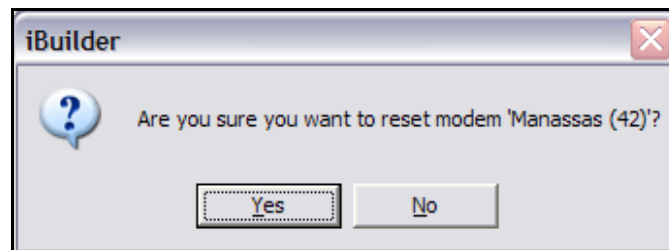
## 12.3 Resetting Remotes

Modifications must be applied to all of the affected remotes in the network by resetting them.



Step 1 Right-click the remote, select **Reset Remote**, and then **Reliable (TCP)**.

Step 2 Select **Yes** to confirm the reset.



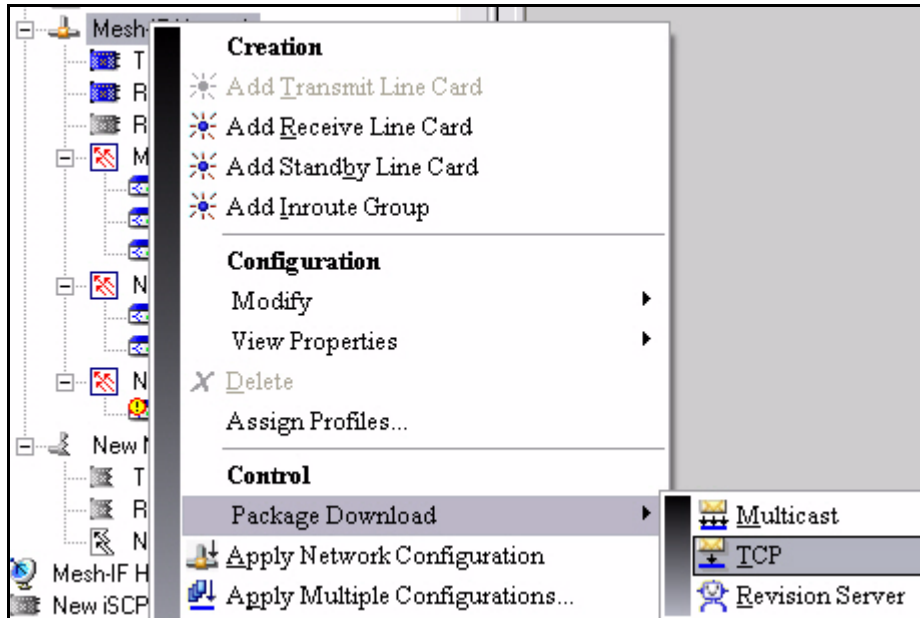
A message appears confirming that the reset command has been issued. The success of the reset is confirmed with a dialog box.

Step 3 Select **OK** to acknowledge the confirmation.

## 12.4 Downloading an Image or Configuration File via TCP

You can download an Image or Options file via the TCP protocol by using the TCP Download feature. However, images and options files can only be downloaded to a single network at a time.

Right-click **Network** and select **Package Download** → **TCP**. The **TCP Package Download** dialog box is displayed. You work with the **TCP Package Download** dialog box the same way you do with the Multicast Download dialog box. Follow the directions in [“Package Section” on page 202](#) and [“Modems and Hubs Sections” on page 204](#). Select the appropriate options in the lower left portion of the **TCP Download** dialog box and click **Start**.



## 12.5 Downloading Remotes Using Revision Server

Prior to release 7.0, it was the responsibility of the network operator to ensure that all remotes were successfully upgraded to the current version of their image files. The network operator had to monitor the network to determine if any remotes failed to receive the initial image upgrade. If so, the operator had to manually resend the image package until all remotes were up-to-date.

Using iDirect's Revision Server, you can configure the NMS to automatically upgrade remote sites that have not yet received the latest download. Once you select a set of remotes to upgrade, the Revision Server packages the current images and options files together. It then periodically transmits the latest package to the selected remotes, stopping only after all remotes in the list have successfully received their upgrades.

You can also use the revision sever to send only options files, without reloading the images. This allows you to change the configuration of one or more remotes and ensure that the changes will be applied without further operator intervention.

The Revision Server has the following characteristics:

- The Revision Server can download multiple networks simultaneously.



- By default, the Revision Server uses up to 10 percent of the downstream bandwidth when it is active. (However, you can modify the download rate when you launch an upgrade.)
- Once you start the Revision Server, it immediately begins to upgrade all the selected remotes. If one or more remotes fail to receive the package during an upgrade cycle, the revision server will automatically begin a new cycle to retransmit the package to those remotes. (The time remaining before the next cycle is displayed on the Revision Server dialog box.) Once all remotes in the list are upgraded, the revision server stops.
- You can command the Revision Server to stop upgrading one or more networks while the upgrade is in progress.

### 12.5.1 How the Revision Server Works

In order to decide which remotes require updates, the Revision Server determines the versions of software and configuration (options file) currently loaded on each remote. It then compares the versions on the remote to the latest versions for that remote as stored at the NMS. Based on this comparison, the NMS assigns each remote a status of **UpRev** or **DownRev**. An **UpRev** remote is up-to-date; i.e., it is loaded with an options file version and a software version that match the versions configured at the NMS. A **DownRev** remote is a remote with an options file version and/or software version that do not match the versions configured at the NMS.

Under normal operation, the Revision Server sits in an idle state waiting for commands from iBuilder. When commanded to perform an upgrade and/or options file application, it operates in a specific “duty cycle” until its assigned tasks are complete or until it is commanded to stop by an iBuilder user.

The Revision Server’s duty cycle is shown in [Figure 12-1, p. 209](#). As the figure shows, the Revision Server performs the following tasks for each cycle:

1. Compiles a list of **DownRev** remotes.
2. Creates a single package file containing the appropriate images (if upgrading) and options files for all down-rev remotes.
3. Multicasts the package to the remotes using 10% of the downstream channel capacity.
4. Waits a calculated amount of time for the multicast to complete and for remotes to receive the package and process it. (When a remote gets a complete package, it picks out the images (if upgrading) and its own options file, writes the file(s) to flash, and resets.)
5. Returns to [step 1](#). When the list of down-rev remotes reaches zero, the revision server returns to the inactive state.



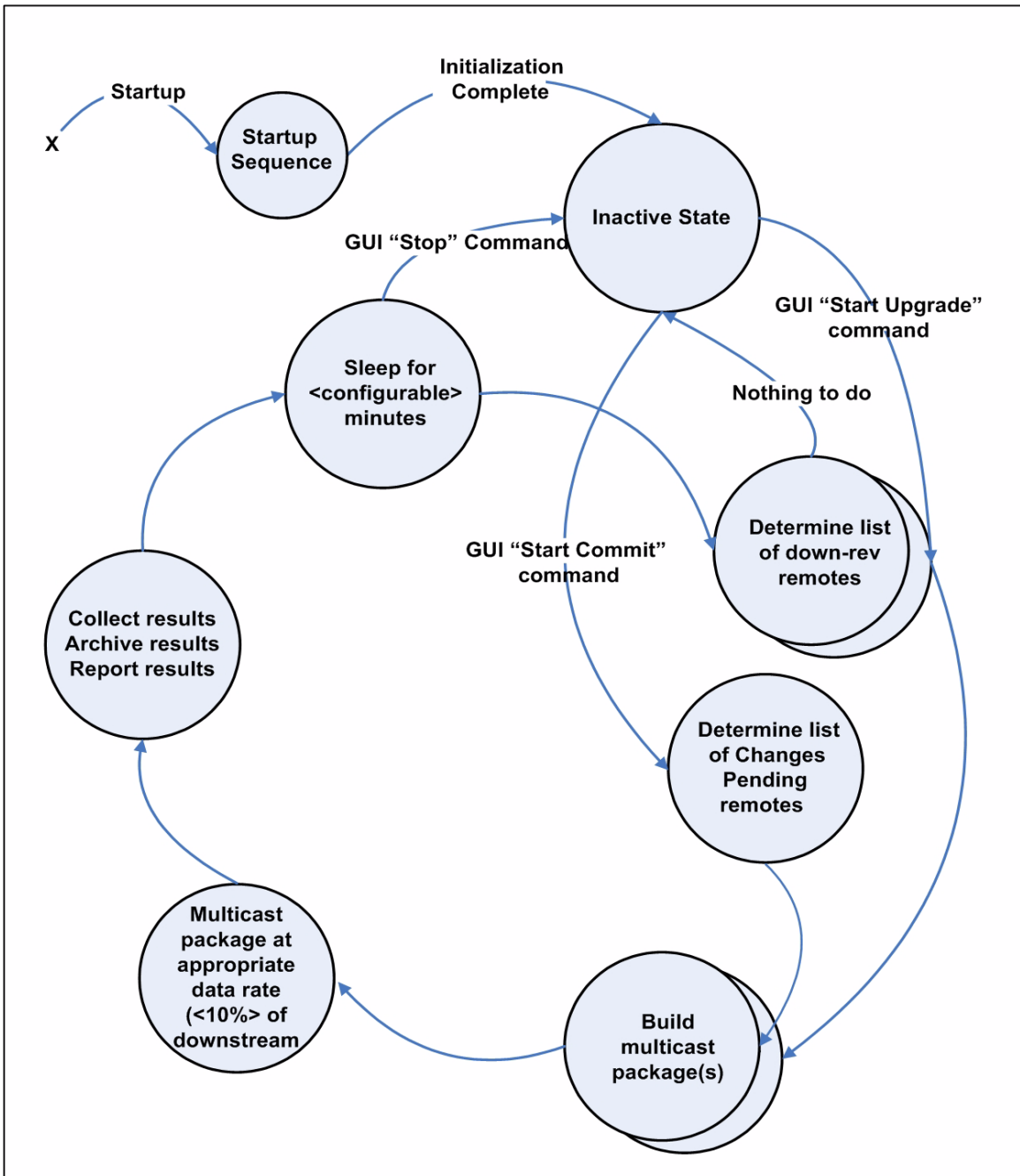


Figure 12-1: Revision Server Duty Cycle

## 12.5.2 When to Use the Revision Server

The Revision Server is useful both during network upgrades (when remotes require new image packages) and during normal operations when applying configuration changes to your network.

There are two ways you can use the Revision Server to automate remote upgrades:

1. Follow the manual upgrade procedure for all of your iDirect equipment, including remotes. Then launch the Revision Server to upgrade any sites that were unreachable at the time of the initial upgrade.
2. Upgrade your hub equipment, including line cards and protocol processors, manually. Then launch the Revision Server to upgrade all remote sites.

When you make changes to your remotes' configuration parameters, you can use the Revision Server to automatically apply those changes by sending the updated options files to the remotes as they become available in the network.



**NOTE**

The Revision Server will upgrade or downgrade your remotes to the iDirect version that is currently running on your NMS Server. Therefore you should upgrade the NMS servers (including your Protocol Processors) before starting a Revision Server upgrade.



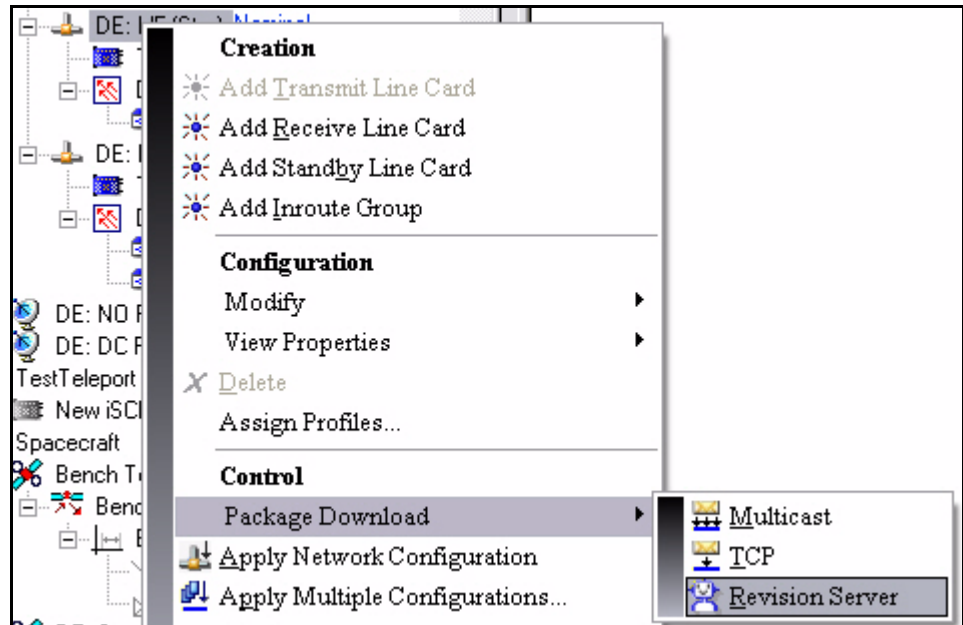
**NOTE**

You can use the Revision Server to upgrade to iDS release 7.0 provided you are upgrading from iDS release 5.05 or later.

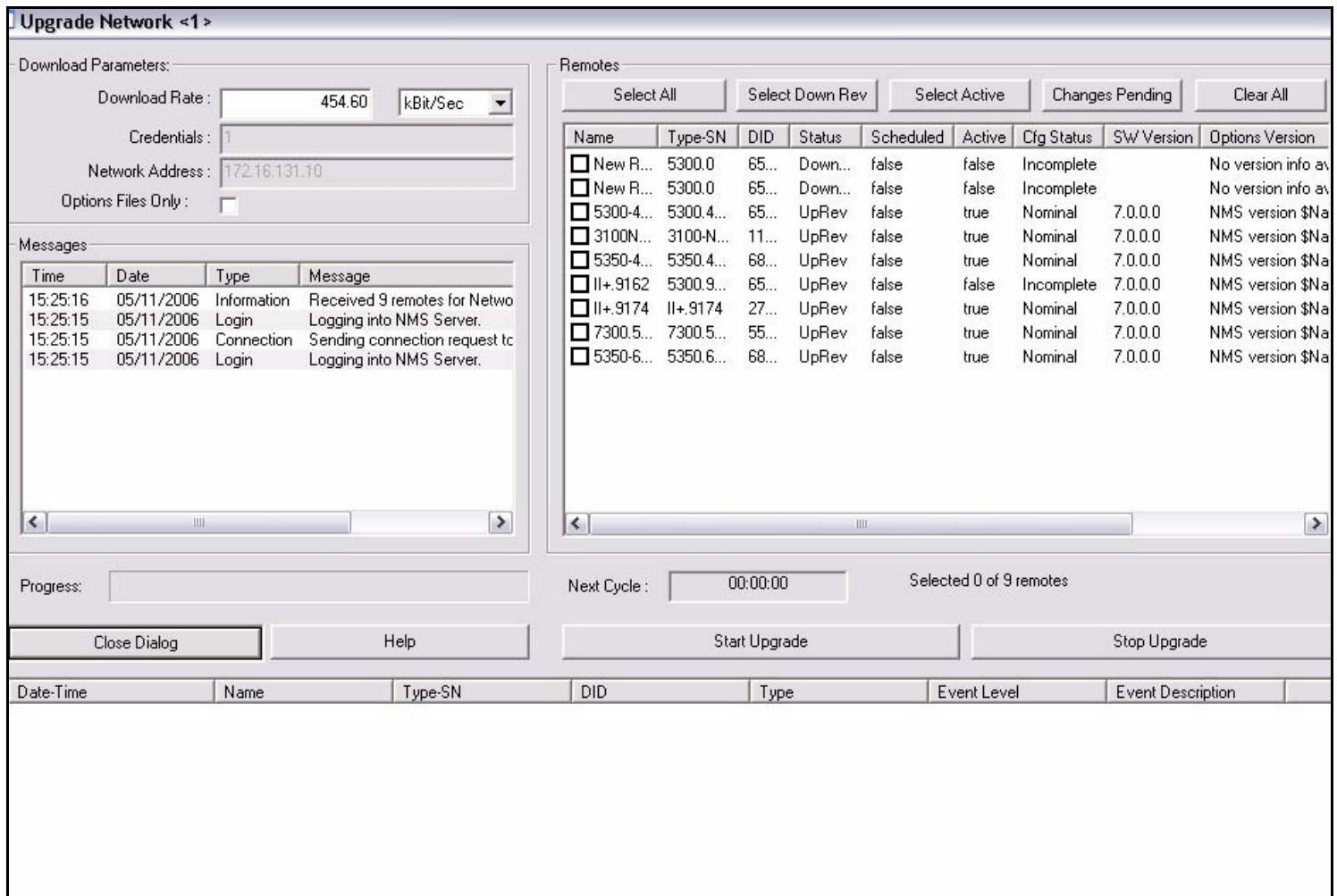
### 12.5.3 Starting the Revision Server

To start the Revision Server, follow these steps:

- Step 1 Right-click your network in the Tree and select **Package Download** → **Revision Server** from the menu.



The Revision Server dialog box will appear, including a list of all the remotes in the network. Remotes with a status of **DownRev** have a different package version from that of the NMS server. **UpRev** remotes are current.



Name	Type-SN	DID	Status	Scheduled	Active	Cfg Status	SW Version	Options Version
<input type="checkbox"/> New R...	5300.0	65...	Down...	false	false	Incomplete		No version info av
<input type="checkbox"/> New R...	5300.0	65...	Down...	false	false	Incomplete		No version info av
<input type="checkbox"/> 5300-4...	5300.4...	65...	UpRev	false	true	Nominal	7.0.0.0	NMS version \$Na
<input type="checkbox"/> 3100N...	3100-N...	11...	UpRev	false	true	Nominal	7.0.0.0	NMS version \$Na
<input type="checkbox"/> 5350-4...	5350.4...	68...	UpRev	false	true	Nominal	7.0.0.0	NMS version \$Na
<input type="checkbox"/> II+.9162	5300.9...	65...	UpRev	false	false	Incomplete	7.0.0.0	NMS version \$Na
<input type="checkbox"/> II+.9174	II+.9174	27...	UpRev	false	true	Nominal	7.0.0.0	NMS version \$Na
<input type="checkbox"/> 7300.5...	7300.5...	55...	UpRev	false	true	Nominal	7.0.0.0	NMS version \$Na
<input type="checkbox"/> 5350-6...	5350.6...	68...	UpRev	false	true	Nominal	7.0.0.0	NMS version \$Na

Time	Date	Type	Message
15:25:16	05/11/2006	Information	Received 9 remotes for Netwo
15:25:15	05/11/2006	Login	Logging into NMS Server.
15:25:15	05/11/2006	Connection	Sending connection request tc
15:25:15	05/11/2006	Login	Logging into NMS Server.

Date-Time	Name	Type-SN	DID	Type	Event Level	Event Description

**Step 2** In the **Remotes** section of the dialog box, select all remotes you want to upgrade by clicking the check boxes. You can also click any of the following buttons to select remotes for download:

- The **Select All** button selects all remotes in the network.
- The **Select Down Rev** button selects only remotes with a status of **DownRev**.
- The **Select Active** button selects only remotes that are currently acquired into the network.
- The **Changes Pending** button selects all remotes with remote-side configuration changes that have not yet been applied.
- The **Clear All** button clears the check boxes for all remotes in the network.

- Step 3 You can change the **Download Rate** specified in the **Download Parameters** section if desired. By default, the download rate is calculated to be 10 percent of the downstream information rate.
- Step 4 Select **Options Files Only** if you only want to send options files to the remotes. No image files will be sent.



## NOTE

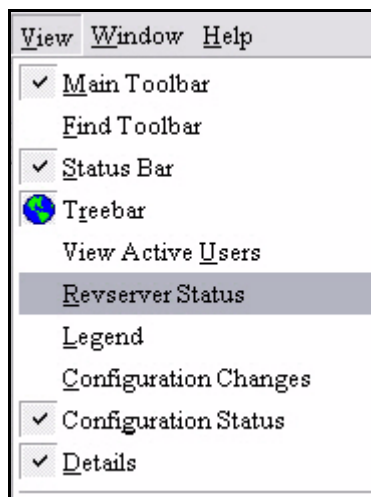
The status of **UpRev** or **DownRev** is determined solely by the version string of the image package. Therefore, remotes with an up-to-date package for which the remote-side options files have not been applied will have a status of **UpRev**.

- Step 5 Click **Start Upgrade** to begin the upgrade process.
- Step 6 Once you have started the upgrade, you can observe the following real-time status in the Revision Server dialog box:
- The **Next Cycle** counter will begin to count down, indicating the time remaining before the Revision Server will restart the upgrade process for any remotes that are not updated during this cycle.
  - In the **Remotes** section of the dialog box, the status will change from **DownRev** to **UpRev** when a remote has successfully received its upgrade.
  - Status messages will be displayed in the **Messages** section of the dialog box, logging the progress of the upgrade.

