Velocity Network Operations Using Pulse

iDirect Velocity™ 1.4

November 04, 2016

iDirect

VT iDirect® is a global leader in IP-based satellite communications providing technology and solutions that enable our partners worldwide to optimize their networks, differentiate their services and profitably expand their businesses. Our product portfolio, branded under the name **iDirect®**, sets standards in performance and efficiency to deliver voice, video and data connectivity anywhere in the world. **VT iDirect®** is the world's largest TDMA enterprise VSAT manufacturer and is the leader in key industries including mobility, military/government and cellular backhaul.

Company Web site: www.idirect.net ~ Main Phone: 703.648.8000
TAC Contact Information: Phone: 703.648.8151 ~ Email: tac@idirect.net ~ Web site: tac.idirect.net

iDirect Government™, created in 2007, is a wholly owned subsidiary of iDirect and was formed to better serve the U.S. government and defense communities.

Company Web site: www.idirectgov.com ~ Main Phone: 703.648.8118
TAC Contact Information: Phone: 703.648.8111 ~ Email: tac@idirectgov.com ~ Web site: tac.idirectgov.com

Document Name:UG_Velocity_Network_Operations_Using_Pulse_RevA_110416.pdf

Document Part Number: T0000808

Revision History

The following table shows all revisions for this document. To determine if this is the latest revision, check the Technical Assistance Center (TAC) Web site.

Revision	Date	Updates
A	11/04/2016	Initial release document for Velocity Release 1.4
B	11/04/2016	Initial release document for Velocity Release 1.4 (Reduced PDF size)

Contents

Figures

Tables

About

Purpose

The document *iDirect Velocity™ Network Operations Using Pulse NMS,* provides detailed information and instructions necessary to configure a Velocity Network, using the iDirect Pulse NMS Web User Interface.

Guidelines are provided for the sequence of developing the network; step-by-step instructions are provided for creating and configuring each network element; and specific NMS operations, designed as troubleshooting aids, are described for use in diagnosing problems that involve specific Velocity Network infrastructure elements.

Audience

This document is intended for use by network engineers and operators, as well as other personnel responsible for configuring, monitoring, and operating iDirect Velocity™ networks.

Getting Help

The iDirect Technical Assistance Center (TAC) and the iDirect Government Technical Assistance Center (TAC) are available to provide assistance 24 hours a day, 365 days a year. Software user guides, installation procedures, FAQs, and other documents that support iDirect and iDirect Government products are available on the respective TAC Web site:

- Contact iDirect
  - TAC Web site: http://tac.idirect.net
  - Telephone: 703.648.8151
  - E-mail: tac@idirect.net
- Contact iDirect Government
  - TAC Web site: http://tac.idirectgov.com
  - Telephone: 703.648.8111
  - Email: tac@idirectgov.com

Please assist us in improving this document by providing feedback. Send comments to:

- iDirect: techpubs@idirect.net
- iDirect Government: techpubs@idirectgov.com

For sales or product purchasing information contact iDirect Corporate Sales:

- Telephone: 703.648.8000
- E-mail: sales@idirect.net

Related Document Set

The following iDirect documents, which contain information relevant to installing and using iDirect satellite network software and equipment, are available at http://tac.idirect.net.

- *Installation, Support, and Maintenance Guide*
- *Terminal Web UI User Guide*
- *iDirect Velocity™ Software Release Notes*
- *iDirect Pulse®NMS Software Release Notes*
- *iDirect Pulse®NMS User Guide*
- *iDirect Velocity™ Network Operations Using Pulse*

1 Configuring Physical Domain Elements

The *physical domain* is composed of the hardware infrastructure components of an iDirect Network — items such as the NOC and SAS sites, hub chassis and line cards, NMS and Protocol Processor (PP) clusters and servers, and other ancillary servers.

The following topics briefly introduce each Physical Domain element and provide step-by-step procedures for configuring each element and its associated parameters.

1.1 Physical Domain Configuration Sequence

NMS tools for working with physical domain elements are accessed from the Physical Domain operations list, of the Pulse Configuration tab. Each physical element, before it can be deployed in an iDirect Velocity™ Network, must first be created in the NMS, and its parameters appropriately configured.

A general sequence for configuring the Physical Domain Elements in the NMS is shown here.

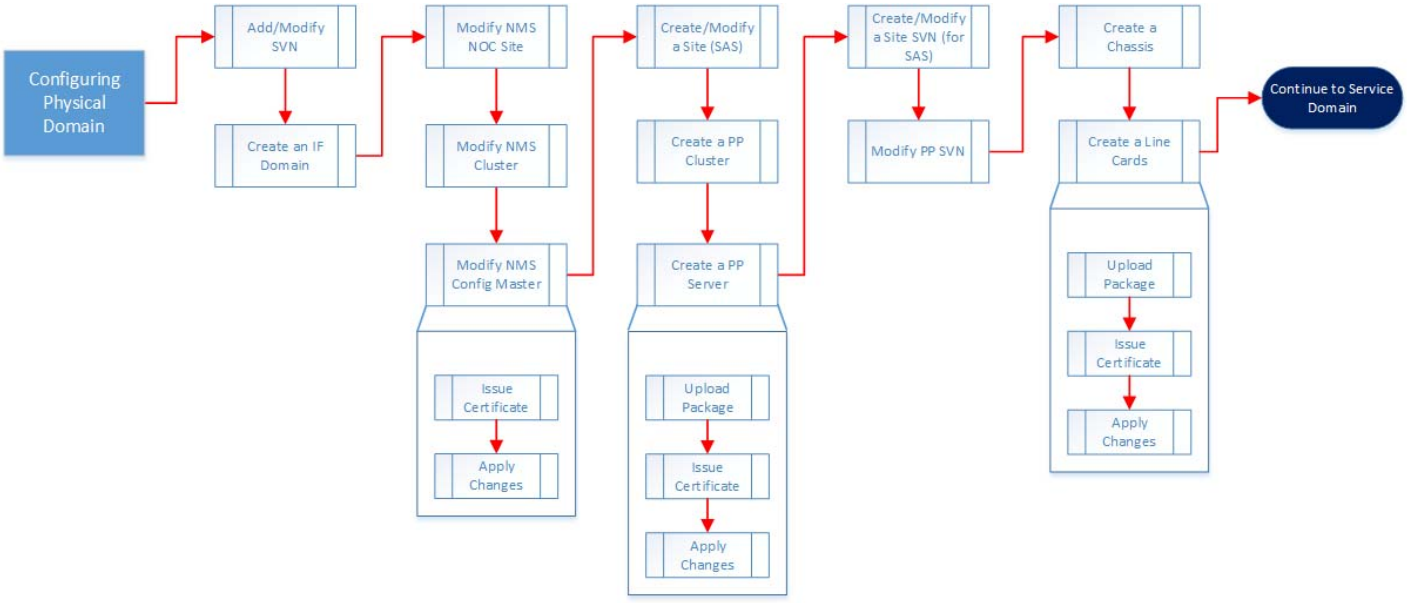

Figure 1-1. Building a Basic Network — Creating Transport Domain Elements

1.2 Creating Velocity Sites

A *Site,* in an iDirect Velocity™ Network, is a collection of processes and machines at a given location — for example a SAS site contains hub equipment such as Protocol Processor servers, line cards and chassis, the NMS and associated servers, and connecting SVNs.

The operational mode of a site can be configured as a SAS (*satellite access station*), NOC (*network operations center*), or an EAP (*external access portal*) site. Each site type can consist of a primary and an optional backup or secondary site. When configuring a site, in Pulse, it can be designated as the primary site or, if implemented, as the backup site.

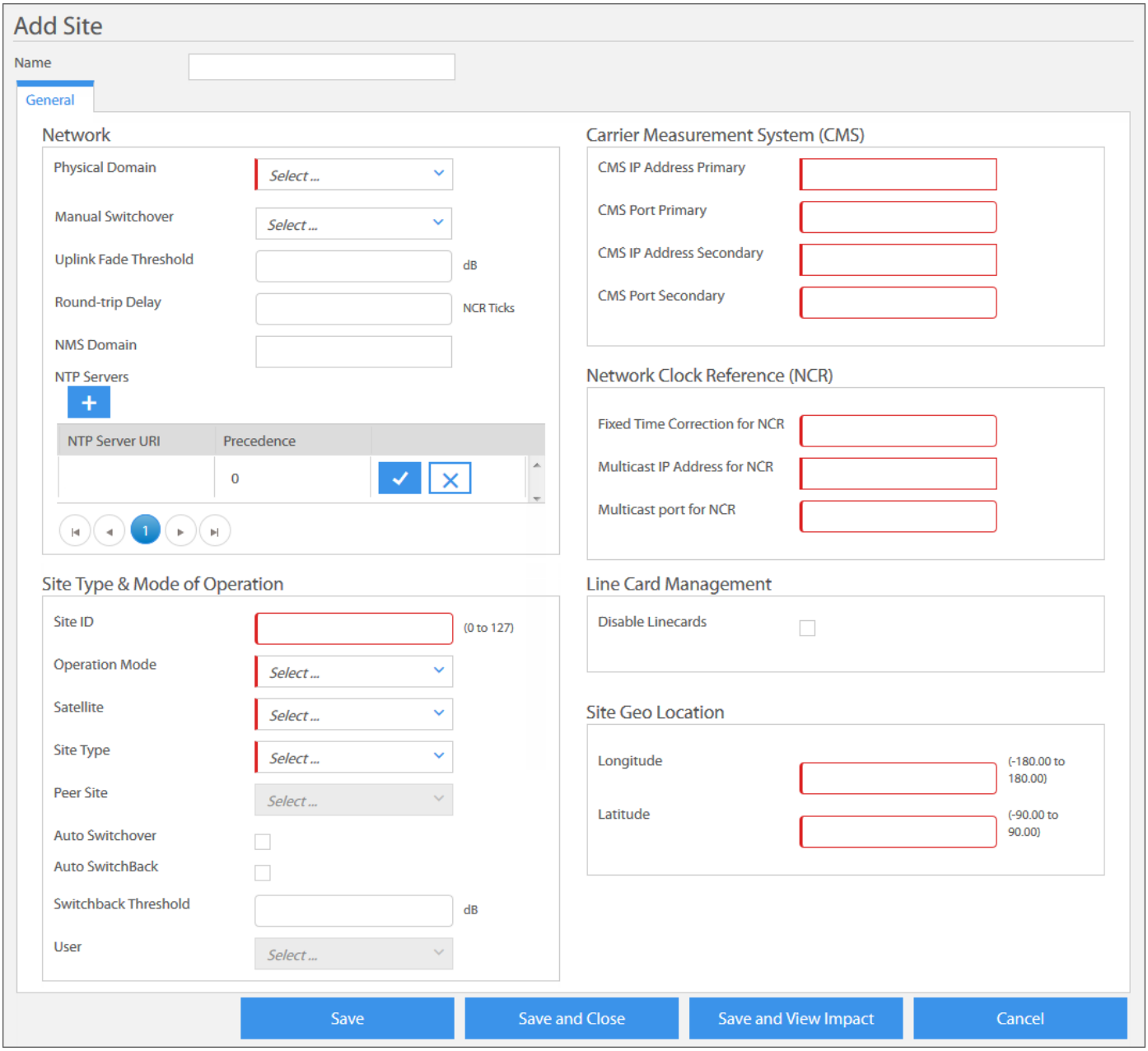

Figure 1-2. Add Site

To add a Site:

1. Click the **Configuration** tab > **Physical Domain** > **More Options > Add> Site**.
2. Type the **Name** of the new Velocity site in the **Add Site** dialog.
3. Under the **Network** section, select the **Physical Domain** to which the Site is associated — this association refers to the Network root to which this Site belongs.

4. Use the **Manual Switchover** drop-down and select whether the site should become a **Forced Primary** site or **Forced Diversity** site during a manual site switchover.
5. Enter the **Uplink Fade Threshold** and the **Switchback Threshold** values. These values, measured in dB, represent fade values at which a primary site will switchover to the secondary and switch back to the primary if the threshold conditions exist.
6. Enter the **Round-Trip Delay** time, in NCR ticks, between the satellite and this site.
7. Enter the appropriate **NMS Domain Name** associated with this site.
8. Under the **NTP Server** section define one or more NTP Servers for use by this site. See *Configure Site NTP Servers*.
9. Under the **Site Type and Mode of Operation** section, enter the **Site ID**, as a value of 0-127. This value uniquely identifies this site.
10. Enter the **Operation Mode** of this site as **NOC**, **SAS**, or **EAP**.
11. Use the **Satellite** drop-down to select the appropriate satellite for this site. This option only applies when **SAS** is selected as the **Operation Mode**.
12. Use the **Site Type** drop-down and select **Primary_Site** or **Backup_Site**.
13. If applicable, use the **Peer Site** drop-down to select, from a list of configured sites, the peer site (primary/backup) that is associated with the site being configured.
14. Select **Auto Switchover** if the site should switch to the Secondary Site in fade conditions; and select **Auto Switchback** to enable automatic switchback to the Primary upon reaching the defined **Switchback Threshold**.
15. Enter the **Switchback Threshold** value in db units.
16. Under **Carrier Measurement System (CMS)**, use **CMS IP Address Primary** and **CMS Port Primary** to enter an IP address and port for the primary *CMS System* server for this site.
17. Use **CMS IP Address Secondary** and **CMS Port Secondary** to enter an IP address and port number for the secondary *CMS System* server for this site.
18. Under the **Network Clock Reference (NCR)** section, use **Fixed Time Correction For NCR**, to enter a value by which the NCR time is adjusted.
19. Use **Multicast IP Address (NCR)** and **Multicast Port (NCR)** to enter the IP address and port number of the site's NCR time server.
20. Under **Line Card Management**, select **Disable Line Cards** if the active line cards should disable their transmit carriers at the Tx line cards for channels that are to be switched.
21. Under **Site Geo Location**, use **Longitude** (-180 to +180) and **Latitude** (-90 to +90) to enter the site geographic location in degrees.

1.2.1 Configure Site NTP Servers

Using the **NTP Servers** dialog, multiple NTP servers can be entered as individual records for use by the site.

To configure an NTP Server for the Site configuration:

1. From the **Add Site** page, under the **NTP Server** section, click the **Add Record** icon to enable the configuration fields for entering a new NTP server record.
2. In **NTP Server URL,** enter the appropriate IP Address/URL for accessing the NTP server.
3. Click the **Update** icon to accept the **NTP Server** record entry.
4. Repeat the steps, from Step (2), to insert additional NTP Server records.
5. Click the **Edit** icon, on an **NTP Server** record, to modify the record; click the **Delete** icon, to remove the record.
6. Click **Save** to save the Site to the NMS database, and continue, or click **Save and Close** to save the Site and open the **Browse Physical Domain** page.

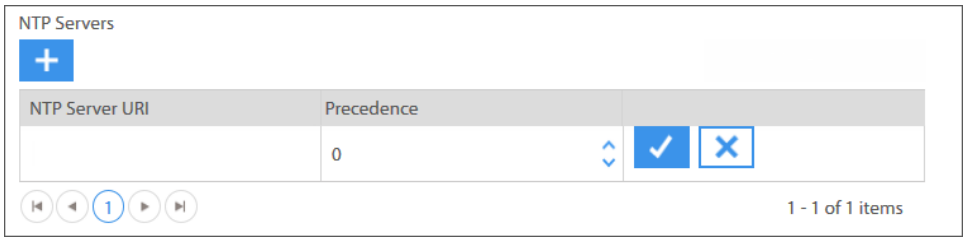

Figure 1-3. Add Site NTP Server Dialog

1.3 About Velocity SVNs

A satellite virtual network or *SVN,* is an IP VPN that contains a satellite network segment. In a Velocity Network an SVN extends to multiple satellite terminals, has its own IP address space, and functions as an independent network. The Velocity network SVN segments include:

Service Provider Customer Network <-> **IP VPN over the Network Operator DCN Network** <-> **SAS Site SVN <-> Satellite/OTA** <-> **Terminal <->Terminal LAN.**

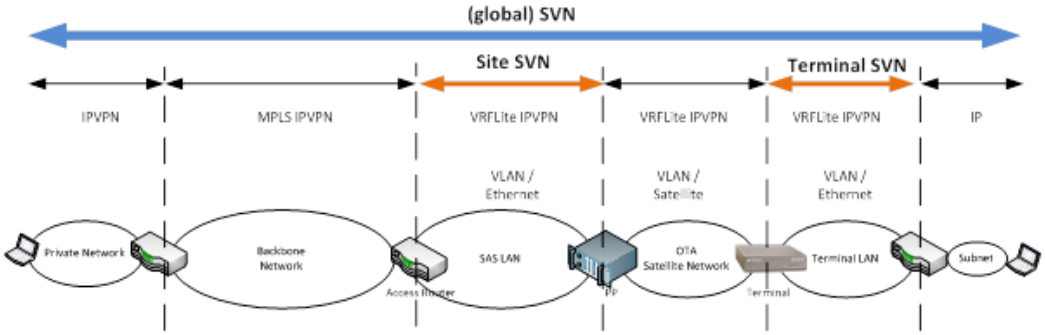

Figure 1-4. iDirect Velocity Satellite Virtual Networks

The traffic within each SVN on these satellite terminals is managed by a virtual network operator (VNO), on which the VNO offer services, and is subject to the global GQoS rules.

In an iDirect Velocity system, three general types of SVNs are required based on the traffic functions that each performs. These required SVN types are outlined below:

- *Customer SVN (Data SVN)* — Transports user traffic from a terminal to its final destination in a customer's private network, and vice versa. The Customer SVN extends from the terminal network, through the satellite router, through a SAS, the backbone network, and to an interface point to the Customer's private network. Each SVN is identified by an SVN ID defined by the satellite operator, and has its own independent IP address space which may be managed by the service provider.
- *Velocity Admin SVN* — Transports internal Velocity administrative traffic between equipment within a SAS, between SASs, between the SAS and NOC, and between the NOC or SAS NMS and satellite routers. This SVN must be assigned SVN ID 1. The management SVN IP address space is managed by the satellite operator, who assigns management IP addresses to all network equipment.
- *Velocity Tunnel SVN* — Transports user traffic between Protocol Processor processes and the linecards that are located in the same SAS or in an associated backup/diversity SAS. The SVN ID of the **Tunnel SVN** is configured by the satellite operator.

Table 1-1 shows what iDirect equipment is a member node on each of these SVNs. Being a node on a specific SVN type means that the equipment has an IP interface or sub-interface within the SVN, and sends and receives traffic on this SVN.

Table 1-1. SVN Type Usage by iDirect Equipment

iDirect Equipment	Customer SVN	Admin SVN	Tunnel SVN
PP Server	•	•	•
Web Cache Server	•	•	
SAS NMS Server		•	
GBWM Server		•	
Hub Chassis		•	
Hub Line Card		•	•
NOC NMS Server		•	
EAP NMS Server		•	

1.4 Velocity SVNs in the NMS

When it comes to configuring any of the SVN types — for example, *Admin*, *Tunnel, or Customer,* which are required in a Velocity Network, the configuration in the NMS is based on an hierarchical structure that places SVNs into four SVN categories, as listed below. These categories affect how SVNs are created in the NMS:

1. SVN (or Global SVN)
2. Site SVN
3. Server SVN
4. Terminal SVN

As shown in the following table, each iDirect equipment type requires the same Server SVN types, however, not all equipment types will require all Server SVN types.

Table 1-2. iDirect Equipment and Required Server SVN Object

iDirect Equipment	Data Server_SVN	Admin Server_SVN	Tunnel Server_SVN
PP Server: PP	•	•	•
Squid Server		•	
PP Server: GBWM		•	

1.4.1 Global SVNs

A *Global SVN* is at the top of the Velocity SVN structure and represents a VPN that extends across the Velocity core network (DCN) to another Site. A parent global SVN must be configured for each of the following SVNs, before any child SiteSVN or ServerSVN is created.

- The **Admin SVN** is a Global SVN that connects iDirect equipment located in Satellite Access Stations (SAS Sites), Network Operations Centers (NOC Sites), and Satellite Terminals. A new Admin SVN requires creating a new Global SVN of type "**AdminVLAN**."
- The **Tunnel SVN** is a Global SVN connecting Velocity Protocol Processors and Line Cards.
- A **Customer SVN** is a Global SVN that connects customer equipment, located in the remote network, behind a Satellite Terminal, through the Teleport and across the DCN to a customer network. Each new Customer SVN requires creation of a new Global SVN of type "**DataVLAN**."

See *Creating a Global SVN*, for the procedures to configure a global SVN.

1.4.2 Site SVNs

The *Site SVN,* just beneath the Global SVN in the Velocity SVN hierarchy, represents the segment of an SVN (VPN) located within a Site — for example within a NOC or SAS. The Site SVN may also be referred to as a NOC VLAN or SAS VLAN, although an IP network. In a Velocity Network, each Site SVN is a part of a Global SVN, and extends across the DCN to another Site. Exactly one Site SVN is created for a each Global SVN within a specific Site.

See *Creating a Site SVN*, for the procedures to configure a Site SVN.

1.4.3 Server SVNs

Each Server SVN is generated automatically as a result of creating a Site SVN and its parent Global SVN. When each Site SVN is created, it can be directly assigned to all of the servers in which it is required, and is automatically created only in those servers. Each of the automatically generated Server SVN must be user-modified to appropriately adjust its IP address assignment. These adjustments are made by opening the specific Blade SVN in the Browse Results window. See *Adding a Protocol Processor Server* on page 36, for procedures to configure a PP Server SVN.

1.4.4 Terminal SVNs

A *Terminal SVN* represents the segment of the SVN that is located in the remote network behind a Satellite Terminal. Within a given terminal, up to 12 SVNs may be configured. To configure the Terminal SVN, see Chapter 6, *Configuring Terminal SVNs*.

1.5 Creating a Global SVN

In the NMS, up to 4000 global SVNs may be created, each having a unique ID and a range of IP addresses. The IP address range of an SVN forms an independent address space from which all of the SVN equipment is assigned an IP address. Although the NMS supports overlapping addresses among SVNs, an IP address may be assigned only once inside a Site SVN.

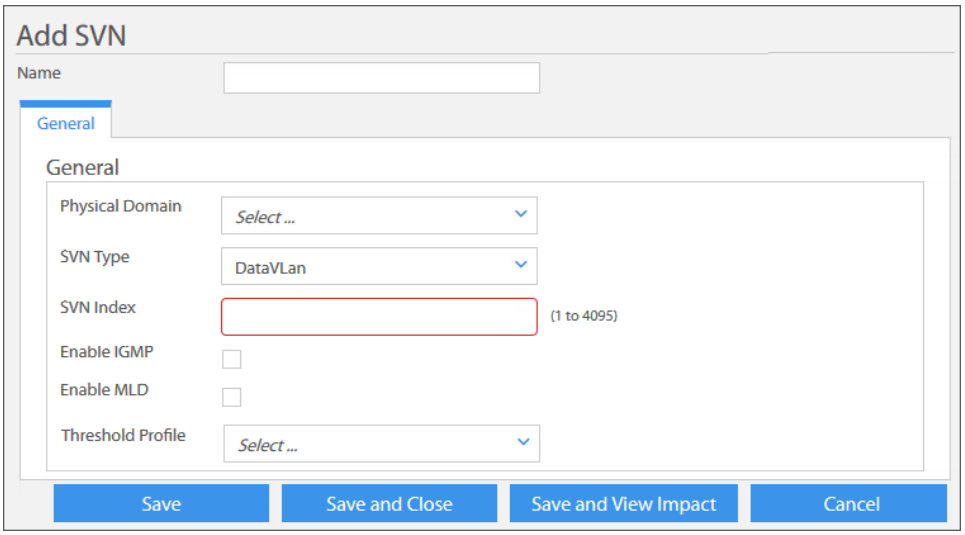

Figure 1-5. Add SVN (Global) Configuration Dialog

Since a Global SVN represents a VPN that extends across the Velocity core network to another Site, a Global SVN must be created for each Customer VLAN, and for each of the iDirect default VLANs, which include the Admin VLAN and Tunnel VLAN. A Global SVN must be created as a parent SVN before any child Site SVN or Server SVN is created. For example, a Global SVN parent must be created prior to creating a child Site SVN.

To add a Global SVN:

1. Click the **Configuration** tab > **Physical Domain > More Options > Add> SVN.**
2. Type the **Name** of the new global SVN.
3. Use the drop-down and select the **Physical Domain** to which the SVN is associated — this association refers to the Network root to which this SVN belongs.
4. In **SVN Index**, enter a value of 1–4095. The **SVN Index** is also used as the VLAN tag in the Teleport/Site and the Terminal LAN. The default **SVN Index** for the Admin SVN is 1 and Tunnel SVN is 4048. With the exception of the Admin VLAN, these values may be changed. The **SVN Index** for the DataVlan are arbitrarily defined.
5. From the list of pre-defined types, select the appropriate **SVN Type** for the global SVN:
   a. **AdminVLAN -** to create an administrative SVN, if not already created by default.
   b. **DataVLAN -** to create a new customer SVN.
   c. **TunnelVLAN -** for creating an iDirect tunnel SVN, if not already created by default.
6. Select **Enable IGMP** (*Internet Group Management Protocol*) to enable this option on this SVN. This protocol is use if the SVN carries multicast traffic.
7. Select **Enable MLD** (*Multicast Listener Discovery*) to enable this protocol option on this SVN. This protocol is used for multicast management on IPv4 networks.
8. Use the **Threshold Profile** drop-down to select threshold rules to apply to this SVN.
9. **Click Save and Close** to save the configuration.

1.6 Creating a Site SVN

All Site SVNs are part of a specific Global SVN, and for each configured Site SVN, there is a 1:1 correspondence to a configured Global SVN. In practice, the **Admin VLAN** is required in all sites; the **Tunnel VLAN** is only required for Teleport sites. Only if required, should **Data VLANs** be configured for the Site. In the cases where Site SVNs are required, the SVN must be created at both the primary and associated backup site, if applicable.

Table 1-3. Site SVN Configuration Requirement Example

Global SVN	SVN Type	Index (ID)*	Example Site SVN Names
AdminVLAN	Admin	1	Admin_SiteSVN_1
TunnelSVN	Tunnel	4048	Tunnel_SiteSVN_1
SVN10	Data		Site_1_SVN10
SVN100	Data		Site_SVN100

1.6.1 Add Site SVN — Configure General Parameters

Site SVNs are created in the NMS, by authorized VNOs, under the **Physical Domain** of the **Configuration** page. The configuration is managed using a **General** parameters tab, and a tab for configuring the **BGP** (*Border Gateway Protocol*) parameters.

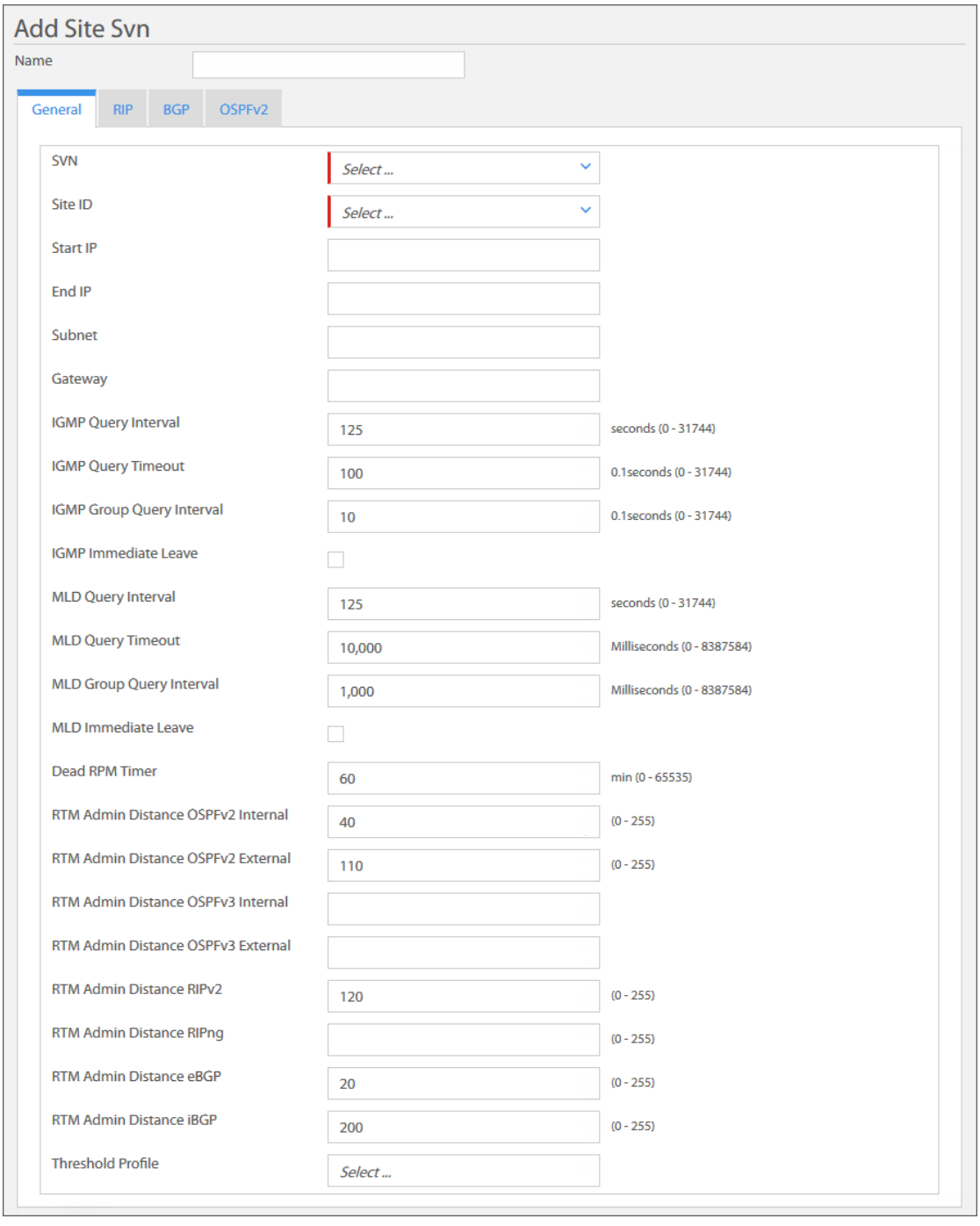

Figure 1-6. Add Site SVN - General Parameters Dialog

To configure Site SVN General parameters:

1. Click the **Configuration** tab > **Physical Domain** > **More Options > Add > Site SVN.** The **Add Site SVN** dialog opens to the **General** tab.
2. Enter a unique **Name** for the new site SVN.
3. Use the **SVN** drop-down and select the Global SVN parent for this Site SVN.
4. Use the **Site ID** drop-down to select the appropriate site for this Site SVN.
5. Enter the **Subnet** and **Gateway** IP addresses for this Site SVN.
6. If applicable (in IPv4 networks), enter the following IGMP protocol parameters:
   a. Use **IGMP Query Interval**, to specify the frequency at which IGMP host query messages are sent. The default is 125 seconds. A larger value causes IGMP queries to be sent less frequently.
   b. Use **IGMP Query Timeout**, to specify the number of seconds to wait after the previous query has stopped querying and before it takes over. The default is 100 seconds.
   c. Use **IGMP Group Query Interval**, to specify the interval that must expire before the router decides that no group members or the source exists on the network. The default value is 10 seconds.
   d. Select **IGMP Immediate Leave**, to enable this option. When enabled, the group entry is removed from the multicast routing table on receiving a leave message for group.
7. Enter the **Dead RPM Timer** value as the interval after which the Routing Protocol Manager (RPM) is declared as down.
8. Use the appropriate fields to enter **RTM** (*Routing Table Manager*) **Admin Distance** values for e**BGP**, and **iBGP** routing protocols.
9. Use the **Threshold Profile** drop-down to select the **Monitor Default Threshold** profile for this Site SVN.
10. **Click Save and Close** to save the Site SVN configuration or click **Save** to continue in modify mode with *Add Site SVN — Configure IPv4 Static Routes*.