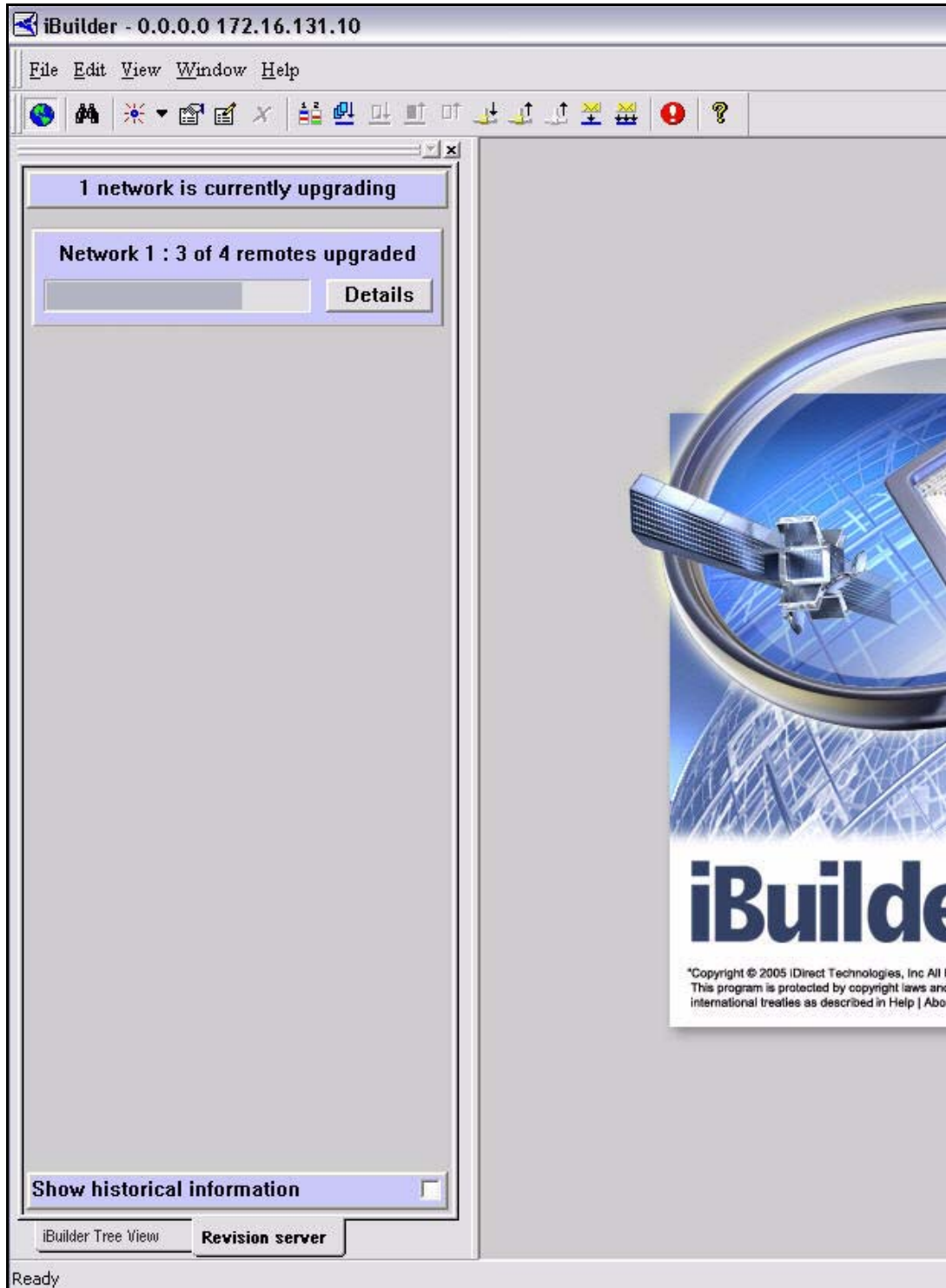
## 12.5.4 Monitoring Upgrades Using the Revision Server Status Pane

The Revision Server Status pane displays the status of all current upgrades, as well as the status of completed upgrades. To display the Revision Server Status pane, follow these steps:

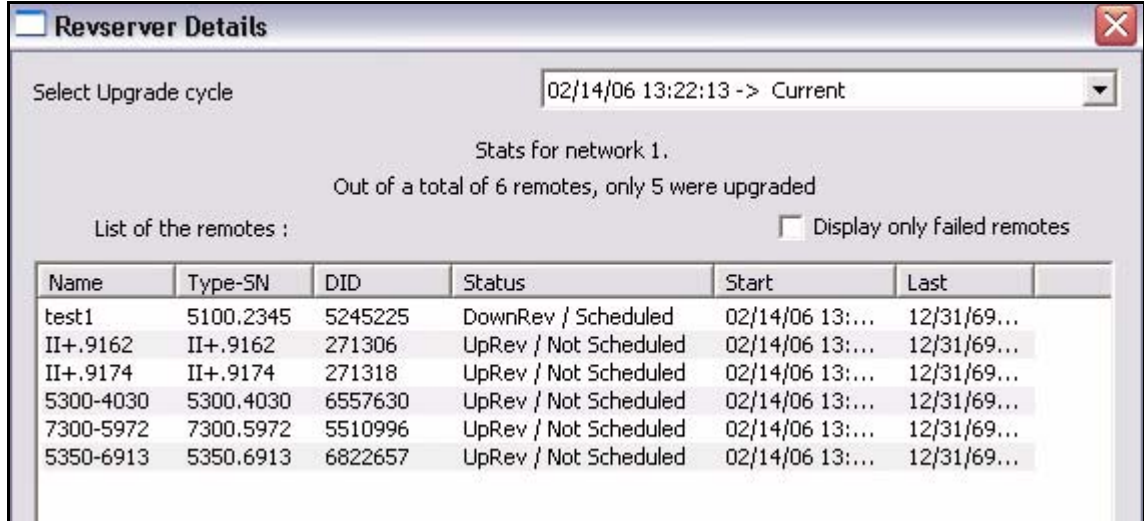
- Step 1 Select **Revserver Status** from the **View** menu.



The Revision Server Status pane will appear in place of the Network Tree, showing the status of all upgrades that are in progress. Note that two tabs appear at the bottom of the pane allowing you to toggle between the Network Tree (**iBuilder Tree View** tab) and the Revision Server Status pane (**Revision Server** tab).



- Step 2 If you want to see the status of completed upgrades as well as current upgrades, select **Show historical information**.
- Step 3 Click **Details** for any upgrade to see more information about that upgrade. This includes the upgrade **Status** of each remote in the upgrade list.



## 12.5.5 Cancelling an Upgrade

You may cancel an upgrade at any time as follows:

- Step 1 Right-click your network in the Tree and select **Package Download** → **Revision Server** to launch the Revision Server dialog box.
- Step 2 Click the **Stop Upgrade** button to cancel the upgrade.



## 13 Creating and Managing User Accounts and User Groups

Prior to iDirect Release 7.0, all user accounts were independent of one another. Beginning with Release 7.0, all users belong to one of a variable number of *User Groups*. Visibility of network elements and access rights to those elements are now defined at the user group level rather than for each user account. This chapter explains how to create and manage user groups and user accounts, and how to define the permissions and access rights associated with each. It discusses the following topics:

- [“NMS User Groups” on page 215](#)
- [“Adding and Managing User Accounts” on page 223](#)
- [“Changing Passwords” on page 229](#)
- [“User Privileges” on page 230](#)
- [“NMS Database Locking” on page 233](#)

### 13.1 Conversion of User Accounts During 7.0 Upgrade Procedure

The database conversion process, which runs automatically when you upgrade your NMS server, performs the following actions on existing user accounts:

- All non-VNO accounts are put into the System group automatically.
- For each VNO account, the upgrade creates a new user group and adds the user account to it.
- Account permissions are maintained, but all VNO visibility settings are turned off. You must use iBuilder to re-establish appropriate visibility for each user group.



#### **WARNING**

As soon as possible after you upgrade for iDS 7.0, you must re-define the visibility settings for each VNO user group. VNO users will be unable to use the system until you have done this.

### 13.2 NMS User Groups

There are three types of NMS User Groups:

- The System User Group
- VNO (Virtual Network Operator) User Groups
- CNO (Customer Network Observer) User Groups

The System User Group provides specific permissions and access rights above all other groups. Members of the system group are the host network operators, system administrators, NOC managers, and other “super users” of the system.

All database items are visible to users in the system group, including all network elements created by VNO users. Individual permissions of system users may vary from account to account.

VNO users may create and manage their own QoS profiles, filter profiles, antenna components, or any other network components, subject to permissions established at the group level by the Host Network Operator (HNO).

VNO User Groups restrict visibility and access rights of group members based on the permissions granted to the group. Creating and managing VNO User Groups is discussed in detail later in this chapter.

CNO User Groups can be created to allow customers to monitor groups of network elements without the ability to add new elements or modify the network in any way. CNO users are restricted to iMonitor read-only access to the network elements that are visible to their CNO User Group. They cannot log into iBuilder.



## NOTE

VNO and CNO User Groups are licensed features. If you plan to define VNO or CNO User Groups in your network, please contact your iDirect Account Manager.

### 13.2.1 Visibility and Access for VNO User Groups

iBuilder distinguishes between *network elements* (such as inroute groups and remotes) and *component folders* (such as QoS and Filter folders) when applying rules for visibility and access within a VNO User Group. Each is discussed separately in the following sections.

#### Visibility and Access for Network Elements

When setting network element visibility and access rights for VNO groups, it is important to keep the following principles in mind:

- Visibility propagates up the tree, but not down the tree. For example if you make a remote **Visible** to a User Group, members of the group will see that remote's "parentage" all the way to the up to the teleport element. However, if you set visibility at the teleport level, group members will see only the teleport when they log in; they will not see any elements underneath it.
- Visibility has three different levels of access rights. When you give visibility of an element to a User Group, for example an inroute group, you have the following additional access rights you can grant or revoke:
  - **Create** access allows users to create new elements underneath this node. For example, you can allow a user to create new remotes in an inroute group.
  - **Write** access allows users to modify the contents of the element itself. For example, a user with **Write** access to an inroute group could modify the inroute group to turn off frequency hopping.
  - **Control** access gives users the right to perform control operations on child elements of the specified node. For example, users with Control access for an inroute group can perform all control operations on remotes in that inroute group.
- Ownership is different from Visibility. When you set a node as **Owned** by a VNO group, you are dedicating that node and all of its children to this VNO group exclusively



(except for system users, of course). No other VNO groups are able to see or interact with this group in any way. Visibility to network elements, however, can be shared across multiple VNOs.

- VNOs cannot see each other; System users see all. When a VNO creates a network element, only the members of that group and the System User Group are able to see the element. When the system group creates or owns a network element, no VNOs can see this element unless they are granted visibility to it.
- User Groups are highly configurable. The implementation of VNO User Groups is quite flexible; you can configure groups in a number of ways. However, unless you are careful when configuring your user groups, this flexibility can result in unwanted results. It is possible to give VNO User Groups various combinations of write and visibility access that may create confusion in practice.

For example, giving a VNO **Write** access to an inroute group, without granting **Control** access at the Network level, could result in a condition from which the VNO user is unable to recover. In this example, a VNO user could modify the inroute group so that it sets the Network to the “Changes Pending” state, yet be unable to apply the changes.

### Visibility and Access for Components Folders

Visibility and access rights are handled differently for components folders than they are for elements of the Network Tree. The following options exist when setting up VNO group visibility and access to components folders in the Tree:

- Users see the contents of folders. By default, users in a VNO group can see the contents of all component folders. However, they cannot change them or add new components.
- QoS Profile and Customer folders are special. By default, VNO users cannot add or modify QoS filters, QoS profiles, or Customers. However, selecting the **Create** property on a QoS or Customer folder allows the customer to create new entries in that folder.

The rules for QoS visibility and control are:

- All VNO users see profiles created in the System User Group.
- Profiles created by VNO members are visible only to members of that VNO User Group and the System User Group.

## 13.2.2 Visibility and Access for CNO User Groups

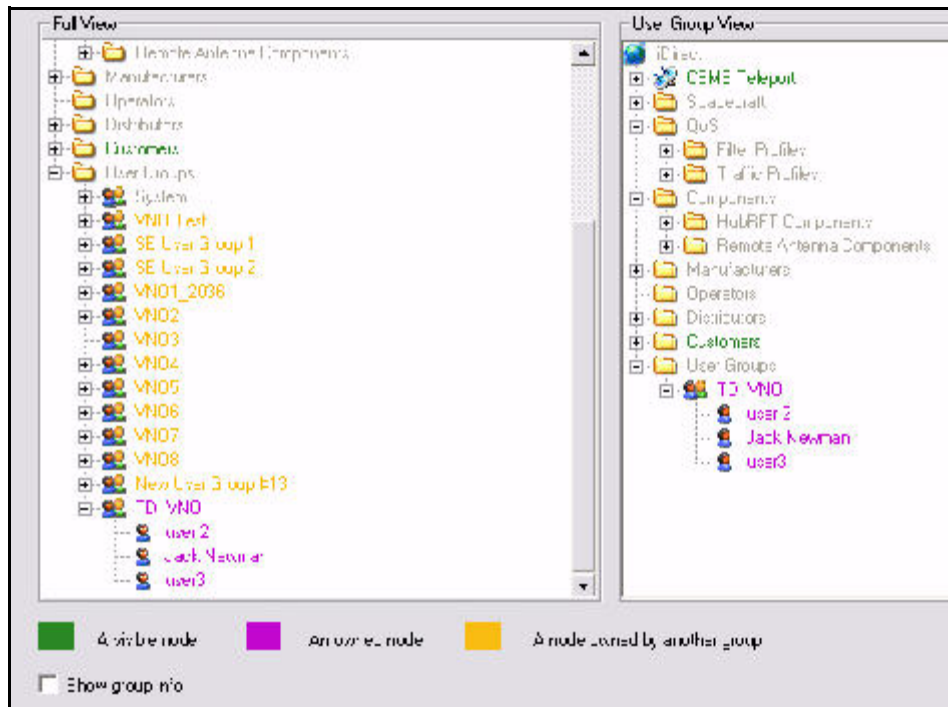
CNO User Groups have the following characteristics:

- CNO users can log in to iMonitor only. They cannot log in to iBuilder.
- Within iMonitor, CNO users can view all network elements that have been made **Visible** to their CNO User Group. The rules of visibility propagation in the network tree that apply to VNOs also apply to CNOs. (See [“Visibility and Access for Network Elements” on page 216](#)).
- CNO users have no access rights other than the ability to view visible elements. Specifically, **Create**, **Write** and **Control** access cannot be granted to CNO users.

- CNO users cannot execute iMonitor Probe functions that modify or control remote modems. However, they can use all Probe read-only functions.
- CNO users cannot select the **Telnet** command from the iMonitor GUI.

### 13.2.3 Creating and Managing VNO and CNO User Groups

You can manage User Groups and their users from iBuilder's Network Tree View. When you add or modify a User Group, the **Group** dialog box is displayed. The **Information** tab contains a **Full View** of the network tree in the left pane and the **User Group View** in the right pane. Notice that the visibility and ownership properties of the Tree elements in the **User Group View** are color coded according to the key at the bottom of the window.

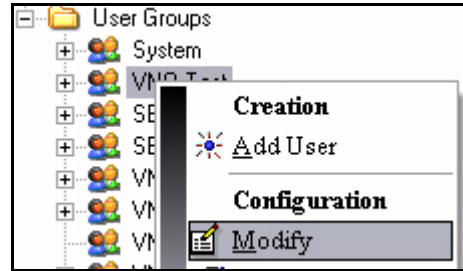
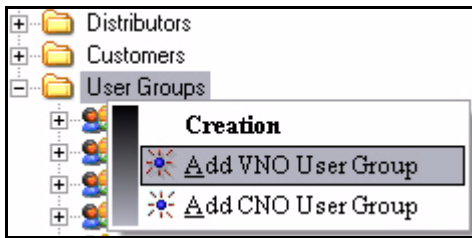


#### Adding or Modifying a VNO or CNO User Group

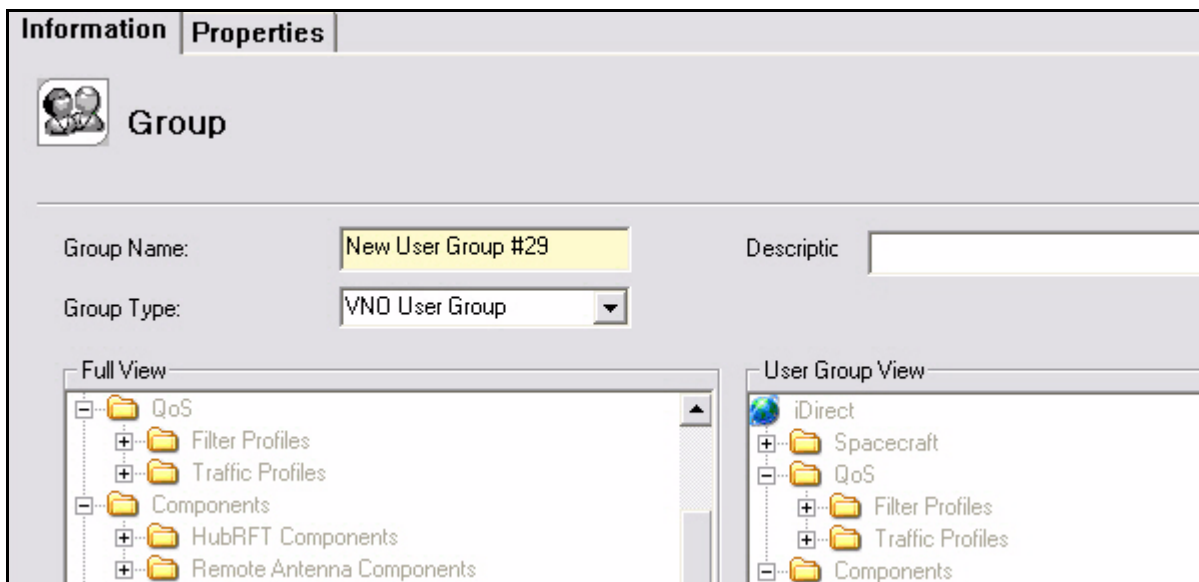
To add or modify a new User Group:

- Step 1 To add a User Group, right-click the **User Group** folder in the Tree and select either **Add VNO User Group** or **Add CNO User Group**. To modify an

existing User Group, right-click the User Group's name in the Tree and select **Modify**. Both alternatives are shown below.

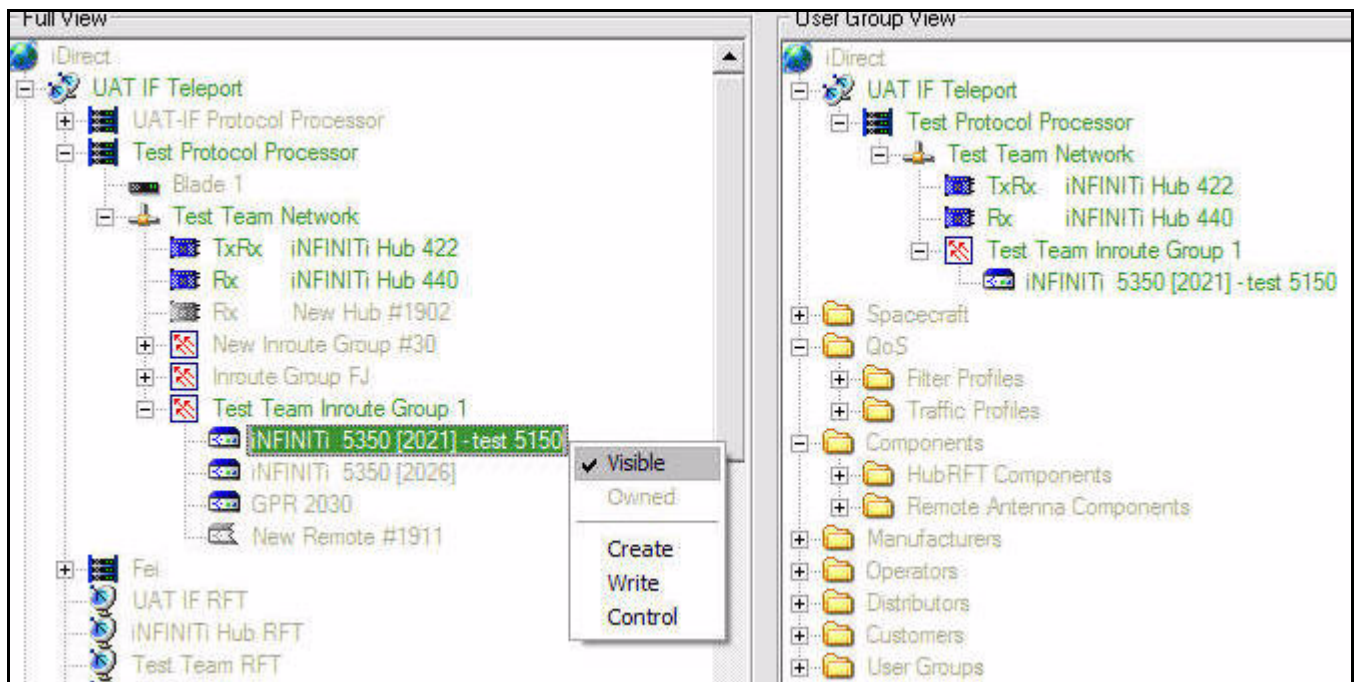
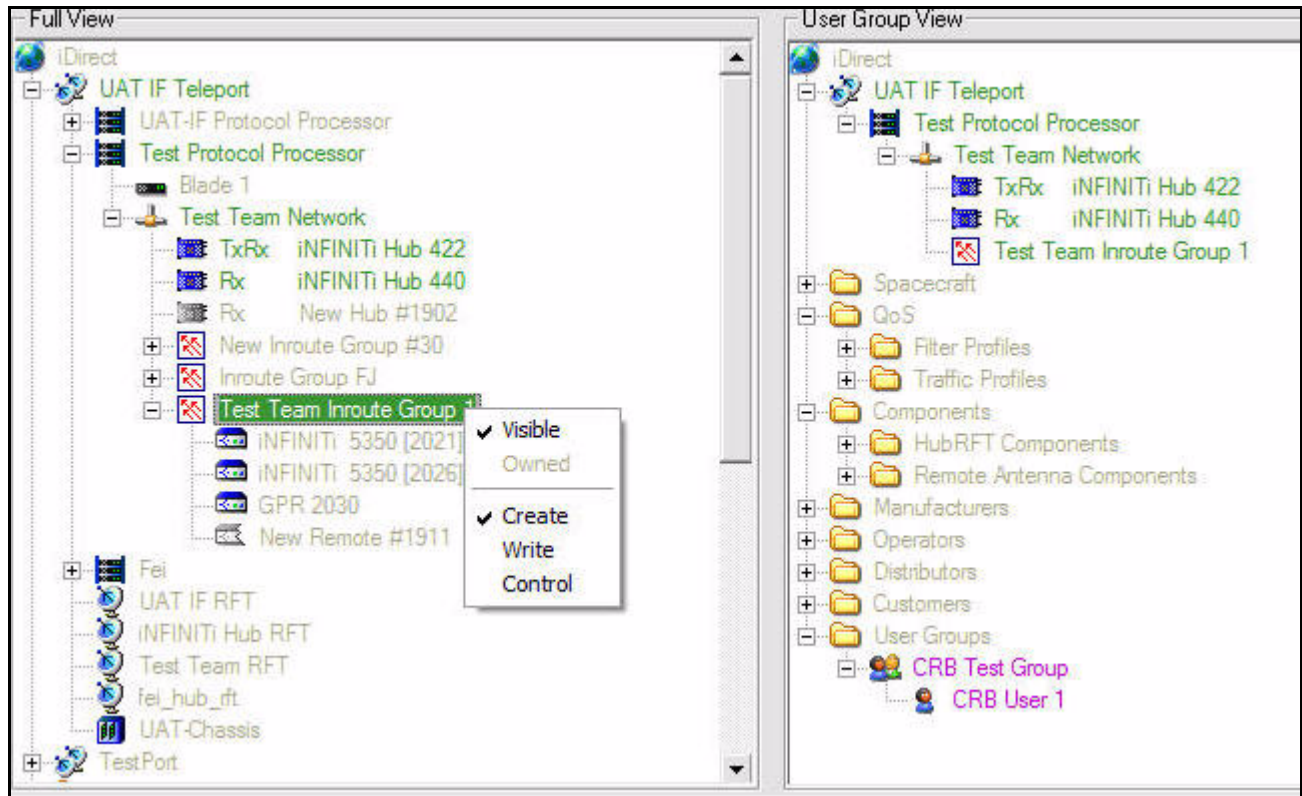


Step 2 In the **Group** dialog box, enter a **Group Name** for the User Group. If desired, you can also change the **Group Type** and add a **Description** of the group.

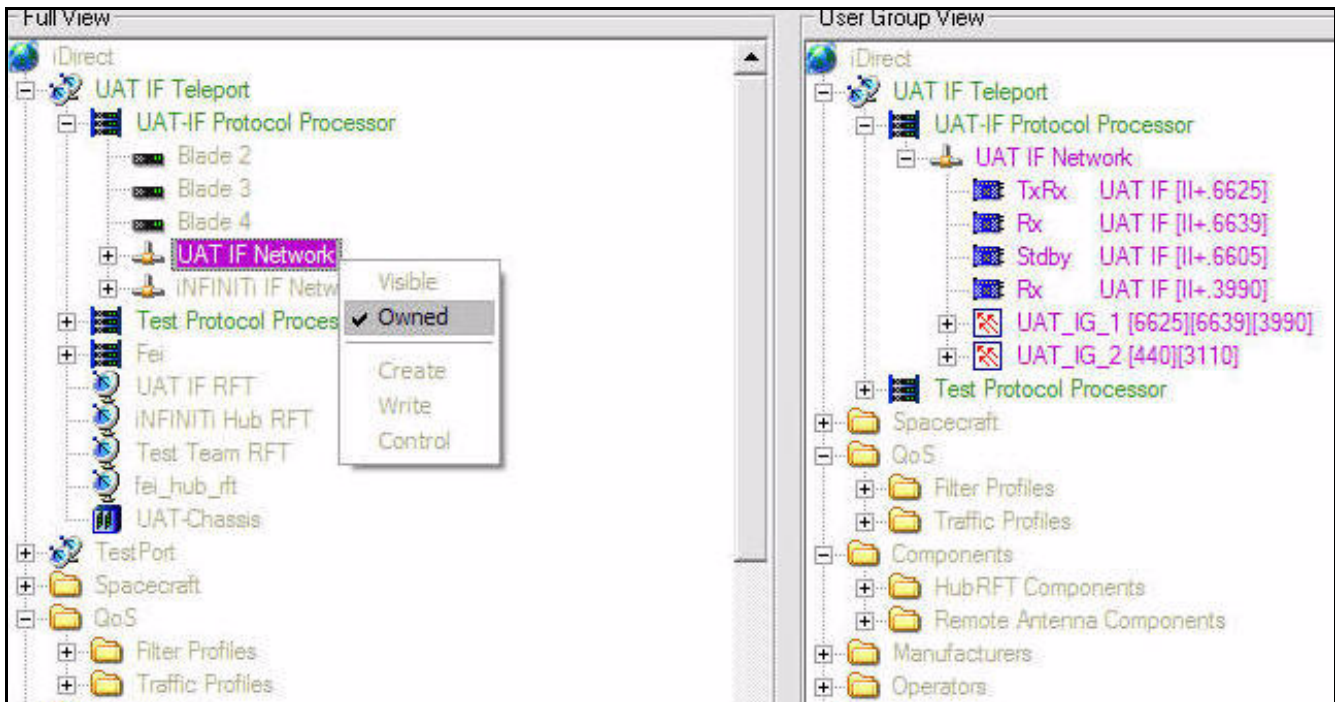


Step 3 On the **Information** tab of the dialog box, right-click on elements in the **Full View** to set their visibility and permissions for the User Group. The menu displays a check mark next to all access rights selected for this element. The **User Group View** shows you which elements this group's users will

have access to, and what their access rights will be. Several examples of VNO User groups are shown here.







**NOTE**

If you are configuring a CNO User Group, you will only be able to select **Visible** from the context menu. Other permissions in the list apply to VNO User Groups only.

### 13.2.4 Setting Global Rate Limits for User Groups

You can use the **Properties** tab of the User Group dialog box to limit the maximum upstream and downstream information rates for a User Group. When either or both of these fields is greater than zero, a rate limit above the specified value cannot be configured for any remote under the group's control.

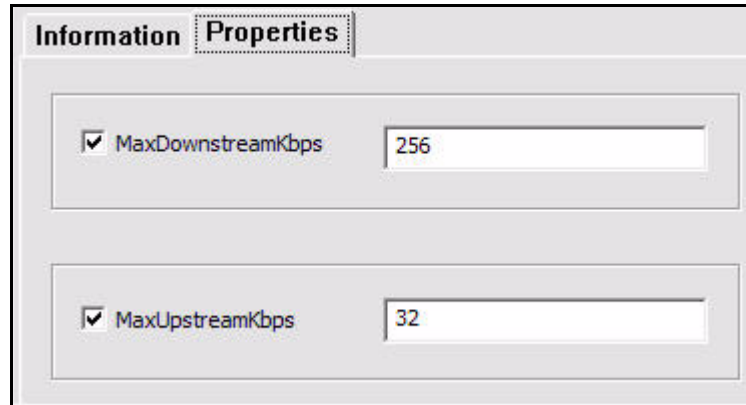


**NOTE**

By default, global rate limits are set to 256 kbps (downstream) and 32 kbps (upstream) when a VNO user group is created. You can use the procedure below to change the default rate limits.

- Step 1 In the **User Group** dialog box, select the **Properties** tab.
- Step 2 To limit the downstream information rate, select the **MaxDownstreamKbps** check box and enter the rate limit in kbps.

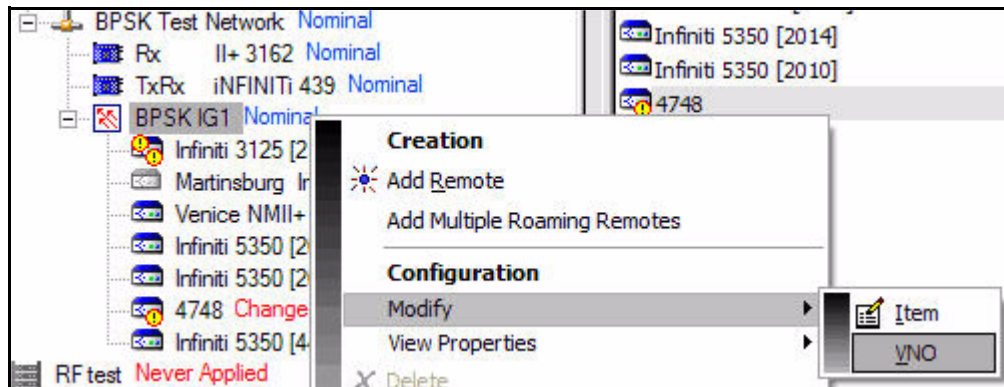
Step 3 To limit the upstream information rate, select the **MaxUpstreamKbps** check box and enter the rate limit in kbps. In this example, remotes created or controlled by members of the User Group are restricted to a maximum of 256 kbps on the downstream and a maximum of 32 kbps on the upstream.



### 13.2.5 Modifying per Node VNO Properties

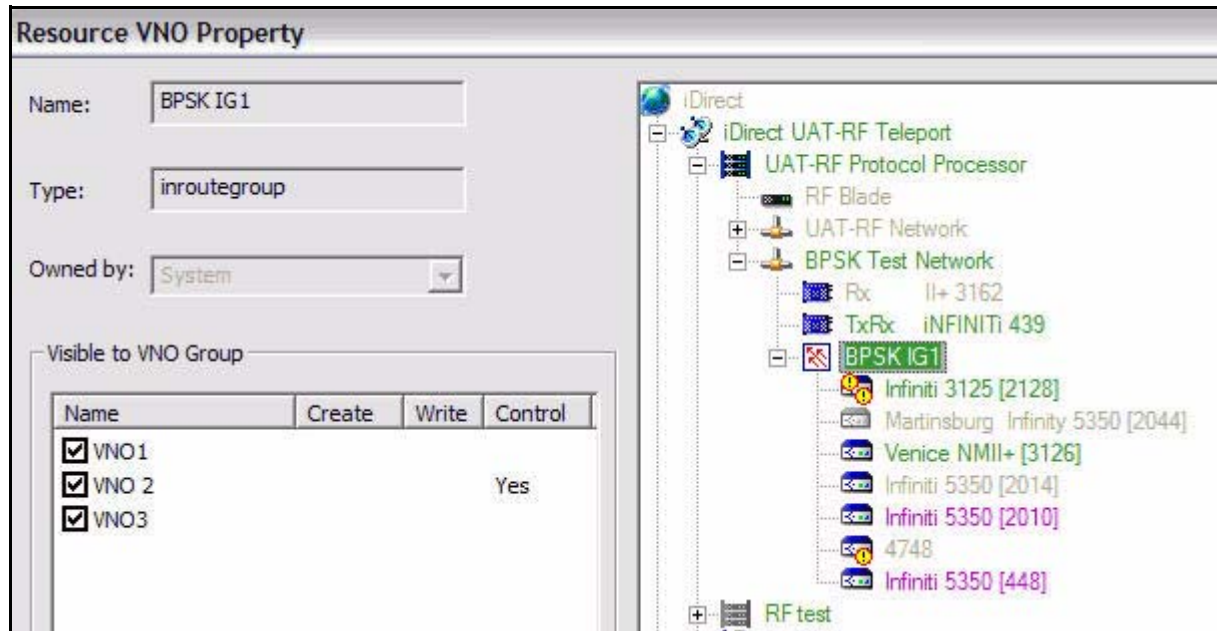
In addition to changing a VNO User Group's properties directly, you can also modify multiple VNO access rights for a particular element in the Network Tree. To view or change all VNO properties for an Inroute Group, for example:

Step 1 Right-click the inroute group and select **Modify → VNO**.

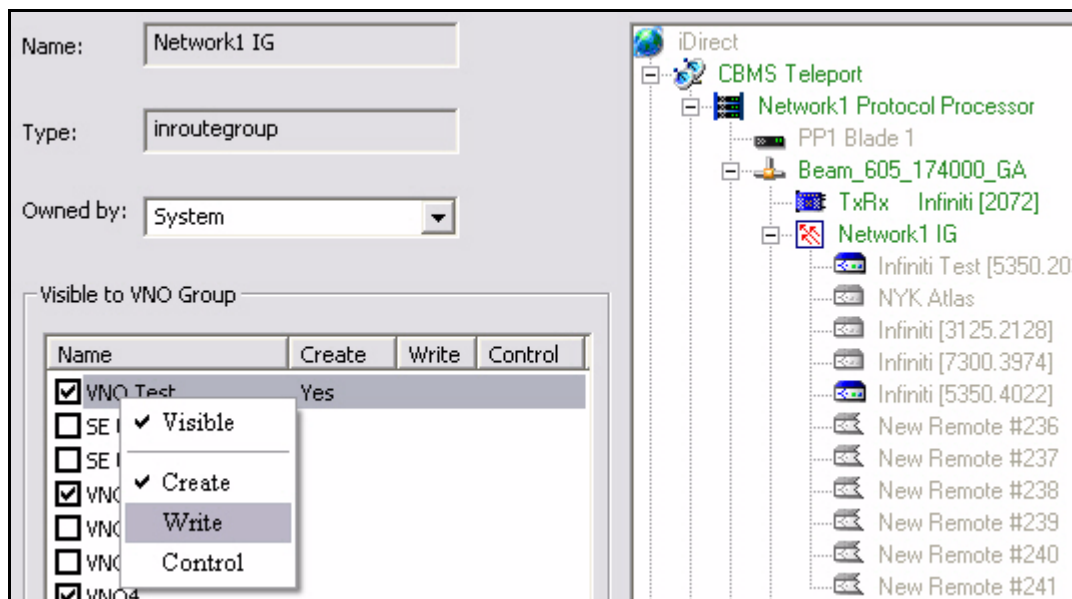


Step 2 To make the element visible to a VNO, select the check box next to the VNO name. (You can also do this by selecting from the context menu as described in the next step.) In this particular example, the inroute group is visible to three different VNO groups. VNO1 and VNO3 can only view the

Inroute Group. VNO2 can perform control operations such as applying configuration changes.



Step 3 To modify a VNO's permissions for the selected element, right-click on the VNO name and select the desired permissions from the menu.



### 13.3 Adding and Managing User Accounts

You can create and manage User Accounts from iBuilder's Network tree. Depending on your permission level within the NMS, you can perform the following actions:

- Add new user

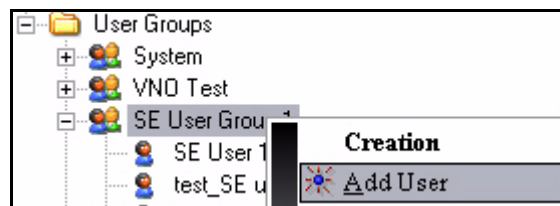
- Clone an existing user and change the name and some of the properties
- Delete a user
- Modify a user's account
- View a user's current properties

The next few sections explain these operations in detail.

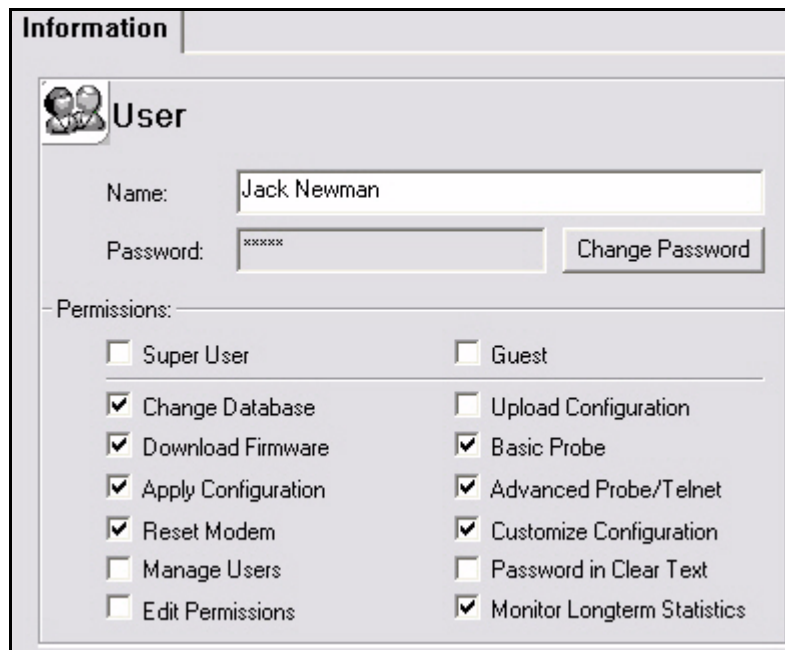
### 13.3.1 Adding a User and Defining User Privileges

To add a new user to a User Group, follow the procedure below.

Step 1 Right-click the User Group in the Network Tree and select **Add User**.



Step 2 When you select **Add User**, the Modify dialog box appears.

A screenshot of a 'User' Modify dialog box. The title bar says 'Information'. Below the title is a 'User' icon and the word 'User'. There are two input fields: 'Name:' with the text 'Jack Newman' and 'Password:' with asterisks. A 'Change Password' button is to the right of the password field. Below these is a 'Permissions:' section with a list of checkboxes. The 'Super User' and 'Guest' checkboxes are unchecked. The following checkboxes are checked: 'Change Database', 'Download Firmware', 'Apply Configuration', 'Reset Modem', 'Basic Probe', 'Advanced Probe/Telnet', 'Customize Configuration', and 'Monitor Longterm Statistics'. The 'Manage Users', 'Password in Clear Text', and 'Edit Permissions' checkboxes are unchecked.



Step 3 Enter a user name and click **Change Password**.



Step 4 Enter and confirm a password for this user.

Step 5 If you click either the **Super User** or **Guest** check box, the permissions allowed for the user level you selected appear with check marks next to them on the Modify dialog box, but they are not selectable. These permissions may vary in accordance with the type of User Group.

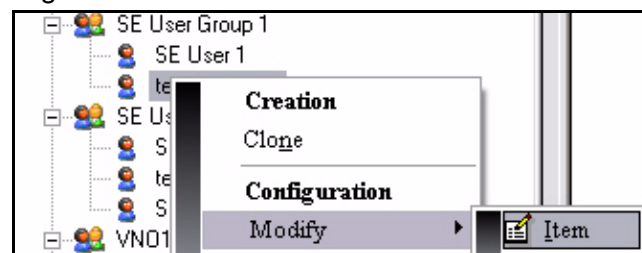
Step 6 If you clear both of the main User Level boxes (**Super User** and **Guest**), the individual permissions detailed in [Table 13-2, "Custom Privileges," on page 231](#) become selectable. Click the boxes next to the customized functions that you want to assign to the user.

Step 7 Click **OK** to save the settings for the user account. The new user will appear in the Network Tree under the User Group you selected.

### 13.3.2 Modifying a User

To modify a user account:

Step 1 Right-click the User Name in the Network Tree and select **Modify** → **Item**.



Step 2 When the **Modify** dialog box appears, change the settings as desired. (For details, see ["Adding a User and Defining User Privileges" on page 224.](#))

Step 3 Click **OK** to save the changes.

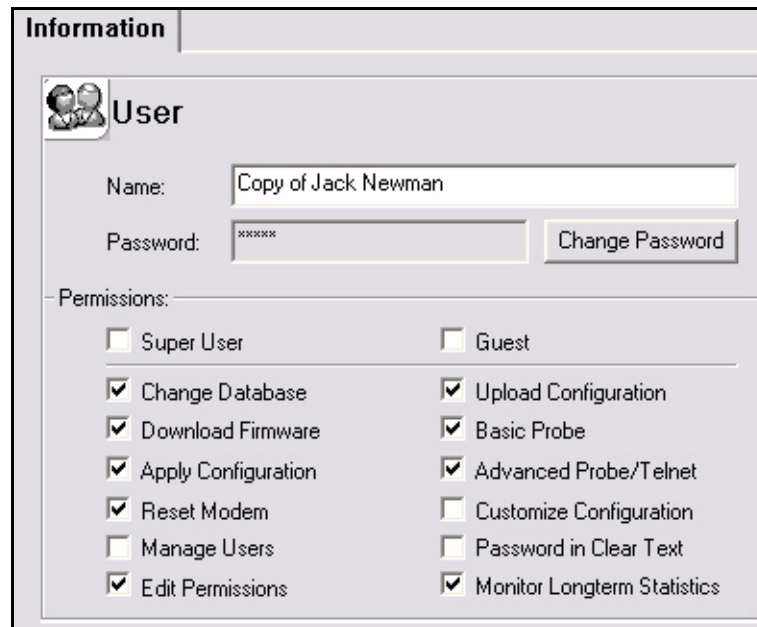
### 13.3.3 Adding a User by Cloning a User's Account

To clone a user in the same User Group:

Step 1 Right-click the User Name in the Network Tree and select **Clone**.



Step 2 A new user appears in the Tree and the **Modify** dialog box is displayed with settings identical to the cloned user.

A screenshot of the 'User' Modify dialog box. The 'Information' tab is active. The 'Name' field contains 'Copy of Jack Newman'. The 'Password' field contains 'xxxxxx' and has a 'Change Password' button next to it. Below the fields is a 'Permissions' section with a list of checkboxes:

- Super User
- Guest
- Change Database
- Upload Configuration
- Download Firmware
- Basic Probe
- Apply Configuration
- Advanced Probe/Telnet
- Reset Modem
- Customize Configuration
- Manage Users
- Password in Clear Text
- Edit Permissions
- Monitor Longterm Statistics

Step 3 Modify the **Name** and **Password**.

Step 4 If desired, change the permissions.

Step 5 Click OK to save the changes.

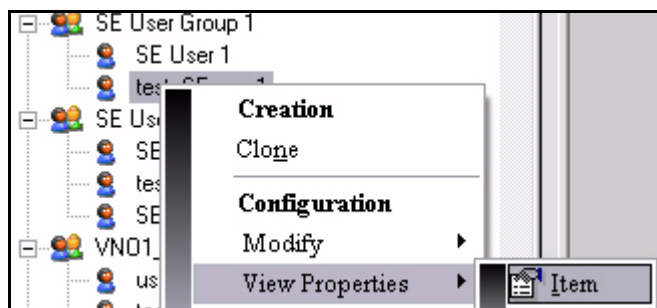
For a detailed description of user permissions, see ["User Privileges" on page 230](#).

### 13.3.4 Viewing a User's Account Properties

To view a user's account properties:

Step 1 Right-click the User Name in the Network Tree

Step 2 Select **View Properties** → **Item**.



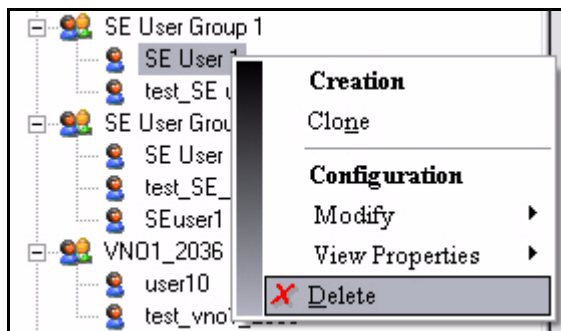
Step 3 View the properties of the user account.

Step 4 Click the **Close** button at the top of the dialog box to exit the pane.

### 13.3.5 Deleting an Existing User's Account

To delete a user from a User Group:

Step 1 Right-click the User Name in the Network Tree and select **Delete**.



Step 2 Click **Yes** to confirm the deletion.

### 13.3.6 Managing Accounts from the Active Users Pane

In addition to managing users accounts from the Network Tree, you can perform some of the same operations from the **Active Users** pane. In addition, the **Active Users** pane allows you to view the list of operators currently logged on to iBuilder and iMonitor.

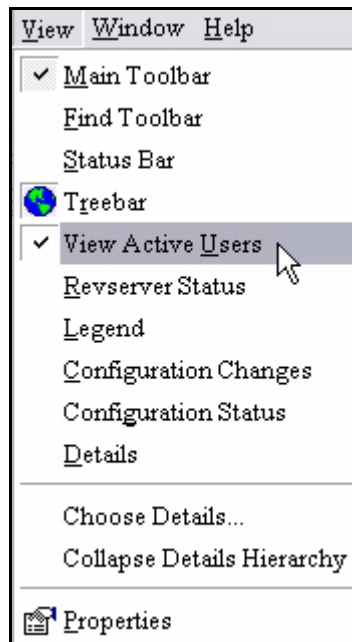
The **Active Users** pane is a standard Microsoft Windows “dockable” display that you can attach to any part of iBuilder’s main window; detach into its own window; or hide altogether. When you first open the pane, it will appear on the right side of the NMS window. The last setting you select is saved between iBuilder sessions.

The **Active Users** pane has four columns. The columns display the **Name**, **Permissions**, **Group** (User Group) and **Logged On** status for all users defined in the system. The **Logged On** column

indicates the logon session count for that user under both iBuilder and iMonitor. This pane is updated in real time as values change.

Name ▲	Group	Permissions	Logged On
admin	System	Super User	Yes - iBuilder(1)
advance	System	DatabaseRe...	No
bsnyder	System	Super User	No
cliu	System	Super User	No
dedsberg	System	Super User	No
dray	System	Super User	No
fzhao	System	Super User	No
guest	System	Guest	No
hcheng	System	Super User	Yes - iBuilder(1)
Maruthi	System	Super User	No
seer	System	Super User	Yes - iBuilder(1)
sushmitha	System	Super User	Yes - iBuilder(1), iMonitor(1)
vokan	System	Super User	No

To open the **Active Users** pane, Select **View → View Active Users** from the main menu.

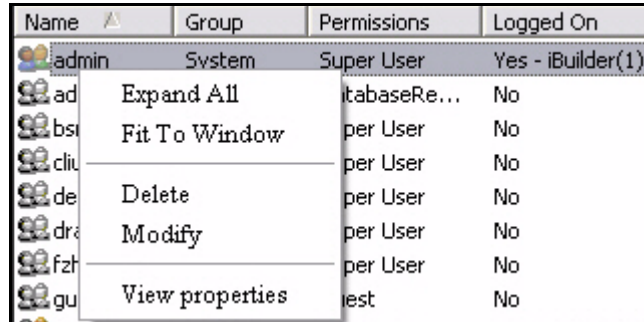


Depending on your permission level within the NMS, you can perform the following actions:

- Delete a user
- Modify a user's account
- View a user's current properties

To perform any of these actions:

- Step 1 Right-click on any user in the **Active Users** pane. A list of the user management options available from this pane is displayed.