1.6.2 Add Site SVN — Configure IPv4 Static Routes

The **Routes V4** dialog, of the Site SVN General tab, supports the entry of IPv4 routes. These routes are moved directly into the routing tables of the protocol processors.

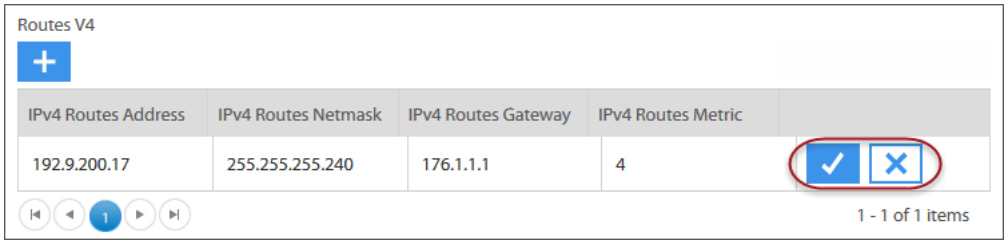

Figure 1-7. IPv4 Routes Configuration Parameters

To add Site SVN IPv4 Route configuration parameters:

1. Click the **Add Record** icon under the **Routes V4** section of the **General** tab of the **Add Site SVN** page.
2. Enter the **IPv4 Routes Address**, **IPv4 Routes Netmask**, and **IPv4 Routes Gateway** addresses.
3. Enter the **IPv4 Routes Metrics** to specify the path cost for this static route entry. The smaller the value, the greater the chance this route will be used for forwarding.
4. Click the **Update Record** icon to accept the record entry. An accepted entry is inserted under **Routes V4** as a new record.
5. Repeat the previous steps to insert additional IPv4 route records.
6. Click the **Edit** icon modify the record; or click the **Delete** icon to remove a record.
7. **Click Save and Close** to save the Site SVN configuration or click **Save** to continue in modify mode.

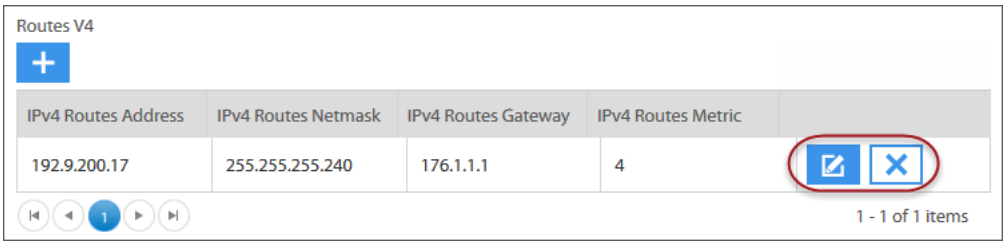

Figure 1-8. IPv4 Routes Record

1.6.3 Add Site SVN — Configure IPv6 Static Routes

The IPv6 address family is used to identify routing sessions for protocols such as BGP that use standard IPv6 address prefixes. Unicast or multicast address prefixes can be specified within the IPv6 address family. IPv6 routes parameters are entered using the Routes V6 dialog.

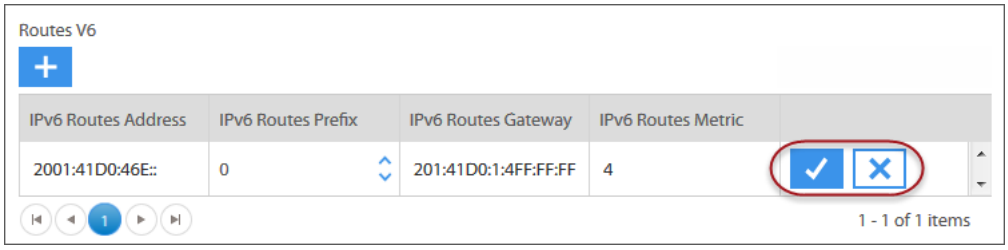

Figure 1-9. IPv6 Route Configuration Parameters

To add Site SVN IPv6 Route configuration parameters:

1. Click the **Add Record** icon under the **Routes V6** section of the **General** tab of the **Add Site SVN** page.
2. Enter the **IPv6 Routes Address**, **IPv6 Routes Prefix**, and **IPv6 Routes Gateway**, addresses.
3. Enter the **IPv6 Routes Metrics** to specify the path cost for this static route entry. The smaller the value, the greater the chance this route will be used for forwarding.
4. Click the **Update Record** icon to accept the record entry. An accepted entry is inserted under the **Routes V6** section as a new record.
5. Repeat the previous steps to insert additional IPv6 route records.
6. Click the **Edit** icon to modify the record; or click the **Delete** icon to remove the record.
7. **Click Save and Close** or click **Save** to continue with the Site SVN configuration.

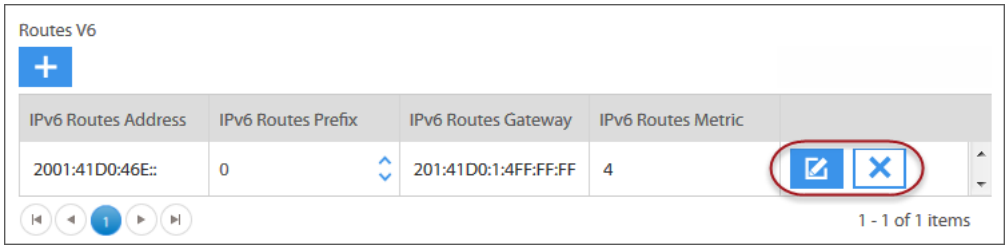

Figure 1-10. IPv6 Routes Record

1.6.4 Add Site SVN — BGP General Parameters

Configuration of the general parameters for *Border Gateway Protocol (BGP)* routing, starts with enabling the feature and providing an Autonomous System (AS) number. This part of the configuration also include selecting the IP addressing family - that is IPV4, IPV6 or both; enabling the BGP outbound route filtering (ORF) feature, to define what route prefixes will be received from BGP peers.

General parameters configuration also supports the enabling of redistribution of specific route types, which allows BGP to learn or import routes from other routing protocols. These specific route redistribution features are disabled by default but may be enabled. Redistribution into BGP can be enabled for static, connected, and RIPv2 routes.

Finally, the BGP General parameters tab provides access to BGP configuration dialogs for **BGP Peer Group, BGP Peer**, the **BGP Configuration Table**, **BGP Router Map, BGP IP Prefix**, and **BGP Aggregate Address** definition.

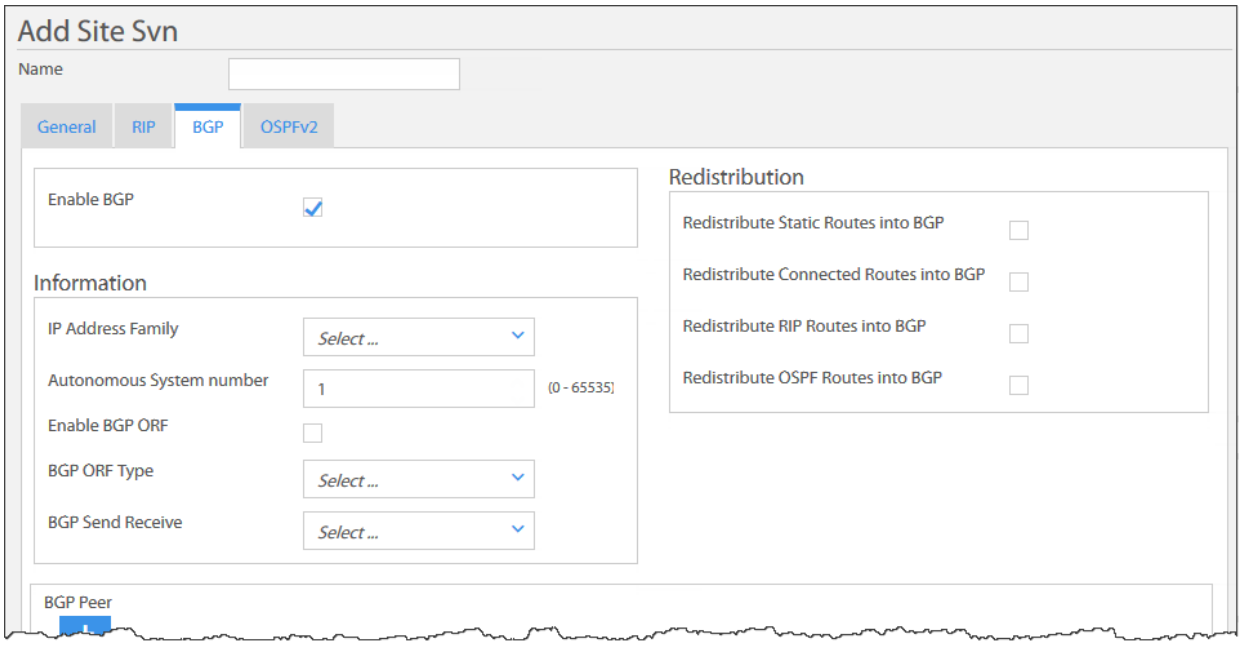

Figure 1-11. Site SVN — BGP General Parameters Dialog

To add Site SVN BGP General configuration parameters:

1. Click the **BGP** tab and select **Enable BGP** to enable the BGP protocol option for the Site SVN. The BGP configuration parameter are enabled.
2. Under the **Information** section, use the **IP Address Family** drop-down and select **IPV4(0)**, **IPV6(1)**, or **Both(2)** to indicate the SVN supported IP address family.
3. Specify an **Autonomous System Number** for the Site SVN interface. This value, which is between 0-65535, must be unique for each Site SVN.
4. Select **Enable BGP ORF** to enable the Outbound Route Filtering of BGP. Enabling this feature supports definition of what prefixes should be received from BGP peers without performing local filtering.

5. Use the **BGP ORF Type** drop-down and select **Community Based(1)**, **Extended Community Based(2)**, or **Prefix Based(3)** as the ORF send/receive filtering method to minimize the number of BGP updates between BGP peers on this SVN.
6. Use the **BGP Send Receive** drop-down and select **Receive(1)**, **Send(2)**, or **Both(3)** to indicate if BGP ORF should be implemented to advertise send, receive, or both send and receive capabilities.
7. Under **Redistribution**, appropriately enable the check box for **Static Routes**, **Connected Routes**, of **RIPv2 Routes**, to indicate which route types to redistribute into BGP.
8. **Click Save and Close** to save the Site SVN configuration or click **Save** to continue in modify mode with *Add Site SVN — BGP Peers*.

1.6.5 Add Site SVN — BGP Peers

BGP Peers refer to two routers that maintain a TCP connection, for the purpose of exchanging BGP route table information. As these peers are configured, they may be assigned to a previously configured BGP peer group. BGP peers are configured using the BGP Peer dialog.

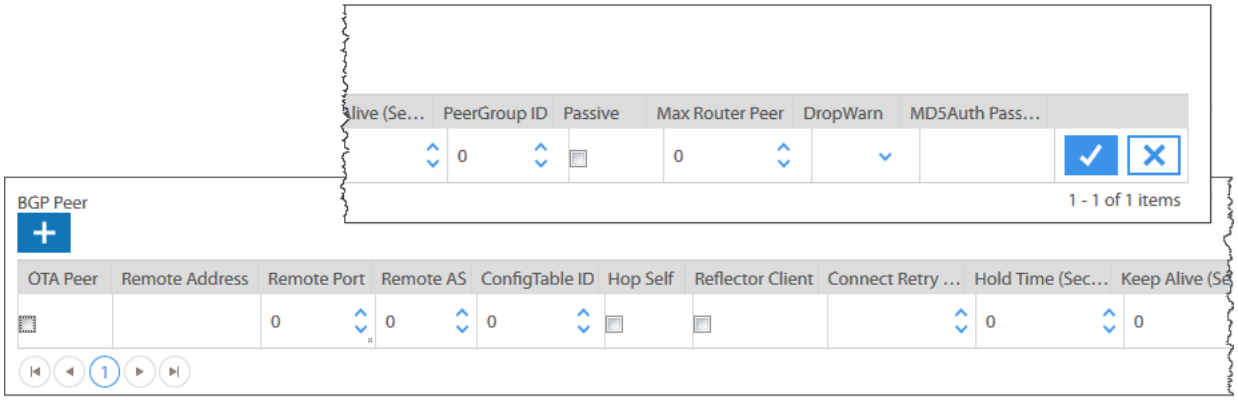

Figure 1-12. BGP Peer Configuration Dialog

To add Site SVN BGP Config Table configuration parameters:

1. With the **Add Site SVN** page open to the **BGP** tab, click the **Add Record** icon, under the **BGP Peer** section, to define a new BGP Peer record.
2. Select **OTA Peer**, to designate this BGP peer as an OTA peer.
3. Use **Remote Address** to enter the IP address of the new BGP peer.
4. Use **Remote Port** to enter the port number on which the BGP peer connects.
5. In **Remote AS**, enter the AS number of the Remote BGP peer. If a value of "0" is entered, the hub will use the AS number of the Satellite Terminal to configure a peer.
6. Use **ConfigTable ID** to enter the number that identifies the table (or list) where peer-specific BGP configuration items may be set for this peer.
7. Select **Hop Self** (set to TRUE), to indicate that this peer should advertise its own peer address as the next hop.
8. Select **Reflector Client** (set to TRUE), to cause the peer to act as a BGP route reflector.

9. In **Connect Retry** enter a time, in seconds, in which the PP can attempt to reconnect to this BGP peer.
10. In **Hold Time**, enter a time, in seconds, after which the peer is declared dead if no keep-alive message is received by the protocol processor.
11. In **Keep Alive**, enter a time in seconds, in which a keep-alive message should be sent to the PP (BGP speaker) by this BGP peer. The range of this value is 0 to 65535; the default value is 60 seconds. A maximum value of 1/3 of the Hold Time value is recommended.
12. Enter a **PeerGroup ID** that identifies the peer group to which the BGP peer is a member.
13. Select **Passive** to designate this peer as passive, and will only accept incoming connections. If disabled, the peer will attempt outbound connections in addition to accepting incoming connections.
14. Use **Max Router Peer** to specify the maximum number of prefixes that may be accepted from this peer.
15. Use the **DropWarn** drop-down to select **Drop(1)** if the peer should be dropped when the configured value for **Max Router Peer** is reached; select **Warn(2)** if a warning should be set when the configured value for **Max Router Peer** is reached.
16. Use **MD5Auth Password** to enter the MD5 password for authentication of this peer. Leave blank if MD5 authentication is not in use.
17. Click the **Update Record** icon to save the **BGP Peer** record. The new entry is inserted into the BGP configuration as a new record, listed under **BGP Peer**.
18. Repeat the previous steps to insert another **BGP Peer** record for this SVN.
19. For a given **BGP Peer** record, click the **Edit** icon to modify the record, and again click the **Update Record** icon. Click the **Delete** icon, to remove the record.
20. **Click Save and Close** to save the Site SVN configuration or click **Save** to continue in modify mode with *Add Site SVN — BGP IP Prefix Parameters*.

1.6.6 Add Site SVN — BGP IP Prefix Parameters

The *BGP IP Prefix list* is essentially a filter, which may be applied to a specific route map. Filtering by prefix list involves matching the prefixes of routes with those listed in a prefix list. When there is a match, the route is used or imported. Whether a prefix is accepted or denied is based upon the following rules:

- An empty prefix list permits all prefixes.
- A prefix is implicit denied if it does not match any of the prefix list entries.
- A prefix match to multiple prefix list entries uses the longest, most specific match.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not continue with the rest of the prefix list. To ensure search efficiency, the most common matches or denies should be placed at the top of the list.

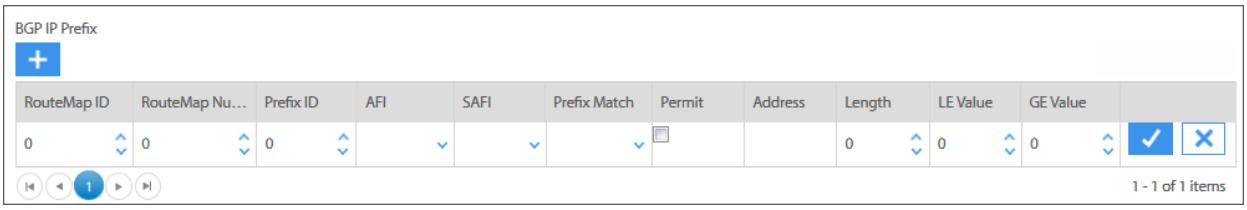

Figure 1-13. BGP IP Prefix Parameters

To configure Site SVN BGP IP Prefix parameters:

1. With the **Add Site SVN** page open to the **BGP** tab, click the **Add Record** icon, under the **BGP IP Prefix** section, to define a new BGP IP Prefix record.
2. Use **RouterMap ID** to specify the index of the route map this prefix should use.
3. Enter a **RouterMap Number** that identifies the route map this prefix should use.
4. Use **Prefix ID** to specify the index of this prefix entry. This number is used to reference more than one filter per route map index.
5. Use the **AFI** drop-down to specify **IPv4(0)** or **IPv6(1)** as the Address Family Identifier of this prefix entry.
6. Use the **SAFI** drop-down to enter the Subsequent Address Family Identifier of this prefix entry, as **MPLS_BGP_VPN(1)**, **Multicast(2)**, **Unicast(3)**, or **Both**. This parameter supplies additional data on the type of the Network Layer Reachability Information that is carried in the prefix—for example, unicast forwarding or multicast forwarding.
7. Use the **Prefix Match** drop-down to select the match criteria to be used by the Route Map that belongs to this Prefix. Select **Match the NLRI Address(1)**, **Match the Source Address(2)**, or **Match the NextHop Address(3).**
8. Select **Permit** if this prefix list is linked to a Route Map that has an ORF association and allows the entry to override the action of the Route Map.
9. In **Address**, enter a valid IPv4 address if **AFI** was specified as '0' or a valid IPv6 address if **AFI** was specified as '1'.
10. Use **Length** to specify the length of the prefix. For example, the length of 128.128/16 prefix is 16.
11. **Use LE Value** to specify the upper value of the range of the prefix length to be matched. **GE** and **LE** allow the range of the matching prefix length to be variable. The range is assumed to span from the **LE**-value to the address length of the family only if the **LE** attribute is specified. A specified **GE**-value and/or **LE**-value must be specified such that: len < GE-value <= LE-value <= address length of family.
12. **Use GE Value** to specify lower value of the range of the prefix length to be matched. **GE** and **LE** allow the range of the matching prefix length to be variable. The range is assumed to span from the GE-value to the address length of the family only if the **GE** attribute is specified. A specified **GE**-value and/or **LE**-value must be specified such that: len < GE-value <= LE-value <= address length of family.
13. Click the **Update Record** icon to save the **IP** prefix record. The new IP entry is inserted into the BGP configuration as a new record, listed under **BGP IP Prefix**.
14. Repeat the previous steps to insert another **BGP IP Prefix** record for this SVN.

15. For a given **BGP IP Prefix** record, click the **Edit** icon to modify the record, and again click the Update Record icon. Click the **Delete** icon, to remove the record.
16. **Click Save and Close** to save the Site SVN configuration or click **Save** to continue in modify mode with *Add Site SVN — BGP Peer Groups*.

1.6.7 Add Site SVN — BGP Peer Groups

A *BGP Peer Group* is composed of member BGP peers that share common update policies, in order to simplify routing configuration and management. These common policies are applied to the group instead of to individual peers, to avoid configuration replication and to promote efficient updating. Instead of performing policy checks during updates to individual peers, the check takes place once for the group, and is then sent to group members.

Peer groups have the following requirements:

- A peer group must be identified as either internal, and having internal (iBGP) members; as external, and having external (eBGP) members; or as a confederated BGP group, where two or more autonomous systems are combined as a single AS.
- Members of an external peer group have different autonomous system (AS) numbers.
- All members must share identical outbound announcement policies — for example, redistribute-list, filter-list, and route-map, except for default-originate, which is handled on a per-peer basis — even for peer group members.
- The inbound update policy for any group member may be customized.

Figure 1-14. BGP Peer Group Parameters

To configure the Site SVN BGP Peer Group parameters:

1. With the **Add Site SVN** page open to the **BGP** tab, click the **Add Record** icon, under the **BGP Peer Group** section, to define a new BGP Peer Group record.
2. Enter a **PeerGroup ID** number that uniquely identifies the group.
3. Enter a **ConfigTable ID** that uniquely identifies the BGP configuration table used by this group, and where various peer-specific BGP configuration items may be set for the entire peer group. An entry of '0' indicates that the is no **Config Table** association.
4. Use the **Area** drop-down to designate the peer group membership type. **IBGP(1)** specifies internal members**; EBGP(2)** specifies external members; and **Confederated EBGP(3)** specifies confederated external members (a group of autonomous systems under a single AS designation).
5. Select **Aggregate**, to enable the aggregate-address or summarization option. This option is disabled by default, and member peers do not understand aggregated confederation AS_PATH information.

6. Select **Hop Self**, to indicate that the peer group should advertise itself as the next hop.
7. Click the **Update Record** icon to save the **BGP Peer Group** record. The new entry is inserted into the BGP configuration as a new record, listed under **BGP Peer** Group.
8. Repeat the previous steps to insert another **BGP Peer Group** record for this SVN.
9. For a given **BGP Peer Group** record, click the **Edit** icon to modify the record, and again click the Update Record icon. Click the **Delete** icon, to remove the record.
10. **Click Save and Close** or click **Save** to continue to *Add Site SVN — BGP Config Table*.

1.6.8 Add Site SVN — BGP Config Table

Using the *BGP configuration table* dialog, one or more BGP Configuration table records may be created, where each record contains a **ConfigTable ID**, an **Import Map ID**, an **Export Map ID**, an **Advertise Map ID**, and a **Non Exist Map ID**.

The Advertise-map specifies match statements that the route must pass before it is passed to the next route map; in the case of a Non-Exist-map, a route is not advertised unless a prefix in the BGP table does not match a prefix in the prefix lists.

.

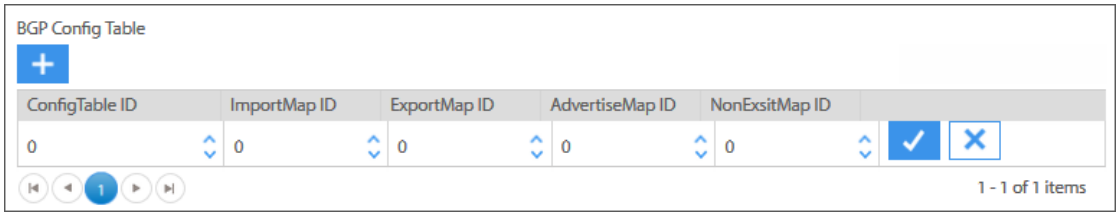

Figure 1-15. BGP Config Table Parameters

To configure the Site SVN BGP Config Table parameters:

1. With the **Add Site SVN** page open to the **BGP** tab, click the **Add Record** icon, under the **BGP Config Table** section, to define a new BGP Config Table record.
2. Use **ConfigTable ID** to enter a numeric identifier for this configuration table record.
3. Enter an index value in **ImportMap ID**, to identify a BGP map to use as the import map.
4. Enter an index value in **ExportMap ID**, to identify a BGP map to use as the export map.
5. Enter an index in value in **AdvertiseMap ID**, to identify a BGP route map to use as the advertise map. Both the **Advertise Map ID** and **Non-Exist Map ID** must be configured for the conditional advertisement feature to function correctly.
6. Use **Non-ExistMap ID** to enter an index that identifies a BGP route map to use as a non-exist map. Both the **Advertise Map ID** and **Non-Exist Map ID** must be configured for the conditional advertisement feature to work correctly.
7. Click the **Update Record** icon to save the **BGP Config Table** record. The new entry is inserted into the configuration as a new record, listed under **BGP Config Table**.
8. Repeat the previous steps to insert another **BGP Config Table** record for this Site SVN.
9. For a given **BGP Config Table** record, click the **Edit** icon to modify the record, and again click the Update Record icon. Click the **Delete** icon, to remove the record.

10. **Click Save and Close** to save the Site SVN configuration or click **Save** to continue in modify mode with *Add Site SVN — BGP Aggregate Address*.

1.6.9 Add Site SVN — BGP Aggregate Address

By configuring a BGP *aggregate-address,* a number of IP addresses can be replaced with a single address that represents a set of included addresses. The aggregate is used to simplify and minimize the size of routing tables. Aggregate networks are configured before being advertised to external peers.

The router's IP routing table must contain networks that represent a subset of the aggregate in order for the aggregate to be advertised; only the aggregate, and not the individual routes, are advertised to external BGP peers. Internal BGP peers receive the individual routes if they originated outside the AS; and do not exchange internal routes via BGP.**To add Site SVN** BGP Aggregate Address configuration parameters**:**

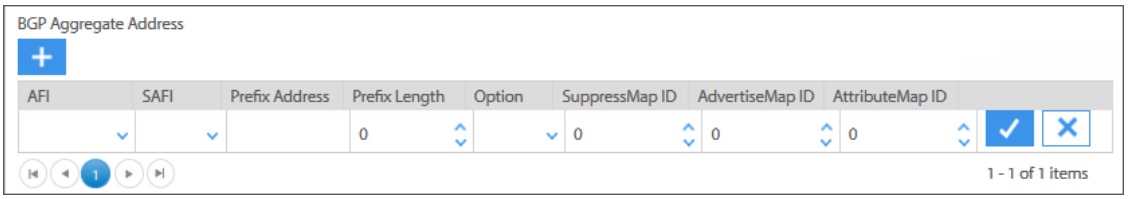

Figure 1-16. BGP Aggregate Parameters

1. With the **Add Site SVN** page open to the **BGP** tab, click the **Add Record** icon, under the **BGP Aggregate Address** section, to define a new Aggregate Address.
2. Use the **AFI** drop-down to specify **IPv4** or **IPv6** as the Address Family of this aggregate address record.
3. Use the **SAFI** drop-down to enter the Subsequent Address Family Identifier of this prefix entry, as **MPLS_BGP_VPN(1)**, **Multicast(2)**, **Unicast(3)**, or **Both**. This parameter supplies additional data on the type of the Network Layer Reachability Information that is carried in the prefix—for example, unicast forwarding or multicast forwarding.
4. Under **Prefix Address,** enter the prefix address of this Aggregate Address.
5. Under **Prefix Length**, enter the length of the prefix of this Aggregate Address.
6. Use the **Option** drop-down to select one of the options to be applied to the configured Aggregate Address. If **None (1)** is chosen, more specific routes are installed in the routing table, but the AS_PATH will lose information as it no longer contains AS_SETs.
7. Use **SuppressMap ID** to specify the index of the Route Map used to suppress routes. The match clauses of this Route Map are used to selectively suppress specific routes from being advertised. No entry should be made if the **Option** field is configured with either **Summary(2)** or **Summary with AS Set(4)**.
8. Use **Advertise Map ID** to specify the index of the Route Map used to advertise routes. The match clauses of this Route Map are used to select routes which, although they match the aggregate address, they should not be aggregated.
9. Use **Attribute Map ID** to specify the index of the Route Map used to set the attributes of aggregated routes. The set clauses of this Route Map are used to set the path attributes of the aggregated route.

10. Click the **Update Record** icon to save the **BGP Aggregate Address** record. The new entry is inserted as a new record, listed under **BGP Aggregate Address**.
11. Repeat the previous steps to insert another **BGP Aggregate Address** record for this SVN.
12. For a given **BGP Aggregate Address** record, click the **Edit** icon to modify the record, and again click the Update Record icon. Click the **Delete** icon, to remove the record.
13. **Click Save and Close** to save the Site SVN configuration or click **Save** to continue in modify mode with *Add Site SVN — BGP Route Map*.

1.6.10 Add Site SVN — BGP Route Map

A *route map* defines the routing policies that are considered before a router examines its forwarding table. The BGP route map configuration is, therefore, a way of defining specific routing policy that takes precedence over the different route processes. In other words, these policies support the filtering of the routing updates that are forwarded by BGP.

To configure the Site SVN BGP Route Map parameters:

1. With the **Add Site SVN** page open to the **BGP** tab, click the **Add Record** icon, under the **BGP Route Map** section, to define a new Route Map configuration for this Site SVN.
2. Enter a numeric **RouteMap ID** that identifies the new Route Map index, which is used by BGP neighbors to reference the Route Map.
3. Enter the **Route Map Number** that identifies a secondary index of this Route Map entry, which is used to reference more than one filter per Route Map index.
4. Select **Permit** to enable the action that is applied to a route that matches the route map entry. This parameter is ignored for a Route Map used for aggregation.
5. Use the **ORF Association** drop-down to choose the type of association, if any, this route map has with the Outbound Route Filtering (ORF) protocol. Specify **Local (1)** if the filtering information contained in this route map is advertised to peers with appropriate ORF support; specify **Remote (2)** if this route map is created to respond to ORF(s) received from a peer; otherwise choose **None(0)**.
6. Enter a value in **Map Cont**, to indicate the Route Map clause at which processing should continue. This entry is only valid for Route Maps of permit type that are used for policy filtering.
7. Use the **AFI** (Address Family Identifier) drop-down to select the address index as **IPv4(0)** or **IPv6(1)**, to match against the AFI type.
8. Use the **SAFI** (Subsequent Address Family Identifier) drop-down to set the index as **MPLS_BGP_VPN(1)**, **Multicast(2)**, **Unicast(3)**, or **Both (0)**, to match against the AFI type.
9. Enter a value in **MaMed**, which the *Multiple Exit Discriminator* attribute must match.
10. Enter a value in **MaAs-Path**, as the regular expression to use when matching the "**AS-Path**" for a route. "**AS**" numbers are matched as decimal numbers.
11. Use one of the following entries in **MaCommunity**:
    a. **If representing non-ORF entries:** enter the regular expression to use when matching elements of the *Community* list for a route.
    b. **If representing ORF entries:** enter a comma separated list of communities that are logically "OR-ed" when matching.

12. Use one of the following entries in **MaExCommunity**:
    a. **If representing non-ORF entries:** enter the regular expression to use when matching elements of the *Extended Community* list for a route.
    b. **If representing ORF entries:** enter a comma separated list of extended communities that are logically "OR-ed" together when matching.
13. Enter a value in **SeMed**, to which the *Multi Exit Discriminator (MED)* is set if there is a match. A value of '0' indicates that the **MED** should be removed.
14. Use the **SeCommunity Action** drop-down to select the action to be taken on the Community List if this Route Map matches the route.
15. Use **SeCommunity**, to enter the regular expression to use when executing the action specified by the **SeCommunity Action** parameter.
16. Use the **SeExCommunity Action** drop-down to select the action to be taken on the Extended Community list if this Route Map matches the route.
17. Use **SeExCommunity**, to enter the regular expression to use when executing the action specified by the **SeExCommunity Action** parameter.
18. Use **SeAsTimes** to enter the number of times the AS number is prefixed to the AS path if there is a match. This value is only valid if the Route Map is used for exporting routes, or for setting attributes for an aggregate route for which the AS_SET option is not set.
19. Use the **SeAs Action** drop-down to select the action taken by the **SeAsTimes** parameter, when this parameter is configured with **SET(1)** or **REM_MATCH_AND_SET(3)** as updating attributes. Other options include **IGNORE(0)** and **REM_MATCH(2)**.
20. In **Se Local Pref**, enter the local preference value to set when a route match occurs.
21. Use the **SeOrigin**, drop-down to select the origin value to set if there is a match. The options include **IBGP(0)**, **EBGP(1)**, or **Incomplete(2)**.
22. Use **Se Weight**, to enter a weighted value to assign to a path if there is a match.
23. In **SNR Metric Router Map Index**, enter the Route Map index for the SNR metric.
24. In **Se NextHop** enter the value to set for the Next Hop if a match occurs. If the value is set, then the match **AFI** and **SAFI** fields must also be set appropriately to ensure that the address type is being set appropriately to IPv4 or IPv6.
25. Click the **Update Record** icon to save the **BGP Route Map** record. The new entry is inserted into the configuration as a new record, listed under **BGP Route Map**.
26. Repeat the previous steps to insert another **BGP Route Map** record for this Site SVN.
27. Click the **Edit** icon on a given **BGP Route Map** record, to modify the record, and again click the **Update Record** icon. Click the **Delete** icon, to remove the record.
28. **C**lick **Save and Close** to save the configuration.

1.7 Creating and Modifying a PP Server SVN

The Velocity system PP cluster is composed of one or more server nodes, which are located in both the Primary and Diversity SAS. In the case of the Global Bandwidth Manager, the cluster is at the NOC site. Each PP server must be a member node of the iDirect Admin SVN, Tunnel SVN, and of each associated Customer SVN.

At the time the Site SVN is created, a PP Server SVN is generated for each PP blade member of a cluster. To complete the configuration, the IP addresses for each PP Server SVN, must be appropriately modified, manually, using addresses available in the Site SVN. The **PP Server SVN** configuration dialog is accessed from the **Physical Domain** menu or using the Actions menu of a selected PP server.

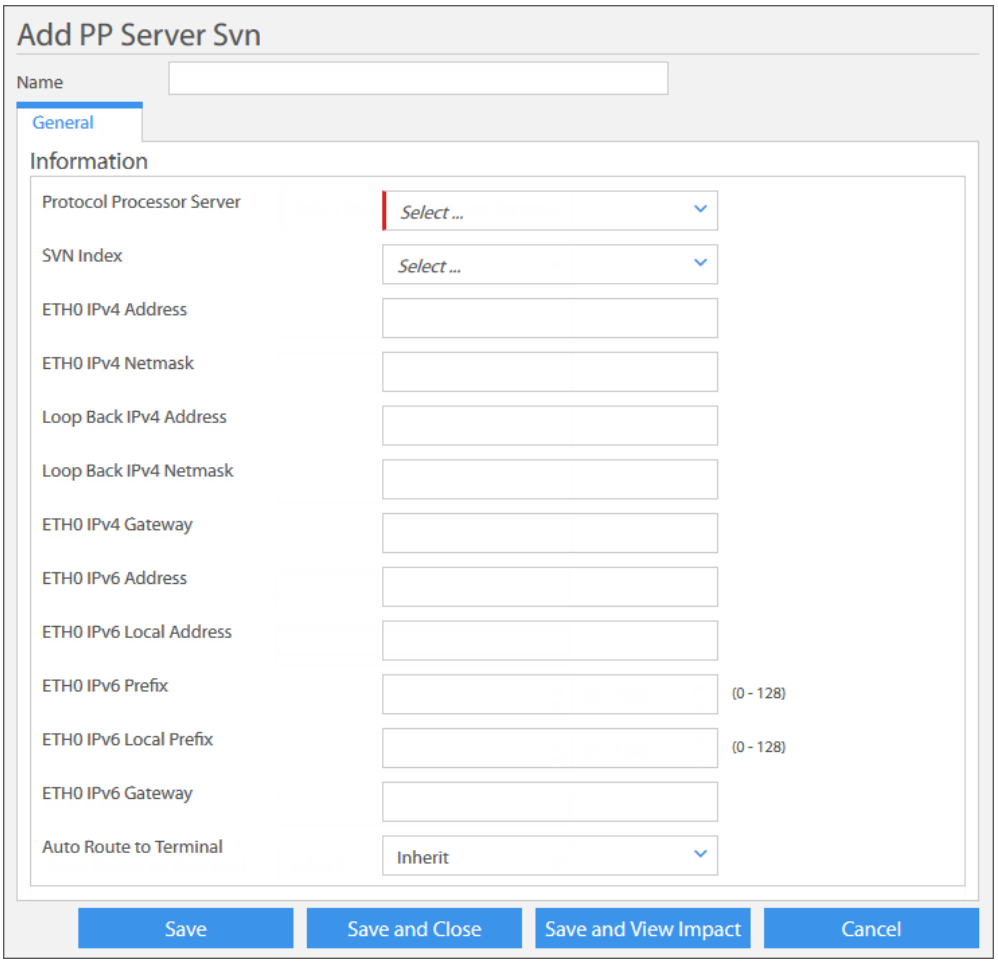

Figure 1-17. Add PP Server SVN Configuration Dialog

To add a PP Server SVN:

1. Click the **Configuration** tab > **Physical Domain** > **More Options > Add> Blade SVN.**
2. Type the **Name** of the new blade SVN.
3. Use the drop-down and select the associated **Protocol Processor Server**.

4. Enter the **ETH0 IPv4 Address** and **Netmask** Address.
5. Enter the **Loop Back IPv4 Address** and **Netmask** Address.
6. Enter the **Gateway** Address.
7. Enter the **ETH0 IPv6 Address** and **Local Address**.
8. Enter the **ETH0 IPv6 Prefix**.
9. Enter the **ETH0 IPv6 Local Prefix**.
10. Enter the **ETH0 IPv6 Gateway** Address.
11. Use the **Auto Route To Terminal** drop-down and choose **Enable**, **Disable**, or **Inherit**.
12. Click **Save** to save the configuration or click **Save and Close** to save the configuration and open the **Browse Blade SVN** window.

1.8 About IF Domains, Chassis, and Line Cards

In an iDirect Velocity network, the SAS provides IP connectivity between a terrestrial IP network, also called the data communications network (DCN), and Velocity satellite terminals via a radio frequency system (RFS) and a satellite. The connection to the terrestrial Internet is via redundant 10 Gbps Ethernet interfaces.

The L-band interface between the SAS and the RFS is via multiple IF Domains that transport service channels between the radio frequency (RF) system and the Velocity line cards. Table 1-4 shows an example of six IF Domains for six reuse frequencies — each has an identifying color code that represents a slot group within each chassis, the IF frequency range, and the RFS polarization segment.

The IF interface between the RFS and the SAS provides three IF signals (domains) for right-hand (RH) polarization and three IF signals for left-hand (LH) polarization. These six IF Domains transport the data of the various channels, between the RFS and the Line Cards.

Table 1-4. Example - Line Card IF Domain Groups and Channel Assignments

IF Domain	Color	IF Frequency	RFS Polarization Segment
1	Brown	950-1700	RH Low
2	Red	950-1700	RH Mid
3	Orange	950-1700	RH High
4	Yellow	950-1700	LH Low
5	Green	950-1700	LH Mid
6	Blue	950-1700	LH High

1.9 Add IF Domains

An *IF domain* is a specific group of line cards and IF frequency ranges at which these line cards operate. Each domain has a combination of transmit and receive line cards installed in specific slots, with defined physical wiring at a given Teleport. The NMS representation of the IF domain is dependent on what is configured by the user, and therefore the NMS configuration and the actual physical wiring should be verified to coincide.

In an iDirect Velocity system there are no fixed assignments of line cards to iNets, and the available channels are arranged into different IF domains such that each channel is in a fixed IF frequency range. This arrangement means that line cards in a Teleport connect to specific IF domains, and each line card can only be assigned to a channel in its IF domain. A line card wired to IF Domain 1, for example, cannot be assigned to an iNet for a channel in IF Domain 2.

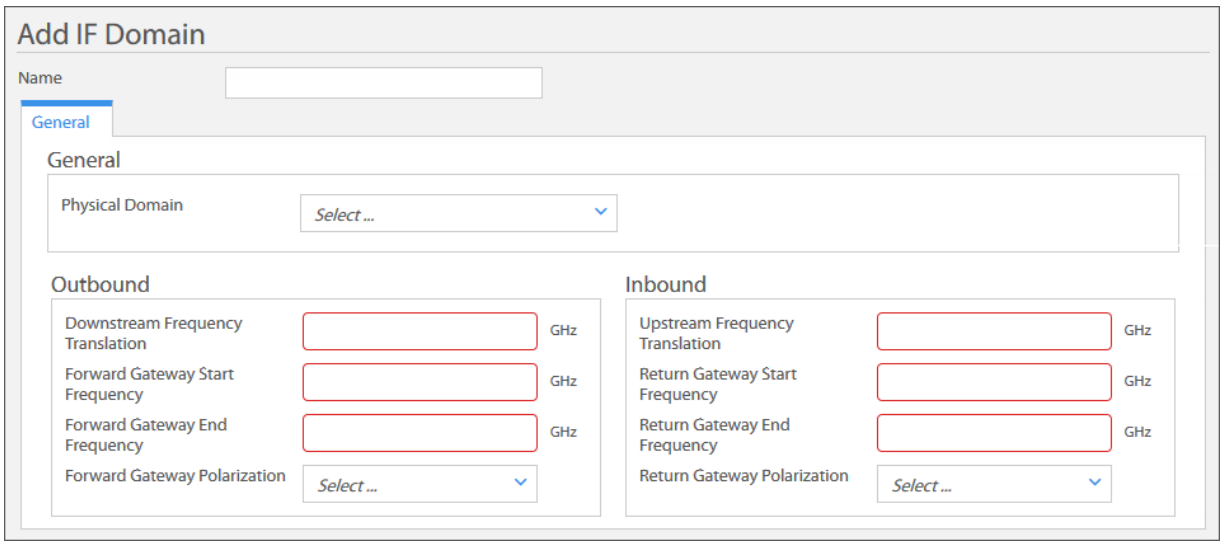

Figure 1-18. Add IF Domain Dialog

To configure an IF domain:

1. Click the **Configuration** tab > **Physical Domain** > **More Options** > **Add > IF Domain.**
2. Type the **Name** of the new IF domain.
3. Select the appropriate **Physical Domain** to which this IF domain is associated.
4. Enter the **Downstream Frequency Translation** value and the **Upstream Frequency Translation** value for this IF domain.
5. Specify the **Forward Gateway Start Frequency** and **Forward Gateway End Frequency**.
6. Specify the **Return Gateway Start Frequency** and the **Return Gateway End Frequency**.
7. Use the **Forward Gateway Polarization** drop-down to select the RFS polarization of the outbound gateway of this IF domain as **Vertical** or **Horizontal**, **LHCP** or **RHCP**.
8. Use the **Return Gateway Polarization** drop-down to select the RFS polarization of the inbound gateway of this IF domain as **Vertical** or **Horizontal**, **LHCP** or **RHCP**.
9. Click **Save** to save the IF Domain and continue or click and **Save and Close**.

1.10 Add Chassis

In a given network there is 1 to (n) chassis, and each chassis has five line card groups, with four line card slots per group. A chassis is added to the NMS, using the **Add Chassis** dialog. The line card in each slot is indirectly associated with a specific IF domain.

If a chassis is one of the required chassis in a multi-satellite per chassis configuration, then one chassis is configured for each additional satellite (Site), where certain configuration parameters are the same for each chassis.

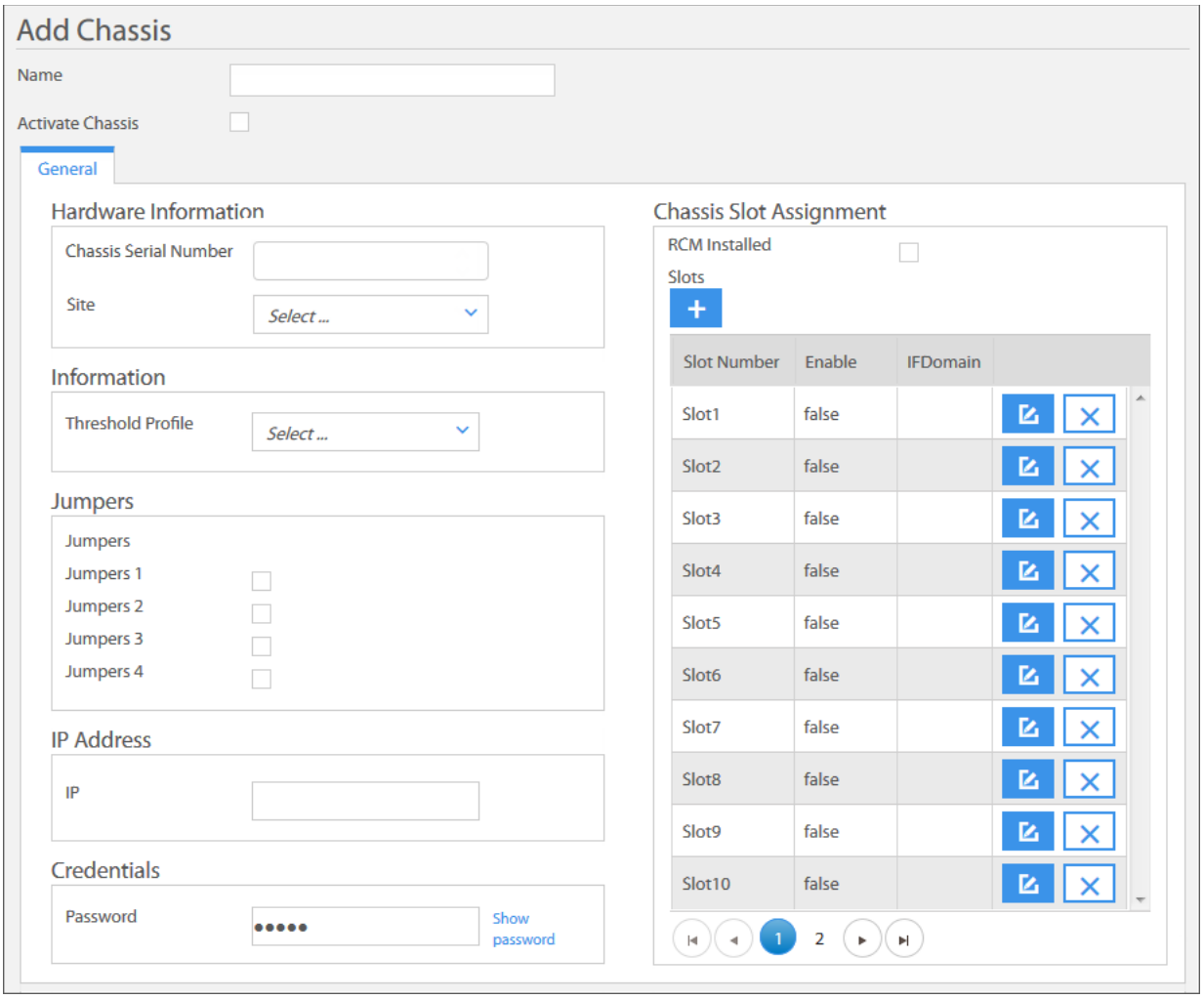

Figure 1-19. Add New Chassis

Prior to configuring a chassis it is important to have the following information:

- Chassis IP Address assignment (Configured on chassis using Midas interface)
- A unique password (Configured on chassis using Midas interface)
- Line card slot assignments to enable

To add a new chassis to the NMS:

1. Click the **Configuration** tab > **Physical Domain > More Options > Add** > **Chassis.**
2. Type the **Name** of the new chassis.
3. Select **Activate Chassis** to set the chassis status as **Activated.**
4. Enter the correct **Chassis Serial Number** of the chassis.
5. Use the **Site** drop-down to select the Teleport site to which this chassis is assigned.
6. Use the drop-down to choose the appropriate **Threshold Profile** for chassis.
7. Enter the chassis **IP** address. This is the IP address assigned using the Midas interface.
8. Enter the administrator **Password** used to access the chassis (default is '**midas'**).
9. Under **Chassis Slot Assignment**, select **RCM Installed** to indicate whether the RCM module is already installed.
10. Under **Slots**, click the **Edit** icon on a slot, and select the adjacent **Enable** check box to enable power to the slot.The available 20-slots of a chassis are listed on two pages.
11. Click **Save** to save the chassis configuration and continue or click **Save and Close**.

1.11 Add Shared Physical Chassis Configuration

If a physical chassis is to be shared across multiple sites, for the purpose of supporting multiple satellites within that chassis, then that chassis must be configured in the NMS, for each site that controls slots in the chassis. If there are three satellites (Sites), then three chassis must be configured in the NMS. The chassis configuration of each site must contain only those slots that are controlled by that site. The remaining slots should be removed.

If, for example, two satellites (sites) are supported in the chassis then slots-1-10 might be configured in the first chassis, while slots 11-20 are removed; and slots 11-20 are configured in the second chassis, while slots 1-10 are removed. For each chassis, the parameters **Serial Number**, **IP Address**, and **Password** must be configured the same.

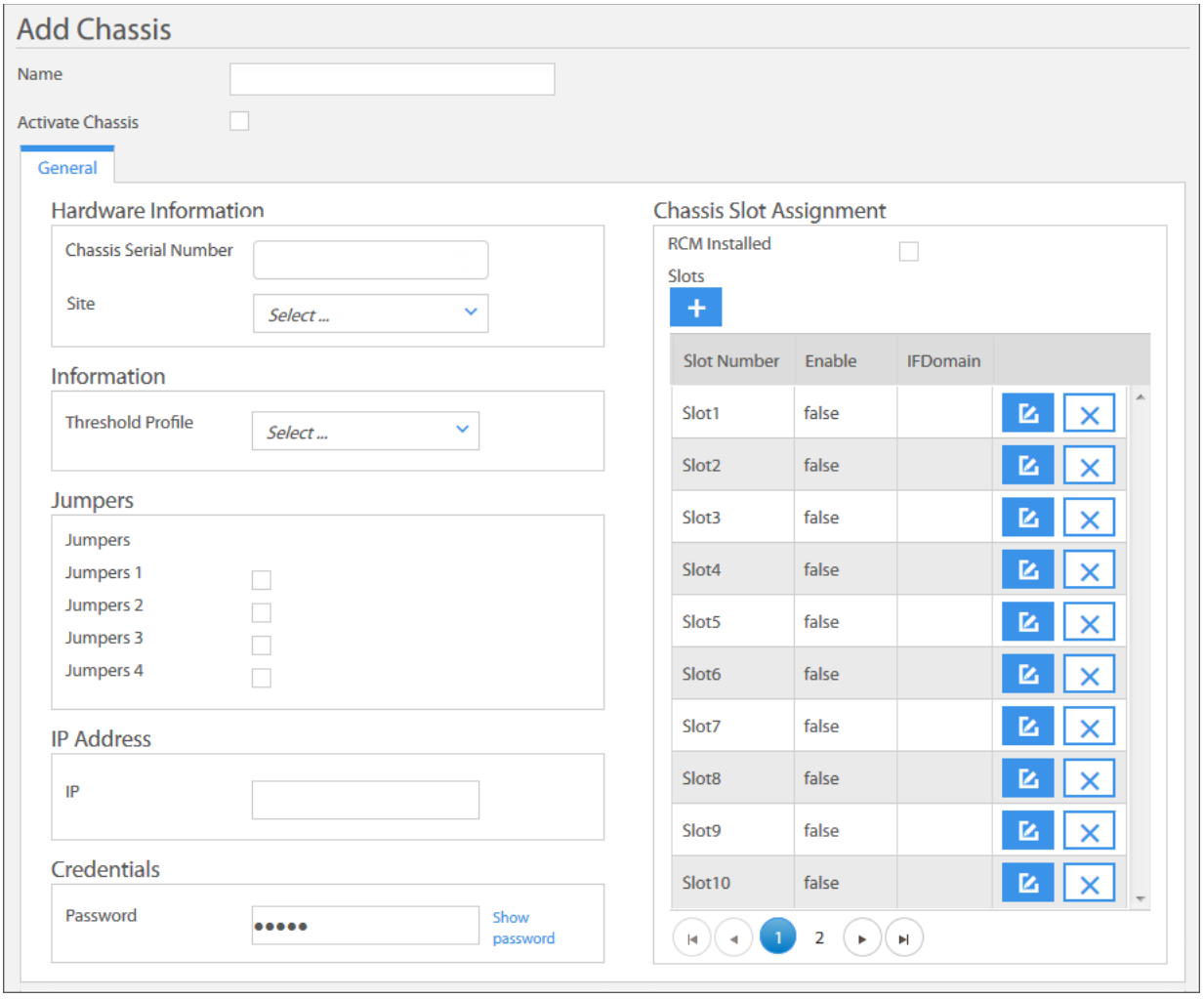

Figure 1-20. Add Shared Chassis

To add a new chassis for each site in a shared chassis (do the following for each site):

1. Click the **Configuration** tab > **Physical Domain > More Options > Add** > **Chassis.**
2. Type the **Name** of the new chassis.
3. Select **Activate Chassis** to set the chassis status as **Activated.**
4. Enter the **Chassis Serial Number** — assign same serial number to each additional chassis of the shared configuration.
5. Use the **Site** drop-down to select the site to which this chassis is assigned.
6. Use the drop-down to choose the appropriate **Threshold Profile** for chassis.
7. Enter the chassis **IP** Address — assign same IP address to each additional chassis of the shared configuration. This is the IP address assigned using the Midas interface.
8. Enter the administrator **Password** used to access the chassis (default is '**midas'**). Assign the same password to each additional chassis of the shared configuration. This is the IP that is assigned using the Midas interface.
9. Select **RCM Installed** to indicate whether the RCM module is installed.
10. Enable, in each chassis, the slots that are controlled by the additional site.
11. use the drop-down to select the appropriate IF Domain of each enabled slot.
12. Remove, from each chassis, slots that are not controlled by the additional site.
13. Save the configuration for the chassis. Repeat for each additional satellite.

1.12 Add Line Cards

The NMS provides configuration support pages for the addition, modification, and deletion of hub line cards. These pages are accessed from the **Physical Domain** menu of the **Configuration** tab.

A new line card is added to the NMS using the Add Line Card configuration dialog.

When configuring a line card it is important to know the following items:

- Line Card Management IP Address
- Line Card Model Type (**Rx** = **Tesla**; **Tx** = **Marconi**)
- Line Card Serial Number
- Line Card Installed IF Domain (and domain frequency) and Chassis Slot Number
- Line Card Access Credentials (User, Administrator, and Guest)

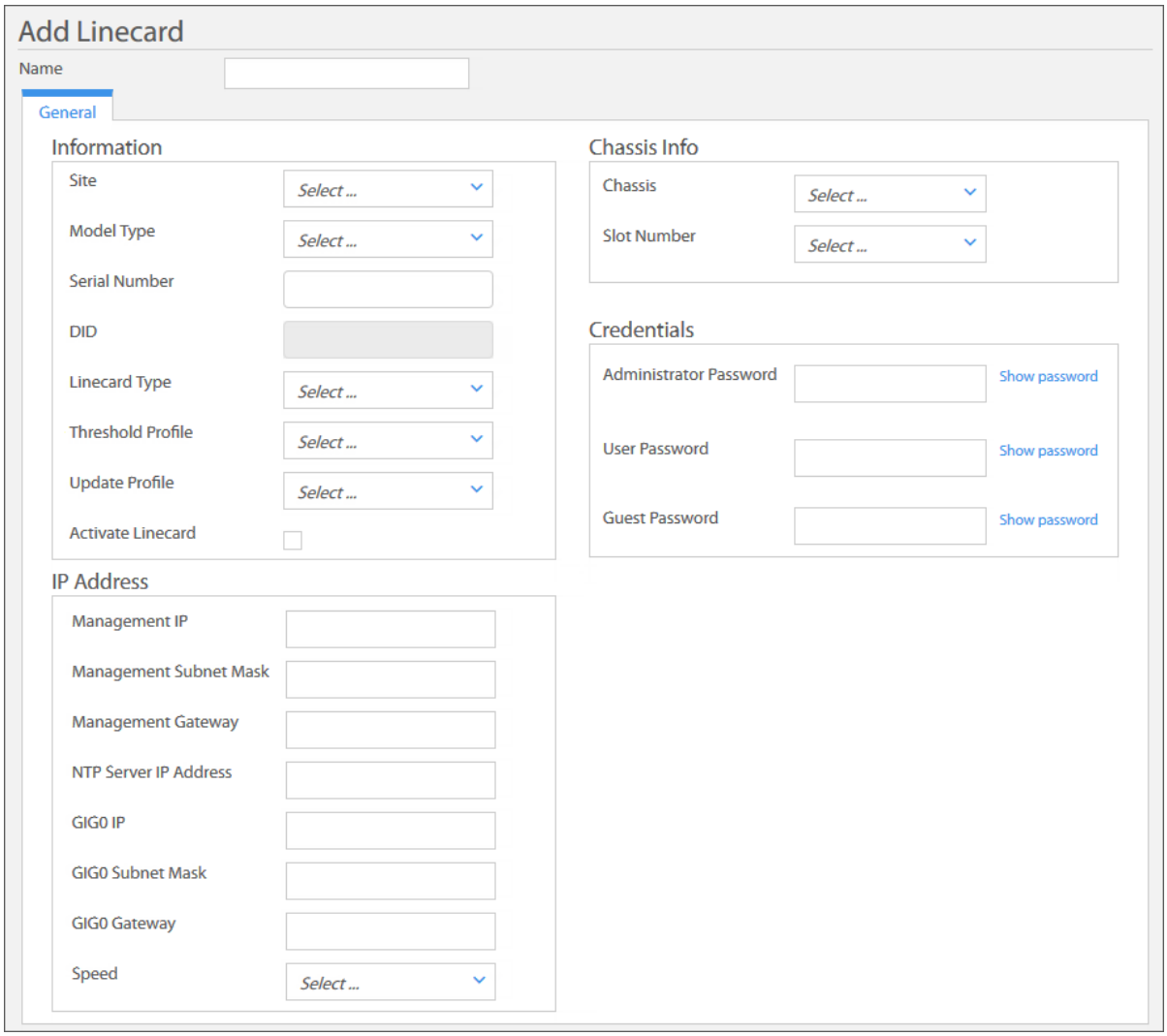

Figure 1-21. Add Line Card Dialog

To add a new line card:

1. Click the **Configuration** tab > **Physical Domain > More Options > Add > Line Card.**
2. Specify a unique **Name** for the line card in the **Add Line Card** dialog.
3. Select the **Model Type** of the line card. The type must match the installed line card. **Marconi** for transmit line cards; and **Telsa** for receive line cards.
4. Enter the line card **Serial Number**. A system-generated Derived ID (**DID**) is displayed**.**
5. Select the **Line Card Type** as **Tx**, for transmit; or **Rx**, for receive.
6. Select the appropriate **Threshold Profile** to be applied to the line card — for example, the **Line Card Default Thresholds.**
7. Select **Activate Line Card** to set the state of the line card as **Activated.**
8. Select the **Update Profile** to be applied to the line card — for example, the **Default Line Card Update Profile**.
9. Under **IP Address**, enter the **Management IP** address, **Management Subnet Mask**, and **Management Gateway** IP address for use by the NMS to communicate with the line card.
10. Specify an **NTP Server IP Address** for this line card.
11. Enter the **GIG0 IP** address, **GIG0 Subnet Mask**, and **GIG0 Gateway** addresses for downstream data communication from the Protocol Processor to the network.
12. Use the **Speed** drop-down and set the GIG0 port speed to 100 Mbps or 1000 Mbps.
13. Enter a **Guest Password**, **User Password**, and **Administrator Password**, for the associated users to access the line card. The default passwords are iDirect.
14. Use the **Threshold Profile** drop-down to select **Line Card Default Thresholds Profile** as the threshold profile to be applied to the line card by the NMS Stats Manager.
15. Select the **Chassis** in which the line card is installed.
16. Select the **Slot Number** of the slot where the line card is installed.
17. Under **Credentials**, **Administrator Password**, **User Password**, and **Guest Password**.
18. Click **Save** to save the line card configuration and continue, or click **Save and Close** to close the dialog and open the **Browse Physical Domain** page.