- Step 2 Select the desired operation from the menu.

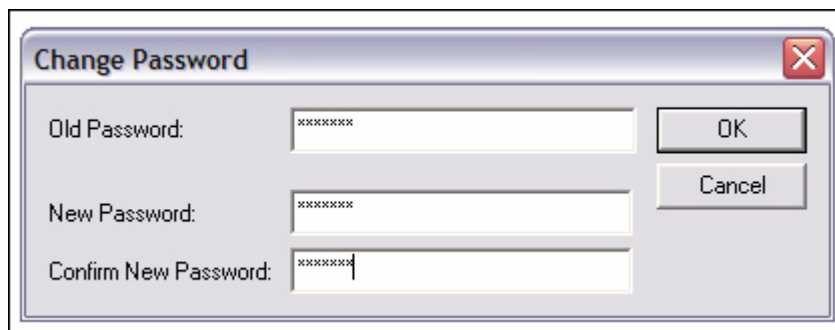
- Step 3 For details, see the section indicated below for your menu selection:

- **Delete:** [“Deleting an Existing User’s Account” on page 227](#)
- **Modify:** [“Modifying a User” on page 225](#)
- **View Properties:** [“Viewing a User’s Account Properties” on page 226](#)

## 13.4 Changing Passwords

You can change your own password, regardless of what authorization level you are assigned. Super Users and users with the *Manage Users* permission can see and change all user passwords.

To change the password, select **File → Change Password** from the Main Menu bar. A user must enter his current password before the change is processed. For security reasons, it is important to change the passwords for the default user names as soon as possible.





## NOTE

Changes to user accounts take place immediately, i.e. you do not have to “apply changes” for users. However, new settings for a specific user will not take effect until the next login under that account. If the user is logged in while you make changes, the old settings remain in effect for the remainder of that session.

## 13.5 User Privileges

The NMS allows users to be assigned a predetermined set of privileges or a custom-defined set of privileges. There are two standard user levels: Super User and Guest. Both the standard user levels and the custom-defined user level are described in detail in this chapter.

Initially, the Super User in the System group is the only user who can set up accounts. User Groups and users can be added or deleted, and user privileges can be added or removed at any time. For System and VNO users, a user’s privilege level is the same for both iMonitor and iBuilder. For example, a user cannot be a Guest in iBuilder and a Super User in iMonitor. CNO users have access to iMonitor only.

The NMS is shipped with a Super User and a Guest account already set up in the System User Group. The Super User can then set up additional user groups and users and assign them to have any of the following user levels:

- Super User
- Guest
- Individually-defined User

If the Super User sets up a user as one of the standard user levels, the NMS system automatically generates a predetermined set of privileges for that user level. (See [Table 13-1: “User Types and Access Privileges”](#).)

If the Super User sets up a user as a custom-defined user, the Super User can assign that user any number of privileges from a list provided in the system. (See [Table 13-2: “Custom Privileges”](#).)

**Table 13-1: User Types and Access Privileges**

Account Type	Access Level	User Name Password	Access Privileges
Pre-Programmed by iDirect	Super User	admin admin	Access to the NMS database and all of its components within this user group, including the ability to configure, modify, and delete anything in the database owned by the group, including users and their privileges. For System Super Users, ability to perform these operations on other User Groups as well.
Pre-Programmed by iDirect	Guest	guest guest	Read-only access to the NMS database and all of its components within this user group. System Guests can read all User Group information.
Custom Defined by Super User	Custom Defined	Defined by Super User or else the VNO Super User must have Manage Users privilege	See <a href="#">Table 13-2: "Custom Privileges"</a> .

The following table lists the various privileges that can be granted or revoked for a custom-defined user.

**Table 13-2: Custom Privileges**

Privilege Name	Description	Applicable NMS Application
Database Read	The most basic privilege; allows retrieval of stored configuration information. This is the only privilege Guest users are granted. You cannot grant or revoke this privilege from iBuilder.	iBuilder, iMonitor
Change Database	Allows modification of configuration information.	iBuilder
Download Firmware	Allows download of firmware to line cards and remote modems.	iBuilder
Apply Configuration	Allows application of configuration changes to networks, hub lines cards, and remote modems.	iBuilder
Reset Modem	Allows remote and line card resets.	iBuilder, iMonitor
Manage Users	Allows modification of user names and passwords.	iBuilder
Edit Permissions	Allows modification of user permission settings.	iBuilder
Upload Configuration	Allows retrieval of a remote modem's or line card's active configuration.	iBuilder
Basic Probe	Allows retrieval of real-time stats in the Probe tab.	iMonitor
Advanced Probe	Allows all Probe functions (reset, telnet, change tx power, etc.).	iMonitor

**Table 13-2: Custom Privileges**

Privilege Name	Description	Applicable NMS Application
Customize Configuration	Allows access to the "Custom" tab in the Remote Modify Dialog Box.	iBuilder
Password in Clear Text	Controls whether or not an NMS user can see remote and protocol processor passwords in clear text.	iBuilder
Monitor Longterm Statistics	Allows monitoring of long term statistics in iMonitor.	iMonitor

### 13.5.1 Super User and Guest Level Privileges

The two basic privilege levels are **Super User** (all privileges) and **Guest** (read-only).

- The **Super User** access level gives the user complete access to all features of the NMS, in both iBuilder and iMonitor, that are available to the User Group in which the Super User is defined.
- **Guest** access level provides read-only access to all parts of the network in iBuilder with no ability to change data or download images. Guest access provides most functions in iMonitor, with the following exceptions:
  - Guest-level users cannot telnet to remote modems.
  - Guest-level users cannot exercise functions on the Probe tab of iMonitor's remote control panel.

### 13.5.2 Super User and Guest Privileges for VNOs

#### Super User within a VNO

A user defined in a VNO as a **Super User** is able to see and operate on only those network(s) that the Super User specifies, with the following additional restrictions. VNO Super Users can add, modify or delete all remotes within their visible nodes. Generally, they are provided with full remote management capability on these nodes.

1. They cannot create or modify any network components in the network tree (Spacecraft/ Carriers, remote/hub antenna components, QoS Profiles).
2. They cannot create or modify Hub RFT or Hub Chassis records.
3. They cannot perform any operations on the Teleport or Protocol Processor entries in the network tree.
4. From the network level in the tree, they cannot perform multicast downloads, delete networks, or create new line cards.
5. They can modify the network record, but only to activate/deactivate remotes.



6. They cannot see or modify acquisition or uplink control parameters.
7. From the hub level in the tree, they cannot perform image downloads, nor can they create or delete line cards.

### Guest User within a VNO

A user defined in a VNO as **Guest** has read-only permissions to the nodes visible to a Super User in that the VNO.

## 13.6 NMS Database Locking

The NMS configuration server guarantees the integrity of your configuration parameters by locking the database when a modification takes place, and releasing the lock when the modification is complete. Prior to release 7.0, there was one global lock shared by all users. The lock became active whenever any iBuilder user launched a Modify dialog box for any network object. During this time no other users could launch any Modify panes.

Beginning with release 7.0, there is one lock for each User Group. Members of different User Groups can modify the database at the same time. Within a User Group, there is still a single lock. The System User Group, however, is granted a global lock; if a user from the System group is modifying a record, no other users, regardless of group membership, can modify the database.

If a user launches a **Modify** pane and forgets to close it, thereby preventing other users in the same User Group from modifying records, you can use the following procedure to free the lock for other users:

- Step 1 Log into the NMS server as “root”.
- Step 2 Type: `telnet localhost 14123`
- Step 3 Log onto the console with user name “**admin**” and password “**iDirect**”.
- Step 4 Type: `clients -v`
- Step 5 Locate the line of the user who has the lock. The line will look something like this:

```
type: iBuilder V $Name: NetModem-Beta51 $, IP:
10.0.19.108:1513, login: crb, server_time: Thu Jul 29
17:54:16 2004
```

The IP address of the lock-holder is shown in the error message pop-up when you try to modify an object.

- Step 6 The section that begins “IP...” contains the information you need to break the lock (it is underlined above).
- Step 7 Type: `kill <ip address>:<port number>`, where <ip address> is the host address, and <port number> is the actual port number. In the example above, you would enter “kill 10.0.19.108:1513”.

Step 8 This command will break the user's lock and other users will now be able to modify network objects.

## 14 Commissioning a Line Card, Private Hub or Mini Hub

This section provides instructions for commissioning iDirect line cards, private hubs, and mini hubs to transmit SCPC outroutes. It discusses the following topics:

- Powering on the equipment
- Determining the IP address
- Downloading the initial image package and options file
- Performing the 1 dB compression test when necessary
- Setting the transmit power for the SCPC carrier
- Setting UPC parameters for mesh outroutes

In addition, the steps are provided for setting the clear sky C/N parameter for a mesh inroute. This procedure must be performed at the hub during commissioning of the first mesh remote that will transmit on the inroute.



### NOTE

Unless otherwise indicated, the term “line card” as used here refers to iDirect Private and Mini Satellite Hubs as well as iDirect Line Cards.

### 14.1 Before You Begin

Before you execute this procedure, the following tasks should have already been performed at the hub:

- The physical teleport installation must be complete.
- The hub antenna should have been pointed and cross polarization test performed.
- The NMS client and server software should be running.
- Using iBuilder, you should have already:
  - Defined your hub equipment, satellite transponder bandwidth, and the upstream carrier to be transmitted by this line card. (See [“Defining Hub RFT Components and the Satellite” on page 61.](#))
  - Added your hub components to the iBuilder Network Tree. (See [“Defining Network Components” on page 77.](#))
  - Added your network to the iBuilder Network Tree. (See [“Defining Networks, Line Cards, and Inroute Groups” on page 93.](#))



### NOTE

If you are adding a new line card, the Tx Out, Rx In and Lan A ports should *not* be connected at this time. Do not connect these cables until instructed to do so by this procedure.

## 14.2 Add the Line Card in iBuilder and Retrieve the Configuration

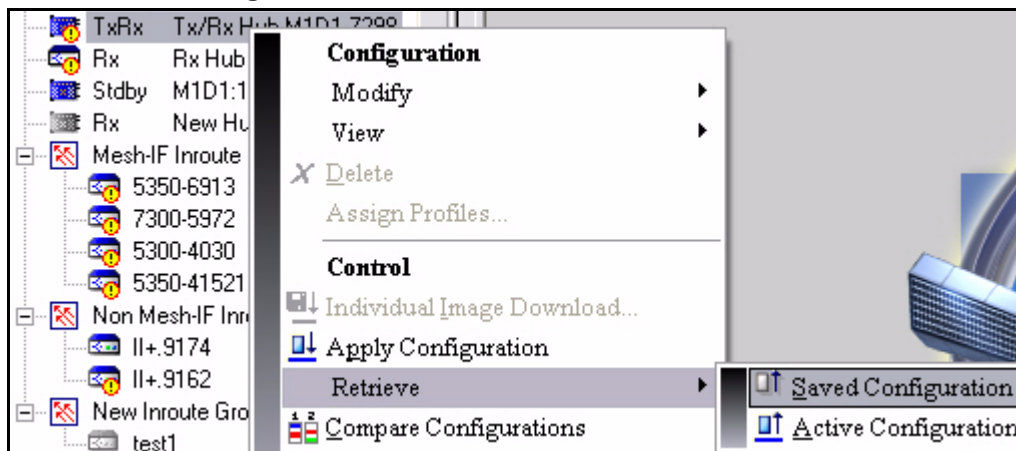
Use iBuilder to add the line card to the Network Tree and configure the line card parameters in the options file.

- Step 1 In iBuilder, right-click your network in the Tree and follow the procedure in [“Adding a Tx Line Card, a Tx/Rx Line Card, or a 10000 Series Hub” on page 94](#) to configure the line card.
- Step 2 Right-click your network in the Network Tree and select **Apply → Network Configuration** from the menu.



**NOTE** Do not apply the line card configuration at this time.

- Step 3 Right-click the line card in the Tree and select **Retrieve → Saved Configuration**.



- Step 4 In the **Save As** dialog box, navigate to the folder on your PC in which you want to save the options file. Then click the **Save** button to save the file to your PC.
- Step 5 After you save the options file, it will be displayed in Notepad as a text file. If desired, review the configuration in Notepad; then close the Notepad window.

## 14.3 Power on the Line Card


Follow these steps to power on the line card or private hub.

- Step 1 If you are commissioning a private or mini hub, plug in the AC power cord.
- Step 2 If you are commissioning a line card:

- a Insert the line card into the slot in the chassis you plan to use.
- b In iBuilder, right-click the chassis in the Network Tree and select **Modify** → **Item**. The Modify Chassis dialog box will appear.
- c Select the check box for the slot that contains the new line card. This will toggle the setting from **Off** to **On**.

**Modify Configuration Object - Mesh-IF Chasis [Modified]**

**Information**

 **Chassis**

Name: Mesh-IF Chasis

IP Address: 172 . 16 . 135 . 19

RCM Installed

State	Jumpers	Slots	Hub Assignment
<input checked="" type="checkbox"/> On		Slot 1	Free
<input checked="" type="checkbox"/> On		Slot 2	M1D1:13594 (Stdby)
<input checked="" type="checkbox"/> On		Slot 3	Rx Hub M1D1 7306 (Rx)
<input checked="" type="checkbox"/> On		Slot 4	Tx/Rx Hub M1D1 7298 (Tx)
<input type="checkbox"/> Off	Jumper 1		
<input type="checkbox"/> Off		Slot 5	Free

Step 3 Wait two minutes.

## 14.4 Determine the IP Address

Follow these steps to determine the IP Address and subnet mask of your line card.

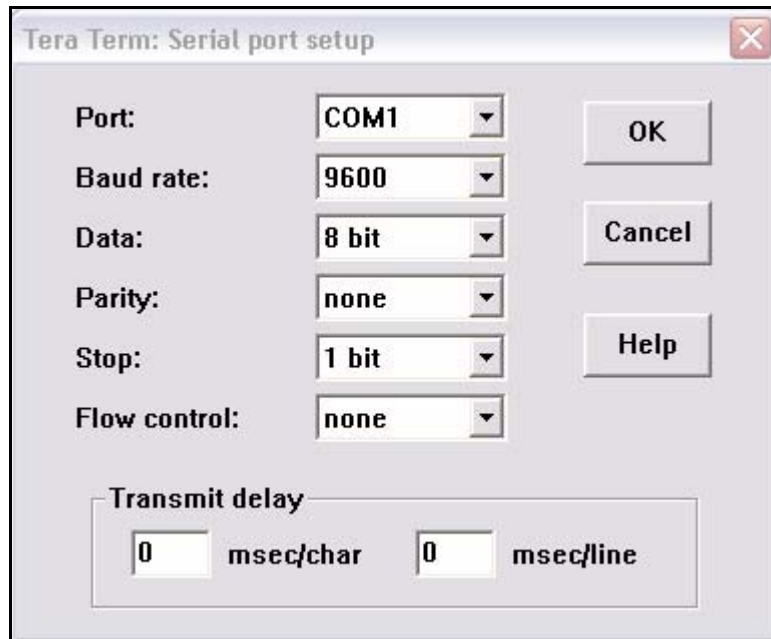


### NOTE

The default IP Address of iNFINITI line cards is 192.168.0.1, with a subnet mask of 255.255.255.0. If you already know the IP address, you can skip this section.

- Step 1 Connect a console cable from the COM1 port on your client PC to the console port on the line card.
- Step 2 Using a terminal emulator program such as Tera Terminal or HyperTerminal, connect to the line card with the following settings:
  - 9600 bps
  - 8 bits
  - No parity
  - 1 stop bit

This is illustrated below using Tera Terminal.



Step 3 Log in as:

**Username:** root

**Password:** <password>

For iNFINITI line cards, **iDirect** is the default password for the root account.

Step 4 At the Linux prompt, type

```
telnet 0
```

The Telnet login screen will appear.

Step 5 Log in to the Telnet session as:

**Username:** admin

**Password:** <password>

For iNFINITI line cards, **iDirect** is the default password for the admin account.

Step 6 At the Telnet prompt, type the following command to determine the IP Address and subnet mask of the line card:

```
laninfo
```

The output of the `laninfo` command is shown here.

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

[HUB:7298] admin@telnet:10.0.50.61;1358
>

[HUB:7298] admin@telnet:10.0.50.61;1358
> laninfo
Address: 172.18.0.81
Netmask: 255.255.255.0