1.13 About Velocity Network Servers

In an iDirect Velocity system, a *cluster* is a rack-mounted group of servers that act as a single system to provide related system resources. As network requirements grow, additional servers are added to a cluster. Currently, only one cluster, of a given type, may be configured at a site, and this cluster must be configured prior to adding servers to the cluster. Velocity clusters include: Protocol Processor Clusters, NMS Clusters, and optional Squid (Web Cache) Clusters.

1.13.1 About Protocol Processor Servers

Protocol Processor configuration involves defining the general parameters that apply to the PP cluster and the individual PP server nodes. These are the Teleport servers (primary/backup), which are responsible for processing functions, traffic routing, load balancing, automatic fail-over and automatic redistribution of load across the remaining PP servers. A PP cluster also resides at the NOC for handling global bandwidth management.

1.13.2 About NMS Servers

The NMS is composed of a comprehensive Web client and required servers that collectively provide control and visibility of all network components. The NMS servers provide support for managing network configuration and control, software version management and updates, as well as for monitoring and reporting on network events and alarms.

Although NMS operations are generally centralized at the NOC, both centralized and distributed operations are supported. In particular, the NMS supports Teleport-level operations if the NOC is not accessible. The NMS cluster contains the following server types:

- *NMS Storage/Compute Servers* — are responsible for processing and computational work as opposed to persistent data storage. The emphasis is on maximizing execution threads, processing speed, memory usage and overall network throughput.
- *NMS Stats Servers* — receive data from PP servers and provide data to the NMS when requested. The main emphasis of these servers is on maximizing local storage throughput and in providing Network File System (NFS) exports to other cluster nodes.

1.13.3 Adding a Protocol Processor (PP) Cluster

In addition to specifying the general parameters of each PP cluster, each single instance process that runs on each cluster will require its own virtual IP address. These addresses must be configured from the IP address space in the Teleport subnet. New PP clusters are added to the NMS using the Add PP Cluster configuration dialog.

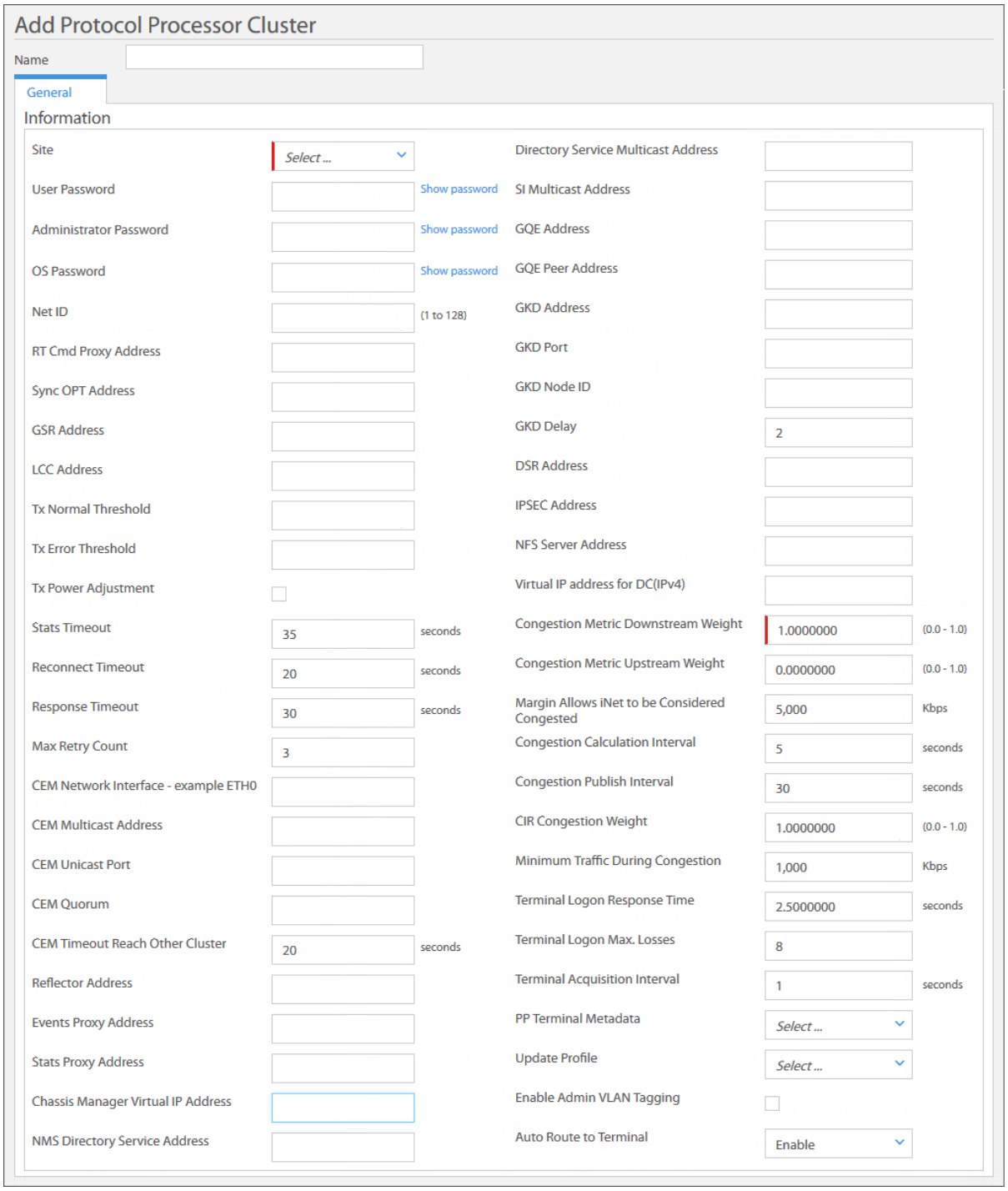

Figure 1-22. Add Protocol Processor Cluster Dialog

To add a protocol processor cluster:

1. Click the **Configuration** tab > **Physical Domain > More Options** > **Add > Protocol Processor Cluster.**

2. Type the **Name** of the new PP Cluster.
3. Use the **Site** drop-down to select the site at which the **PP Cluster** is located.
4. Enter a **User Password** for gaining access to the cluster at the application level.
5. Enter a **Administrator Password** for gaining administrative access to the cluster.
6. Enter an **OS Password** for gaining access to the cluster at the system level.
7. Enter the network identification (**Net ID)** of the network to which the PP cluster belongs. It is important that this network ID is unique to every cluster.
8. Enter a unique virtual IP address for each of the single instance PP cluster processes:
   a. **RT Cmd Proxy Address —** process that accepts real-time probe commands from the NMS GUI, for execution on specific network elements for debugging purposes.
   b. **Sync OPT Address —** process that receives PP options files from the Update Manager.
   c. **GSR Address** (Global System Registry) **—** each PP cluster node registers its managed processes with the GSR, which in turn provides access information that allows communication with these resources by all other nodes in the cluster.
   d. **LCC Address** (Line Card Controller) **—** process that manages Teleport line cards to iNets/carriers assignment, line card fail-over, and communicate with chassis manager process to control on/off power to chassis slots.
9. In **Tx Normal Threshold**, specify an acceptable deviation from the Tx line card EIRP.
10. In **Tx Error Threshold**, enter a deviation from the Tx line card EIRP, considered an error.
11. In **Stats Timeout**, specify a time out value for communication with the Stats process.
12. In **Reconnect Timeout**, specify a time out value after which a reconnect attempt to establish cluster-to-node communication is allowed.
13. In **Response Timeout**, specify a response time out, in seconds.
14. In **Max Retry Count**, enter the maximum retry attempts for cluster-node communication
15. In **CEM Network Interface**, specify an interface name for the cluster election manager's (CEM) LAN interface, for example – **ETH0**.
16. In **CEM Multicast Address**, enter multicast address for CEM -to-PP node communication.
17. In **CEM Unicast Port**, enter a unicast port number for the cluster election manager.
18. In **CE Quorum**, specify a minimum number of working PP servers to keep cluster running.
19. In **CEM Timeout Reach Other Cluster**, specify a communication time out, in seconds, for when communicating with other clusters.
20. In **Reflector Address**, enter a virtual IP address for PP cluster process that relays messages from the congestion control process to the process in all nodes that manages an alleviate network congestion.
21. In **Events Proxy Address**, specify an IPv4 address for the events server proxy.
22. In **Stats Proxy Address**, enter an IPv4 address for the stats server proxy.
23. In **Chassis Manager Virtual IP Address**, specify IPv4 address for communication between this cluster and the Chassis Manager.

24. In **NMS Directory Service Address**, specify a valid IPv4 address for addressing communication with the NMS Directory Service process.
25. In **Directory Service Multicast Address**, specify a valid multicast address for communication with the Directory Service.
26. In **SI Multicast Address** enter a Multicast IP Address for system messages that are broadcast by the Protocol Processor to the Satellite Terminals.
27. Global Key Distribution (GKD) is required to generate the Network Acquisition Keys (ACC Keys) used by Satellite Terminals to join a TRANSEC network. Use the following fields appropriately to enter GKD parameters**:**
    a. **GKD Address** — the virtual IP Address of the GKD master process
    b. **GKD Port** — the port number the GKD master process
    c. **GKD Node ID —** Node identification number
    d. **GKD Delay —** the connection delay
28. In **NFS Server Address**, enter the IP address of the Network File System server.
29. In **Virtual IP Address for DC(IPv4)**, enter the IPv4 address of the designated coordinator (DC) node. This node runs a process that manages resources across all cluster nodes.
30. Use the congestion parameter defaults, or enter following values that are used for congestion management and PP server load balancing calculations:
    a. **Congestion Metric Downstream Weight/Congestion Metric Upstream Weight**
    b. **Margin Allows iNet to be Considered Congested**
    c. **Congestion Calculation Interval**
    d. **Congestion Publish Interval**
    e. **CIR Congestion Weight**
    f. **Minimum Traffic During Congestion**
31. In **Terminal Logon Response Time**, specify the timeout period, after which the terminal considers that an acquisition burst was not received if no response has yet arrived.
32. In **Terminal Logon Max. Losses**, enter the maximum number of failed acquisition attempts, before the terminal is flagged as being out of service.
33. Enter **Terminal Acquisition Interval**.
34. Do not use the **PP Terminal Metadata** field. This field is reserved for future use.
35. Select a configured **Update Profile** that the Update Manager should apply to this PP cluster. See the *iDirect Pulse NMS user Guide*, *Adding an Update Profile*.
36. Select **Enable Admin VLAN Tagging** if this feature is required for the PP cluster.

1.13.4 Adding a Protocol Processor Server

The NMS provides configuration pages that enable operators to add, modify, and delete PP servers. New PP servers are added to the NMS using the Add Protocol Processor Server configuration dialog. A new PP server can be configured for an existing Teleport or at the NOC, as a node in the PP cluster for global bandwidth management.

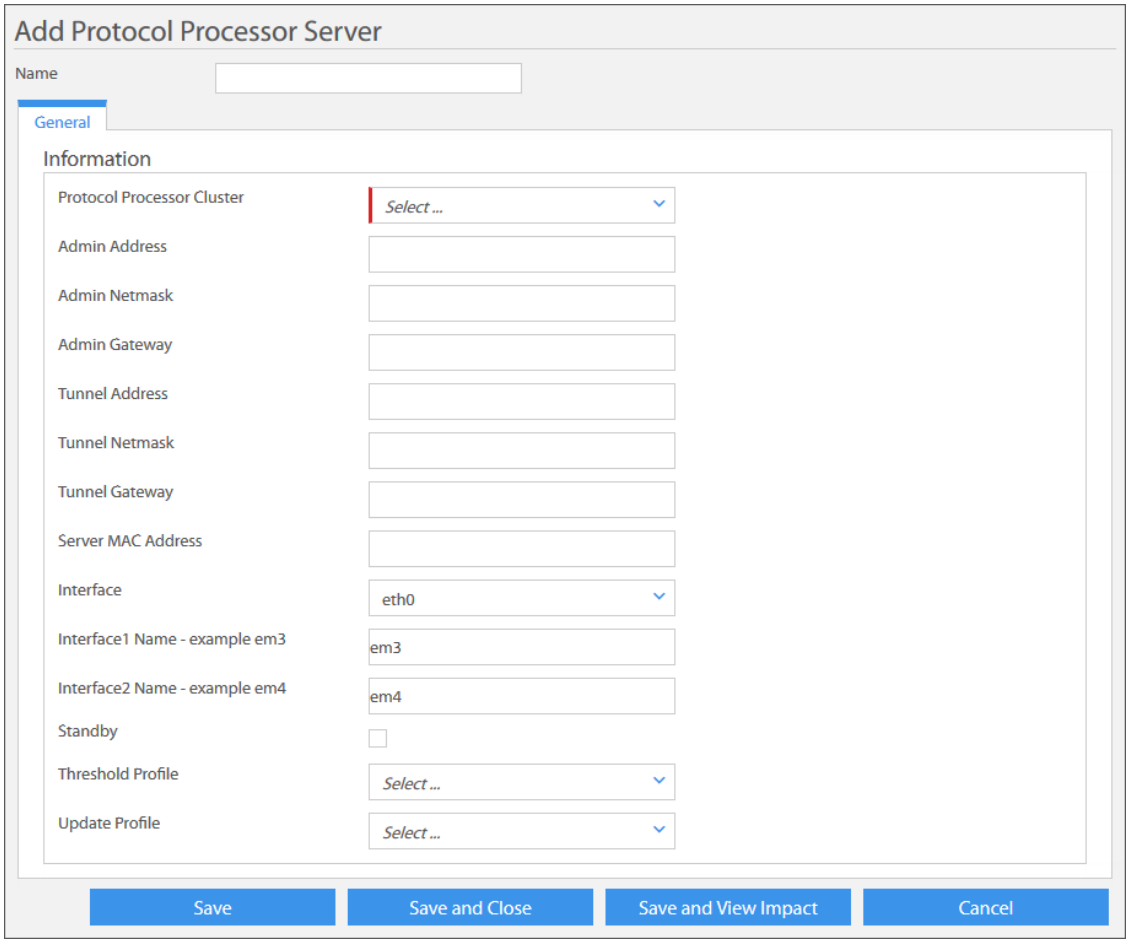

Figure 1-23. Add Protocol Processor Server Dialog

To add a Protocol Processor server:

The PP Cluster should be configured before configuring the PP cluster server nodes.

1. Click the **Configuration** tab > **Physical Domain > More Options > Add > Protocol Processor Server.**
2. Type the **Name** of the new PP server.
3. Under the **Information** section, use the drop-down to select the **Protocol Processor Cluster** to which the new PP server is a member node.
4. For the interface, specify the following IP address information:
   a. Add the **Admin Address**.

   b. Add the **Admin Netmask** address.

   c. Add the **Admin Gateway** address. This is the IP address of the upstream router interface connected to the to upstream LAN segment.

5. Enter the **Server MAC Address** of the PP server.
6. Use the **Interface** drop-down to select **ETH0**.
7. In **Interface1 Name,** specify the name of the existing interface.
8. In **Interface2 Name,** specify the name of the existing interface.
9. Enable **Standby** if this PP server should assume the standby mode of operation.
10. Select a user-defined **Threshold Profile** to apply to this PP Server. Default threshold profiles are listed, however users may define and select a threshold profile appropriate for the PP Server. See the *iDirect Pulse NMS user Guide*, *Adding a Stats Threshold Profile*.
11. Select the **Update Profile** to apply to this PP server. Default update profiles are listed, however users may define and select an update profile appropriate for the PP server. See the *iDirect Pulse NMS user Guide*, *Adding an Update Profile*.
12. Click **Save** to save the PP Server and continue, or click **Save and Close** to close the dialog and open the **Browse Physical Domain** page to search for the new PP server.

1.13.4.1 NMS Generated PP Server SVNs

When a new Protocol Processor (PP) Server is added to the NMS, as part of an existing PP cluster, associated PP Server SVNs are automatically generated in the NMS. The NMS performs the following actions:

- Automatically create ServerSVN for the **Admin** and **Tunnel** SiteSVN parents, and associate them with the new PP Server. After these SVNs are created, the user must modify and re-save each after assigning an appropriate IP address.
- Automatically create a ServerSVN for every **Customer SVN**, and associate each with the new PP server. After these elements are generated, the user must modify each Customer SVN to assign an appropriate IP address and then re-save the SVN.
- After IP addresses are assigned and saved for all ServerSVNs, the user must **Apply Changes** to the new PP Server configuration.

1.13.5 Adding an NMS Cluster

The NMS *server cluster* is implemented at both the primary SAS, and optional backup SAS where applicable, and at the NOC site. Whereas multiple NMS clusters are possible at a SAS site, only a single cluster configuration is supported at the NOC site. A new NMS cluster is added to the NMS using the Add NMS Cluster dialog. The NMS cluster must be configured before any servers are added to the cluster.

To add a NMS server cluster:

1. Click the **Configuration** tab > **Physical Domain** > **More Options** > **Add** > **NMS Cluster.**
2. Type the **Name** of the new NMS Cluster.
3. Use the **Site** drop-down and select the site at which the NMS cluster is located.
4. In **CEM Network Interface**, specify an interface name for the cluster election manager (CEM) LAN interface, for example – **ETH0**.
5. In **CEM Multicast Address**, specify a valid multicast address for the cluster election manager.
6. In **CEM Unicast Port**, specify a valid unicast port for use by the cluster election manager.
7. In **CEM Quorum**, specify the minimum number of NMS servers that must remain functional in order for the cluster to remain up and running. In the iDirect implementation, this value is calculated as the (**Total Number/2) +1**. The calculation ensures a non-zero value.
8. In **CEM Timeout Reach Other Cluster**, specify a communication time out duration for when communicating with other clusters.
9. Specify the **Number of Apache Instances**, to be used by this NMS cluster.
10. In **Directory Service Multicast Address**, specify a valid multicast address for the Directory Service process.
11. Use the following fields to enter virtual IP addresses for the NMS Cluster processes**:**
    a. **Virtual IP Address for FAT DRBD**
    b. **Virtual IP Address for Regular DRBD**
    c. **Virtual IP Address for Local DRBD**
    d. **Virtual IP Address for SQL Store**
    e. **Virtual IP Address for Directory Server**
    f. **Virtual IP Address for Web IPv4** (necessary for Web access)
    g. **Virtual IP address for Global File Store IPv4**
    h. **Virtual IP address for Local File Store IPv4**
    i. **Virtual IP Address for DCIPv4** (designated coordinator node for the cluster)
12. Enter a **User Password** for gaining access to the cluster at the application level.
13. Enter a **Administrator Password** for gaining administrative access to the cluster.
14. Enter an **OS Password** for gaining access to the cluster at the system level.
15. Click **Save** to save the NMS Cluster configuration and continue, or click **Save and Close** to close the dialog and open the **Browse Physical Domain** page.

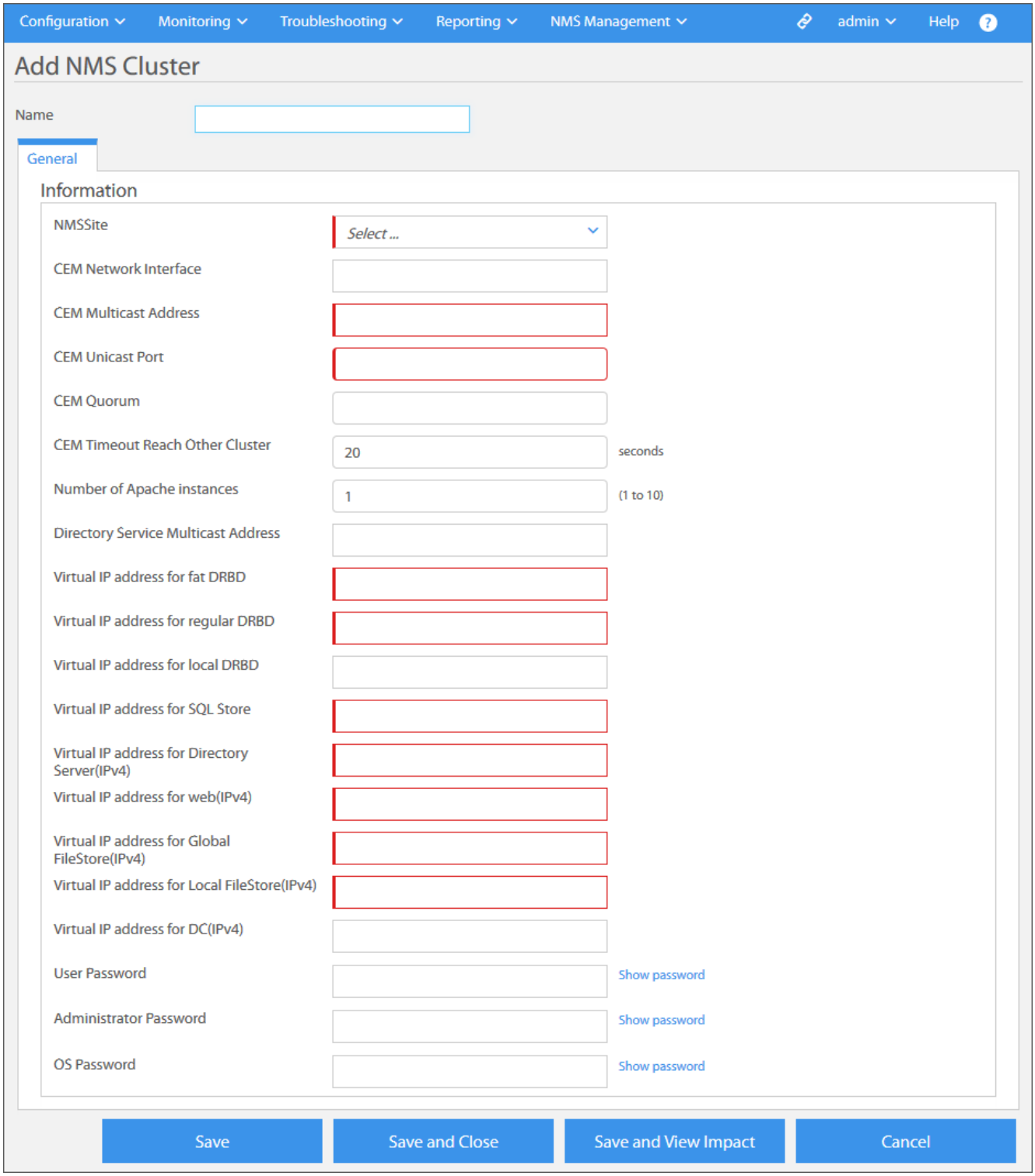

Figure 1-24. Add NMS Cluster Dialog

1.13.6 Adding an NMS Server

The NMS includes configuration pages that support adding, modifying, and deleting NMS servers. The Add NMS Server dialog is used to add a new NMS server to the NMS.

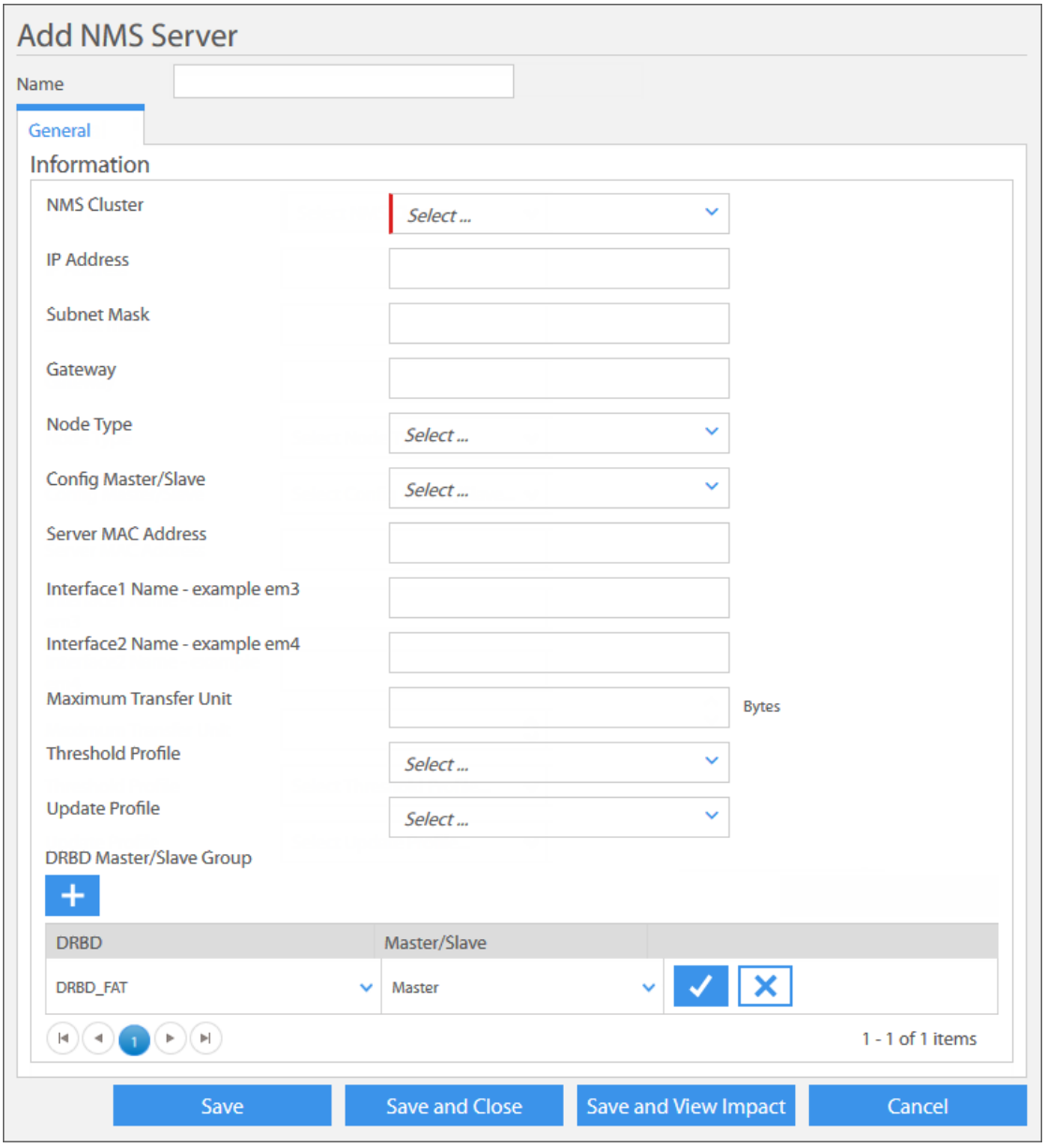

Figure 1-25. Add NMS Server Dialog

To add an NMS server:

1. Click the **Configuration** tab > **Physical Domain** > **More Options > Add** > **NMS Server.**
2. Type the **Name** of the new NMS server.
3. Under the **Information** section, use the drop-down to select the **NMS Cluster** to which the new NMS server is a member node.
4. Enter the following IPv4 address information for the upstream interface:
   a. Add the NMS Server **IP Address**.
   b. Add the **Subnet Mask** address.
   c. Add the **Gateway** address. This is the IP address of the upstream router interface connected to the to upstream LAN segment.
5. Use the **Node Type** drop-down to designate the type of NMS server node.
6. Use the **Config Master/Slave** drop-down to designate the server as a configuration **Master** or **Slave**.
7. Enter the NMS **Server MAC Address**.
8. Specify names for **Interface1 Name** and **Interface2 Name** respectively.
9. Use **Maximum Transfer Unit** to specify, in bytes, the maximum data transmission size.
10. Select a configured **Threshold Profile** to apply to this NMS server. See the *iDirect Pulse NMS user Guide*, *Adding a Stats Threshold Profile*.
11. Select a configured **Update Profile** that the Update Manager should apply to this NMS server. See the *iDirect Pulse NMS user Guide*, *Adding an Update Profile*.
12. **Click Save and Close** to save the NMS Server configuration.

1.13.7 Adding a Squid Cluster

The functionally equivalent Linux servers of the Squid Cluster form a separate high availability (HA) cluster that provide Web Caching resources to the NMS Web application. The workload is allocated among ten active logical servers, each of which supports a single physical server. The remaining servers provide redundancy support.

Squid Web caching software provides the NMS with faster Web page access. Together, the Web Cache Servers implement Squid instances for each SVN, whereby by two Squid instances that reside on different servers support each SVN. Larger SVNs may require more instances.

The Add Squid Cluster dialog is used to add a new Squid cluster in the NMS.

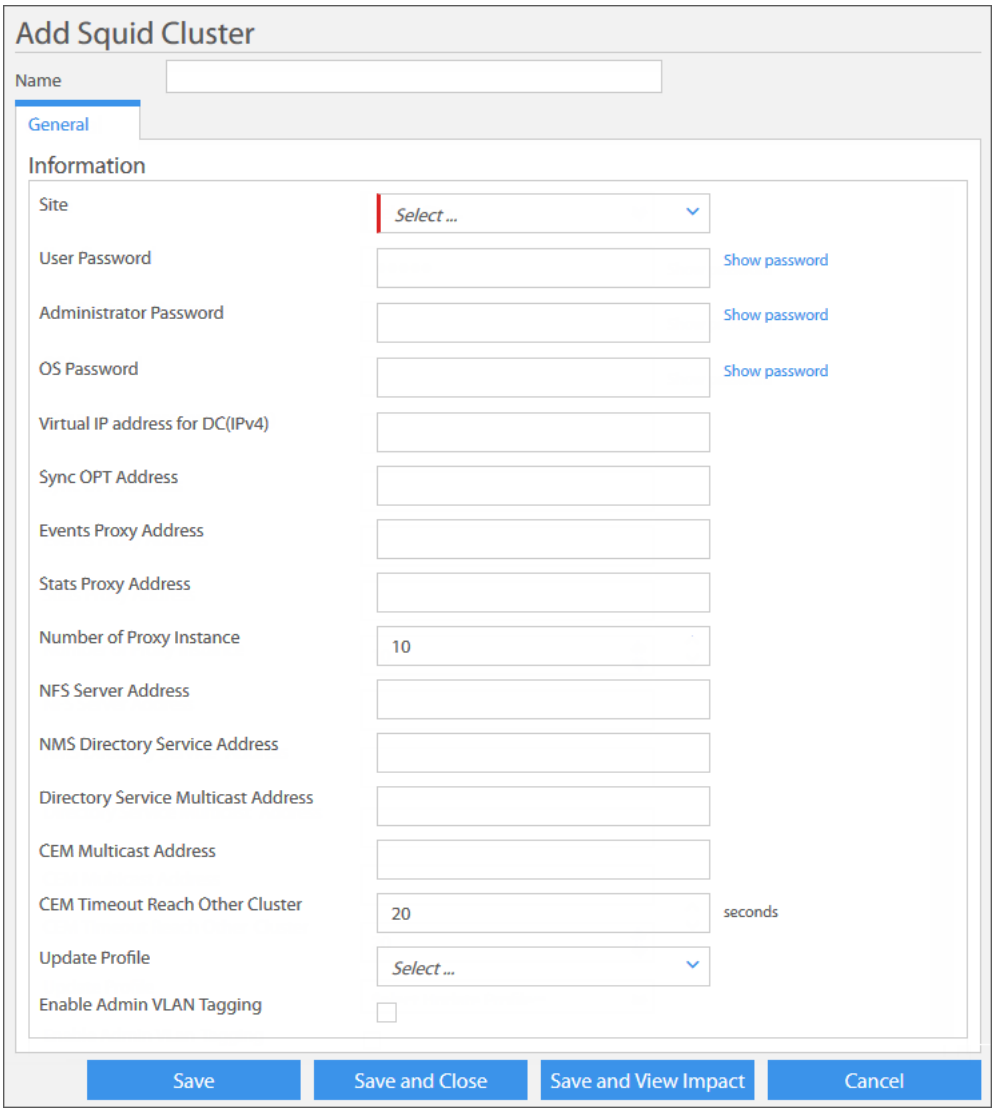

Figure 1-26. Add Squid Cluster Dialog

To add a new Squid server:

1. Click the **Configuration** tab > **Physical Domain** > **Add More Options** > **Add > Squid Cluster.**
2. Type the **Name** of the new Squid server.
3. Use the **Site** drop-down to select the site at which the **Squid Cluster** is located.
4. Enter a **User Password** to access to the cluster at the application level; an **Administrator Password** to gain administrative access to the cluster; and an **OS Password** to gain system level access to the cluster.
5. In **Virtual IP Address for DC**, enter the IPv4 address of the designated coordinator (DC) node in the Squid cluster. This node runs the process that manages resources across all nodes in the cluster.
6. Enter a **Virtual IP Address** for communicating with the cluster.
7. In **Sync OPT Address** enter the virtual IP address for the process that receives Squid options files from the Update Manager.
8. In **Events Proxy Address**, enter an IPv4 address to connect with the events server proxy.
9. In **Stats Proxy Address**, enter an IPv4 address to connect with the stats server proxy.
10. Select **Prefetch Enable** to enable pre-fetch services on this Squid Cluster.
11. **In Number of Proxy Instance, enter the maximum number of proxy instances.**
12. In **NFS Server Address**, enter the IP address of the Network File System server.
13. In **NMS Directory Service Address**, specify a valid IPv4 address for addressing communication with the NMS Directory Service process.
14. In **Directory Service Multicast Address**, specify a valid multicast address for communication with the Directory Service.
15. In **CEM Multicast Address**, specify a unique multicast address for communication between the CEM and cluster nodes.
16. In **CEM Timeout Reach Other Cluster**, specify a communication time out, in seconds, for when communicating with other clusters.
17. Use the **Update Profile** drop-down and select a configured update profile that the Update Manager should apply to this Squid cluster.
18. **Click Save and Close** to save the Squid Cluster configuration to the NMS database.

1.13.8 Adding a Squid Server

The Add Squid Server configuration dialog is used to add a new Squid server to the NMS, and to an existing Squid cluster.

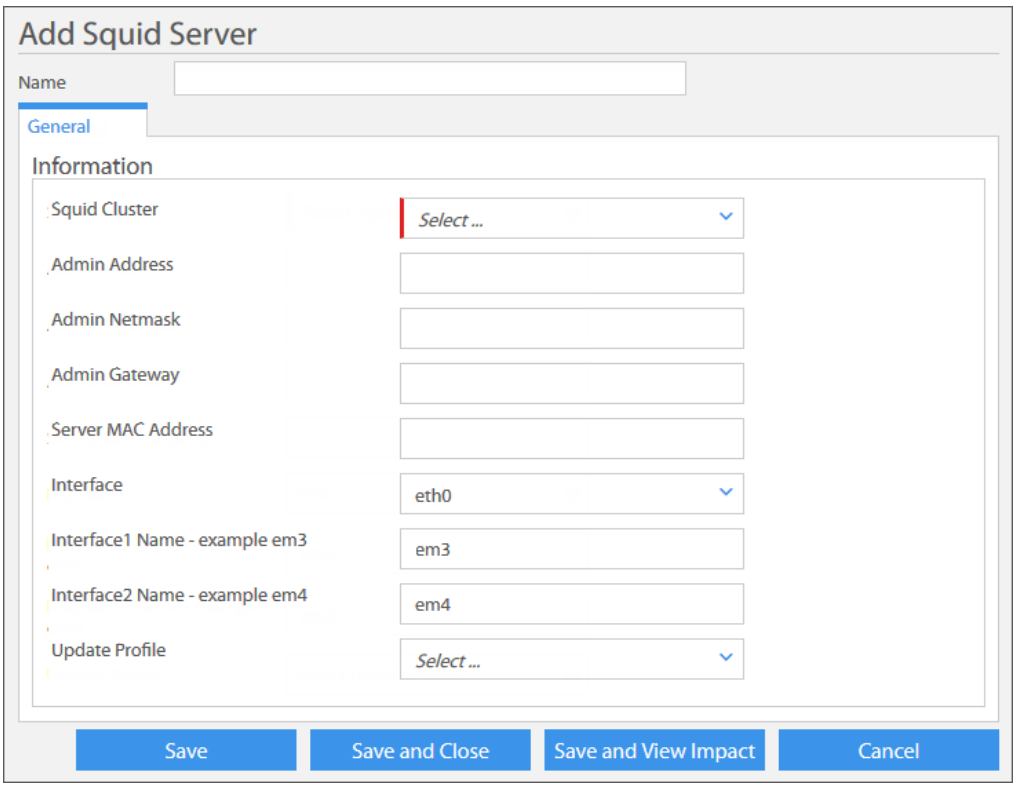

Figure 1-27. Add Squid Server Dialog

To add a new Squid server:

1. Click the **Configuration** tab > **Physical Domain > More Options** > **Add > Squid Server.**
2. Type the **Name** of the new Squid server.
3. Use the **Squid Cluster** drop-down to select the cluster in which the new server is a node.
4. For the upstream interface, enter the following IP address information:
   a. Add the **Admin Address**.
   b. Add the **Admin Netmask** address.
   c. Add the **Admin Gateway** address. This is the IP address of the upstream router interface connected to the to upstream LAN segment.
5. Enter the **Server MAC Address** of this Squid server.
6. Use the **Interface** drop-down and select **ETH0** as the interface to which the Squid server is connected.
7. In **Interface1 Name,** type a name for the interface — for example em3.

8. In **Interface2 Name,** type a name for the interface — for example em4.
9. Use the **Update Profile** drop-down and select a configured update profile that the Update Manager should apply to this Squid cluster.
10. **Click Save and Close** to save the Squid server configuration to the NMS database.

1.13.8.1 NMS Generated Squid Server SVNs

When a new Web Cache Server is added to an existing Squid Cluster, the required Server SVNs are automatically generated in the NMS. The NMS performs the following actions:

- Automatically create Server SVN for the Admin Site SVN parent, and associate it with the newly created Squid Server. After the is generated, the user will need to modify the **Admin Server SVN** to assign an appropriate IP address and re-save.
- After the SVN is generated, the user must navigate to the Squid Blade
- After the Server SVN is created and modified, the next step is to create the Squid Proxy and configure the Customer SVNs that it will support.
- After all of the Server SVNs are modified and saved, the user must **Apply Changes** to the new Squid Server configuration.

1.13.9 Adding a Squid Proxy

The *Squid proxy*, is a web proxy cache server application that provides caching services to a variety of network protocols, such as HTTP or FTP. The Add Squid Proxy dialog is used to add to the NMS a new Squid proxy or instance to an existing Squid cluster.

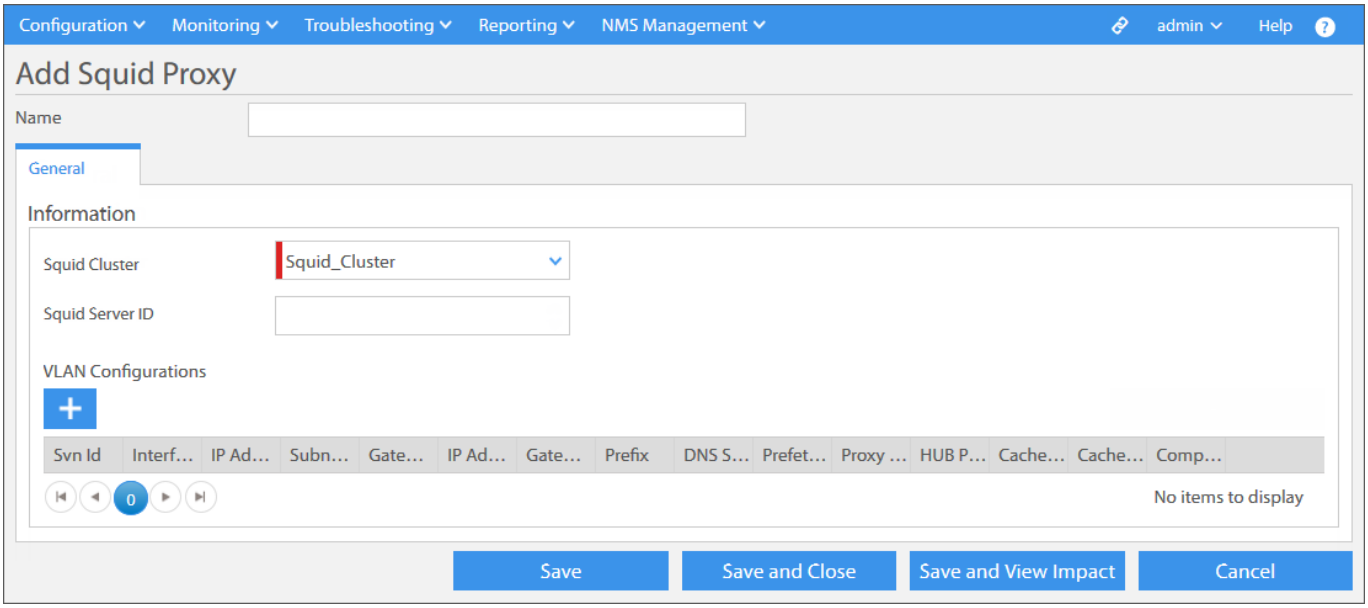

Figure 1-28. Add Squid Proxy Dialog

To add a new Squid server:

1. From the **Browse Physical Domain** window, find the Squid Cluster for which a new Squid proxy is to be added.
2. Click the **Actions** button, and select **Add Squid Proxy.**
3. Type the **Name** of the new Squid Proxy.
4. Use the **Squid Cluster** drop-down to select the cluster in which to add the new proxy.
5. Enter a **Squid Blade ID**, to designate the appropriate Squid Blade for this proxy.
6. Under the **VLAN Configurations** section, click the **Add Record** icon to insert a new VLAN configuration record for this Squid proxy.
7. Use the **SVN ID** drop-down to select a pre-configured SVN.
8. Use the **Interface** drop-down to select the **SAT0** or **ETH0** interface to which the proxy will connect.
9. If applicable, use **Gateway** and **IP Address** to enter IPv4 addresses for the proxy.
10. If applicable, use **Gateway IPv6** and **IP Address IPv6** to enter IPv6 addresses for the proxy.
11. Enter a **DNS Server Address.**
12. Select **Pre-fetch Enable** to allow the proxy to pre-fetch content.
13. Enter a **Proxy Port** number that the Squid will listen for requests.
14. In **Cache MemSize**, enter the cache size in MBytes.
15. Select **Cache Disable** to prohibit the proxy from caching.
16. Select **Compression Enable** to allow the proxy to pre-fetch content.
17. Click the **Update Record** icon to accept the entry. An accepted entry is entered as a new record under **VLAN Configurations**.
18. Repeat the previous steps, from Step (6), to insert additional VLAN configuration records for this proxy instance.
19. To modify a configured **VLAN Configuration** record, click the **Edit** icon on the record, make required changes and again click the **Update Record** icon.
20. Click the **Delete** icon to remove a record.
21. **Click Save and Close** to save the Squid Proxy configuration to the NMS database.

1.13.9.1 NMS Generated Squid Proxy Server SVN Objects

Like with the creation of any server in the NMS, when a new Squid Proxy Server is configured in the NMS, the required Server SVNs are automatically generated in the NMS.

1.14 Physical Domain Browse Actions

Using the **Browse Physical Domain** command, users can interact with configured Physical Domain elements in to perform a variety of specific operations. These operations are called "actions." An action can be performed on a single element, using the **Action** button for that element, or simultaneously on multiple elements, by using the browse window **Group Actions** button. Which actions are possible is based on the specific element type, and only those actions are displayed when an element is selected.

Physical Domain element actions, excluding Site, Cluster, and Site SVN, are briefly described as follows:

Table 1-5. Physical Domain — Browse Actions

Action	Applicable Elements	Brief Description
View Element	All Physical Elements	View configured information for the selected element.
Copy	All Physical Elements	Create a cloned copy of the selected element, which can be modified, renamed, and saved as a new element.
Modify Element	All Physical Elements	Modify the configured information for the selected element, and re-submit with changes.
Delete Element	All Physical Elements	Remove the selected element from the NMS database.
Impact Analysis	N/A	View impact on other elements, if changes are applied to the selected element.
Progress Report	All Physical Elements	View a summary report of update manager progress since applying changes to the selected element.
Apply Configuration	All Physical Elements	Apply the configured NMS changes to the selected element, using the pending option file configured for the selected network system.
Retrieve Pending Option File	All Physical Elements except IFDomain, SVN, and Site SVN	Load from the NMS database, and display the pending copy of the options file for the selected domain element.
Retrieve Active Option File	Physical Elements except IFDomain, SVN, and Site SVN	Load and display the options file currently active in the selected physical domain element.
Compare Configurations	Physical Elements except IFDomain, SVN, and Site SVN	Compare the pending options file and the active options file for the selected physical domain element.
Modify Engineering Debug Keys	Physical Elements except IFDomain, SVN, Site SVN	Modify custom key associated with the selected element, to enable or disable, add or modify functionality.
Issue Certificate	NMS, PP, and Squid Servers; and Line Card only	In Velocity, all network elements are in the PKI system—to communicate with each other, each requires a certificate created by the CA Foundry.
Revoke Certificate	NMS, PP, and Squid Servers; and Line Card only	This action results in retracting an assigned certificate from a network element.
Download Certificate	NMS, PP, and Squid Servers; and Line Card only	Transfer a certificate from the NMS to the local PC or laptop device. The certificate can then be manually transferred to a designated element.
Manage Software Version	NMS, PP, and Squid Servers; and Line Card only	View software packages available the on NMS, and install appropriate software package as required.

Table 1-5. Physical Domain — Browse Actions

Action	Applicable Elements	Brief Description
Manage Blob File	NMS, PP, and Squid Servers; and Line Card only	View software BLOB files available on the NMS, and install appropriate BLOB as required.

1.14.1 Browse Actions for Site, Cluster, and Site SVN

Browse actions for Site, Cluster, and Site SVN elements, are listed and briefly described as follows:

Table 1-6. Physical Domain Elements — Browse Actions for Sites, Clusters, and Site SVNs

Action	Applicable Elements	Brief Description
Add NMS Server	NMS Cluster,	Add new NMS server node to cluster. See *Adding an NMS Server*.
Add Resource	NMS Cluster,	Add new NMS server node to cluster.
Add (PP) Blade SVN	PP Server	Add new PP Blade SVN to this PP server. See *Creating and Modifying a PP Server SVN*.
Delete Blade SVN	PP Server SVN	Remove the SVN associated with the PP blade from the NMS.
Add PP Cluster	Site (Teleport, NOC)	Add a new PP server cluster to the selected site. See *Adding a Protocol Processor (PP) Cluster*.
Add NMS Cluster	Site (Teleport, NOC)	Add a new NMS server cluster to the selected site. See *Adding an NMS Cluster*.
Add Squid Cluster	Site (Teleport)	Add a new Squid cluster to the selected site. See *Adding a Squid Cluster*.
Add Squid Server	Squid Cluster,	Add new Squid server node to a Squid cluster. See *Adding a Squid Server*.
Add Squid Proxy	Squid Cluster	Add new Squid Proxy to a Squid Cluster. See *Adding a Squid Proxy*.

2 Configuring Transport Domain Elements

The *transport domain* represents a set of logical elements that are associated with the space segment of an iDirect Velocity™ Network. This domain includes satellites, beams, service channels, signaling carriers, iNets, inroute groups, service areas and regulatory areas.

The following topics briefly introduces each Transport Domain element and provides step-by-step procedures for configuring each element and its associated parameters.

2.1 Transport Domain Configuration Sequence

The NMS tools for working with transport domain elements are accessed from the **Transport Domain** operations menu on the NMS **Configuration** tab.

Each transport domain element, before it is deployed in an iDirect Velocity™ Network, must be created, and its parameters configured in the NMS. The Pulse NMS supports creating, browsing, editing, and deleting of Transport Domain element configurations.

A general sequence for configuring Transport Domain Elements in the NMS is shown here.

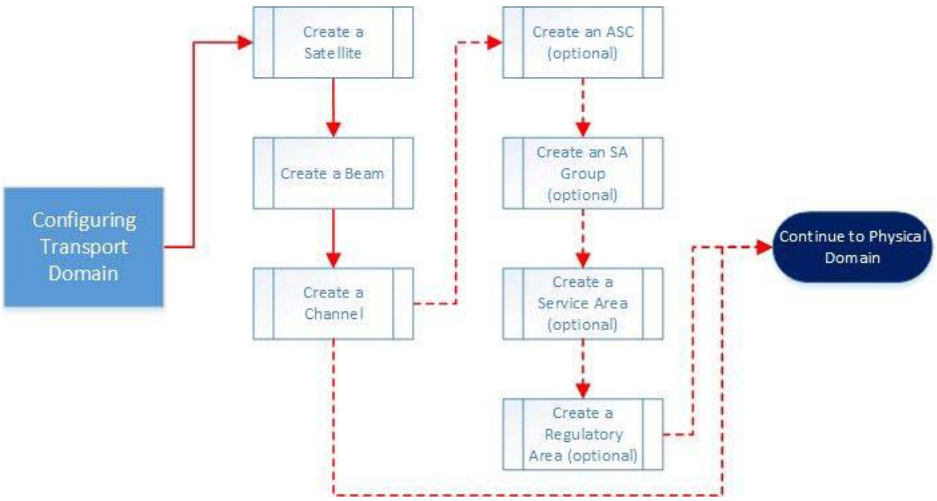

Figure 2-1. Building a Basic Network — Creating Transport Domain Elements

2.2 Adding a Satellite

The satellite element in an iDirect Velocity system, is modeled based on the parameters configured in the NMS, using the **Add Satellite** configuration dialog. To view, copy, or modify an existing satellite configuration, first find the element using the **Browse Transport Domain**; then choose from the **Actions** options — **View Satellite** or **Modify Satellite**.

The Satellite Acquisition Preference feature gives network operators the ability to configure a Preference parameter to the satellite, so that an acquiring terminal will use the configured preference to determine which visible beam/satellite to select when attempting acquisition. This configurable preference can influence the terminal to select an owned beam as opposed to a leased beam, or a spot beam over a wide beam.

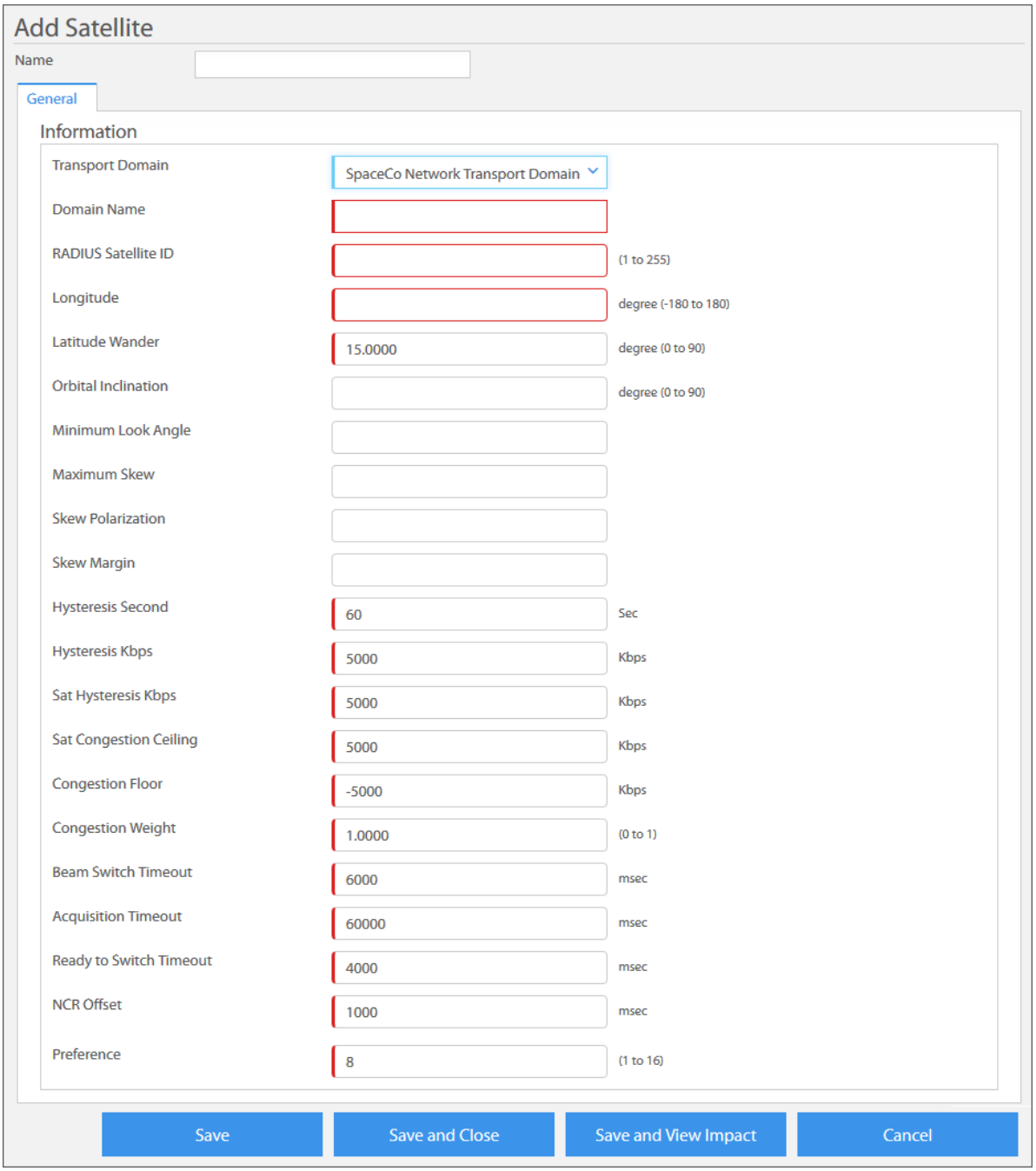

Figure 2-2. Add Satellite Dialog

To add a satellite:

1. Click **Configuration > Transport Domain > More Options** > **Add > Satellite.**
2. Click in the **Name** field and enter the name of the new satellite.
3. Select the appropriate **Transport Domain** to which the new satellite is associated.

4. Enter a **Domain Name** for this satellite.
5. Enter the **Radius Satellite ID** for this satellite.
6. Use **Longitude**, to enter the longitudinal position of the satellite.
7. Enter **Latitude Wander**, as the maximum oscillations north and south of the equator.
8. Enter **Orbital Inclination** as an angle between 0 to 90 degrees. This parameter, generally provided by the satellite provider, is only a factor if a satellite exhibits instability.
9. Use **Minimum Look Angle** to enter the lowest angle above the horizon at which the antenna is allowed to transmit.
10. Enter the **Maximum Skew**. This value represents the maximum angle of skew that a terminal's antenna tolerates before it stops transmitting.
11. Enter the **Skew Polarization** angle. This parameter, which ranges from -45.0^{o} to +45.0^{o}, is the value by which a satellite with horizontal or vertical polarization may be skewed with respect to its orbit.
12. Enter the **Skew Margin** to optimize upstream carriers for mobile remotes in Adaptive TDMA inroute groups that use non-circular polarization.
13. Use **Hysteresis Second** to enter a value in seconds, which represents the minimum time between beam switches — a terminal will not switch more often than this time.
14. Use **Hysteresis Kbps** to enter value to limit switching between beams in same satellite; and use **Satellite Hysteresis,** to enter a value that limits switching between satellites.
15. In the **Sat Congestion Ceiling** field, enter the maximum value in Kbps that represents a congestion ceiling in the current beam when making a satellite switch decision; and in **Congestion Floor**, enter the minimum value in Kbps, which represents the (negative) congestion level below which all beams are treated the same.
16. In the **Congestion Weight** field, enter a value between 0 and 1. A "0" value means that congestion is not considered, and that maps alone are considered. A value of "1" means the congestion is considered in the normal way. Adjusting the value between "0" and "1" increases or decreases the influence of congestion on whether to switch beams.
17. Use **Beam Switch Timeout** to enter a value, in milliseconds, which represents the interval after which the satellite determines that the switching has failed.
18. Use **Acquisition Timeout** to enter a value, in milliseconds, which represents the interval after which the satellite determines that a terminal has failed to acquire.
19. Use **Ready to Switch Timeout** to enter a value, in milliseconds, which represents the time-out value for a terminal to lock to the second downstream and confirm.
20. In **NCR Offset,** enter a value, in milliseconds, which represents the fixed time offset between the "ready-to-switch" and "switch" commands.
21. Use the **Preference** field default of 8, or specify a new value. This value is used by terminals to determine which satellite to point to when it is simultaneously in the footprint of multiple satellites in the same network at the time of acquisition. A value of 1 = the highest preference; a value of 16 = the lowest. Multiple satellites may share the same priority.
22. Click **Save** to save the satellite configuration to the NMS.

2.3 Adding a Beam

The NMS **Add Beam** dialog for configuring beams, supports the configuration of both *circular* and *non-circular beams*. After a beam is created, one or two channels may be assigned to each channel slot; or a channel slot may also go unused. See *Adding a Channel*, for assigning channel slots.

To modify an existing beam configuration, first find the element using the **Browse Transport Domain** command. After finding the element, use the **Actions** option — **Modify Beam**.

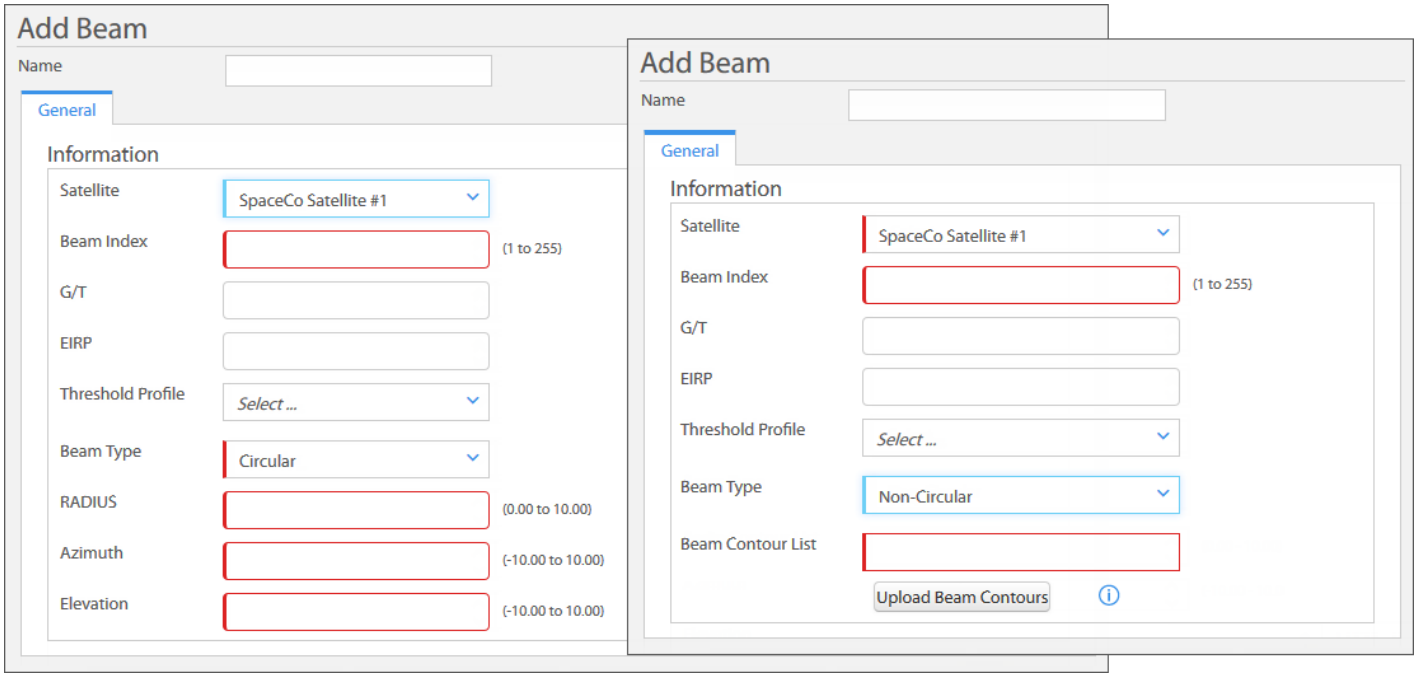

Figure 2-3. Add Beam Dialog — Circular and Non-Circular Beam Options

The **Add Beam** command is accessed from the **Transport Domain** menu, under **Configuration**.