[HUB:7298] admin@telnet:10.0.50.61;1358
>
```

Step 7 Note the IP address and subnet mask. You will need this information when downloading the image package and options file.

## 14.5 Download the Image Package and Options file

When installing a new line card or private hub, you can use iSite to download the image package containing the software and firmware before establishing connectivity with the NMS. (For information on downloading images from iBuilder, see [“Upgrading Software and Firmware” on page 201.](#))

These steps assume that you are still connected to the console port of the line card and that you have not yet connected your line card to the LAN.

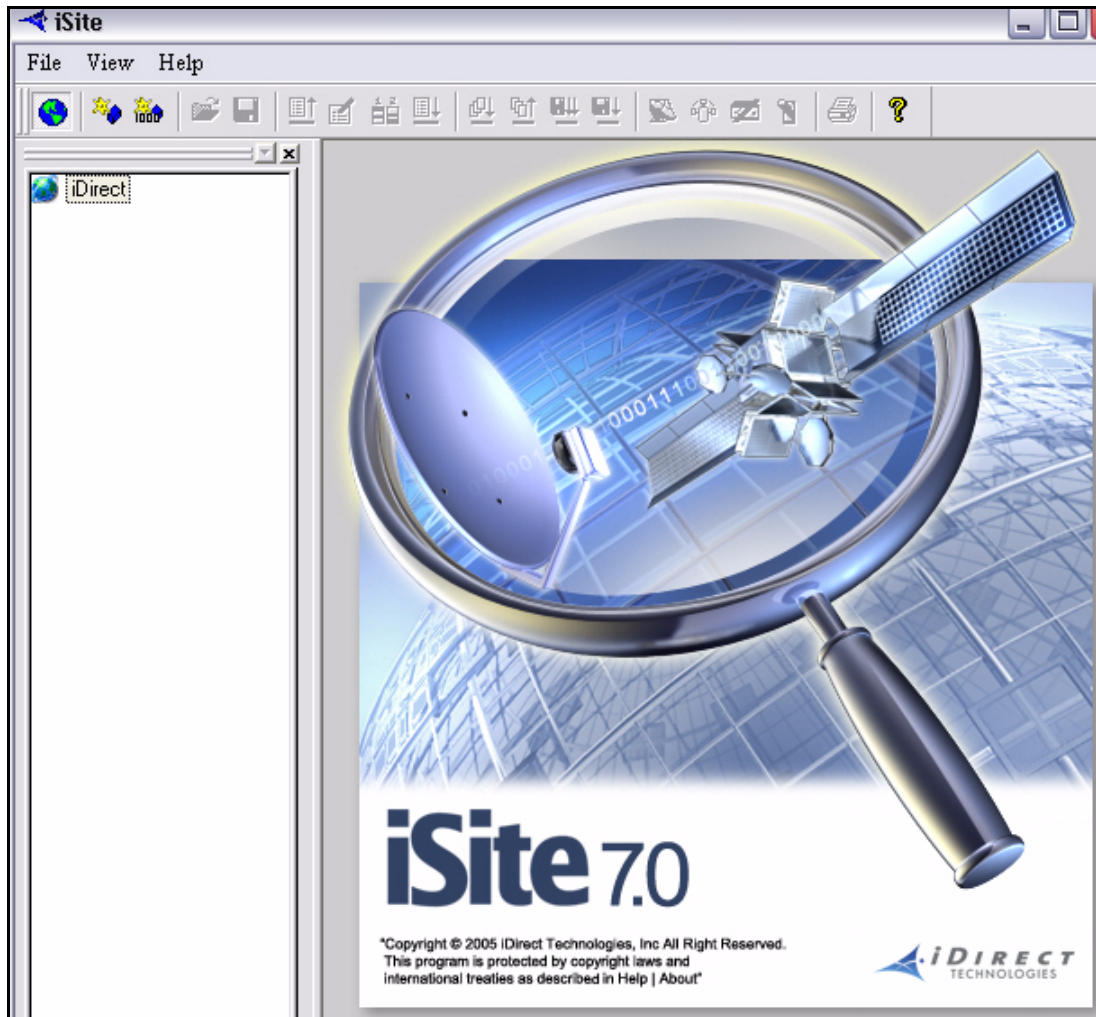
Step 1 Configure the IP address and subnet mask on your PC to be an IP address in the same subnet as the IP address of the line card.



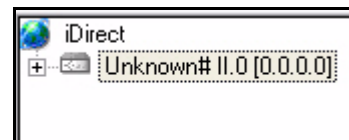
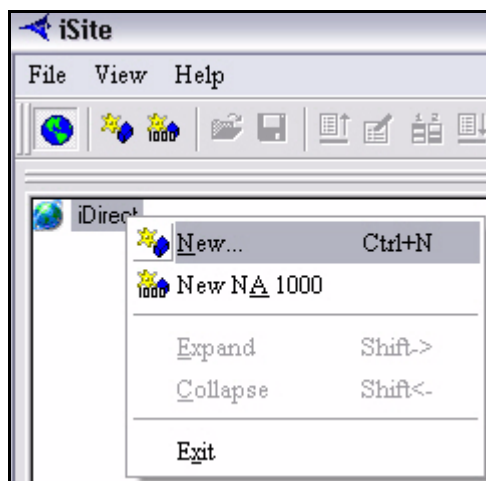
**NOTE** The default IP Address of iNFINITI line cards is 192.168.0.1, with a subnet mask of 255.255.255.0.

Step 2 Connect a cross-over Ethernet cable between the LAN port of the line card and your PC or laptop.

Step 3 Launch iSite. The main iSite screen will appear.



Step 4 Right-click the globe in the Network Tree and select **New**. An **Unknown** element appears in the Tree.



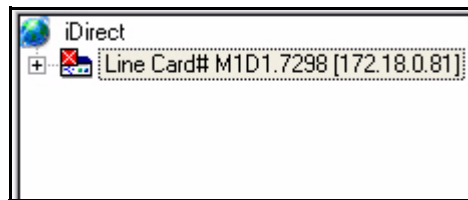


- Step 5 Right-click the new element and select Login to display the **Login** dialog box.

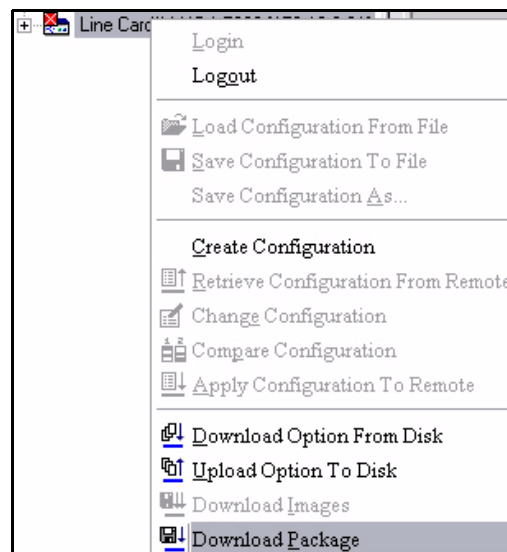


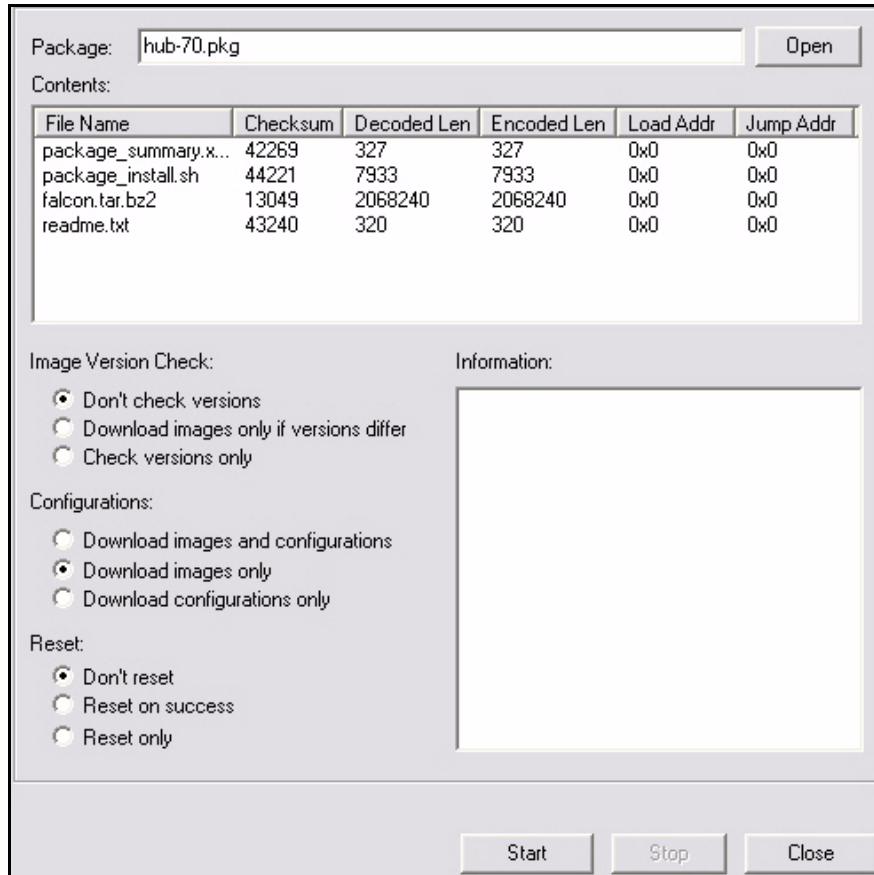
- Step 6 Enter the **IP Address** of the line card and a password. (For iNFINITI line cards, iDirect is the default password.)

- Step 7 Select **Admin** in the **Login as** section and click **OK**. The line card will appear in the Network Tree, replacing the unknown element.



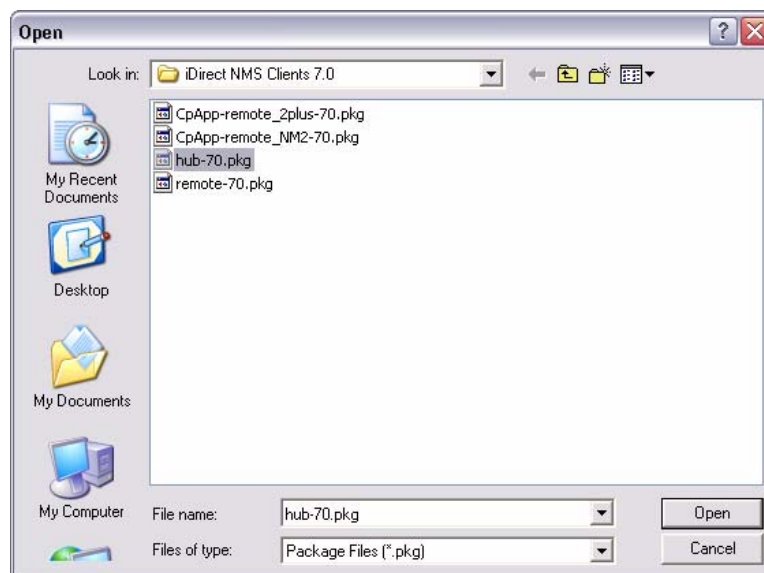
- Step 8 In the Network Tree, right-click the line card and select **Download Package** to display the Download Package dialog box.



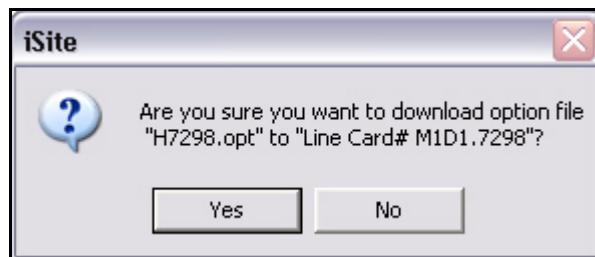


Step 9 In the **Download Package** dialog box:

- a Click the **Open** button to display the **Open** dialog box. Then navigate to the folder on the client PC that contains your iDirect image packages. (Typically, this is the same folder that contains your client software.)



- b Select the image package (.pkg file) for your line card in the **Open** dialog box and click the **Open** button. (iNFINITI line cards and hubs use the same image package. The file name for this package should begin with “hub” as shown in the example above.)
  - c In the **Download Package** dialog box, select:
    - **Don't check versions**
    - **Download images only**
    - **Don't reset**
  - d Click the **Start** button to download the package.
- Step 10 Right-click line card in the Network Tree and select **Download Option From Disk** to display the **Open** dialog box.
- Step 11 Navigate to the folder containing the options file that you saved from iBuilder when executing [step 4](#) of [section 14.2](#) on [page 236](#). Then select the options file.
- Step 12 Click the **Open** button.
- Step 13 Click **Yes** to download the options file to the line card.



- Step 14 Right-click line card in the Network Tree and select **Reset** from the menu.

At this point the new configuration (including the new IP address of line card) will be applied and you will lose connectivity to the line card. Do not disconnect the console cable.

## 14.6 Connect the Transmit and Receive Ports

Follow these steps to connect the transmit and receive ports of your line card or private / mini hub to the network.



### WARNING

Connecting the transmit port of your line card will result in the transmission of a carrier on the satellite. This step should only be performed while on line with the satellite provider.

If you are adding a Tx-only line card:

- Step 1 Connect the Tx coax patch cable to the line card's Tx Out port.
- Step 2 Connect the Tx coax patch cable to the corresponding Tx patch panel port above the line card slot.

If you are adding a Tx/Rx line card or a Tx line card that is configured for mesh:

- Step 1 Connect the Tx coax patch cable to the line card's Tx Out port.
- Step 2 Connect the Tx coax patch cable to the corresponding Tx patch panel port above the line card slot.
- Step 3 Connect the Rx coax patch cable to the line card's Rx In port.
- Step 4 Connect the Rx coax patch cable to the corresponding Rx patch panel port below the line card slot.

If you are adding an Rx-only line card:

- Step 1 Connect the Rx coax patch cable to the line card's Rx In port.
- Step 2 Connect the Rx coax patch cable to the corresponding Rx patch panel port below the line card slot.

If you are adding a private hub or mini hub:

- Step 1 Connect the Rx cable to the Rx In port on the back panel.
- Step 2 Connect the Tx cable to the Tx Out port on the back panel.

## 14.7 Perform 1 dB Compression Point Test with the Satellite Operator

This step determines the maximum transmit power level at which line card or private hub operates before starting to saturate the BUC. This test should not be necessary if your teleport is using an SSPA or a BUC with more than five watts of power. However, if you are using a BUC with five watts of power or less, this test should be performed to ensure that you do not overdrive the BUC.

The 1 dB Compression Point test is performed at the direction of the satellite operator using a CW carrier. The satellite operator should inform you of the transmit frequency for the test.

To perform the test, follow these steps:

- Step 1 If you do not have a console connection to the line card, establish one now by following the steps in [section 14.4](#) on [page 237](#). (Note that the IP address that you configured for your line card should now be loaded on the line card. You may need to reconfigure the IP address of your PC to match the new subnet.)
- Step 2 Set the transmit frequency of the line card by typing:

```
tx freq <fx>
```

where *fx* represents the L band frequency in MHz.

- Step 3 Set the initial transmit power of the line card by typing:

```
tx power <pwr>
```

where *pwr* represents the power setting in dBm. Typically you should begin with a low value such as -25 dBm to minimize the chance of interfering with other carriers.

- Step 4 Turn on a CW signal by typing:

```
tx cw on
```

At this point the satellite operator should see your signal.

- Step 5 While the satellite operator is observing your CW carrier, increase the transmit power in 1 dBm increments until a 1 dBm change in power no longer results in a corresponding 1 dBm change in signal strength as measured by the satellite operator. The last point at which the CW changes by 1 dB is the 1 dB compression point.

- Step 6 Disable the CW signal by typing:

```
tx cw off
```

## 14.8 Set the Transmit Power for the Outroute

Work with the satellite operator to determine the contracted power at the satellite.



### NOTE

The **tx pn** commands in these steps are used to transmit a modulated carrier at the configured data rate, FEC rate, and modulation. The satellite operator may request you to transmit a CW carrier rather than a modulated carrier. In that case, replace the **tx pn** commands with **tx cw on** and **tx cw off**. Note, however, that iDirect recommends using a modulated carrier to set the transmit power.



### NOTE

Whenever **tx pn** or **tx cw** commands are used, you must reset the line card to restore normal operation. Be sure to follow the instructions in the next section to reset your line card after applying the configuration.

- Step 1 If you do not have a console connection to the line card, establish one now by following the steps in [section 14.4](#) on [page 237](#).

Step 2 Configure the line card to transmit at the frequency indicated by the satellite operator by typing:

```
tx freq <fx>
```

where *fx* represents the L band frequency in MHz.

Step 3 Configure the line card to transmit a signal with pseudo-random data by typing:

```
tx pn on
```

Step 4 Working with the satellite operator, adjust the transmit power to achieve the contracted power at the satellite. To change the tx power to a new value, type:

```
tx power <pwr>
```

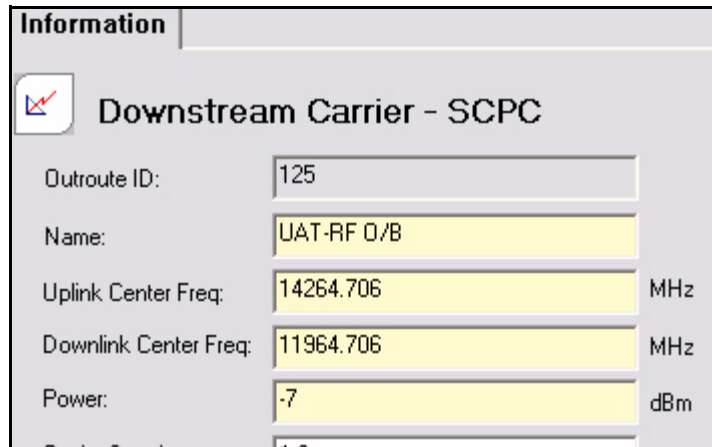
where *pwr* represents the power setting in dBm.


Step 5 Disable the PN carrier by typing:

```
tx pn off
```

Step 6 Open iBuilder and select the line card in the Network Tree. Then select **Modify → Assigned Downstream Carrier** from the context menu.

Step 7 In the **Downstream Carrier** dialog box, enter the value for **Power** determined in [step 4](#).



Information	
 <b>Downstream Carrier - SCPC</b>	
Outroute ID:	125
Name:	UAT-RF D/B
Uplink Center Freq:	14264.706 MHz
Downlink Center Freq:	11964.706 MHz
Power:	-7 dBm



## NOTE

For an iSCPC downstream, the transmit power is configured in the **Transmit Properties** section of the iSCPC line card modify dialog box. Click the iSCPC line card in the network tree and select **Modify→Item** to display that screen.

Step 8 Exit the console window by typing:

`exit`

Step 9 You can disconnect the console cable at this time.

## 14.9 Connect to the LAN and Apply the Line Card Configuration

Connect your line card to the LAN and apply the updated configuration.

Step 1 Connect the Ethernet to the LAN A port on the line card or private / mini hub.

Step 2 In iBuilder, right-click the line card in the network tree and select **Apply** → **Configuration** from the menu. Select the option to **Reset** your line card.

## 14.10 Set the Clear Sky C/N Parameter for a Mesh Outroute

If you are configuring a mesh outroute, you must use iMonitor to determine the value of the SCPC loopback clear sky C/N. You will then use iBuilder to configure that value for the outroute.



### NOTE

You must determine the clear sky C/N value under clear sky conditions at the hub.



### WARNING

Following this procedure while the hub is in a rain fade will adversely affect the performance of uplink power control. This can cause your remote modems to overdrive the power on the satellite.

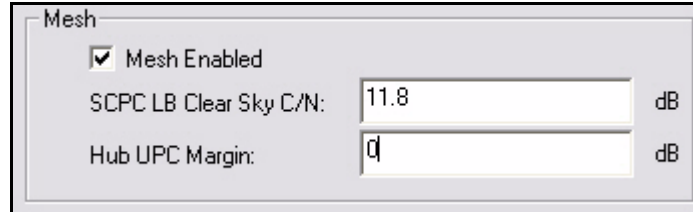
Follow these steps to determine and set the outroute **SCPC LB Clear Sky C/N** parameter in iBuilder:

Step 1 In iMonitor, right-click the line card in the network tree and select **Line Card Stats**. Then click **OK** in the **Select Items** dialog box. (The line card should already be selected in the **Line Cards** area of the dialog box.)

Step 2 In the **Hub Stats Results** pane, determine the value for **SCPC LB C/N [dB]**.

Time	Name	Type-SN	Tx Attempts	Tx Bytes	SCPC LB C/N [dB]
2/27/2006 9:06:16 AM	Mesh HLC(2...	M1D1.2076	66	3068	11.88
2/27/2006 9:06:36 AM	Mesh HLC(2...	M1D1.2076	76	3736	11.84
2/27/2006 9:06:56 AM	Mesh HLC(2...	M1D1.2076	66	2996	11.87
2/27/2006 9:07:16 AM	Mesh HLC(2...	M1D1.2076	82	4314	11.88
2/27/2006 9:07:36 AM	Mesh HLC(2...	M1D1.2076	345	192985	11.88
2/27/2006 9:07:56 AM	Mesh HLC(2...	M1D1.2076	604	318320	11.77

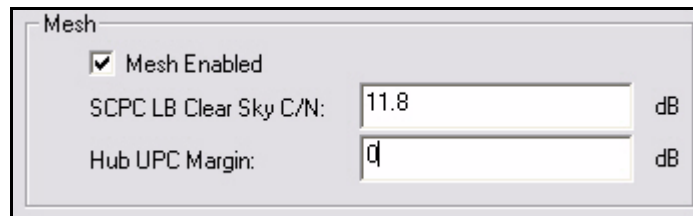
- Step 3 In iBuilder, right-click the line card in the network tree and select **Modify → Configuration**.
- Step 4 In the Line Card Modify dialog box, enter the value for **SCPC LB Clear Sky C/N** determined in [step 2](#).



## 14.11 Set the UPC Margin for a Mesh Outroute

Determine from the hub operator the amount of margin, in dB, that is built into the teleport's UPC system. iDirect uses this value in its power control algorithm. Once you have determined the margin, follow these steps to enter that value into iBuilder as the **Hub UPC Margin** for your mesh outroute:

- Step 1 In iBuilder, right-click the line card in the network tree and select **Modify → Configuration**.
- Step 2 In the Line Card Modify dialog box, enter the **Hub UPC Margin**.



## 14.12 Set the Clear Sky C/N Parameters for a Mesh Inroute Group

When commissioning the first remote on a mesh inroute, you must set the clear sky C/N parameter for the inroute group *before* setting the initial transmit power for the remote. To accurately determine the value for clear sky C/N, you must first configure a custom key to disable uplink power control. Once clear sky C/N is entered, you must delete the key to re-enable uplink power control.

For complete instructions on remote commissioning, including mesh remotes, see the [Installation and Commissioning Guide for iDirect iNFINITI Series Satellite Routers](#).

Follow the steps in this section to correctly set the clear sky C/N for the mesh inroute group.



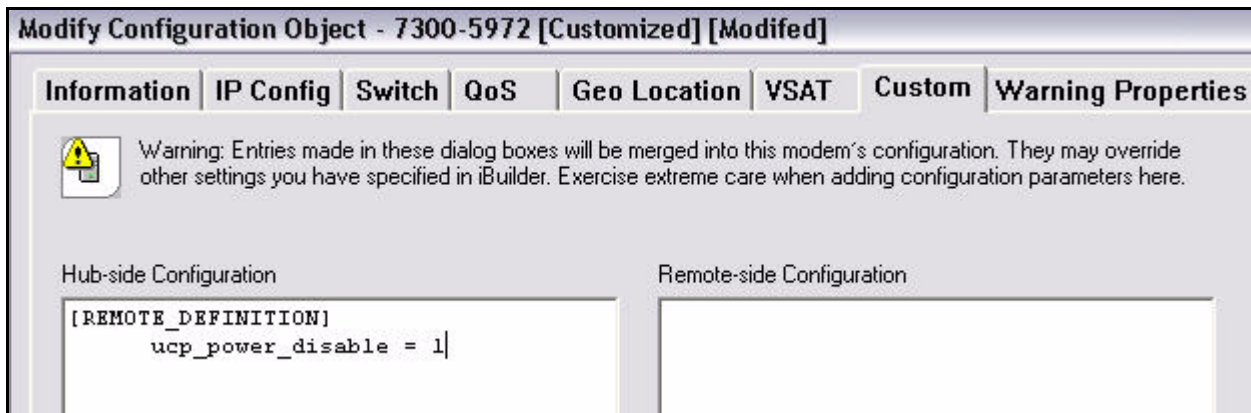
### NOTE

This procedure only applies during commissioning of the *first* mesh remote in a mesh inroute group. It should be performed after the remote has been acquired by the hub but before setting the initial transmit power in iBuilder.



- Step 1 In iBuilder, right-click the remote in the network tree and select **Modify** → **Item**.
- Step 2 Select the **Custom** tab in the Modify Remote dialog box.
- Step 3 Configure the following custom key under **Hub-side Configuration**:  

```
[REMOTE_DEFINITION]
ucp_power_disable = 1
```

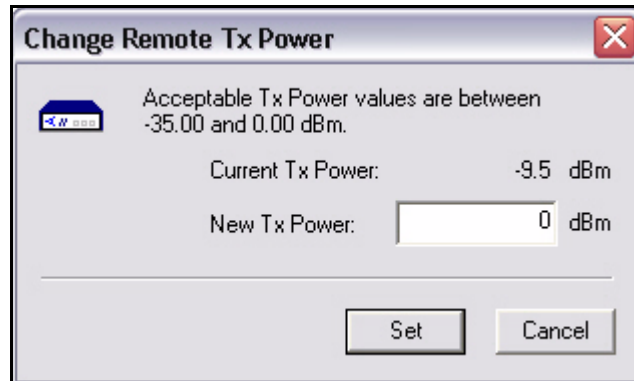


- Step 4 Right-click the remote in the network tree and apply the hub-side configuration.
- Step 5 In iMonitor, right-click the remote in the network tree and select **Probe** from the menu.
- Step 6 In the **Remote Power** area of the screen, click the **Change** button.



- Step 7 Working with the satellite operator, adjust the transmit power of the remote until the contracted Tx Power on the satellite is reached for the TDMA

carrier. Adjust the power by entering a power setting in **New Tx Power** and clicking the **Set** button.



Step 8 In iMonitor, right-click the mesh remote in the network tree and select **Control Panel** from the menu.

Step 9 Select the **UCP Info** tab.

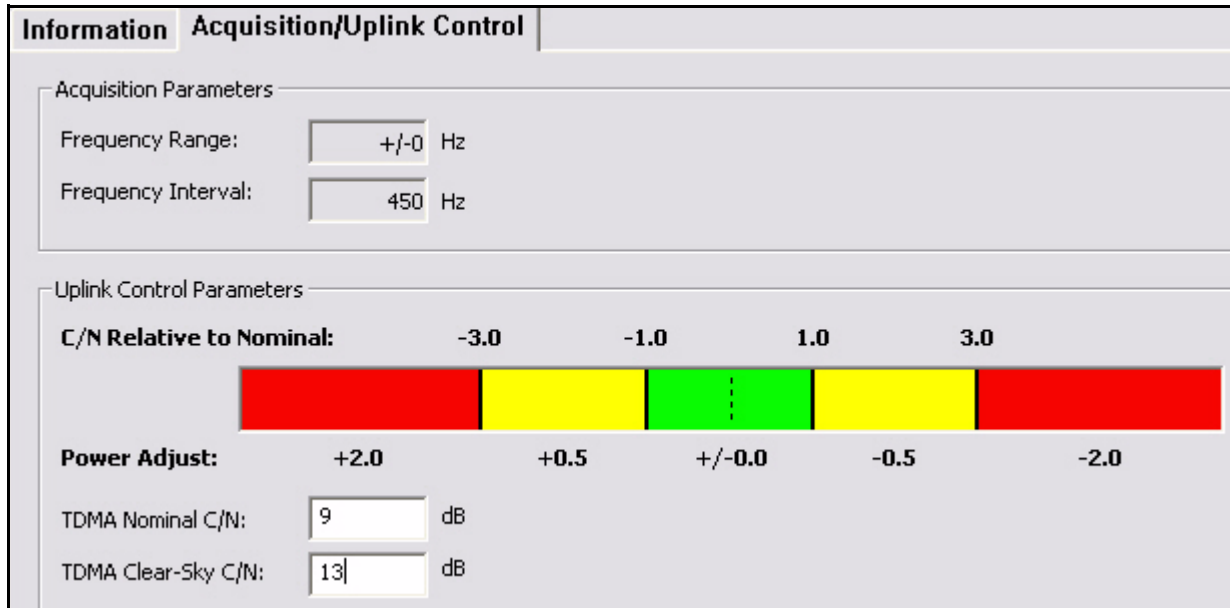
Step 10 Record the average value displayed in the column **Up C/N [db]**.

Time	Date	Up C/N [dB]	Power Adjustment...	Symbol Off...	Freq Offset [Hz]
09:02:19	02/07/06	13.32	0.0	3	1
09:02:39	02/07/06	13.68	0.0	3	1
09:02:59	02/07/06	13.66	0.0	3	1
09:03:19	02/07/06	13.29	0.0	3	3
09:03:39	02/07/06	13.29	0.0	3	-2
09:03:59	02/07/06	13.14	0.0	3	1
09:04:19	02/07/06	13.08	0.0	3	1
09:04:39	02/07/06	13.29	0.0	3	1
09:04:59	02/07/06	12.80	0.0	3	1
09:05:19	02/07/06	13.08	0.0	3	1
09:05:39	02/07/06	13.16	0.0	3	3
09:05:59	02/07/06	13.02	0.0	3	3
09:06:19	02/07/06	12.63	0.0	3	2

Step 11 In iBuilder, right-click the inroute group in the network tree and select **Modify → Item** from the menu.

Step 12 Select the Acquisition/Uplink Control tab.

Step 13 In **TDMA Clear Sky C/N**, enter the value recorded for **Up C/N [dB]** from iMonitor.



**Information** **Acquisition/Uplink Control**

Acquisition Parameters

Frequency Range:  Hz

Frequency Interval:  Hz

Uplink Control Parameters

**C/N Relative to Nominal:** -3.0 -1.0 1.0 3.0

**Power Adjust:** +2.0 +0.5 +/-0.0 -0.5 -2.0

TDMA Nominal C/N:  dB

TDMA Clear-Sky C/N:  dB

Step 14 In iBuilder, right-click the remote in the network tree and select **Modify → Item**.

Step 15 Select the **Custom** tab in the Modify Remote dialog box.

Step 16 Delete the following custom key:

```
[REMOTE_DEFINITION]
```

```
ucp_power_disable = 1
```

Step 17 Right-click the remote in the network tree and apply the hub-side configuration by selecting **Apply Configuration → Reliable Hub-Side (TCP)** from the menu.

## 14.13 Set the TDMA C/N Nominal Parameter for an Inroute Group

Whenever you add an inroute group, you should set the **TDMA C/N Nominal** parameter on the **Acquisition/Uplink Control** tab for that inroute group according to the TDMA carrier modulation type. The value for **TDMA C/N Nominal** is determined based on the link budget analysis for your network, which takes into consideration the modulation and FEC rate of the carrier.

For details on setting this parameter in iBuilder, see [“Adding an Inroute Group” on page 109](#).



## 15 Adding Mesh Capabilities to a Star Network

Converting a star network to support mesh traffic will require changes to your existing inroute groups, inroutes and remotes. This chapter documents the prerequisites and procedures for a successful conversion from a network that supports star traffic only to one that can also carry mesh traffic. It discusses the following topics:

- [“Prerequisites for Converting an Existing Star Network to Mesh” on page 253](#)
- [“Recalibrating a Star Outbound Channel for Mesh” on page 253](#)
- [“Converting a Star Inbound Channel to Mesh” on page 254](#)
- [“Reconfiguring Star Remotes to Carry Mesh Traffic” on page 255](#)

### 15.1 Prerequisites for Converting an Existing Star Network to Mesh

Prior to converting an existing star network to carry mesh traffic, the following actions should be taken:

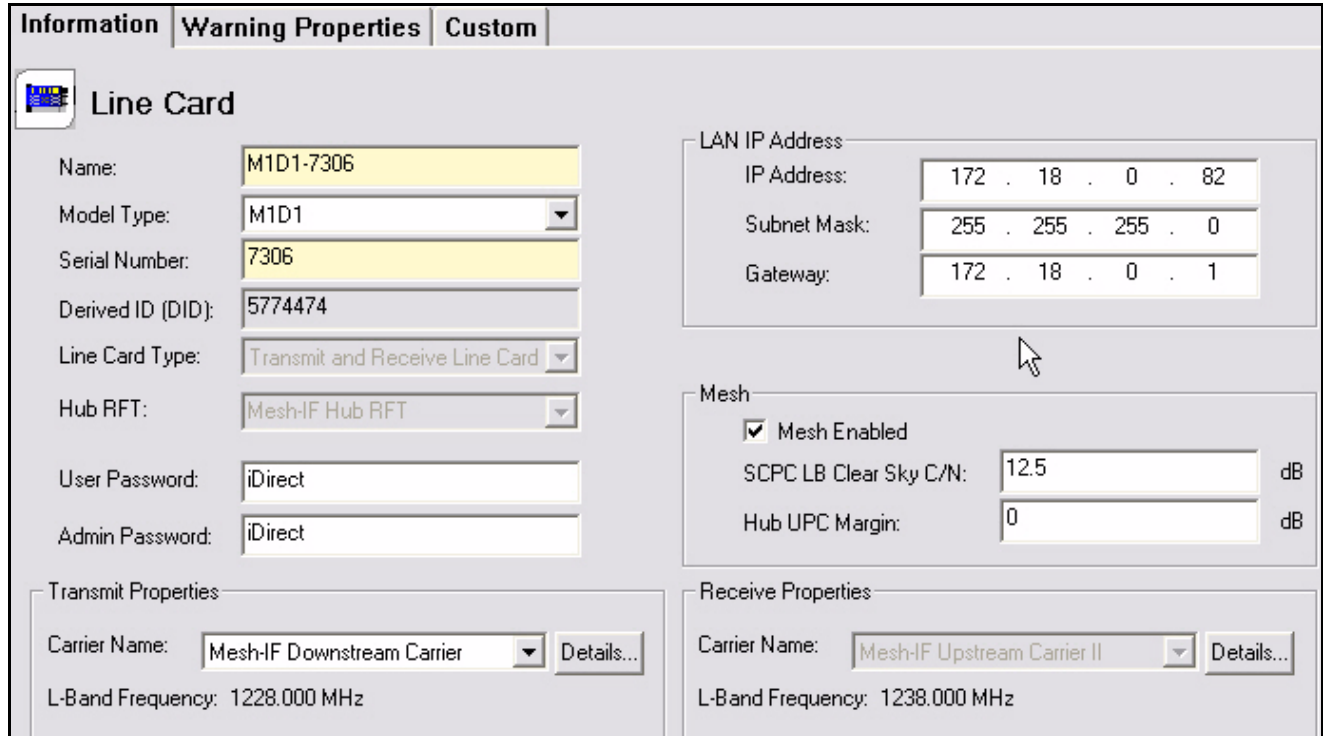
- Perform a new Link Budget Analysis (LBA) to ensure that the equipment is correctly sized to support mesh. This is discussed in detail in [chapter 3, “Mesh Technical Description,”](#) of the [iDirect Technical Reference Guide](#).
- Verify that the satellite transponder configuration for the hub and each remote is able to support the mesh architecture. All hubs and remotes must lie in the same geographic footprint so that they are able to receive their own “loopback” transmissions to the satellite. This requirement precludes the use of the majority of spot beam and hemi-beam transponders for mesh networks.
- Verify that all of the following mesh hardware requirements are met:
  - A Private Hub supporting mesh must use an externally referenced PLL LNB
  - An M1D1 line card must be used to transmit the mesh outroute.
  - An M1D1 line card or M0D1 line card must be used to receive the mesh inroute. (This line card can be the same M1D1 line card used for the mesh outroute.)
  - All mesh remotes must be equipped with PLL LNBs.
  - Each remote BUC and antenna must be properly sized to close link budget for a given data rate.
  - A mesh remote must be an iNFINITI 5300 or 7300 series modem.

For a detailed discussion of these prerequisites, see [chapter 3, “Mesh Technical Description,”](#) of the [iDirect Technical Reference Guide](#).

### 15.2 Recalibrating a Star Outbound Channel for Mesh

If you plan to use an existing M1D1 transmit line card to support mesh remotes, you must recalibrate the line card to determine the clear sky C/N values, and reconfigure the line card in iBuilder. Follow these steps to recalibrate a star outroute to support mesh remotes:

- Step 1 Right-click the M1D1 line card in the iBuilder's tree and select **Modify→Configuration** from the menu.
- Step 2 When the **Line Card** dialog box appears, select the **Mesh Enabled** check box in the **Mesh** area of the screen.



- Step 3 Click the M1D1 line card in the iBuilder's tree and select **Modify→Configuration** from the menu.
- Step 4 Configure the Uplink Power Control (UPC) parameters for the mesh outroute:
  - a Follow the steps in [section 14.10](#) on [page 247](#) to determine and set the **SCPC LB Clear Sky C/N** parameter for the mesh outroute.
  - b Follow the steps in [section 14.11](#) on [page 248](#) to determine and set the **Hub UPC margin** for the mesh outroute.

### 15.3 Converting a Star Inbound Channel to Mesh

You can configure either an M1D1 line card or an M0D1 line to receive a mesh inroute. The same M1D1 line card that transmits the mesh outroute can also receive the mesh inroute.

Whether you are converting an existing inroute to mesh or adding a new mesh inroute, you must calibrate the inbound carrier and set the Clear Sky C/N parameters for the mesh inroute group. This must be performed during commissioning of the first mesh remote in the inroute group.

For details on how to calibrate the inbound channel to support mesh, see [section 14.12](#) on [page 248](#).



**NOTE**

Subsequent mesh inbound channels can be calibrated and added to the network without affecting existing outbound or inbound channels.



**NOTE**

There can only be a single inroute in any mesh inroute group.

## 15.4 Reconfiguring Star Remotes to Carry Mesh Traffic

This section describes the steps necessary to reconfigure an existing star remote to carry mesh traffic. Once the remote has been reconfigured for mesh, it will be able to send and receive single-hop traffic to and from other remotes in the mesh inroute group.

Reconfiguring a star remote for mesh involves the following steps:

- Enabling the remote for mesh in iBuilder
- Recommissioning the initial transmit power of the remote and entering the new value in iBuilder. (This can be achieved without personnel at the remote site.)
- Determining the outbound and inbound Clear Sky C/N parameters for the remote and entering them in iBuilder

Enabling Mesh for a remote in iBuilder automatically configures the second demodulator on the remote to receive the mesh inroute. When you apply the new configuration, inroute parameters such as the carrier frequency, symbol rate, and FEC rate are sent to the remote.

The remote C/N at the hub will typically be higher in a mesh network than in a star network. The UPC algorithm adjusts the transmit power of all remotes to operate within a common C/N range at the hub. A remote with a C/N significantly higher or lower than this range will not acquire into the network.

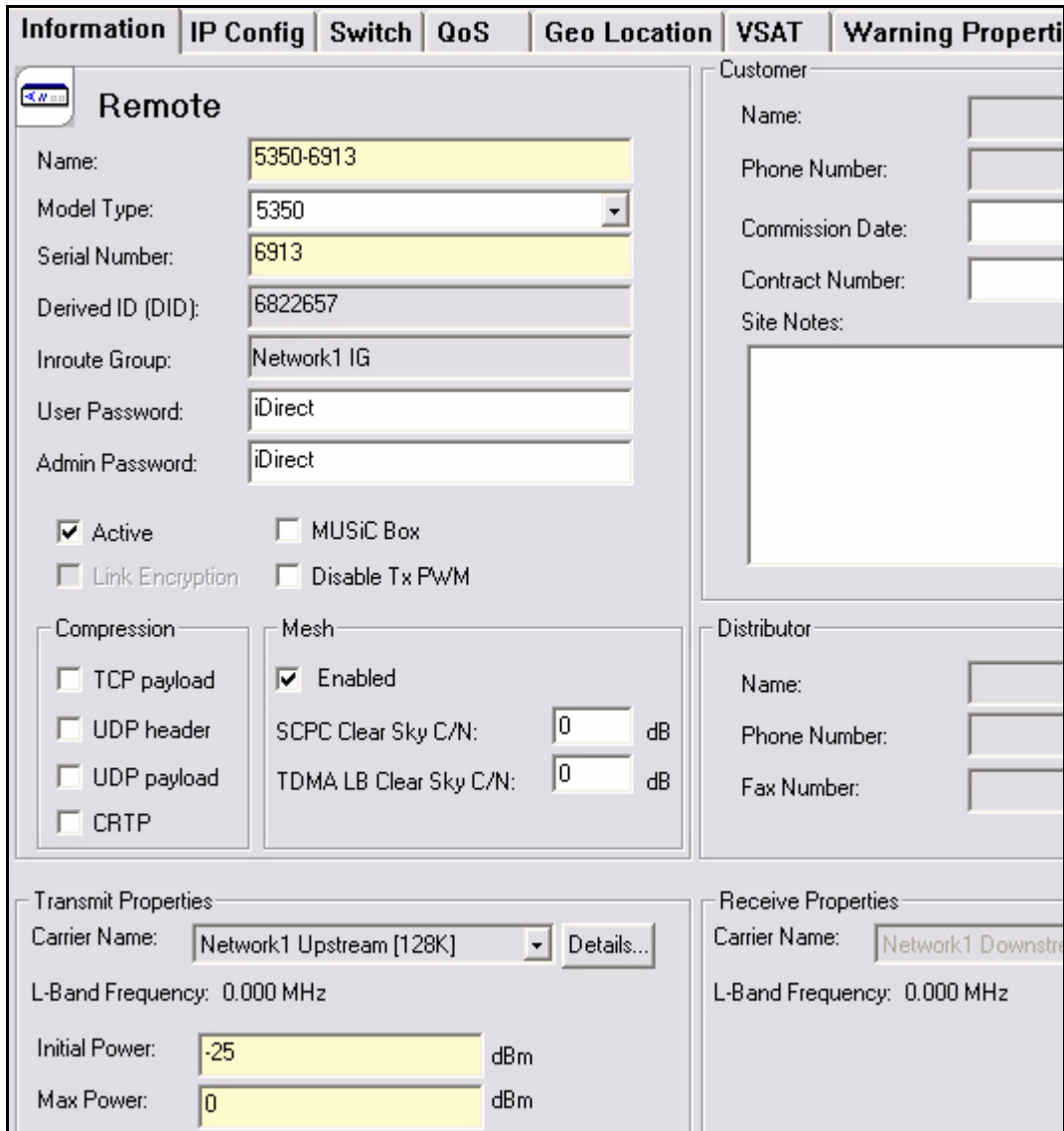


**NOTE**

Incorrect commissioning of a remote may prevent the remote from acquiring into the network.

Follow these steps to configure an existing remote to carry mesh traffic:

- Step 1 Right-click the remote in the network tree and select **Modify**→**Item** to display the Remote Modify dialog box.



- Step 2 In the **Mesh** section of the screen, select **Enabled**.
- Step 3 To determine and set the new initial power for the remote follow the steps in [Section 13.2 “Set the Initial Tx Power for a Remote”](#) of the [Installation and Commissioning Guide for iDirect iNFINITI Series Satellite Routers](#).
- Step 4 To set the Clear Sky C/N parameters for the remote, follow the steps in [Section 13.3 “Set the Clear Sky C/N Parameters for a Mesh Remote”](#) of the [Installation and Commissioning Guide for iDirect iNFINITI Series Satellite Routers](#).





**NOTE** Once recommissioned for mesh, a remote will typically have a higher initial transmit power setting than it had in the star network.



**NOTE** A similar procedure should be followed when moving a remote from a mesh network to a star network, i.e. the initial Tx power should be adjusted to accommodate the star requirements.



## Appendix A Configuring a Distributed NMS Server

You can distribute your NMS server processes across multiple IBM e-server machines. The primary benefits of machine distribution are improved server performance and better utilization of disk space.

iDirect recommends a distributed NMS server configuration once the number of remotes being controlled by a single NMS exceeds approximately 800. iDirect has certified the new distributed platform for up to 3000 remotes with iDS 7.0. This number should increase with future releases.

### A.1 Prerequisites

Before you begin the configuration process, ensure that you have the following in place:

- Four NMS e-servers, each installed with the same version of NMS software; three of these servers are used for running various services and the fourth is used as a backup server. If you already have a single Primary NMS server and a single Backup NMS server in place, you will need to add two more NMS servers with the same version of software the current Primary NMS is running.
- IP addresses for all additional NMS servers must be on the same subnet as the Primary and Backup servers. These servers are on the upstream side.
- If the NMS servers have private IP addresses and you need to access these servers (for running iBuilder and iMonitor) externally, then you have the following options: configure a VPN system to allow access to the servers, or NAT the private addresses to the public addresses and run the iDirect provided script on every client PC that will run iBuilder and iMonitor clients. See [“Running the NAT Script” on page 268](#) for the script.

### A.2 Distributed NMS Server Architecture

The distributed NMS architecture allows you to match your NMS server processes to e-server machines however you want. For example: you can run all server processes on a single platform (the current default); you can assign each server process to its own machine; or you can assign groups of processes to individual machines.

Server configuration is performed one time using a special script distributed with the **nms\_servers** installation package. Once configured, the distribution of server processes across machines will remain unchanged unless you reconfigure it. This is true even if you upgrade your system.

The only supported distribution scheme is shown in the figure below.

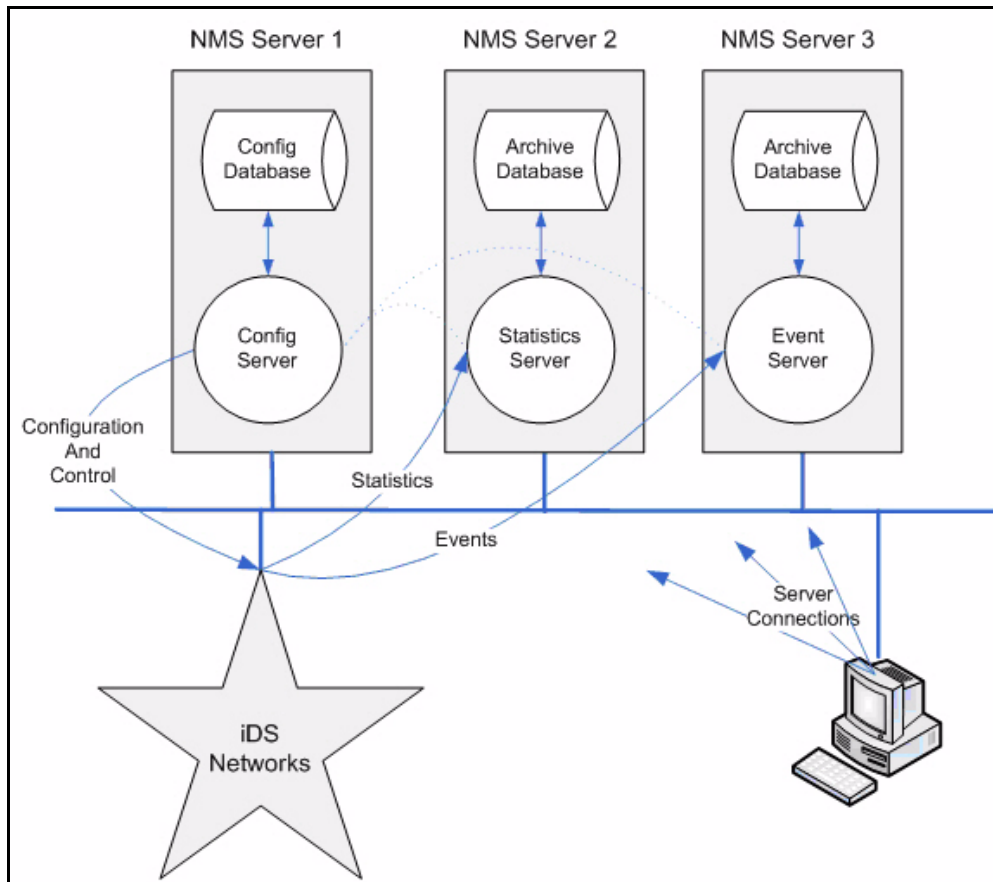


Figure A-1: Sample Distributed NMS Configuration

This configuration has the following process distribution:

- NMS Server 1 (Primary) runs the configuration server (**cfgsvr**), and the Protocol Processor controller process.
- NMS Server 2 (Auxiliary) runs only the Statistics server (**nrdsvr**).
- NMS Server 3 (Auxiliary) runs the Event server (**evtsvr**) and the Latency Server (**latsvr**). The **latsvr** is not shown in this diagram.

### A.3 Logging on to iBuilder and iMonitor

From the iBuilder or iMonitor user's perspective, a distributed NMS server functions identically to a single NMS server. In either case, users provide a user name, password, and the IP address or Host Name of the NMS configuration server when logging in. The configuration server stores the location of all other NMS servers and provides this information to the iBuilder or iMonitor client. Using this information, the client automatically establishes connections to the server processes on the correct machines.

## A.4 Setting up a Distributed NMS Environment

You may set up or modify a Distributed NMS environment at any time while your network remains operational. However, you will be required to stop your NMS server processes briefly and restart them on the new machine(s) for the new configuration to take effect.



### NOTE

There is a slight probability that problems will occur if the database server process should exit during the reconfiguration. You can avoid this possibility by stopping your NMS processes prior to setting up the new configuration. In that case, the NMS outage will be slightly longer.

To configure a distributed NMS, you will run the script **NMS-configuration-client.pl**. This script resides on the primary NMS server. When executed, it queries the local subnet, determining the IP addresses of all NMS server machines and the current assignment of NMS processes to server machines. The script then asks you to specify the new distribution and updates the assignments before exiting. You then restart the NMS processes.

To configure a distributed NMS and retain historical data, begin with Step 1. To configure a distributed NMS and *not* retain historical data, begin with Step 9.

- Step 1 Verify that all four servers are configured with correct IP addresses, there is IP connectivity between all the of the servers, and that iDirect NMS software is installed on each server such that NMS server 1, 2, and 3 are installed as primary and NMS server 4 is installed as backup.
- Step 2 Log on to the NMS 2 as root.
- Step 3 Stop the NMS processes on the server by entering the following command:  

```
service idirect_nms stop
```
- Step 4 Repeat [Step 2](#) and [Step 3](#) on NMS 3.
- Step 5 Log on to the NMS 1 as root.
- Step 6 Change your directory as follows:  

```
cd /var/lib/mysql/nrd_archive
```
- Step 7 To copy the database from NMS 1 to NMS 2, enter the following command:  

```
scp * root@x.x.x.x:/var/lib/mysql/nrd_archive/
```

Where,  
  
**x.x.x.x** represents the IP address of NMS 2.
- Step 8 Repeat [Step 7](#) and replace **x.x.x.x** with the IP address of NMS 3.
- Step 9 Establish an SSH connection to the NMS 2 as root and convert it to the new configuration by entering the following command:

```
/home/nms/utils/db_maint/DB-Conversion.pl
```

Step 10 When the **DB-Conversion.pl** script completes, restart the NMS configuration by entering the following command:

```
service idirect_nms start nms_config
```

Step 11 Repeat [Step 9](#) and [Step 10](#) for NMS 3.

**The following steps must be done during a maintenance window as network downtime will occur.**

Step 12 Logon to NMS 1 as root.

Step 13 Stop the NMS services by entering the following command:

```
service idirect_nms stop
```

Step 14 Run the conversion script by entering the following command:

```
/home/nms/utils/db_maint/NMS-configuration-client.pl
```

The conversion script prompts you to select which services are to run on which servers. At a minimum, the **nrdsvr** runs on NMS 2; the **evtsvr** and the **latsvr** run on NMS 3. Then **nmssvr**, **nms\_config**, **nms\_monitor**, **cntrl**, **revsvr**, and **snmpsvr** run on NMS 1.

Enter the number of the respective NMS when prompted. Sample output is shown below.

```
root@x3550 ~
# /home/nms/utils/db_maint/NMS-configuration-client.pl

NMS Config Client >>> Looking for NMS installations with bcast
255.255.255.255, please wait...
=====
List of existing NMS configurations
=====
From NMS.ServerConfiguration on computer with 192.168.76.82 :
127.0.0.1      nms_cfg_server_ip
127.0.0.1      nms_evt_server_ip
127.0.0.1      nms_lat_server_ip
127.0.0.1      nms_nrd_server_ip

From NMS.ServerConfiguration on computer with 192.168.76.80 :
192.168.76.80 nms_cfg_server_ip
192.168.76.80 nms_evt_server_ip
192.168.76.80 nms_lat_server_ip
192.168.76.80 nms_nrd_server_ip

From NMS.ServerConfiguration on computer with 192.168.76.65 :
127.0.0.1      nms_cfg_server_ip
127.0.0.1      nms_evt_server_ip
```

```
127.0.0.1      nms_lat_server_ip
127.0.0.1      nms_nrd_server_ip
```

From NMS.ServerConfiguration on computer with 192.168.76.67 :

```
127.0.0.1      nms_cfg_server_ip
127.0.0.1      nms_evt_server_ip
127.0.0.1      nms_lat_server_ip
127.0.0.1      nms_nrd_server_ip
```

```
=====
List of IPs, where NMS installation was presented:
=====
```

```
192.168.76.82      (1)
192.168.76.80      (2)
192.168.76.65      (3)
192.168.76.67      (4)
```

```
NMS Config Client >>> Please enter index for MySQL server
                        (use number in parentheses above)
```

```
1
```

```
NMS Config Client >>> Server MySQL assigned to IP address
192.168.76.82
```

```
NMS Config Client >>> Please enter index for CFG server
                        (use number in parentheses above)
```

```
1
```

```
NMS Config Client >>> Server CFG assigned to IP address 192.168.76.82
```

```
NMS Config Client >>> Please enter index for EVT server
                        (use number in parentheses above)
```

```
3
```

```
NMS Config Client >>> Server EVT assigned to IP address 192.168.76.65
```

```
NMS Config Client >>> Please enter index for NRD server
                        (use number in parentheses above)
```

```
2
```

```
NMS Config Client >>> Server NRD assigned to IP address 192.168.76.80
```

```
NMS Config Client >>> Please enter index for LAT server
                        (use number in parentheses above)
```

```
3
```

```
NMS Config Client >>> Server LAT assigned to IP address 192.168.76.65
```

```
NMS Config Client >>> storing to NMS table ServerConfiguration
```

```
NMS Config Client >>> Done
```

Step 15 Start all services on NMS 1 by entering the following command:

```
service idirect_nms start
```

Step 16 Log on to NMS 2 and repeat [Step 15](#).

Step 17 Log on to NMS 3 and repeat [Step 15](#).

## A.5 Removing the SNMP Proxy Server from Auxiliary NMS Servers

Before you continue, you must remove the SNMP proxy service from NMS 2 and NMS 3. To remove the **snmpproxy** from NMS 2 and NMS 3, perform the following:

Step 1 Log into NMS 2 as root.

Step 2 Enter the following command:

```
rpm --erase nms_snmpproxy
```

The snmpproxy service is erased from the server.

Step 3 Verify that the **snmpproxy** service is no longer running by entering the following command:

```
service idirect_nms status
```

A list of all of the services that are running on the logged in machine displays.

Step 4 Repeat these steps for NMS 3.

The SNMP proxy service is removed from the servers.

## A.6 Regenerating the Options Files

Now that you have removed the SNMP proxy from the servers, you are ready to regenerate the options files. The steps to do this follow:

Step 1 Log on to NMS 1 as root.

Step 2 Enter the following command:

```
telnet 0 14123
```

Step 3 Enter the Username and Password when prompted as follows:

```
Username: admin
```

```
Password: iDirect
```

Step 4 Enter the following commands:

```
cfg status recalc netmodem.*
```

```
cfg status recalc rmtdef.*
```

```
cfg status recalc netdef.*
```

```
cfg status recalc ppglobal.*
```





## NOTE

Once these commands have been entered successfully, all the devices (remote, HLC, network, PP) will display “Changes Pending” in iBuilder. ***Downtime will be incurred while devices reboot.***

- Step 5 Launch iBuilder and apply the changes ***in the following order***: all remotes, all Hub Line Cards, network, and Protocol Processor.

## A.7 Granting Read Permissions to NMS 2 and NMS 3

Now that you have regenerated the options files, you are ready to grant “read” permissions to NMS 2 and NMS 3. Follow these steps to change the permissions:

- Step 1 Log on to NMS 1 and enter the following command:

```
mysql --exec='GRANT ALL ON *.* TO "root"@"x.x.x.x"'
```

Where,

**x.x.x.x** represents the IP address of NMS 2.

- Step 2 Enter the following commands to flush the register:

```
mysql --exec='FLUSH PRIVILEGES'
```

- Step 3 Repeat these steps and replace **x.x.x.x** with the IP address of NMS 3.

- Step 4 Restart the Event and NRD servers to force a reconnection to the config server using the new permissions.

To verify that the new permissions have been correctly configured, perform the following step on *both* NMS 2 and NMS 3:

- Step 1 Enter the following command from the command line prompt:

```
mysql --host=x.x.x.x
```

Where,

**x.x.x.x** represents the IP address of NMS 1.

If this command immediately connects you to the mysql prompt on NMS 1, then the new permissions have been correctly configured on the server from which you are connecting.

## A.8 Assigning QoS Profiles

Once you have set up your distributed NMS, you must redirect your IP packets for remote NMS traffic to the correct NMS servers by modifying the NMS Service Levels in your Upstream and Downstream Traffic Profiles.

For the Upstream Traffic Profile, modify the Service Levels as follows:

- Assign the destination IP address for NMS\_TCP to NMS 1
- Assign the destination IP address for NMS\_UDP to NMS 2
- Assign the destination IP address for NMS\_ICMP to NMS 3

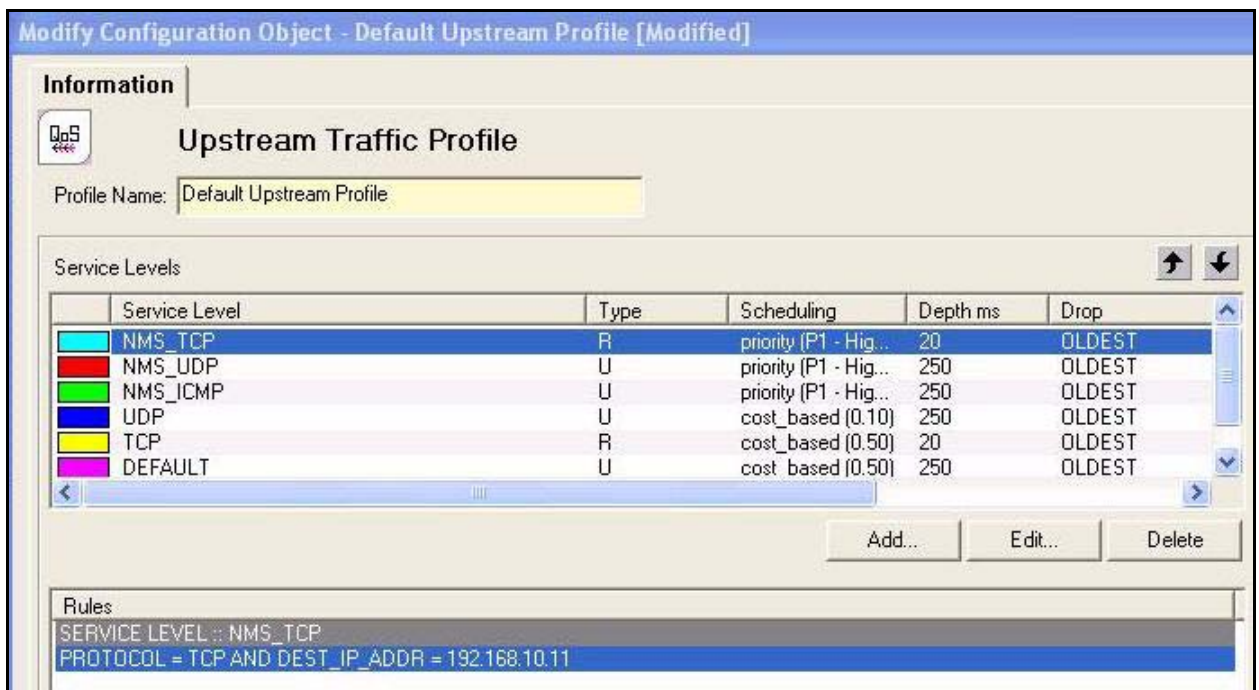
For the Downstream Traffic Profile, modify the Service Levels as follows:

- Assign the source IP address for NMS\_TCP to NMS 1
- Assign the source IP address for NMS\_ICMP to NMS 3

For each of the above Service Levels, (the Upstream Traffic Profile is shown in this example) follow these steps to reassign the destination IP address of the upstream traffic:

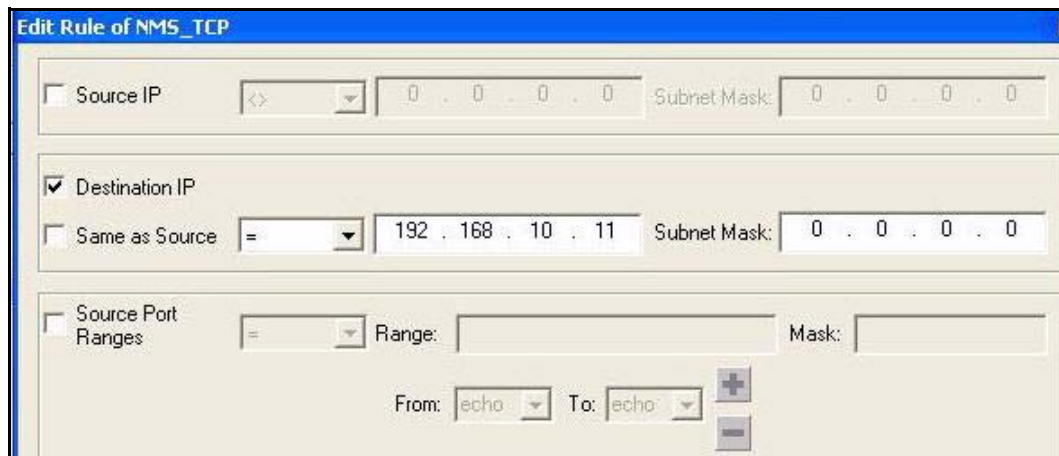
Step 1 In the iBuilder tree, right-click the Default Traffic Profile folder and select **Modify → Item**.

Step 2 In the **Service Levels** area of the dialog box, select the appropriate **Service Level** for the IP packet type you want to modify. (NMS\_UDP, NMS\_TCP or NMS\_ICMP).



Step 3 In the **Rules** area of the dialog box, select the Rule for that traffic and click the **Edit** button.

- Step 4 Change the Destination IP address to match the NMS server's IP address for this type of traffic. (TCP traffic must be routed to config server, UDP traffic to nrd server, and ICMP traffic to both evt server and lat server.)



- Step 5 There will be “Changes Pending” on all remotes. Apply the changes.

## A.9 Verifying Correct Operation

Now that you have completed the configuration steps, the **cfgsvr**, **nrdsvr**, **evtsvr**, and **latsvr** should all be running on the appropriate servers. To ensure proper operation, you must verify that no service is running on more than one server. Enter the following command on each server and verify that the correct services are running:

```
ps -ef | grep svr | grep -vi mysql | grep -vi logger
```

A list of running services displays.

If a service is running on a server that it should not be, use the following command to kill the service:

```
killall service
```

Where,

***service*** represents the name of the service

For example, if the **evtsvr** process is running on NMS 1, enter the following command to kill the process:

```
killall evtsvr
```

Verify that your servers are configured to run dbBackup and dbRestore. For configuration procedures, refer to the *iDirect NMS Redundancy* technical note, which is available for download on the TAC web page located at <http://tac.idirect.net>.

## A.10 Running the NAT Script

The iDirect NAT script translates private IP addresses to public IP address so that you can run iBuilder and iMonitor from an external source. This section describes how to run the script for iBuilder and iMonitor.

The steps for running the script for iBuilder are as follows:

- Step 1 On your PC or laptop, open Note Pad.
- Step 2 Copy the following lines into Note Pad:

```
@ECHO OFF
SET ENV_NRD_NMSAPI_IPADDR= x.x.x.x
```

Where,

**x.x.x.x** represents the IP address of NMS 2

```
SET ENV_EVT_NMSAPI_IPADDR= x.x.x.x
```

Where,

**x.x.x.x** represents the IP address of NMS 3

```
SET ENV_LAT_NMSAPI_IPADDR= x.x.x.x
```

Where,

**x.x.x.x** represents the IP address of NMS 3

```
ibuilder.exe
```

- Step 3 Rename the Note Pad file to **ibuilder.bat**.
- Step 4 Save the file to the same directory where iBuilder is located.

The steps for running the script for iMonitor are as follows:

- Step 1 On your PC or laptop, open Note Pad.
- Step 2 Copy the following lines into Note Pad:

```
@ECHO OFF
SET ENV_NRD_NMSAPI_IPADDR= x.x.x.x
```

Where,

**x.x.x.x** represents the IP address of NMS 2

```
SET ENV_EVT_NMSAPI_IPADDR= x.x.x.x
```

Where,

```
x.x.x.x represents the IP address of NMS 3  
SET ENV_LAT_NMSAPI_IPADDR= x.x.x.x
```

Where,

```
x.x.x.x represents the IP address of NMS 3  
imonitor.exe
```

Step 3 Rename the Note Pad file to **iMonitor.bat**.

Step 4 Save the file to the same directory where iMonitor is located.

## A.11 Managing a Distributed NMS

The various forms of the **NMS-configuration-client.pl** command are shown here. It is unlikely that you will need to use any command arguments when configuring your distributed NMS.

```
# ./NMS-configuration-client.pl -h
```

```
NMS-configuration-client.pl [-cd=NAME] [-ad=NAME]  
[-udp=UDPPORT] [-bcast=BCASTADDRESS]
```

```
-cd : Change config database from [nms]  
-ad : Change archive database from [nrd_archive]  
-udp: Change default UDP port [70123]  
  
-bcast: Change default bcast address[255.255.255.255]
```

The **NMS-domain-commands.pl** command stops, starts or restarts the NMS server processes on all NMS machines. You can run the command on any of the server machines.

The various command forms are:

```
# ./NMS-domain-commands.pl -h
```

Usage:

```
NMS-domain-commands.pl [-udp=UDPPORT] [-exec="<command> <server name>  
<server name> ..."]
```

```
-udp      : Change default UDP port [70123]
```

```
<command> is <start | stop | restart | reload | status >
```

```
<server name> is <nmssvr | evtsvr | nrdsvr | latsvr | cntrlsvr | snmpsvr  
| nms_monitor>
```

For example, the following two commands show the status of NMS server processes. The first example shows the status of all processes. The second example shows the status of the **nms\_monitor** process.

```
./NMS-domain-commands.pl -exec="status"  
./NMS-domain-commands.pl -exec="status nms_monitor"
```

The following three commands start, restart and stop server processes, respectively. The first example starts the evtsvr process. The second example restarts the latsvr process. The final example stops all processes.

```
./NMS-domain-commands.pl -exec="start evtsvr"  
./NMS-domain-commands.pl -exec="restart latsvr"  
./NMS-domain-commands.pl -exec="stop"
```

An example of the output for NMS-domain-commands.pl script is presented below:

```
# ./NMS-domain-commands.pl -exec="status"  
+++++  
Using configuration from MySQL NMS.ServerConfiguration table on computer  
127.0.0.1:  
  
>>>> 10.11.64.71:  
nms_config (pid 22540) is running...  
nmssvr is stopped  
cntrlsvr is stopped  
latsvr (pid 22596) is running...  
snmpsvr is stopped  
nms_monitor is stopped  
  