To add a beam:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Beam**.
2. Enter a **Name** for the beam — for example, based on satellite, beam type and number.
3. Select the **Satellite** to which this beam is associated; then enter the **Beam Index**.
4. Enter the gain-to-noise temperature ratio in **G/T. G** is the antenna gain (db) at the receive frequency, and **T** is the equivalent noise temperature (^{o}K) of the receive system.
5. Use the **EIRP** field to enter the e*ffective isotropic radiated power* value for the beam.
6. Use the drop-down to select the appropriate **Threshold Profile** for this beam.
7. Select the **Beam Type** as **Circular** or **Non-Circular**. The associated fields are enabled. Use the following instructions based on a **Circular** or **Non-Circular** beam type selection:
   a. **Circular Beam**: Specify the **RADIUS**, **Azimuth**, and **Elevation**.

b. Non-Circular: If the non-circular beam option is selected, the **Beam Contour List** text box is enabled for input. Contour-points are input as shown in the **Note** below:

c. Non-Circular: As an alternative to entering a contour array, click the **Upload Beam Contours** button to upload a single GXT formatted file to define the beam contour array. This file should define the beam contours with the fewest number of points.

8. Click **Save** to save the configuration to the NMS.

9. Retrieve the Pending Option File for the Pulse Network, and verify that the configured beam definitions are correct.

10. Click **Save** to save the configuration to the NMS.

NOTE: The following applies when specifying non-circular beam contour list coordinates:

- A minimum array of at least 3 contour-points are required to specify a contour polygon
- A maximum of array of 50 contour-points may be specified in a single contour polygon
- A point is a 2-element array of the form [latitude, longitude]
- **Example:** [[Lat1,Long1], [Lat2, Long2], [Lat3, Long3], [Lat4, Long3], [Lat4, Long5]]
- A single contour is enclosed in brackets
- Each contour of a multi-contour set is enclosed in brackets and separated by comma
- The Latitude range is [-90.0 -to- 90.0]; the longitude range is [-180.0 -to- 180.0]
- A configuration of intersecting contour-points in a single contour is invalid
- A configuration of multiple contours with intersecting contour-points is invalid

2.4 Adding a Channel

A *channel* is a fixed region of bandwidth on a satellite feeder link that is dynamically mapped onto a beam. In a Velocity network, to define a channel is to assign it to a specific beam, configure the outbound and inbound parameters — for example, bandwidth, frequency, and polarization. The Add Channel dialog is used to configure a new channel in the NMS.

To modify an existing channel configuration, find the element using the **Browse Transport Domain** command. After finding the element, use the **Actions** option — **Modify Channel**.

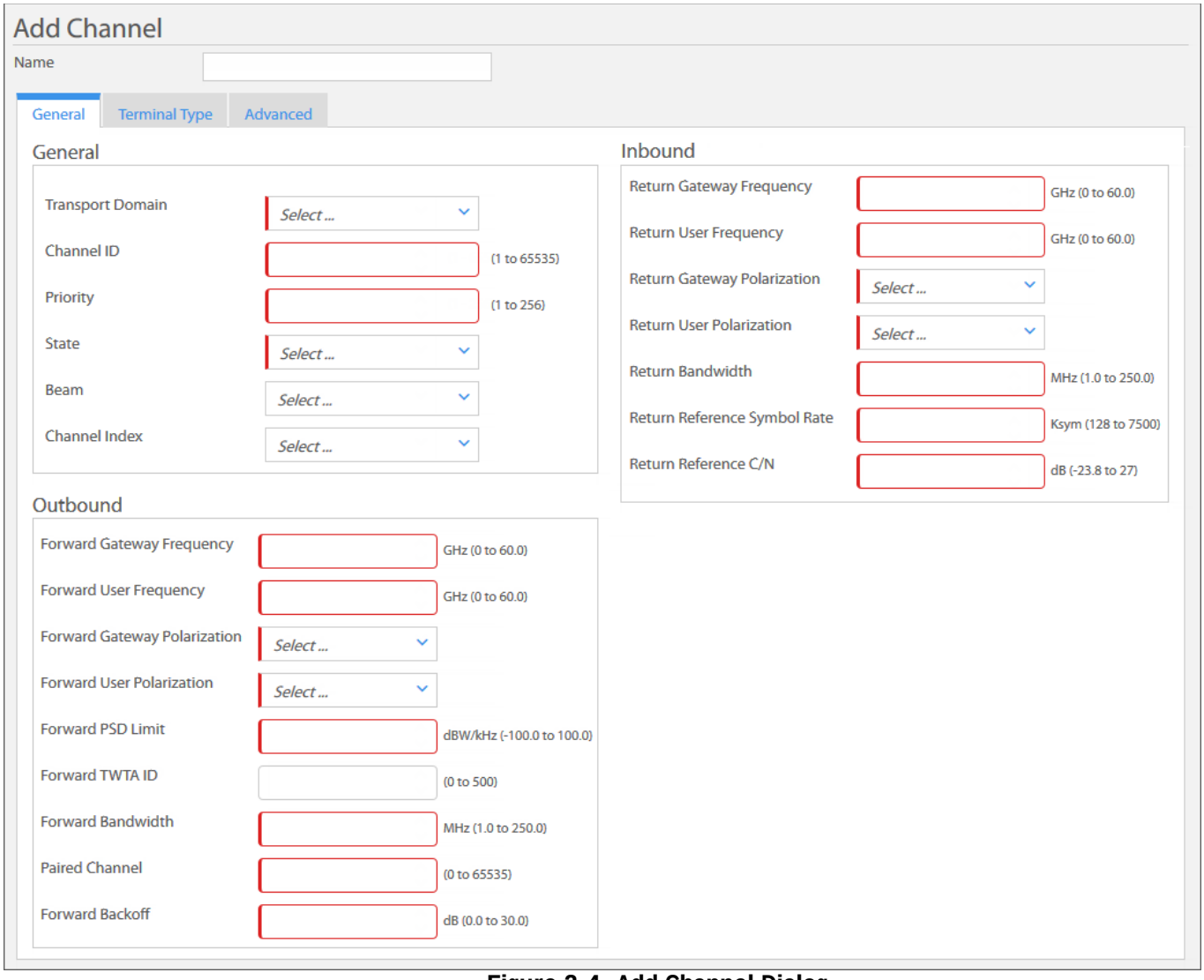

Figure 2-4. Add Channel Dialog

To add a channel:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Channel**.
2. Enter the **Name** of the new channel.

3. Use the **Transport Domain** drop-down and select the appropriate Transport Domain to which the channel belongs. For example —Pulse Network Transport Domain.
4. Enter the **Channel ID**. This value uniquely identifies the channel from all other channels. A value of '0' is not valid when the **Paired Channel** parameter is also configured.
5. Enter the channel **Priority**. This parameter, which can be used in case of Teleport failover, establishes priority for recovering channels. Priority 1 is highest; 256 is lowest.
6. Use the **State** drop-down to specify the initial state the channel should assume.
7. Use the **Beam** drop-down to select beam to which the channel should be assigned.
8. Use the **Channel Index** drop-down to select the index value between 1 and 4, which represents the channel slot to which the channel should be assigned.
9. Under the **Outbound** section, enter the following parameters:
   a. **Forward Gateway Frequency** — enter the center frequency of the channel uplink.
   b. **Forward User Frequency** — enter the center frequency of the channel downlink.
   c. **Forward Gateway Polarization** — enter the uplink polarization as **Vertical, Horizontal**, **LHCP,** or **RHCP.**
   d. **Forward User Polarization** — enter the downlink polarization as **Vertical, Horizontal**, **LHCP,** or **RHCP.**
   e. **Forward PSD Limit** — enter the Outbound Maximum Power Spectral Density, expressed as the minimum bandwidth over which the channel power may be spread.
   f. **Forward TWTA ID** — enter the identifier of the transponder TWTA.
   g. **Forward Bandwidth** — enter the outbound channel bandwidth in MHz.
   h. **Paired Channel** — enter the **ID** of the channel that shares the same transponder TWTA; a value of '0' indicates that no other channel shares the same TWTA.
   i. **Forward Backoff** — enter the Teleport EIRP backoff from nominal, where nominal is the level at which a transponder is at full load.
10. Under the **Inbound** section, enter the following parameters:
    a. **Return Gateway Frequency** — enter the center frequency of the channel downlink.
    b. **Return User Frequency** — enter the center frequency of the channel uplink.
    c. **Return Gateway Polarization** — enter the downlink polarization as **Vertical, Horizontal**, **LHCP,** or **RHCP.**
    d. **Return User Polarization** — enter the uplink polarization as **Vertical** or **Horizontal**, **LHCP** or **RHCP**.
    e. **Return Bandwidth** — enter the inbound channel bandwidth in MHz.
    f. **Return Reference Symbol Rate** — enter the reference carrier symbol rate. This value, in symbols per second, is applicable to all satellite terminal types.
    g. **Return Reference CN** — enter the C/N ratio for demodulation of the conceptual reference carrier, using the desired reliability in steps of 0.2 dB.

11. Click **Save and Close** to save the configuration to the NMS or click **Save** to continue in the modify mode with *Add Channel Per Terminal Type RF Limits*.

2.4.1 Add Channel Per Terminal Type RF Limits

The **Terminal Type** tab of the **Add Channel** dialog, allows the entry of RF Limit parameter records that may be associated with individual Terminal Types that are allready defined in the NMS. Each record represents the RF constraints that are applied to the associated NMS Terminal Type when it attempts to acquire the channel. An NMS Terminal Type that does not have associated RF Limits configured for the channel cannot operate in the channel.

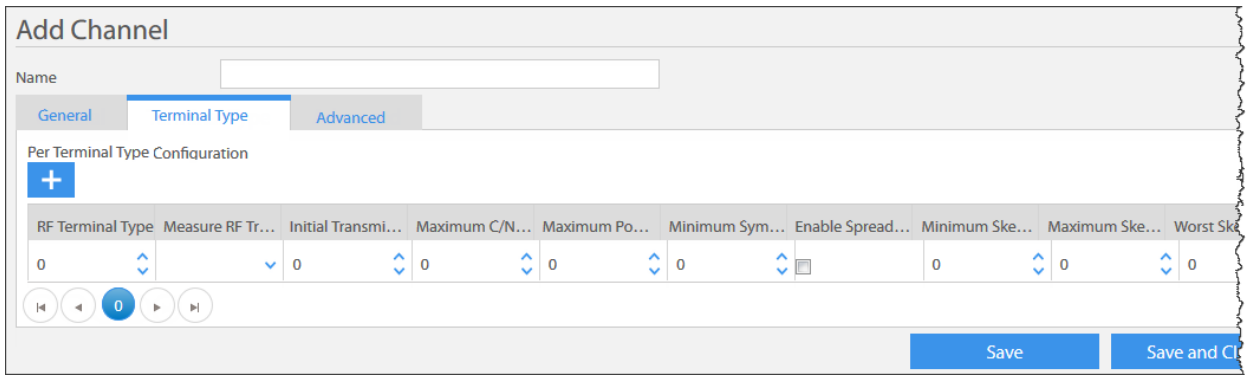

Figure 2-5. Add Channel - Per Terminal Type RF Configurations Dialog

To define Per Terminal Type Configuration records:

1. From the **Add Channel** dialog, click the **Terminal Type** tab, and under **Per Terminal Type Configuration**, click the **Add Record** button. Th e record fields are enabled.
2. Specify an **RF Terminal Type** for which the RF configuration limits are being specified.
3. Use the **Measure RF Transmit Power At** drop-down to specify the **BUC/Antenna Flange** or the **Modem TF/IF Port** as the location at which transmit power measurements should be taken during commissioning for the specified terminal type.
4. Enter the **Initial Transmit Power (db)** of the specified terminal type.
5. Enter the **Maximum C/N (db)** of the specified terminal type.
6. Enter the **Maximum Power (db)** the specified terminal type is allowed to transmit.
7. Enter the **Minimum Symbol Rate (Ksym)** of the specified terminal type.
8. Select **Enable Spread Spectrum** to enable the feature for the specified terminal type.
9. Enter, in degrees, **Minimum Skew Angle**, **Maximum Skew Angle**, and **Worst Skew Angle**.
10. Click the **Update** button to insert a new **Terminal Type Configuration** record.
11. Use **Frequency Steps** to enter the number of incremental frequency step changes that an acquiring terminal should make before attempting to acquire on another satellite.
12. Use **Frequency Step Size** to enter the value by which the terminal should shift the frequency when hunting for the correct frequency.
13. Repeat the above steps to insert another **Terminal Type Configuration** record.

14. Click **Edit** to modify a selected record; click **Delete** to remove a selected record.
15. Click **Save and Close** to save the configuration to the NMS.

2.4.2 Add Channel Access Bitmask

Each channel has an *access class value* or bit mask that determines whether a terminal is allowed or denied access to the channel, particularly during periods of high demand. This access class value is configured from the **Advanced** tab of the **Add Channel** dialog.

In operation the channel access class value (or bit pattern) is logically combined, using the AND operation, with the **Access Bitmask** of a Satellite Terminal that is attempting to join the channel. If the logical result is non-zero, the terminal is allowed into the sub-channel — otherwise it is not.

The access value is composed of eight bits — **Access Bitmask 1** through **Access Bitmask 8**. The default access class value of any sub-channel is the bit pattern 11111111, where each bit represents a specific class to which a terminal may be assigned.

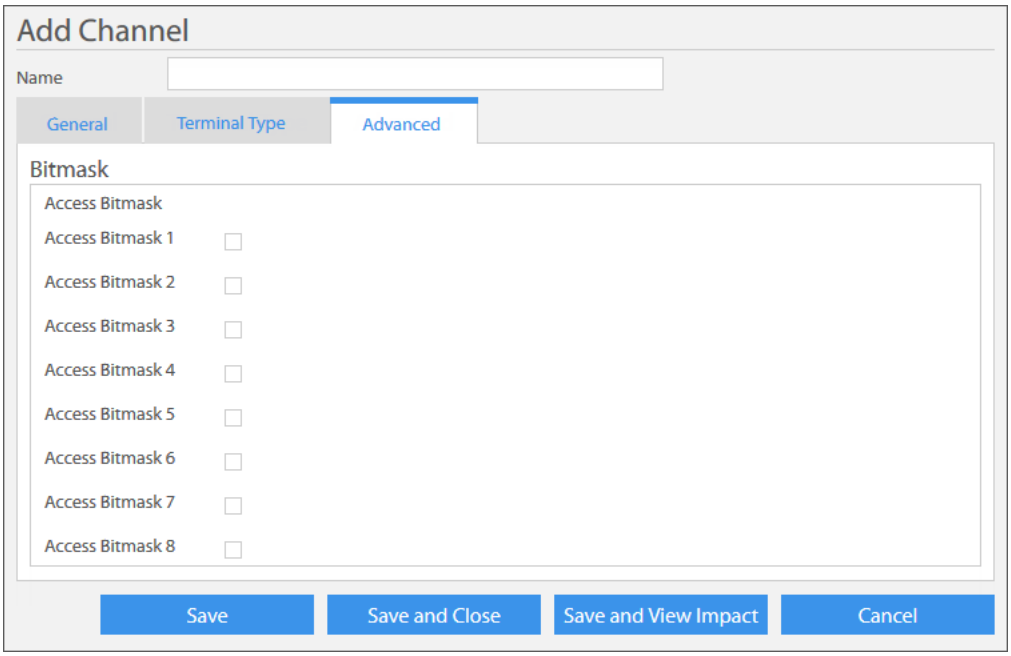

Figure 2-6. Add Channel - Access Bitmask Dialog

To define the channel access bitmask:

1. From the **Add Channel** dialog, click the **Advanced** tab to open the **Bitmask** dialog.
2. Select appropriate **Access Bitmask** positions (1-8) to specify the channel access class.
3. Click **Save and Close** to save the configuration to the NMS.

2.5 About Acquisition Signaling Carriers

In a Velocity network, a signaling carrier is used to broadcast the current satellite beam configuration information to the terminals within the network. This broadcast includes beam footprint data, contained in a low-resolution beam map, and link parameters such as outbound carrier frequency, symbol rate and polarization. Terminals require this information to join the satellite network.

In the Velocity system, the ASC information exchange is one-way (downstream only), and allows satellite network operators to reconfigure a satellite without stranding a terminal.

The following are some key characteristics of the ASC feature:

- Terminals with invalid/non-existent cached beam maps can acquire by locking onto an ASC and receiving a new beam map
- Generally one DVB-S2 ASC is configured per beam
- Multiple ASCs per satellite is supported
- Supports channelizer (1:n uplink-to-downlink) and non-channelizer (1:1 uplink-to-downlink) satellites
- PP beam map content update interval of 5 seconds
- Beam map describes beams on all satellites in the network
- Supports configuration of alternate downlinks with priority

2.5.1 ASC Variations

The Velocity network supports three variations of the ASC based on the following characteristics:

- **Dedicated ASC** — This ASC variation is dedicated to signaling only, and has a single uplink and a single downlink.
- **Dedicated ASC with Fan-Out** — This ASC variation is dedicated to signaling only, but that supports a single uplink that is replicated on multiple downlinks in different beams.

2.5.2 Configure a Dedicated ASC

A *dedicated acquisition signaling carrier (ASC)* is a DVB-S2 signaling carrier in which the hub broadcasts current satellite network configuration information, to terminals, on a single uplink and a single downlink. For each beam, this information includes a low resolution beam map, the outbound carrier frequency, symbol rate, and polarization. Terminals require this information in order to join or reacquire the satellite network.

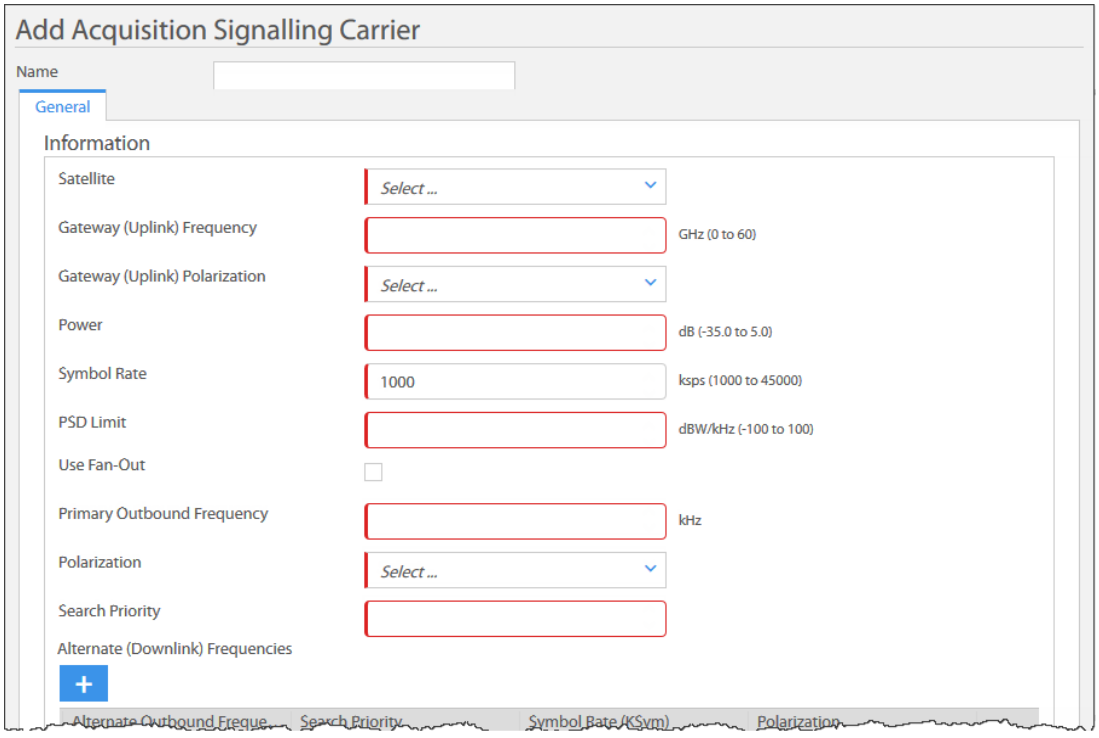

Figure 2-7. Add Acquisition Signaling Carrier Dialog

To add a dedicated acquisition signaling carrier (ASC):

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Acquisition Signaling Carrier**.
2. Use the Satellite drop-down to select the appropriate satellite.
3. Enter a **Name** for the simple dedicated ASC. This may be one of several dedicated ASCs.
4. Enter the ASC **Gateway (Uplink) Frequency**. This is the hub line card-to-satellite uplink.
5. Select the **Gateway (Uplink) Polarization** as **Vertical** or **Horizontal,** or as **LHCP** or **RHCP**.
6. Enter the ASC uplink **Power** and **Symbol Rate**. A minimum of 1000 Ksps is required.
7. Enter the Outbound **PSD** (power spectral density) **Limit** for this ASC.
8. Un-check the **Use Fan-Out** check box, which is checked by default.
9. Enter the **Primary Outbound Frequency**, in kHz, for this dedicated ASC.
10. Select the primary outbound **Polarization** as **Vertical or Horizontal;** or as **LHCP** or **RHCP**.

11. Enter the primary outbound **Search Priority** as an integer value that determines the terminal search order for the appropriate frequency. A lower value has greater priority.
12. Click **Save and Close**. Auto-navigate to **Browse Acquisition Signaling Carrier** window.
13. On the newly modified ASC, click **Actions** and select **Apply Configuration**.
14. If applicable, continue with *Add ASC Alternate Downlink Frequencies*.

2.5.3 Configure a Dedicated ASC with Fan-Out

A *dedicated acquisition signaling carrier (ASC) with fan-out* is a single DVB-S2 signaling carrier in which the hub broadcasts the current satellite configuration, on a single up-link that is replicated on multiple downlinks in different beams. The downlinks will all have the same symbol rate and carrier waveform, but may have different frequency and polarization. Frequency and polarization depends on the beam in which each downlink is transmitted.

Configuring a dedicated ASC with fan-out involves two parts—configure the gateway uplink parameters, and then configure the primary downlink frequency and polarization records.

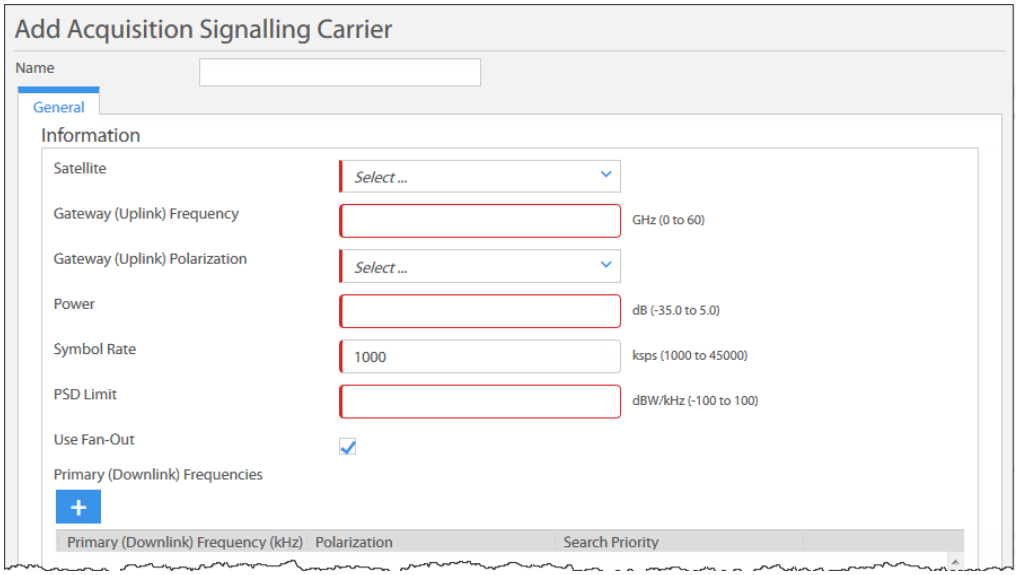

Figure 2-8. Add Acquisition Signaling Carrier with Fan-Out

To add a dedicated acquisition signaling carrier (ASC) with fan-out:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Acquisition Signaling Carrier**.
2. Enter a **Name** for the new Acquisition Signaling Carrier.
3. Use the **Satellite** drop-down to select the appropriate satellite.
4. Enter the ASC **Gateway (Uplink) Frequency**. This is the hub line card-to-satellite uplink.
5. Select the **Gateway (Uplink) Polarization** as **Vertical** or **Horizontal;** or as **LHCP** or **RHCP**.
6. Enter the ASC uplink **Power** and **Symbol Rate**. A minimum of 1000 Ksps is required.
7. Enter the Outbound **PSD** (Power Spectral Density) **Limit** for this ASC.

8. Select **Use Fan-Out** to enable this ASC to replicate the uplink on multiple downlinks. See *Add ASC Primary Down-Link Frequency Fan-Outs*, to continue the ASC fan-out configuration.

2.5.3.1 Add ASC Primary Down-Link Frequency Fan-Outs

After configuring the uplink parameters of a new ASC with fan-out, the next step is to configure the ASC primary downlinks on which the uplink is replicated and beam map information is transmitted onto different beams and to the associated terminals.

As noted earlier, the downlinks all have the same symbol rate and DVB-S2 waveform. Each downlink, however, may have a different frequency and polarization that depends on the beam on which the downlink is transmitted. The ASC downlinks on which the uplink is replicated are configured using the **Primary Downlink Frequencies** dialog.

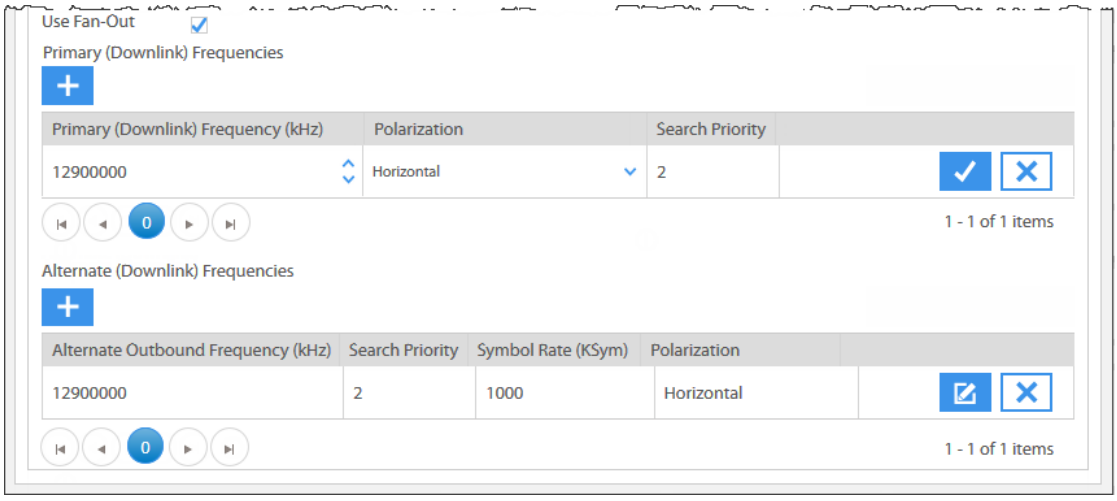

Figure 2-9. Add Primary/Alternate Downlink Frequency Records Dialog

To define primary downlink frequency records:

1. From the **Add Acquisition Signaling Carrier** dialog, click the **Add Record** icon under the **Primary (Downlink) Frequencies** section. The fields are enabled.
2. Enter a **Primary (Downlink) Frequency**, in kHz, for the first downlink record.
3. Specify the **Polarization** as **Vertical or Horizontal;** or as **LHCP** or **RHCP**.
4. Enter the primary downlink **Search Priority.** This integer value determines the terminal search order for the appropriate frequency. A lower value has greater priority.
5. Click the **Update** icon to accept the new **Primary Downlink Frequency** record.
6. Repeat the previous steps to create multiple **Primary Downlink Frequency** records for this ASC with fan-out.
7. Click **Save and Close. A**uto-navigate to **Browse Acquisition Signaling Carrier** window.
8. Click **Actions** on the newly modified ASC with fan-out, and select **Apply Configuration**.
9. If required, at this time, also configure **Alternate (Downlink) Frequencies** that could be used at a later time. See *Add ASC Alternate Downlink Frequencies*.

2.5.4 Add ASC Alternate Downlink Frequencies

When configuring a new ASC, it may be appropriate to also add one or more alternate downlink frequencies to be stored in the CONSTELLATION_OPT file of the associated satellite terminals. These alternate frequencies represent possible ASC downlinks on which terminals could receive beam map information as opposed to the configured primary frequency on which terminals will join or rejoin the network. Alternate frequencies are, in fact, the frequencies for ASCs that have not yet been configured or rolled out onto the satellite.

See Appendix B, *Re-Configuring an ASC*, for **Alternate Downlink Carriers** being added to a previously configured ASC.

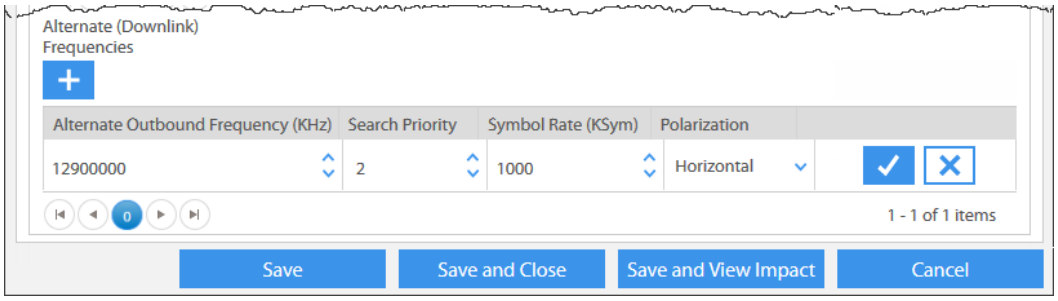

Figure 2-10. Add Alternate Downlink Frequency Records Dialog

To define alternate downlink frequency records:

1. From the **Add Acquisition Signaling Carrier** dialog, click the **Add Record** icon under **Alternate (Downlink) Frequencies** section. The fields are enabled.
2. Enter an **Alternate Outbound Frequency**, in kHz, for this record.
3. Enter a **Search Priority**. This integer value determines the search order when multiple alternate frequency are configured. A lower integer value has greater priority.
4. Specify the **Symbol Rate**, for the new alternate frequency record, in Ksps.
5. Specify the **Polarization** as **Vertical or Horizontal;** or as **LHCP** or **RHCP**.
6. Click the **Update** icon to accept the new Alternate Downlink Frequency record.
7. Repeat the previous steps to create additional Alternate Downlink Frequency records.
8. Click **Save and Close.** Auto-navigate to **Browse Acquisition Signaling Carrier** window.
9. Click **Actions** on the newly modified ASC, and select **Apply Configuration**.
10. Verify that the **Pulse Network** option file correctly reflects the ASC alternate downlink definitions.
11. Verify that the constellation options file is pushed to the in-network terminals. After verifying ASC definitions at the Network level, select Apply Configuration.