>>>> 10.11.64.72:  
nms_config (pid 1628) is running...  
evtsvr (pid 1744) is running...  
nrdsvr (pid 1681) is running...  
snmpsvr (pid 1712) is running...  
nms_monitor is stopped
```

## A.12 dbBackup/dbRestore and the Distributed NMS

The **dbBackup** and **dbRestore** scripts are completely compatible with the new distributed NMS. You may choose to have one-for-one or one-for-n redundancy for your NMS servers.

One-for-n redundancy means that one physical machine will back up all of your active servers, If you choose this form of redundancy, you must modify the **dbBackup.ini** file on each NMS server to ensure that the separate databases are copied to separate locations on the backup machine.

The figure below **shows** three servers, each copying its database to a single backup NMS. If NMS 1 fails, you will not need to run dbRestore prior to switchover since the configuration data will have already been sent to the backup NMS. If NMS 2 or NMS 3 fails, you will need to run dbRestore

prior to the switchover if you want to preserve and add to the archive data in the failed server's database.

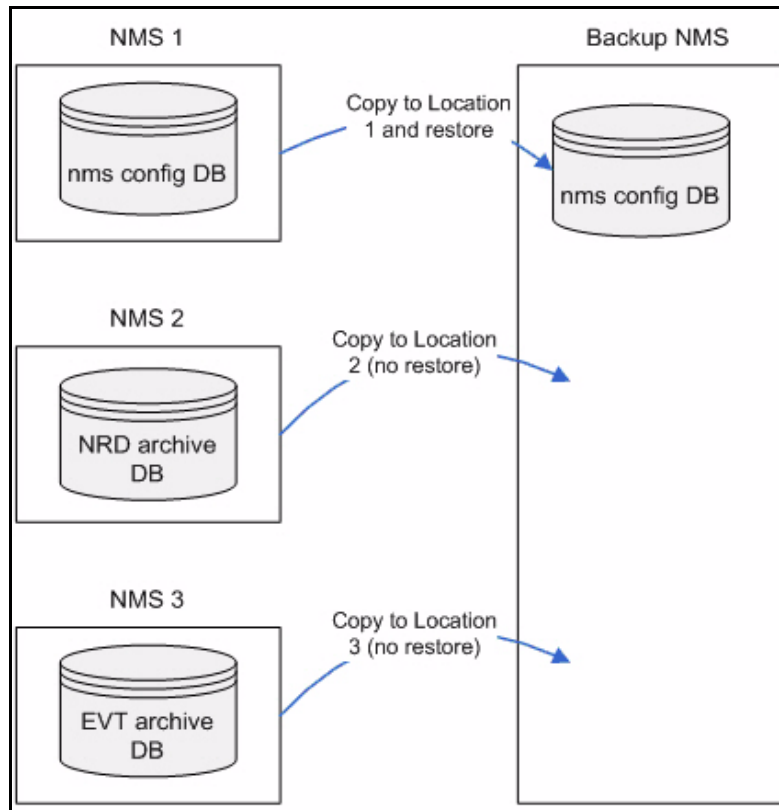


Figure A-2: dbBackup and dbRestore with a Distributed NMS





## Glossary of Terms and Acronyms

<b>Acquisition</b>	A process where by the satellite modem locks onto the proper satellite carrier.
<b>ACU</b>	Antenna control unit.
<b>ADC</b>	Analog-to-Digital Converter. A device that converts analog signals to a digital representation.
<b>Analog</b>	Method of signal transmission in which information is relayed by continuously altering the wave form of the electromagnetic current. An analog signal is responsive to changes in light, sound, heat and pressure. See also digital.
<b>Antenna</b>	Device for transmitting and receiving radio waves. Depending on their use and operating frequency, the form on an antenna can change from a single piece of wire to a dish-shaped device.
<b>Antenna Alignment (pointing)</b>	The process of optimizing the orientation of a satellite antenna's main direction of sensitivity towards the satellite to maximize the received signal level and to minimize the chance of receiving unwanted interference from other satellite systems.
<b>Aperture</b>	A cross sectional area of the antenna which is exposed to the satellite signal.
<b>Apogee</b>	Point in an elliptical satellite orbit that is farthest from the surface of the earth.
<b>Asynchronous</b>	A communications strategy that uses start and stop bits to indicate the beginning and end of a character, rather than using constant timing to transmit a series of characters. Asynchronous methods are especially efficient when traffic comes in bursts (and not regularly paced). Modems and terminals are asynchronous communications devices.
<b>Attenuation</b>	Weakening, usually measured in decibels, of a signal (loss) that occurs as it travels through a device or transmission medium (e.g. radio waves through the atmosphere).
<b>Attitude Control</b>	The orientation of the satellite in relationship to the earth and the sun.
<b>Azimuth</b>	The horizontal co-ordinate used to align the antenna to the satellite. See also Elevation.
<b>Bandwidth</b>	The amount of data a cable can carry; measured in bits per second (bps) for digital signals, or in hertz (Hz) for analog signals. A voice transmission by telephone requires a bandwidth of about 3000 cycles per channel (3KHz). A TV channel occupies a bandwidth of 6 million cycles per second (6 MHz) in terrestrial systems. In satellite based systems a larger bandwidth of 17.5 to 72 MHz is used to spread or "dither" the television signal in order to prevent interference.
<b>Baud</b>	The number of times an electrical signal can be switched from one state to another within a second.
<b>Bit Error Rate (BER)</b>	The ratio of the number of information bits received in error to the total number of bits received, averaged over a period of time. It is used as an overall measure of the quality of a received digital bit stream.

<b>Bit Rate</b>	The number of bits transmitted within a second (bps) in a digital communication.
<b>Broadcast</b>	Sending a single message to all the nodes of a network.
<b>C band</b>	Band of frequencies used for satellite and terrestrial communications. Most communications satellites use a range from 4 to 6 gigahertz (billion cycles per second). Requires larger ground antennas, usually twelve feet in diameter, for television reception.
<b>Capacity</b>	A proportion of the satellite's bandwidth which is used to establish one or more communication channel.
<b>Carrier</b>	The basic radio, television, or telephony transmit signal. The carrier in an analog signal.
<b>Carrier Frequency</b>	The rate at which the carrier signal repeats, measured in cycles per second (Hertz). This is the main frequency on which a voice, data, or video signal is sent. Microwave and satellite communications transmitters operate between 1 to 14 GHz.
<b>Channel</b>	A band of radio frequencies assigned for a particular purpose, usually for the establishment of one complete communication link, or a path for an electrical signal. Television signals require a 6 MHz frequency band to carry all the necessary picture detail. Channel frequencies are specified by governmental agencies.
<b>CIR</b>	See Committed Information Rate.
<b>Coaxial Cable</b>	A transmission line in which the inner conductor is completely surrounded by an outer conductor, so that the inner and outer conductor are coaxially separated. The line has a wide bandwidth capacity which can carry several television channels and hundreds of voice channels.
<b>Collocated (satellites)</b>	Two or more satellites occupying approximately the same geostationary orbital position. To a small receiving antenna the satellites appear to be exactly at the same place. The satellites are kept several kilometers apart in space to avoid collision.
<b>Committed Information Rate (CIR)</b>	The guaranteed network bandwidth availability.
<b>Common Carrier</b>	An organization which operates communications circuits. Common carriers include the telephone companies as well as the owners of the communications satellites.
<b>Communications Satellite</b>	A satellite in Earth orbit which receives signals from an Earth station and retransmits the signal to other Earth stations.
<b>COMSAT</b>	Communication Satellite Corporation, the U.S. signatory for INTELSAT.
<b>Continuous Wave (CW)</b>	Signal consisting of a single frequency especially used in testing satellite modems and antennas.
<b>Decibel (Db)</b>	The standard unit used to express the ratio of two power levels. It is used in communications to express either a gain or loss in power between the input and output devices.
<b>Decoder</b>	A television set-top device that converts an electronically scrambled television picture into a viewable signal.

<b>Delay</b>	The time it takes for a signal to go from the sending station through the satellite to the receiving station (around one-quarter of a second).
<b>Demodulator</b>	A satellite receiver circuit which extracts or “demodulates” the desired signals from the received carrier.
<b>Digital</b>	Representation of information as bits of data for transmission. Digital communications technology permits higher transmission speeds and a lower error rate than analog technology. As an analog signal is received and amplified at each repeater station, any noise is also amplified. A digital signal, however, is detected and regenerated (not amplified), and any noise is lost unless it corresponds to a value that the regenerator interprets as digital signal.
<b>Dish</b>	Slang for parabolic antenna.
<b>Downlink</b>	The part of the satellite communications link that involves signal retransmission from the satellite and reception on the ground. See also Uplink.
<b>Downstream Carrier</b>	Downstream carrier (synonymous to outbound carrier) is the carrier from the Hub to the remote modem, via the satellite.
<b>Duplex</b>	Two-way communications. The telephone line is full duplex in that both directions of communication occur at the same time. Walkie-talkie communications is half-duplex– only one party may transmit at a time.
<b>Earth Station</b>	A combination of devices (antenna, receivers) used to receive a signal transmitted by one or more satellites.
<b>Elevation</b>	The upward tilt (vertical coordinate) of a satellite antenna measured in degrees, required to align the antenna with the communications satellite. See also Azimuth.
<b>Elliptical Orbit</b>	Orbits in which the satellite path describes an ellipse, with the Earth located at one focus.
<b>Encoder</b>	A device used to electronically alter a signal so that it can only be understood on a receiver equipped with a special decoder.
<b>Equatorial Orbit</b>	An orbit with a plane parallel to the Earth's equator.
<b>Excess Information Rate (EIR)</b>	The bandwidth over and above the committed information rate that a device is allowed to use without guaranteeing that the data will always be delivered to its destination.
<b>FEC</b>	Forward Error Correction is an error correction method that adds redundant bits to a bit stream, so that the receiver can detect and correct errors in transmission.
<b>FEC Block</b>	The basic FEC unit is a FEC block.
<b>Feed</b>	1) The transmission of video content from a distribution center. 2)The feed system of an antenna.
<b>Focal Length</b>	Distance from the center feed to the center of the dish.
<b>Footprint</b>	The geographic area over which a satellite antenna receives or directs its signals.

<b>Free Slots</b>	Slots left in the dynamic sub-frame after all stream, guaranteed (CIR) and preemptive (EIR) bandwidth requests are satisfied. Free slots are allocated to all VSATs (up or down), except the master, in a round-robin fashion.
<b>Frequency</b>	The number of times that an alternating current goes through its complete cycle in one second of time. One cycle per second is also referred to as one hertz.
<b>Frequency Coordination</b>	A process designed to eliminate frequency interference between different satellite systems or between terrestrial microwave systems and satellites.
<b>Full duplex</b>	Transmission that occurs in both directions simultaneously over the communications media (e.g. telephone).
<b>Geostationary satellite</b>	An satellite orbiting Earth at such speed that it appears to remain stationary with respect to the earth's surface. See also Clarke Orbit.
<b>Geosynchronous satellite</b>	A satellite orbiting Earth at Earth's rotational speed and at the same direction. A satellite in geosynchronous orbit is known as a geosynchronous or geostationary satellite. The orbit is "synchronous" because the satellite makes a revolution in about 24 hours. The satellites are about 35,800 kilometers (22,350 miles) above Earth, and they appear to be stationary over a location.
<b>Ground Segment</b>	All the Earth stations that are operating within a particular satellite system or network.
<b>Ground Station</b>	A radio station, on or near the surface of the Earth, designed to transmit or receive to/from a spacecraft.
<b>Guaranteed Bandwidth</b>	The capability for transmitting continuously and reliably at a specified transmission speed. The guarantee makes it possible to send time-dependent data (such as voice, video, or multimedia) over the line.
<b>Guaranteed Slots</b>	Slots configured per VSAT and made available to that VSAT upon its request. When the queue is depleted, these slots are taken away by the master and distributed to other requesting VISNs as preemptive slots.
<b>Guard Band (guardband)</b>	A thin frequency band used to separate bands (channels) in order to prevent interference and signal leakage.
<b>Guard Channel</b>	Unused frequency space between carriers that prevents adjacent carriers from interfering each other.
<b>Half Duplex</b>	A communications form in which transmissions can go in only one direction at a time. With half-duplex operation, the entire bandwidth can be used for the transmission. In contrast, full-duplex operation must split the bandwidth between the two directions.
<b>High Band</b>	The upper part of the Ku band downlink frequency range, from 11.7 GHz to 12.75 GHz.
<b>HPA</b>	High Power Amplifier. Earth station equipment that amplifies the transmit RF signal and boosts it to a power level that is suitable for transmission over an earth-space link.

<b>Hub RFT</b>	Hub Radio Frequency Terminal - Equipment that includes the antenna, U/C (up Converter), D/C (Down Converter) HPA, and LNA, which provides the up and down conversion of signals in a satellite-based network.
<b>IF</b>	Intermediate Frequency. The frequency range 70 to 140 MHz used for the distribution of satellite signals from the LNB at the dish to the user's satellite receiver. It is always used in direct-to-home systems and is the most suitable for distribution of digital signals in communal systems – IF systems.
<b>Inbound Carrier</b>	See <b>Upstream Carrier</b> .
<b>Inclination</b>	The angle between the orbital plane of a satellite and the equatorial plane of the Earth.
<b>Indoor Unit (IDU)</b>	The satellite modem and indoor devices (in contrast to outdoor units, ODU).
<b>Information Rate</b>	The user data rate including IP headers plus iDirect overhead. The downstream overhead is approximately 2.75% of the information rate.
<b>INTELSAT</b>	International Telecommunications Satellite Organization. Agency that operates a network of satellites for international transmissions.
<b>Interfacility Link (IFL)</b>	The cable that connects the indoor unit with the outdoor unit.
<b>Intermediate Frequency (IF)</b>	Generally, 70 MHz or 140 MHz.
<b>Ka band</b>	The frequency range from 18 GHz to 31 GHz.
<b>Ku Band</b>	Frequency range from 10.9 GHz to 17 GHz, increasingly used by communications satellites. Requires smaller ground antennas, usually four feet (1.2 meter) in diameter.
<b>L-Band</b>	The frequency range from 0.5 GHz to 1.5 GHz.
<b>LNA</b>	Low Noise Amplifier – The preamplifier between the antenna and the earth station receiver. For maximum effectiveness, it should be located as near the antenna as possible, and is usually attached directly to the antenna receive port.
<b>LNB</b>	Low Noise Block Converter is the converter on the down link that takes the Ku, Ka, or C-Band signal from the satellite and converts it to a lower frequency (L-band) signal that can be fed through the IFL cable to the modem.
<b>Low Earth Orbit (LEO) satellite</b>	Satellites that are not stationary from a fixed point on earth and have the lowest orbit of all communication satellites. Most handset-to-satellite systems are based on LEO satellites using L-Band.
<b>Low Noise Amplifier (LNA)</b>	The preamplifier between the antenna and the Earth station receiver. For maximum effectiveness, it must be located as near the antenna as possible, and is usually attached directly to the antenna receive port.
<b>Margin</b>	The amount of signal in dB by which the satellite system exceeds the minimum levels required for operation.
<b>Multiplexing</b>	Techniques that allow a number of simultaneous transmissions to travel over a single circuit.

<b>ODU</b>	Outdoor unit, such as an antenna dish.
<b>Outbound Carrier</b>	See <b>Downstream Carrier</b> .
<b>Passband</b>	The range of frequencies handled by a satellite translator or transponder.
<b>Perigee</b>	The point in a satellite's orbit where it is closest to Earth.
<b>Polarization</b>	Design technique used to increase the capacity of the satellite transmission channels by reusing the satellite transponder frequencies.
<b>QPSK (Quadrature Phase Shift Keying)</b>	Digital modulation scheme used in transmission communications to allow increased sending capacity.
<b>Rain Outage</b>	Loss of signal at Ku or Ka Band frequencies due to absorption and increased sky noise temperature caused by heavy rainfall.
<b>Satellite</b>	A sophisticated electronic communications relay station orbiting 22,237 miles above the equator moving in a fixed orbit at the same speed and direction of the Earth (about 7,000 m.p.h. east to west).
<b>Satellite Communications</b>	The use of geostationary orbiting communication satellites to relay transmission from one Earth station to another or to several Earth stations. It takes only three satellites to cover the whole Earth.
<b>Satellite Pass</b>	Segment of orbit during which the satellite "passes" nearby and in the range of a particular ground station.
<b>Shared hub</b>	Satellite communications operations center that is shared among several separate network users; often used for VSAT operations.
<b>Single-Channel-Per-Carrier (SCPC)</b>	A method used to transmit a large number of signals over a single satellite transponder.
<b>SNR</b>	Signal to Noise Ratio - In analog and digital communications, signal-to-noise ratio, (S/N or SNR), is a measure of signal strength relative to background noise. The ratio is usually measured in decibels (dB).
<b>Spillover</b>	Satellite signal that falls on locations outside the beam pattern's defined edge of coverage.
<b>Subcarrier</b>	In satellite television transmission, the video picture is transmitted over the main carrier. The corresponding audio is sent via an FM subcarrier. Some satellite transponders carry as many as four special audio or data subcarriers.
<b>Symbol Rate</b>	Symbol Rate refers to the number of symbols that are transmitted in one second. From the symbol rate, you can calculate the bandwidth (total number of bits per second) by multiplying the bits per symbol times the symbol rate.
<b>TDM (Time Division Multiplexing)</b>	A type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval ("slot" or "slice") for the transmission of each channel. (i.e. the channels take turns to use the link.)
<b>TDMA (Time Division Multiple Access)</b>	A communications technique that uses a common channel (multipoint or broadcast) for communications among multiple users by allocating unique time slots to different users.

<b>Transmission Control Protocol (TCP)</b>	A protocol developed for the internet to get data from one network device to another; TCP uses a retransmission strategy to ensure that data will not be lost in transmission.
<b>Transmission Rate</b>	Includes all over-the-air data. This includes the user data (information rate), iDirect overhead, and FEC encoding bits.
<b>Transponder</b>	A device in a communications satellite that receives signals from the earth, translates and amplifies them on another frequency, and then retransmits them.
<b>UHF</b>	Ultra High Frequency. Band in the 500-900 MHz range, including TV channels 14 through 83.
<b>Uplink</b>	The Earth station used to transmit signals to a satellite and the stream of signals going up to the satellite.
<b>Upstream Carrier</b>	Upstream carrier (synonymous to inbound carrier) is the carrier from the remote modem to the Hub, via the satellite.
<b>VHF</b>	Very High Frequency, Refers to electromagnetic waves between approximately 54 MHz and 300 MHz.
<b>VSAT</b>	Very Small Aperture Terminal. Means of transmission of video, voice, and data to a satellite. Used in business applications.





## Index

### A

- accelerated GRE tunnels 133
- acquisition aperture length 73
- activating
  - remotes 177
- active users pane 227
- antenna 61
- antenna, adding 61
- applying changes to roaming remotes 199
- applying configurations 190

### B

- bandwidth
  - adding 68
- beam selection
  - see beam switching
- beam switching for roaming remotes 152
- before you start
  - information needed 11
  - preparing equipment 12
- blades
  - adding 85
- BUC 143 to 144
- button
  - accept changes 18
  - right mouse 29

### C

- carrier
  - acquisition aperture length 73
  - adding downstream 69
  - adding upstream 71, 74
  - information rate 73
  - large block 73
  - small block 73
  - symbol rate 73
  - transmission rate 73
  - uplink/downlink center frequency 73
- carrier grooming 107
- chassis

- adding the initial hub chassis 171
- configuring and controlling 172
- installing 12
- setting the IP address 171
- choose details
  - feature 40
  - view 40
- cloning
  - profiles
    - within opposite stream folder 160
    - within same folder 160
  - remotes 145
  - user accounts 225
- CNO User Groups
  - adding and modifying 218
  - visibility and access 217
- commissioning line cards
  - See hub commissioning 235
- comparing configurations 188
- compression
  - CRTTP performance characteristics 156
  - enabling compression types on remotes 153
  - RTP header compression performance characteristics 156
  - TCP payload compression 155
  - UDP header compression 155
  - UDP header compression performance characteristics 155
  - UDP payload compression 156
  - UDP payload compression compared to TCP payload compression 156
- configuration changes 37
  - accepting 53
- configuration state 49
  - changing 52
- configurations
  - changes on roaming remotes 198
  - comparing 188
  - deleting 182
  - downloading
    - canceling 192
    - chassis 193
    - line card 194
    - network 194
    - protocol processor 193

- using revision server 207
- modifying 182
- saving
  - TCP vs. UDP 196
- saving to single elements 193
- status 49
- uploading last modified vs. existing 183
- uploading multiple modified vs. existing 186
- viewing 182

context menu button 29

converters

- adding 62

CRTP 156

CRTP performance characteristics 156

customers

- adding 121 to 122
- listing on remotes 121

## D

database locking 233

deactivating

- remote 177

details

- choosing 40
- choosing details feature 40
- creating sets of 40
- view 38

DHCP 127

distributors

- adding 121 to 122
- listing on remotes 121

DNS 127

down converter 61

- adding 62

downloading

- concurrently to remotes and hub 201
- images
  - TCP 207
- interactions 205
- multicast 202
- multiple images 202
- out of network remotes 204
- using revision server 207

downloading configurations 190

- canceling 192
- chassis 193

- line card 194
- network 194
- protocol processor 193

## E

elements 19

## F

failover, line cards 101

FEC blocks 71

find toolbar 32

folders 19

- adding entries 22
- BUCs 19
- customers 20
- distributors 19 to 20
- empty 20
- Hub RFT components 20
- LNBs 19
- manufacturers 19
- operators 20
- QoS profiles 19
- remote antenna components 19
- top level of 22

free slot allocation 110

frequency hopping 108

frequency translation 63

## G

geo location

- remotes 142

globe

- sorting
  - globe
  - hide element 25
- tree 25

globe, iDirect 19

GRE tunnels 133

guest user 232

## H

high power amplifier See HPA

HPA 61

- adding 64
- hub commissioning 235 to 251
  - 1 dB compression test 244
  - downloading line cards using iSite 239
  - setting C/N for mesh inroute 248
  - setting C/N for mesh outroute 247
  - setting IP address on line card 237
  - setting tx power on line card 245
  - setting UPC margin for mesh outroute 248

- Hub RFT
  - adding 82

- Hub RFT Components 61

- hubs
  - assigning inroute groups 111

## I

- iBuilder

- description 13
  - installing 15

- images 201

- compatible versions 201
  - downloading 201
    - interactions 205
    - out of network 204
    - TCP 207
  - downloading multiple units 202
  - UDP multicast 202

- iMonitor

- description 13

- information rate 73

- NetModems vs. Series models 71, 73

- inroute groups

- adding 107
  - assigning to hubs 111
  - description 107
  - enabling CRTP for mesh remotes 111
  - enabling for mesh 110
  - enabling UDP header compression for mesh remotes 111
  - enabling UDP payload compression for mesh remotes 110
  - mesh-enabled, described 108
  - uplink control parameters 113

- installation

- NMS applications 15

- interface

- using NMS GUI 23

- IP configuration on remotes 123 to 134

- iSCPC

- adding upstream SCPC carriers 74
  - carrier assignment to remotes 120
  - downstream carriers 69
  - iSCPC line cards 99
  - iSCPC remotes 116
  - overview 8

- iSite 13

- using to download a line card 239

## L

- LAN

- interface 125
  - remotes 123 to 126

- large block 73

- latitude

- teleport 78

- legend 36

- line cards

- adding
    - receive 97
    - standby 101
    - transmit 94
    - transmit/receive 94
  - automatic failover 101
  - commissioning *See* hub commissioning
  - configuring for mesh 96
  - downloading using iSite 239
  - failover sequence 104
  - failure recovery 106
  - free slot allocation 110
  - iSCPC line cards 99
  - setting tx power 245
  - Tx vs. Rx-only 103
  - types supporting mesh 94

- LNB 143 to 144

- locking

- database 233

- logging in 16

- passwords 16
  - to other servers 17

- longitude

- spacecraft 66
  - teleport 78

## M

- main toolbar 32
- management interface 125
- mesh
  - adding a mesh inroute group 110
  - adding a mesh line card 96
  - configuring remotes for mesh 119
  - configuring TCP as single-hop traffic 111
  - converting a network from star to mesh 253 to 257
  - converting a star inroute to mesh 254
  - enabling CRTP per inroute group 111
  - enabling UDP header compression for mesh inroute groups 111
  - enabling UDP payload compression for mesh inroute groups 110
  - hardware requirements 253
  - line card types that support 94
  - mesh-enabled inroute groups 108
  - prerequisites for converting from star to mesh 253
  - recalibrating a star outroute for mesh 253
  - reconfiguring a star remote for mesh 255
  - setting inroute C/N 248
  - setting outroute C/N 247
  - setting outroute UPC margin 248
  - transponder configuration requirements 253
  - uplink control parameters on mesh inroute groups 112
  - uplink control parameters on mesh line cards 96
  - uplink control parameters on mesh remotes 119
  - VLAN tagging on mesh remotes 124
- mobile state 142
- modifying
  - accepting changes 18

## N

- NAT 129
- NetManager, replaced by iSite 13
- network tree, *See* tree
- networks
  - adding 93
  - free card slot allocation 110
  - inroute groups
    - adding 107
    - assigning to hubs 111
    - description 107
  - line cards

- adding receive 97
- adding transmit 94
- adding transmit/receive 94

## NMS

- applications 12
- distributed NMS server 259
- main components 11
- multiple users accessing 17
- servers used 14
- setting up a distributed environment 261

## O

- ODU Tx 10 MHz 63
- ODU Tx DC power 63
- options files 181
  - hub-side and remote-side 181
- orbital inclination 66

## P

- panes
  - active users 35, 227
  - choose details 40
  - configuration changes 37
  - details 38
  - legend 36
  - network tree, *See* tree
  - See also* dialog boxes
- passwords 16, 229, 231
- profiles
  - QoS
    - See* remotes:QoS 167
- properties
  - viewing element 38
- protocol processor
  - adding 83
  - blades 85
  - installing 12

## Q

- QoS 168
  - see also* remotes:QoS
  - changing multiple profiles 168
  - changing profile assignments 168
  - creating and managing profiles 157
  - modifying profiles 159

- profile folders 158
- profiles 167, 169
  - changing assignments
    - remotes 168
- remotes 138
- up/downstream filters 159

## R

- receive line card
  - adding 97
- receive properties
  - remotes 120
- remotes 115
  - activating 177 to 178
  - adding 115 to 144
  - antenna 144
  - applying configurations 196
  - BUC 143 to 144
  - cloning 145
  - configuring
    - actions to perform beforehand 115
    - data to know beforehand 115
  - configuring for mesh 119
  - configuring RIPv2 on 124
  - customers 121 to 122
  - deactivating 177 to 178
  - deactivating before deleting 182
  - DHCP 127
  - distributors 121 to 122
  - DNS 127
  - downloading
    - using revision server 207
  - downloading configurations
    - out of network 204
  - geo location 142 to 143
  - information tab 116 to 123
  - IP configuration 123 to 134
  - iSCPC remotes 116
  - LAN 123 to 126
  - LAN "same as" option 125
  - LAN interface 125
  - link encryption on NetModem II Plus 119
  - listing customers 121
  - listing distributors 121
  - LNB 143 to 144
  - management interface 125
  - mobile state 142
  - model type 118
  - moving 179
  - multicast groups 131

- MUSIC 119
- NAT 129
- passwords 118
- port forwarding 132
- QoS 138, 167 to 169
  - modifying profiles 159
  - profile folders 158
  - profiles 167, 169
  - up/downstream filters 159
- receive properties 120
  - carrier name 120
- reconfiguring for mesh 255
- remote antenna 144
- resetting 206
- roaming remotes 145 to 153
  - applying changes 199
  - beam switching for 152
  - configuration changes 198
  - managing configuration of 149
  - options files for 198
  - pending changes across networks 199
- serial number 118
- serial number, system-generated 118
- static routes 129
- switch tab 134 to 138
  - copying data to a spreadsheet 138
  - dedicating a port to a VLAN 135
  - default settings 135
  - setting a port as a trunk 136
  - setting the port speed and port mode 137
- transmit properties 120
  - power 120
  - power, max 120
- uplink control parameters on 119
- upstream SAR on mesh-enabled remotes 140
- VLAN 123 to 126
- VSAT 143
- requirements
  - system 15
- resetting 206
- resetting elements 192
- retrieving configurations
  - modified vs. existing 186
  - multiple 186
  - single
    - last modified vs. existing 183
- revision server 207 to 214
  - cancelling an upgrade 214
  - duty cycle explained 208
  - starting 210

- status pane 212
  - using to download remotes 207
  - when to use 209
- right mouse button 29
- right-click
  - menu options 34
- RIP, see RIPv2
- RIPv2 124 to 125, 130
- roaming remotes, see remotes: roaming remotes
  
- RTP header compression performance characteristics 156

## S

- SAR 139
  - on mesh enabled remotes 140
- saving configurations
  - single elements 193
  - TCP vs. UDP 196
- servers 14
- slot allocation
  - free 110
- small block 73
- spacecraft 65 to 66
  - adding 65
  - longitude 66
- spectral inversion 63
- static routes 129
- status
  - elements 49
- status bar 34
- super user 232
- switch, eight-port: see remote: switch tab
- symbol rate 71, 73
- system requirements 15

## T

- TCP payload compression 155
- TCP vs. UDP download 192
- teleport 77 to 82
  - adding 77
  - adding a backup 78
  - latitude 78

- longitude 78
- toolbars
  - choose details 40
  - configuration changes 37
  - details 38
  - find 32
  - icons 32
  - legend 36
  - main 32
  - main menu 34
  - status bar 34
  - view menu 34
- translation frequency 67
- transmission rate 71, 73
- transmit line card
  - adding 94
- transmit properties
  - remotes 120
- transmit/receive line card
  - adding 94
- transponder
  - adding 66
- tree
  - description 29
  - elements 19
  - folders 19
- tree view, See tree
- treebar, See tree

## U

- UDP payload compression 156
- up converter 61
  - adding 62
- upgrade assistant
  - See revision server
- uplink control parameters
  - configuring for inroute groups 113
  - configuring on mesh line cards 96
- uplink/downlink center frequency 71, 73
- User Groups
  - CNO user groups 218
  - NMS user groups 215
  - VNO user groups 218
- users

- active users pane 227
- adding user accounts 224
- changing passwords 229
- cloning user accounts 225
- conversion during upgrade 215
- deleting user accounts 227
- guest 232
- levels of 230
- locking others out 233
- managing 230
- modifying user accounts 224 to 225
- multiple 17
- passwords 231
- permissions 230
- privileges
  - defined 230
  - predetermined 230 to 231
- super user 232
- types 230
- viewing user accounts 226
- VNO guest 232
- VNO super user 232

- global vs. customized 56
- of line cards 97
- of protocol processors 85
- of remotes 145
- setting global properties for network elements 56
- windows, *See* panes
  - See also* dialog boxes

## V

### VLAN

- adding 88
- default vs. upstream 125
- on eight-port switch: *see* remote: switch tab
- remotes 123 to 126
- tagging on mesh remotes 124
- upstream interface 88

VNO guest, *see* users: VNO guest

VNO super user, *see* users: VNO super user

### VNO User Groups

- adding and modifying 218
- creating and managing 218
- modifying visibility and access 222
- setting rate limits 221
- visibility and access 216

VSAT 143

## W

warning properties 55 to 59

- categories of warnings 55
- clearing customized properties 59
- configurable properties 55
- customizing for specific network elements 58
- distinguishing customized warnings 59