2.6 Adding a Map

In Velocity, maps define geographic regions from which service area (SA) groups are defined. Map files that are required for the configuration of SA Groups, must be added and activated in the NMS before being used. Map file types include regulatory offset (FOM_RO) maps, service area maps (FOM_SA), and maps that contain both regulatory and service areas (FOM_RO&SA).

Only a Service Provider can perform map operations: Add Map, Set Map type, Activate Map, View Map, Deactivate Map, and Delete Map. To perform these map actions, first find the map. Select **Configuration** > **Transport Domain** > **Browse Maps**. After finding the map, use the **Actions** menu to select the appropriate command. A map is only usable in the NMS if it has been appropriately activated.

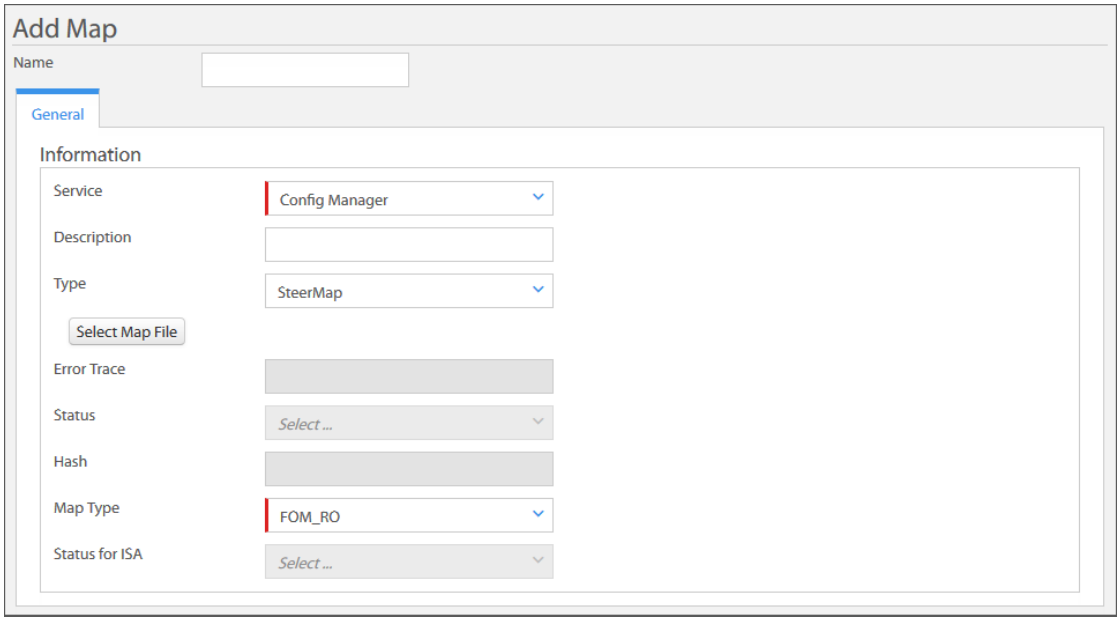

Figure 2-11. Add Map Dialog

To add a service area:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Map**.
2. Enter a meaningful **Name** for the map — for example VNO_Geo_RA_Map# or VNO_RA_Map#.
3. Use the **Service** drop-down to select **Config Manager** as the associated NMS service.
4. Enter a **Description** for the new map.
5. Use the **Type** drop-down and select **SteerMap** or **FixedMap**, based on whether the map being uploaded is associated with a fixed beam or steerable beam.
6. Use the **Map** drop-down and select the appropriate geographic map for this SA group.
7. Use the **Type** drop-down to identify the map type as **FOM_RO**, **FOM_RO&SA**, or **SA**. Steerable maps are can only be specified as FOM_RO only; the fixed type supports all three uses **FOM_RO**, **FOM_RO&SA**, or **SA**.

8. To activate the map, based on its use type, click **Save and Close** to open the Browse Window, listing the Maps.
9. Find new map and click the **Actions** button and choose the appropriate **Activate** option.

2.7 Adding a Service Area Group

A *Service Area Group* (SA Group), in Velocity, maps to a single active service area (SA) map in the NMS, and represents an identifier pool from which SAs can be designated when defining geoscopes or when defining regulatory areas (RAs). An SA Group is created in the NMS by a Service Provider (SP), and only usable by a VNO to which permission is granted by the SP.

A new SA Group is added to the NMS using the **Add Service** dialog. Other operations include View, Copy, Modify, and Delete SA Group. To perform these operations, first find the element using the **Browse Transport Domain** command; then use the appropriate SA Group **Action.**

The new SA Group can be one of the following types based on intended use:

- Geoscope — SA Group type contain SAs used for defining SSPP geoscopes only
- Regulatory Area — SA Group type contains SAs used for defining Regulatory Areas only
- Geoscope/Regulatory Area — SA Group type contains SAs that can be used both for defining SSPP geoscopes and for defining Regulatory Areas

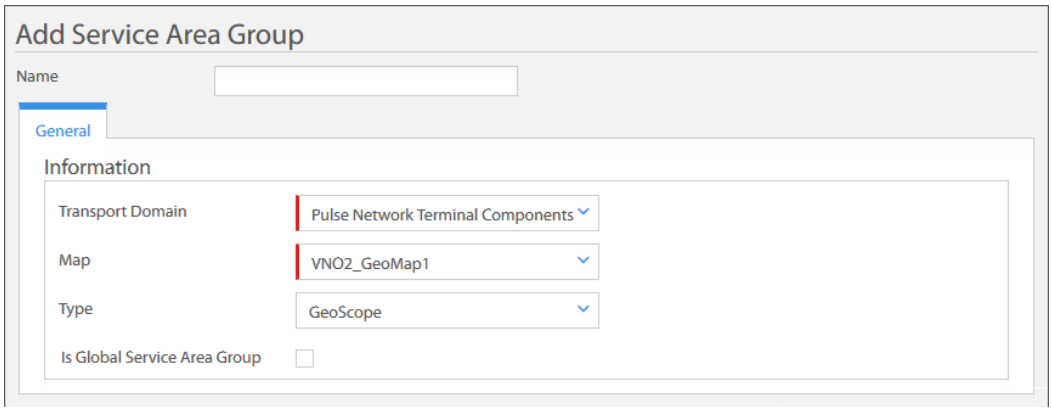

Figure 2-12. Add Service Area Dialog

To add a service area:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Service Area Group**.
2. Enter a meaningful **Name** for the Service Area Group.
3. Select the **Transport Domain** to which the new SA Group belongs.
4. Use the **Map** drop-down and select the SA map on which the SA Group is based. Multiple SA Groups can be defined from a given SA map, but an SA Group must contain one map.
5. Use the **Type** drop-down to identify the use type for this SA Group as **Geoscope**, **Regulatory Area**, or as **Geoscope/Regulatory Area**.
6. Click **Save and Close.**

2.8 Adding a Service Area

In Velocity, a *Service Area (SA)* is a geographical area, based on a specific SA map. Each SA can be designated as being a part of a specific SA Group. The new SA can be added, using the **Add Service Area** page, to a specific SA Group that already exists in the NMS

Generally, the Service Provider adds SAs to an SA Group, however a VNO can add SAs to an SA Group to which it has been assigned permission. When created, each new SA is added to an SA Group, and is identified by an integer value called the **Service Area Identifier**. That identifier is used in the NMS to identify the SA when used in defining a geoscope or a regulatory area.

To modify a service area configuration, first find the element using the **Browse Transport Domain** command. After finding the element, use the **Actions** option — **Modify Service Area**.

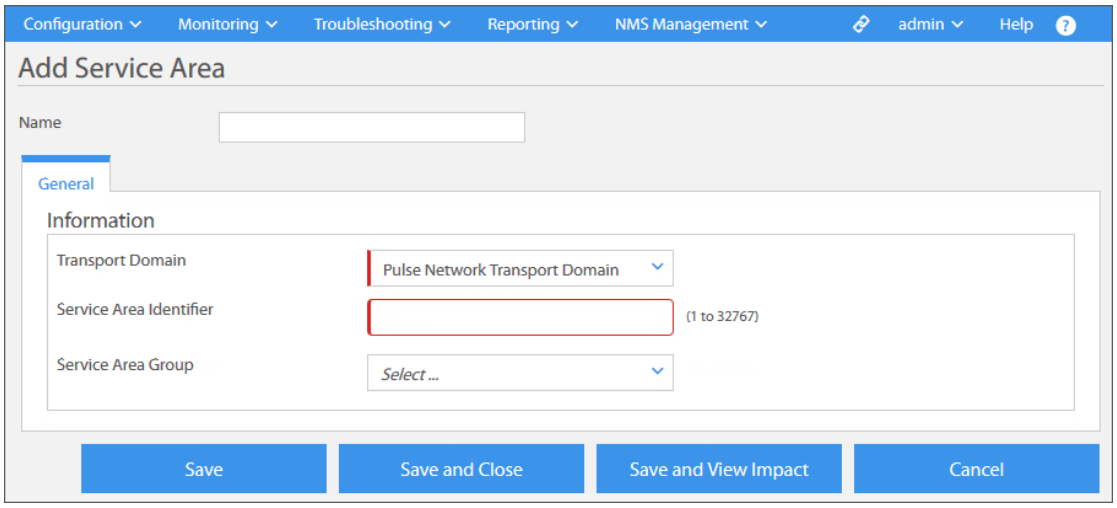

Figure 2-13. Add Service Area Dialog

To add a service area:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Service Area**.
2. Enter a meaningful **Name** for the new Service Area — for example, indicate the associated SA Group as part of the name.
3. Select the **Transport Domain** to which the new SA belongs.
4. Select the **Service Area Group** to which this new SA will belong.
5. Enter a unique **Service Area Identifier** (1-32767) for the new SA.
6. Click **Save** to save the configuration and remain in **Modify** mode, or click **Save and Close.**

2.9 Adding a Regulatory Area

A *Regulatory Area (RA)* is an area defined from one or more service areas from a specific SA Group. The RA, usually a country, is an area in which regulatory authorities impose specific restrictions or limitations on a terminal.

The **Add Regulatory Area** dialog is used to configure a new RA in the NMS. The dialog allows the RA to be configured such that certain per terminal type restrictions are enforced, whenever that terminal type enters or acquires into the RA.

Other RA operations include View RA, Copy RA, Modify RA, and Delete RA. To perform these operations, first find the element using the **Browse Transport Domain** command; then use the appropriate Regulatory Area **Action.**

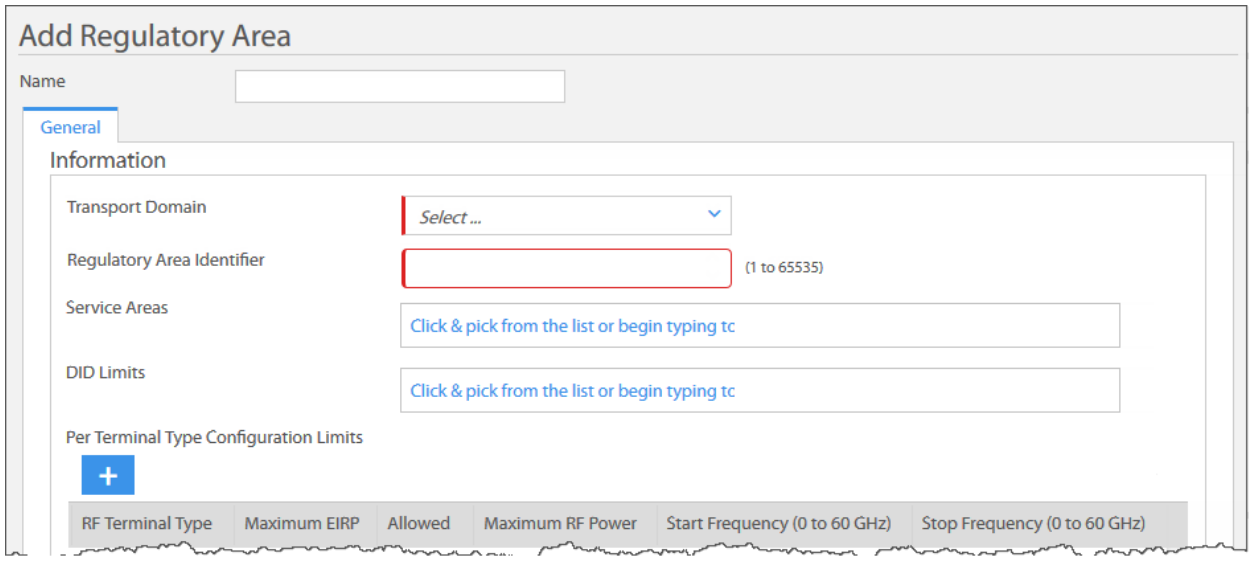

Figure 2-14. Add Regulatory Area General Dialog

The following configuration options are available when adding a Regulatory Area:

To add a regulatory area:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Regulatory Area**.
2. Enter a meaningful **Name** of the new regulatory area — for example, indicate SA Group.
3. Select the **Transport Domain** to which the regulatory area belongs.
4. Enter a unique **Regulatory Area Identifier** (1-65) for the new RA.
5. Use the **Service Areas** multi-select box, to select the SAs to define the new RA.
6. Use the **DID Limits** multi-select box, to choose one or more Terminal DIDs (device ID) for which RF constraints should be applied when in this regulatory area.
7. Continue with *Add Regulatory Area Terminal Type Limits* to specify terminal type limits.

2.9.1 Add Regulatory Area Terminal Type Limits

The **Per Terminal Type** dialog of the **Add Regulatory** page, allows the entry of RF Limit parameter records that may be associated with individual Terminal Types that are allready defined in the NMS. RF limits like the maximum EIRP and the frequency sub-band can be can be limited within the regulatory area, based on the specified terminal type. A separate record can be configured to specify the RF constraints that are applied to the associated NMS Terminal Type when that terminal type attempts to enter the regulatory area. An NMS Terminal Type that does not have associated RF Limits configured for the RA cannot operate in the regulated area.

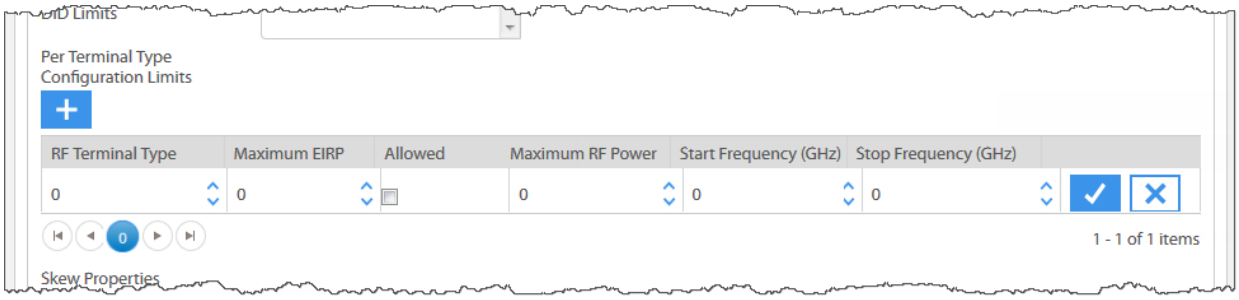

Figure 2-15. Regulatory Area – Per Terminal Type Configuration Limits

To add a regulatory area Per Terminal Type Limits:

1. From the **Add Regulatory** dialog, under **Per Terminal Type Configuration Limits**, click the **Add Record** icon, to enable the record fields.
2. Specify an **RF Terminal Type** for which the RF configuration limits are being specified.
3. Enter the **Maximum EIRP** allowed for the specified terminal type.
4. Select **Allowed** to indicate whether the RF terminal type is permitted to operate in the regulatory area.
5. Enter the **Maximum RF Power** for the specified terminal type.
6. Enter a **Start Frequency (GHz)** and **Stop Frequency (GHz)** to define the sub-band limits for which the specified power limit applies in the specified terminal type. These frequencies (0 -to- 60 GHz) should be specified to not fall in the middle of the channel.
7. Click the **Update** icon to insert the record as a new **Per Terminal Type Configuration Limits** record.
8. Repeat the above steps to insert another **Per Terminal Type Configuration Limits** record for the configured regulatory area.
9. For a given **Per Terminal Type Configuration Limits** record, click the **Edit** icon to modify the record; click the **Delete** icon to remove the selected record
10. See *Add Regulatory Area Skew Properties*, if skew properties should be added.
11. Click **Save** to save the configuration to the NMS and continue in the **Modify** mode, or click **Save and Close** to save and open the **Browse Transport Domain** window.

2.9.2 Add Regulatory Area Skew Properties

Using the **Skew Properties** dialog, a **Reference Skew Angle** and **Reference Maximum C/N** can be defined. A **Tilt Tolerance Value** can be set after selecting the **Tilt Tolerance Type** to be used by the specified terminal type. A separate skew properties record can be configured for each terminal type for which limits apply.

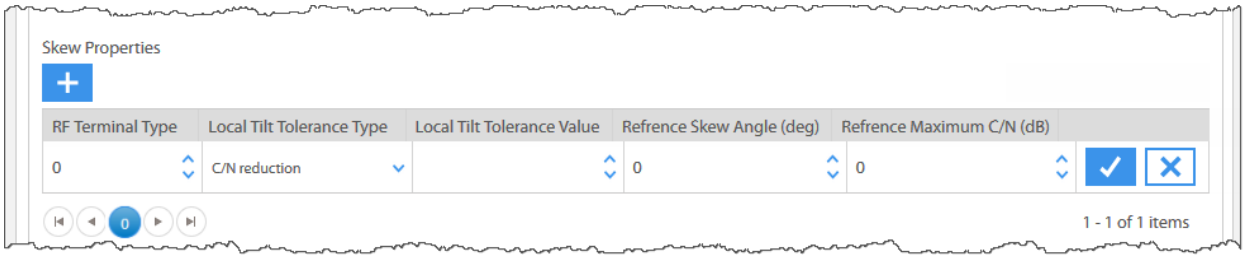

Figure 2-16. Regulatory Area – Per Terminal Skew Properties Configuration

To add a regulatory area Per Terminal Type Skew Properties:

1. From the **Add Regulatory** dialog, under **Skew Properties**, click the **Add Record** icon, to enable the record fields.
2. Specify an **RF Terminal Type** for which the skew properties are being defined.
3. Use the drop-down to choose the **Local Tilt Tolerance Type** for this terminal type.
4. Enter the **Local Tilt Tolerance Value** for this terminal type.
5. Enter a **Reference Skew Angle**, in degrees, for the specified terminal type.
6. Enter a **Reference Maximum C/N** value for the specified terminal type.
7. Click the **Update** icon to insert the new **Skew Properties** record for the terminal type.
8. Repeat the above steps to insert another **Skew Properties** record for the terminal type.
9. For a given **Skew Properties** record, click the **Edit** icon to modify the record; click the **Delete** icon to remove the selected record.
10. Click **Save** to save the configuration to the NMS and continue in the **Modify** mode, or click **Save and Close** to save and open the **Browse Transport Domain** window.
11. Continue to *Add Regulatory Area PSD Table*.

2.9.3 Add Regulatory Area PSD Table

Using the **PSD Table** dialog, the **Skew Angle** and **Relative PSD Level** can be configured on a per RF terminal type basis. The PSD Level limits the power spectral density during acquisition, for the specified terminal type. A separate record can be configured to specify the skew angle and PSD level for each terminal type for which limits apply.

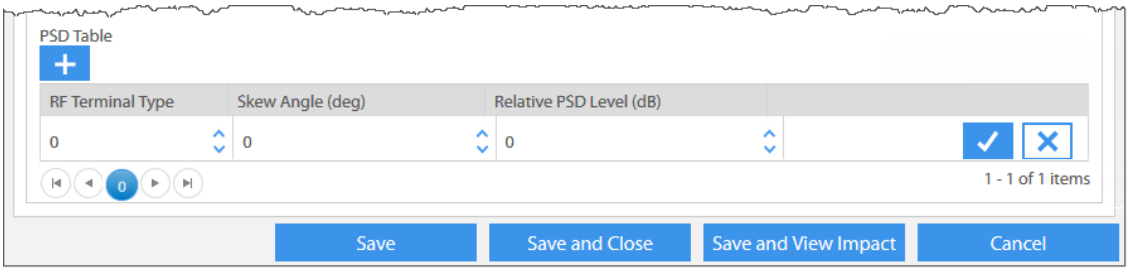

Figure 2-17. Regulatory Area – Per Terminal RF Type Limits Configuration

To add a regulatory area Per Terminal PSD Tables:

1. From the **Add Regulatory** dialog, under **PSD Table**, click the **Add Record** icon, to enable the PSD Table record fields.
2. Specify an **RF Terminal Type** for which the RF configuration limits are being specified.
3. Enter a **Skew Angle**, in degrees, for the specified terminal type.
4. Enter a **Relative PSD Level** for the specified terminal type.
5. Click the **Update** icon to insert the new **PSD** (power spectral density) **Table** record.
6. Repeat the above steps to insert another **PSD Table** record for the terminal type.
7. For a given **PSD Table** record, click the **Edit** icon to modify the record; click the **Delete** icon to remove the selected record from the configuration.
8. Click **Save** to save the configuration and remain in **Modify** mode, or click **Save and Close.**

2.10 Adding an iNet

A Velocity *iNet* consists of a single DVB-S2 outbound carrier and an Adaptive-TDMA inbound group, which consists of a set of TDMA inbound carriers. In a Velocity system, the Teleport supports bi-directional terminal communication by way of an iNet. The iNet provides the upstream and downstream service for both service carriers and for shared signaling carriers.

With main payload beams, a single iNet can be configured per beam channel slot — allowing a maximum of two iNets per beam. At any given time, 0, 1, or 2 iNets (channel may be active in a payload service beam. In the case of steerable beams, for example, which support a total bandwidth of 100 MHz, two iNets per channel are possible, since at most an iNet can support 50 MHz of bandwidth. As a result, up to 4 iNets are supported by each steerable beam; and at any given time, a steerable beam may have 0, or anywhere from 1 to 4 active iNets.

New iNets are configured in the NMS using the **Add iNet** dialog. To modify an existing iNet, first find the element using the **Browse Transport Domain** command. After finding the iNet, use the **Actions** option—**Modify iNet**.

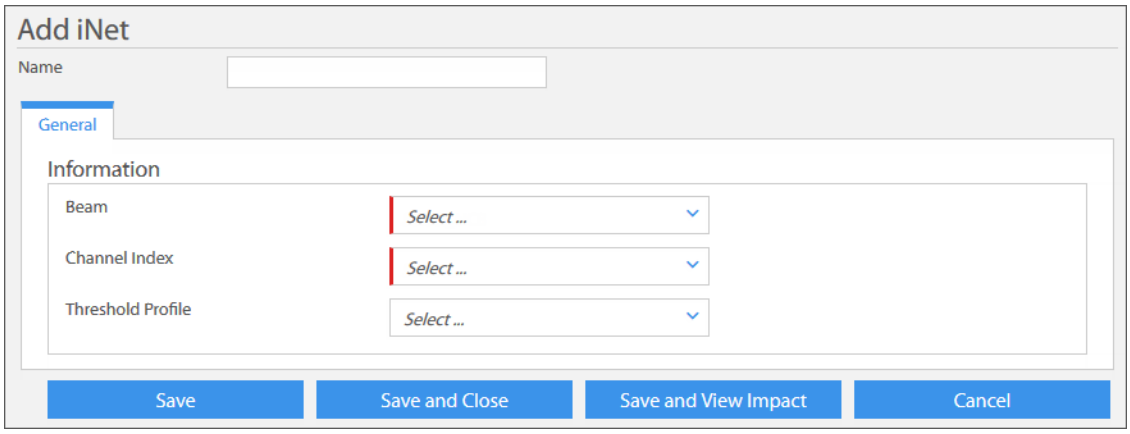

Figure 2-18. Add iNet Dialog

To add an new iNet:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > iNet.**
2. Type a **Name** for the new iNet.
3. Using the **Beam** drop-down, select a beam to which the iNet will be assigned.
4. Using **Channel Index**, perform one of the following based on beam type:
   a. for a main payload beam — select 1 or 2 to specify the beam channel slot to use for this iNet.
   b. for a steerable beam — select 1, 2, 3, or 4 to specify the beam channel slot to use for this iNet. If no option is selected, then no channel slots are assigned in the beam.
5. Use the **Threshold Profile** drop-down to select the appropriate threshold profile for this iNet.
6. Click **Save** to save the iNet configuration and continue in the **Modify** mode; or click **Save and Close** to save the configuration and open the **Browse Transport Domain** window.

2.11 Adding an Inroute Group

In an iDirect Velocity network, a TDMA upstream carrier is referred to as an *inroute*. As such, an inroute group represents a collection of upstream carriers. Characteristic of an inroute group, is that member carriers are assigned consistent transmission attributes – for example MODCOD and FEC rate. This characteristic allows a satellite terminal to transmit on one of multiple inroutes without having to change anything except for its transmission frequency.

In the Velocity system, inroute groups are dynamically assigned by the protocol processor, based on various conditions.

New inroute groups are configured in the NMS using the **Add inroute Group** dialog. To modify an existing inroute group, first find the element using the **Browse Transport Domain** command. After finding the element, use the **Actions** option — **Modify Inroute Group**.

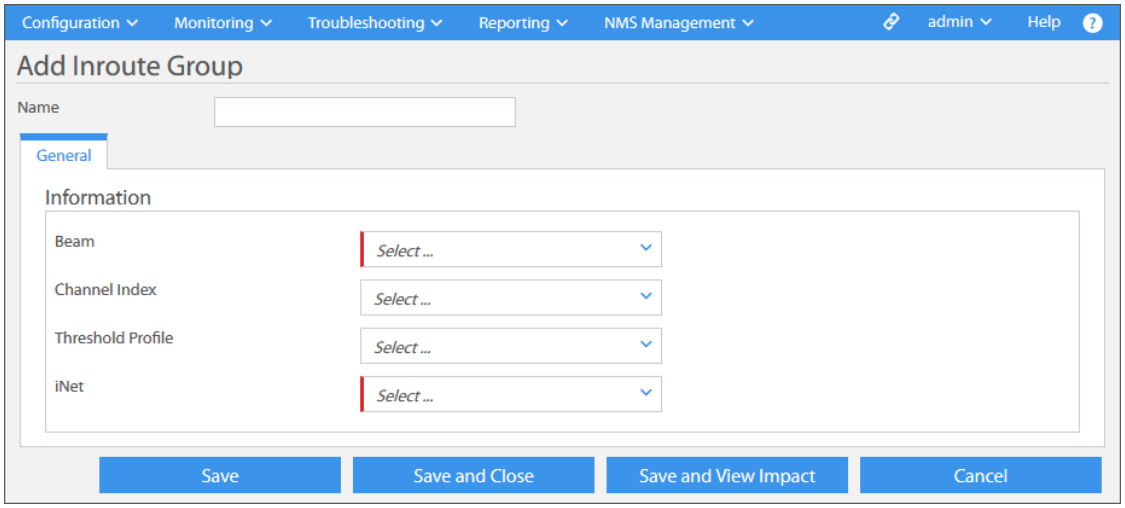

Figure 2-19. Add Inroute Group — Dialog

To create a new inroute group:

1. Click the **Configuration** tab > **Transport Domain > More Options > Add > Inroute Group.**
2. Type a **Name** for the new inroute group.
3. Use the **Beam** drop-down to select a beam in which the inroute group will operate.
4. Using the **Channel Index** drop-down, select 1, 2, 3, or 4 as the relative channel number to assign for use by this inroute group.
5. Use the **Threshold Profile** drop-down to select the appropriate threshold profile for this Inroute Group.
6. Use the **iNet** drop-down and select an iNet to assign to the inroute group.
7. Click **Save** to save the **Inroute Group** configuration and continue in the **Modify** mode; or click **Save and Close** to save and open the **Browse Transport Domain** window.

2.12 Transport Domain Browse Actions

Using the Pulse **Browse Transport Domain** command, users can interact with configured Transport Domain elements in the Browse Results list to perform a variety of operations. These operations are called "actions." An action can be performed on a single element, using the **Action** button for that element, or simultaneously on multiple selected elements, by using the browse window **Group Actions** button.

Only the actions which are possible, based on the element type, are displayed when an element type is selected. All actions are not possible with all elements.

The Transport Domain element actions are listed and briefly described as follows:

Table 2-1. Transport Domain — Browse Actions

Action	Applicable Elements	Brief Description
View Object	All Transport Elements	View configured details for the selected transport element.
Copy	All Transport Elements	Create a cloned copy of the selected element, which can be modified, named, and saved as a new element.
Modify Element	All Transport Elements	Modify the configured information for the selected element, and re-submit with changes.
Delete Element	All Transport Elements	Remove selected element from the NMS database.
Apply Configuration	N/A	Apply the configured NMS changes to the selected element, using the element's pending option file.
Impact Analysis	All Transport Elements	View impact on other elements, if changes are applied to the selected element.
Progress Report	All Transport Elements	View a summary report of update manager progress since applying changes to a selected element.
Retrieve Pending Option File	Satellite Only	Load from the NMS database, and display the pending copy of the options file for the selected element.
Retrieve Active Option File	Satellite Only	Load and display the options file currently active in the selected domain element.
Compare Configurations	Satellite Only	Compare the pending options file and the active options file for the selected domain element.
Modify Engineering Debug Keys	Satellite Only	Modify custom key associated with the selected element to affect functionality.
Add Inet	Beam Only	Add an iNet under the selected beam.
Add Inroute Group	Beam Only	Add an Inroute Group under the selected beam.
Add Beam	Satellite Only	Add a new beam under the selected beam.
Add Acquisition Signaling Carrier	Satellite Only	Add an ASC under the selected satellite.

3 Configuring Network Domain Elements

The *network domain* is immediately above the transport element domain in the element domain hierarchy — it consists of elements such as iNet Profiles, Inroute Group Profiles, Upstream Carriers, Downstream Carriers, and Inroute Composition Groups.

The following topics briefly introduces each Network Domain element and provides step-by-step procedures for configuring each element and its associated parameters.

3.1 Network Domain Configuration Sequence

The NMS tools for working with Network Domain elements are accessed from the **Network Domain** operations menu on the NMS **Configuration** tab.

Each network domain element, before it is deployed in an iDirect Velocity™ Network, must be created, and its parameters configured in the NMS. The NMS supports creating, browsing, editing, and deleting of Network Domain element configurations.

A general sequence for configuring Network Domain Elements in the NMS is shown here.

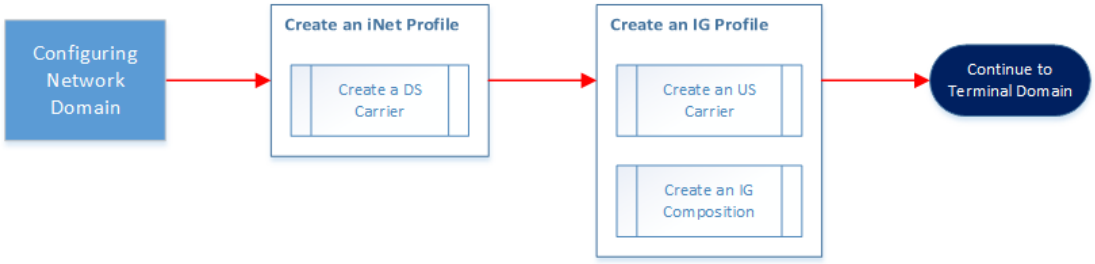

Figure 3-1. Building a Basic Network — Creating Network Domain Elements

3.2 Defining an iNet Profile

In an iDirect Velocity Network, an *iNet* consists of a single *DVB-S2/ACM outbound carrier* and an *Adaptive-TDMA inbound group*. An *iNet Profile*, once configured and saved, represents a set of parameters that can be used to define new iNets that will share these same configuration parameters. The iNet Profile supports configuration of a general set of iNet parameters and the definition of a single downstream carrier component.

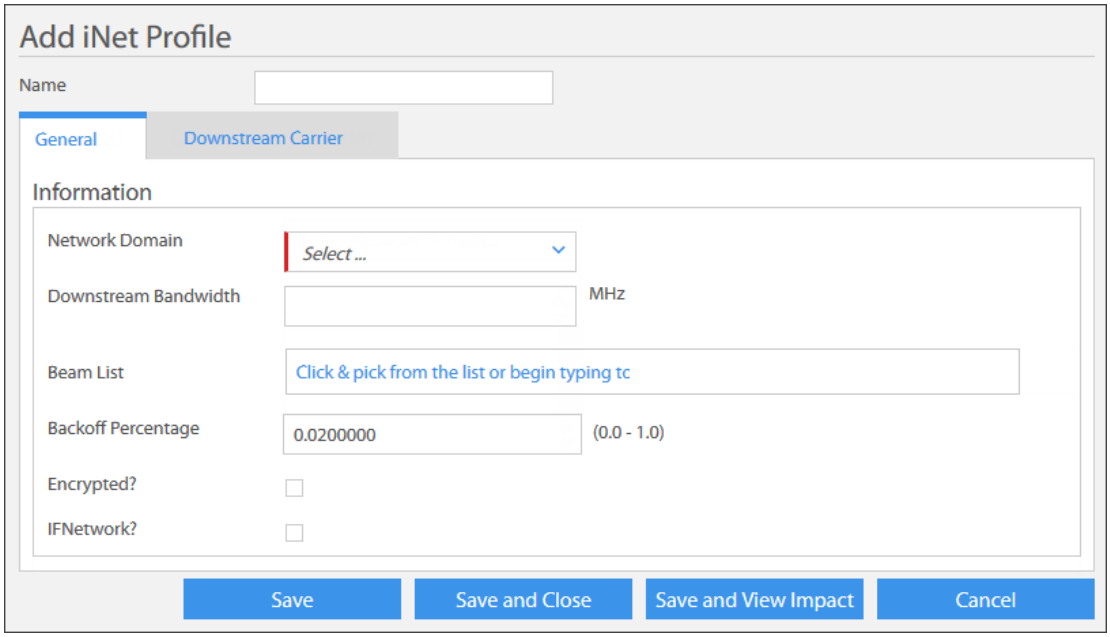

Figure 3-2. Add iNet Profile — Dialog

To define an iNet profile:

1. Click the **Configuration** tab > **Network Domain** > **Add > iNet Profile.**
2. Enter a **Name** for the iNet Profile.
3. Select the **Network Domain** to which the new iNet Profile is associated.
4. Enter the **Downstream Bandwidth** of this iNet Profile.
5. From the **Beam List** multi-select box, select one or more beams in which iNets from this profile will operate. Click the "X" to remove a beam that has been entered.
6. Enter a **Back-off Percentage**, to define the percentage by which the queue depth of the forward link is increased or decreased.
7. Select the **Encrypted** check box to enable data encryption for this iNet Profile.
8. Select **IF Network** if this iNet should be enabled for L-Band/Bench Test network use. This selection specifies that iNets created from this profile will be used in an **IF Network**.
9. Click **Save and Close** to save the configuration to the NMS or click **Save** to continue in the modify mode with *Adding the iNet Profile Downstream Carrier*.

3.2.1 Adding the iNet Profile Downstream Carrier

A single Downstream Carrier can be configured for each iNet profile. The Downstream Carrier dialog allows entry of parameters that support Adaptive Coding and Modulation (ACM) on the DVB-S2 forward link. The MODCOD range supported on the Downstream Carrier is defined by the minimum and maximum MODCOD; as well as the DVB-S2 margins and threshold values.

The parameters applied to the Downstream Carrier, control the DVB-S2 network behavior with *Adaptive Coding and Modulation (ACM)*.

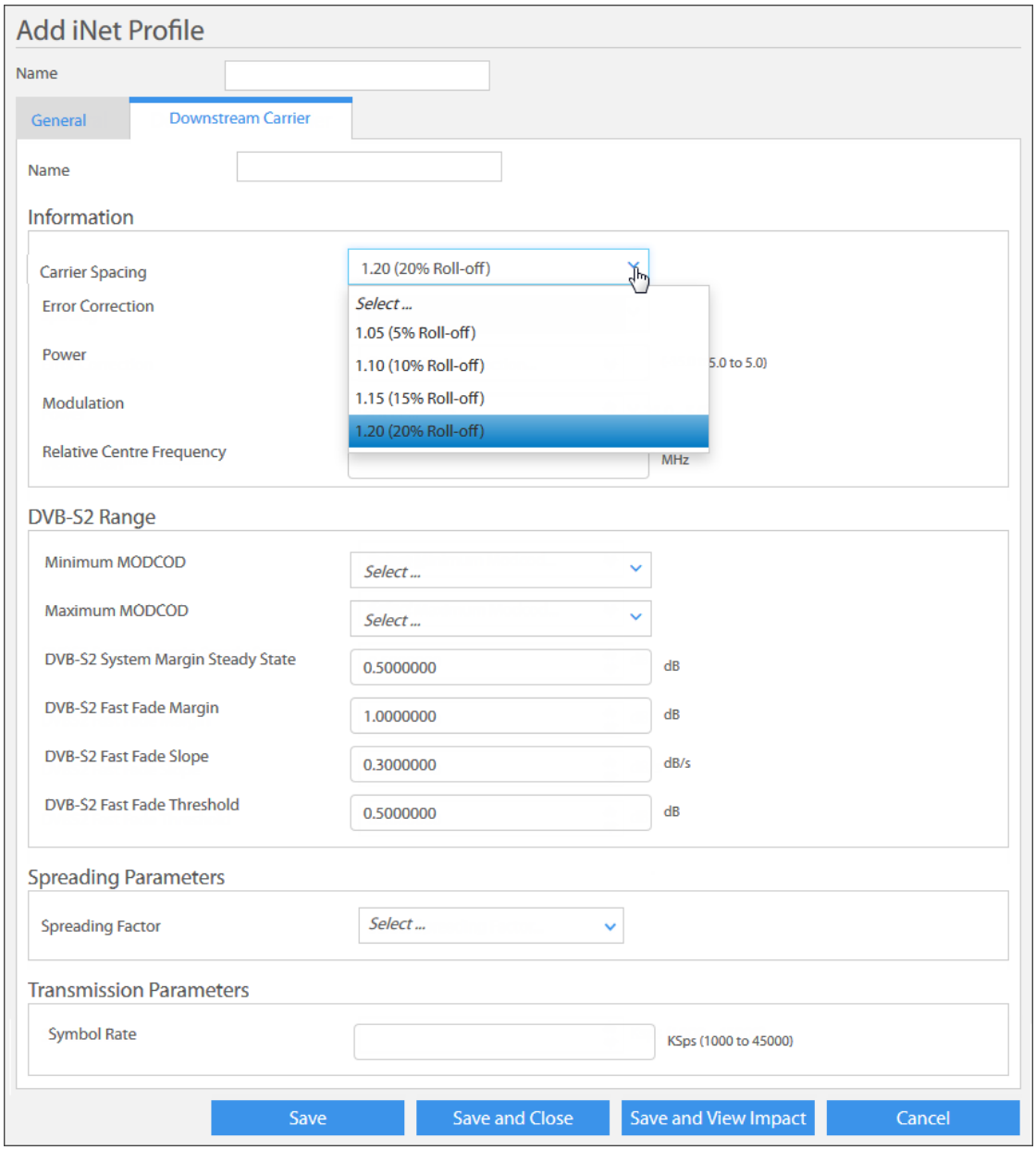

Figure 3-3. Add iNet Profile — Downstream Carrier Configuration Dialog

Based on the reported signal-to-noise ratio of a terminal, these parameters affect the thresholds that subsequently determine the current Modulation and Coding (MODCOD) setting at which a terminal operates in both clear and in fade conditions.

To define an iNet downstream carrier:

1. With the **Add iNet Profile** dialog open, click the **Downstream Carrier** tab.
2. Enter a **Name** for the new downstream carrier.
3. Use the **Carrier Spacing** drop-down list (5%, 10%, 15%, or 20%) to specify the carrier roll-off factor.
4. If applicable, select an **Error Correction** value. This parameter is only valid when **CCM** is also specified.
5. In **Power**, enter a value for the transmit carrier power. The default value is -10 dBm.
6. Use the **Modulation** drop-down to select the carrier modulation as **CCM** (*Constant Coding and Modulation*) or **ACM** (*Adaptive Coding and Modulation*). Constant coding and modulation, which is not supported in a Velocity network, is simulated by selecting **CCM** and specifying the same **Minimum MODCOD** and **Maximum MODCOD**.
7. Enter the **Relative Center Frequency** for the Downstream link.
8. Enter the following **DVB-S2 Range** parameters, as required, or use the default values:
   a. Use **Minimum MODCOD** and **Maximum M ODCOD** to specify the MODCOD range supported by the DVB-S2 downstream carrier. The lowest available MODCOD is QPSK 1/4; The highest available MODCOD is 16APSK 8/9.
   b. **DVB-S2 System Margin Steady State** (default = 0.5 dB) — the margin added to the SNR thresholds measured at hardware qualification, to arrive at an operational SNR threshold for steady state operation.
   c. **DVB-S2 Fast Fade Margin** (default = 1.0 dB) — the margin added to the SNR thresholds measured at hardware qualification, to arrive at an operational threshold during "fast fade." During fade, this margin is added to the *Steady State Margin*.
   d. **DVB-S2 Fast Fade Slope** — the rate of drop in the receive signal strength, for a terminal, which causes the terminal to enter a "fast fade" state. If, during steady state operation, the terminal SNR drops at a rate greater than or equal to the *Fade Slope Threshold*, then the terminal is considered to be in a fast fade state.
   e. **DVB-S2 Fast Fade Threshold** (default = 0.5 dB) — the drop in receive signal strength between two consecutive SNR measurements, by a terminal, which causes the terminal to enter a "fast fade" state. If, during steady state operation, a terminal reports an SNR drop greater than or equal to the *Fast Fade Threshold*, then the hub considers the remote to be in the fast fade state.
9. If applicable, use **Spreading Factor** to specify a spread factor of SF=2, SF=4, or SF=8. A spread factor should only be specified when **CCM** is also specified, and not with **ACM**.
10. Under **Transmission Parameters**, enter a **Symbol Rate** for the DVB-S2 downstream carrier profile.
11. Click **Save** to save the **iNet Profile** and downstream carrier and continue in the **Modify** mode; or click **Save and Close** to save and open the **Browse Network Domain** window.

3.3 Defining an Inroute Group Profile

In a Velocity network, an *inroute* refers to an adaptive-TDMA upstream carrier, or more specifically, a specific frequency on which a satellite terminal transmits a burst during a time slot. An *inroute group (IG)* is a collection of carrier plans that define the symbol rate, MODCOD, and FEC rate used by a terminal for the TDMA inroute transmission.

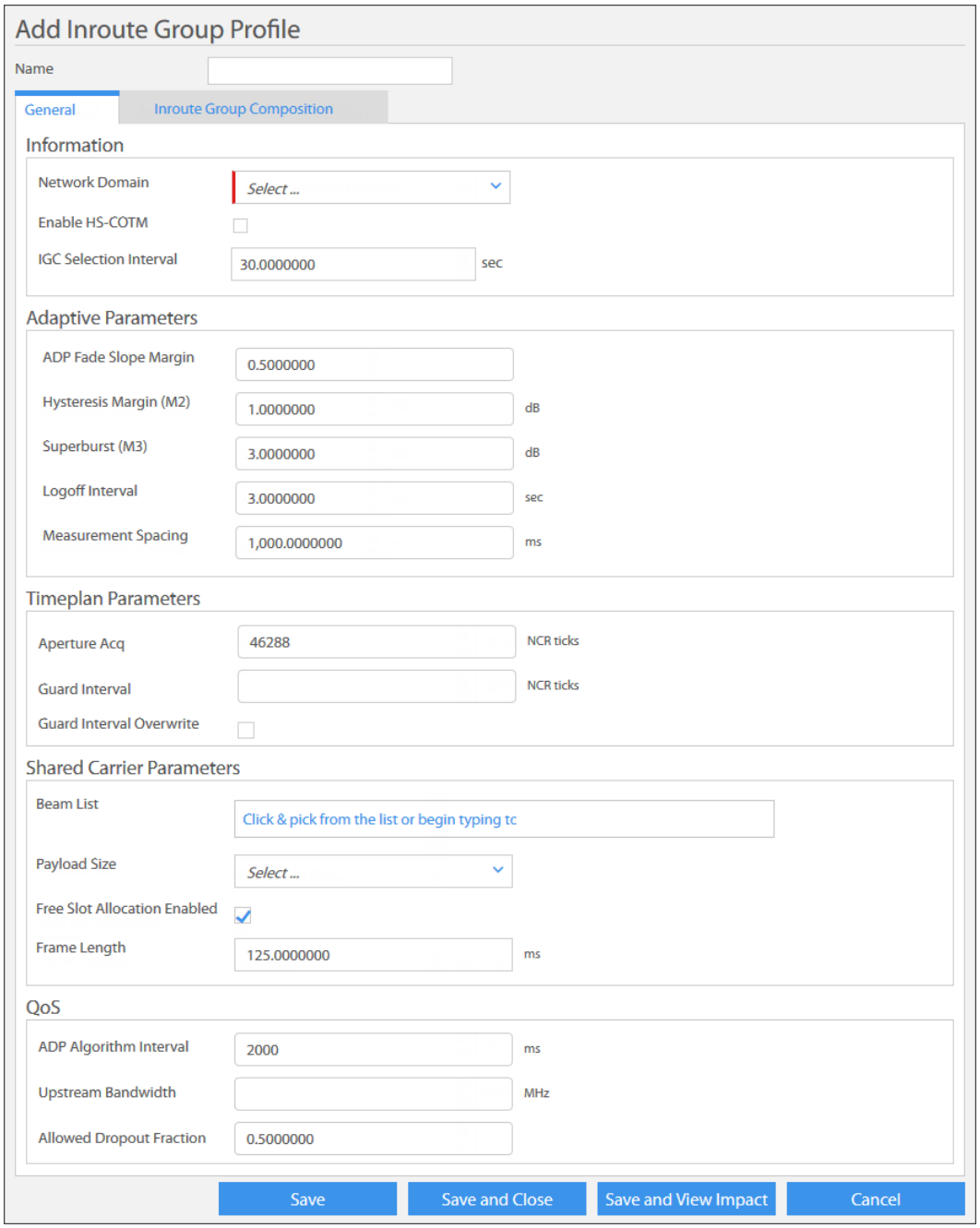

Figure 3-4. Add Inroute Group Profile - General Parameters Dialog

The carriers in an IG are assigned consistent transmission attributes — for example MODCOD and FEC rate, such that a terminal can transmit on any one of the inroutes while only changing its transmission frequency. To accomplish this characteristic, the NMS supports the configuration of an *inroute group profile (IGP)*, from which inroute groups inherit the properties of the beams associated with the IG Profile.

From the **General** tab of the **Add Inroute Group Profile** dialog, you specify basic information like **Name**, associated **Network Domain**, and whether to enable the **HS-COTM** option. There are also sections for specifying **Adaptive-TDMA**, **Timeplan Parameters**, **Shared Carrier Parameters,** and Quality of Service (**QoS**) parameters.

To define an inroute group profile:

1. Click the **Configuration** tab > **Network Domain** > **Add > Inroute Group Profile.** The **Add Inroute Group Profile** dialog opens to the **General** parameters tab.
2. Enter a **Name** for the new Inroute Group Profile.
3. Use the **Network Domain** drop-down and select the domain to which the Inroute Group Profile is associated.
4. Select **Enable HS-COTM** to enable the feature for inroute groups from this profile.
5. Enter the **IGC Selection Interval** — the frequency at which the IGC selection algorithm executes to select the optimal IGC for the current network conditions. The algorithm may run more often if demanded by network performance. The default is 30 seconds.
6. Enter the following **Adaptive Parameters** or use the default values, which will be applied to the inroute groups that use this IGP:
   a. **ADP Fade Slope Margin** — allows for fade that can occur during the reaction time of the power control algorithm, as well as for any uncertainty in the C/N_0 estimations.
   b. **Hysteresis Margin (M2)** — is added to the **Fade Slope Margin** in determining whether a remote should switch to a more efficient upstream carrier of a different MODCOD/symbol rate. This margin prevents frequent switching between carriers.
   c. **Superburst (M3)** — represents the initial nominal upstream carrier for the remote based on the C/N of the acquisition burst.
   d. **Logoff Interval** — is the PP wait time before declaring a terminal is out of network.
   e. **Measurement Spacing** — the number of seconds between UCP (uplink control link parameters) measurements of satellite terminal bursts by the hub during steady-state ("Clear Sky") operation. During fade, the UCP algorithm increases the terminal update interval from every 5 seconds to every 1 second, should the (ADP Fade Slope Margin + ADP Hysteresis Margin) threshold be exceeded (*Fast Fade*).
7. Enter the following **Timeplan Parameters** or use default values, which will be applied to the inroute groups that use this IGP:
   a. **Aperture Acquisition** — the length, in microseconds, of the window in which remotes send acquisition bursts on the upstream carriers. The default is 46288 ticks.
   b. **Guard Interval** — the guard time, in NCR ticks, which account for the symbol timing uncertainty that exists when Satellite Terminals transmit TDMA bursts.
   c. **Guard Interval Overwrite** — select to allow addition margin to the Guard Interval.

8. Enter the following **Shared Carrier Parameters** or use the default values, which will be applied to all of the carriers in an inroute group that uses this IGP:
   a. **Beam List** — select the beams in which inroute groups from this profile can operate.
   b. **Payload Size** — the payload size to be used by all inroute groups associated with this Inroute Group Profile. The default payload size is 170 bytes.
   c. **Free Slot Allocation Enabled** — if free or unused TDMA slots should be assigned to remotes in a fair manner, respecting the configured CIR/MIR of remotes. Otherwise, the bandwidth manager assigns TDMA slots to remotes for each TDMA allocation interval based on current CIR/MIR demand and configuration.
   d. **Frame Length** — the frame length of the upstream carriers in the inroute group. The system calculated default value is 125 milliseconds.
9. Enter the following **QoS Parameters** or use the default values, which will be applied to an inroute group that uses this inroute group profile:
   a. **ADP Algorithm Interval** is the processing update interval, in milliseconds, of the adaptive algorithm.
   b. **Upstream Bandwidth** — the bandwidth assigned to carry traffic from the remote to the hub within an IGC. The IGC must be equal to or less than the total Upstream Bandwidth assigned here and not more than the bandwidth assigned to the channel.
   c. **ADP Allowed Dropout Fraction** — the threshold value determined by an algorithm that uses the number of in-network terminals that would have to drop out of network before another IGC is selected. If this value were exceeded the IGC would not be selected for use unless it were 'Fixed' or configured as the default IGC.
10. Click **Save and Close** to save the configuration to the NMS or click **Save** to continue in the modify mode with *Adding Inroute Group Profile Upstream Carriers*.

3.3.1 Adding Inroute Group Profile Upstream Carriers

The **Inroute Group Composition** tab of the **Add Inroute Group Profile** page is where TDMA **Upstream Carrier** records are defined. These upstream carriers become part of the inroute group profile. Once the desired upstream carrier records are created, they can later be added to an **Inroute Group Composition**.

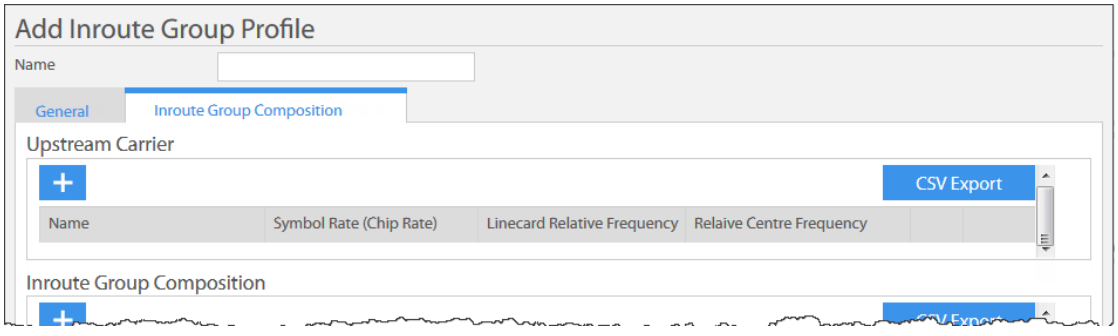

Figure 3-5. Add Inroute Group Profile - Upstream Carrier Tab

To add upstream carriers to the inroute group profile:

1. Click the **Upstream Carrier** tab of the **Add Inroute Group Profile** dialog.
2. Click the **Add Record** icon, to open the **Add Upstream Carrier** dialog.
3. Enter a **Name** for the new TDMA upstream carrier.
4. Enter a **Guard Band**. This narrow frequency band value separates bands in order to prevent interference between upstream carrier signals.
5. Enter the **Relative Center Frequency** of the upstream carrier. This value is a positive or negative offset from the **Line Card Relative Frequency** value.
6. Enter a **Symbol Rate (Chip Rate)** value from 128 to 5875 Ksps, for the new carrier.
7. Enter the following **Acquisition (ACQ) Parameters**:
   a. **ACQ Enabled** — select to allow Satellite Terminals to send ACQ messages to the hub. This option should not be enabled for more than 8 carriers maximum.
   b. **ACQ Guard Interval** of TDMA bursts. The **Guard Interval** is the guard time in NCR ticks that account for symbol timing uncertainty when a remote transmits TDMA bursts.
   c. **ACQ Method** — the acquisition method terminals will use to acquire on this carrier. The options include the **Superburst** or the traditional waveform, if no option is selected; or **Spread Spectrum** is selected for spreading carriers.
   d. **ACQ Slot Number** specify the number of ACQ slots in the time frame, as "0" or "1."
8. Enter the **Line Card Relative Frequency** — the relative frequency of the transmit line card. This value is always zero for inroute group profiles used by a fixed beam.
9. Click **Save** to accept the new carrier and return to the main **Upstream Carrier** tab. Each carrier is inserted under **Upstream Carrier**, as a new carrier record.
10. Repeat the above steps, from Step (2), to insert additional **Upstream Carrier** records.
11. For a given **Upstream Carrier**, click the **Edit** icon to modify the record; click **Delete** to remove the selected Carrier.
12. Click **Save and Close** to save the configuration to the NMS or click **Save** to continue in the modify mode with *Creating an Inroute Group Composition*.

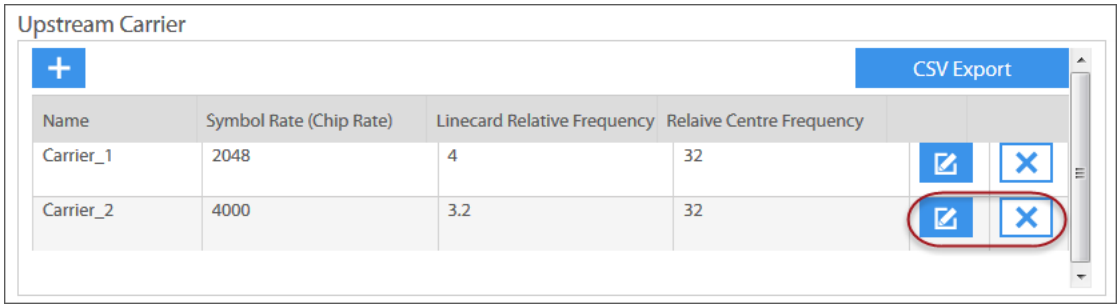

Figure 3-6. Upstream Carrier Records

3.3.2 Creating an Inroute Group Composition

A set of defined carriers assigned to an inroute group is called an *Inroute Group Composition (IGC)*. When several upstream carriers are configured, then individual inroute group compositions may be defined from the user-specified combination of carriers.

Up to eight IGCs can be configured for a single inroute group, using the **Inroute Group Composition** dialog. At any time, only one IGC is assigned to operate in the inroute group. Determining the number and composition of IGCs for each inroute group is part of the network design process.

During operation, use of IGCs allow the Modulation and Error Rate of the Adaptive carriers in an Inroute Group to be dynamically adjusted to suit current network conditions. The Protocol Processor regularly evaluates the configured IGCs and selects the IGC that best matches the current overall state of the network. An IGC currently assigned to an inroute group determines how the bandwidth in the inroute group is partitioned at the that particular time.

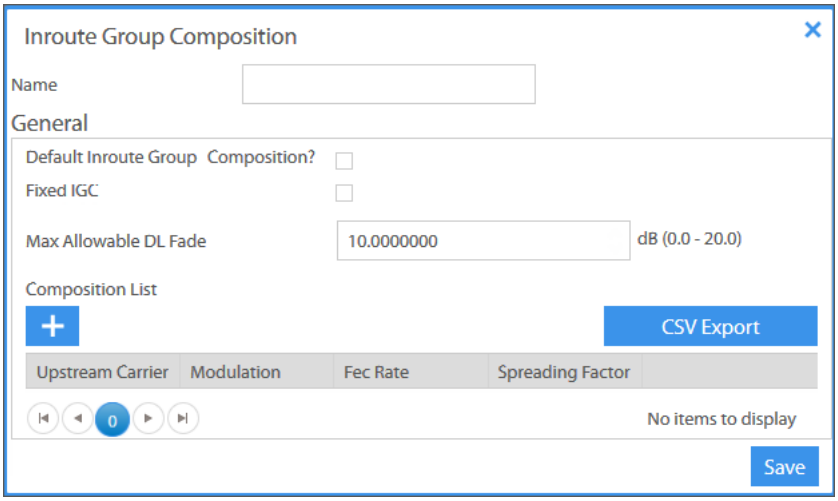

Figure 3-7. Add Inroute Group Composition Dialog

To define an inroute group composition:

1. Start with the **Add Inroute Group Profile** dialog open to the **Inroute Group Composition** tab, with the configured **Upstream Carriers** displayed.
2. Click the **Add Record** icon, under the section **Inroute Group Composition**. The **Add Inroute Group Composition** dialog opens.
3. Enter a **Name** for the new Inroute Group Composition (IGC).
4. Select **Default Inroute Group Composition** to designate this IGC as the default IGC for the Inroute Group. During operation, the default IGC is selected if the **Allowed Dropout Factor** is exceeded for all IGCs configured for the inroute group.
5. Select **Fixed IGC** to indicate that the inroute group should lock to this IGC. When a fixed IGC is specified, all other configured IGCs are ignored and not used.
6. In **Max. Allowable DL Fade**, enter the maximum fade value between 0.0 and 20.0 dB.
7. Under the **Composition List** section of the page, click the **Add Record** icon to insert an Upstream Carrier as a member of the Composition list of the new IGC.

8. For each record, select an **Upstream Carrier**; select the **Modulation** and **FEC Rate**; and if applicable, select a **Spreading Factor** or select **No Spreading**.
9. Click the **Update** icon to insert the carrier to the IGC list.
10. Repeat the previous steps, from Step (7), to add another **Upstream Carrier** to the **Composition List** records, under **Upstream Carrier**.
11. To modify the upstream carrier parameters of a **Composition List** record, click the **Edit** icon, make the changes and again click the **Update** icon.
12. Click the **Delete** icon to remove an Upstream Carrier from the **Composition List**.
13. When the Composition List is completed, click **Save** to insert the **IGC** and return to the **Inroute Group Composition** tab. The IGC is inserted as a new IGC, listed by **Name**, under the **Inroute Group Composition** section of the dialog.
14. Repeat the previous steps, from Step (2), to add another **IGC** record to the IG Profile.
15. For a given **IGC** record, click the **Edit** icon to modify the record, click the **Update** icon to accept the record; and click **Delete** to remove the IGC from the Inroute Group Profile.
16. Click **Save** to save the **Inroute Group Profile** and continue in the **Modify** mode; or click **Save and Close** to save and open the **Browse Network Domain** window.

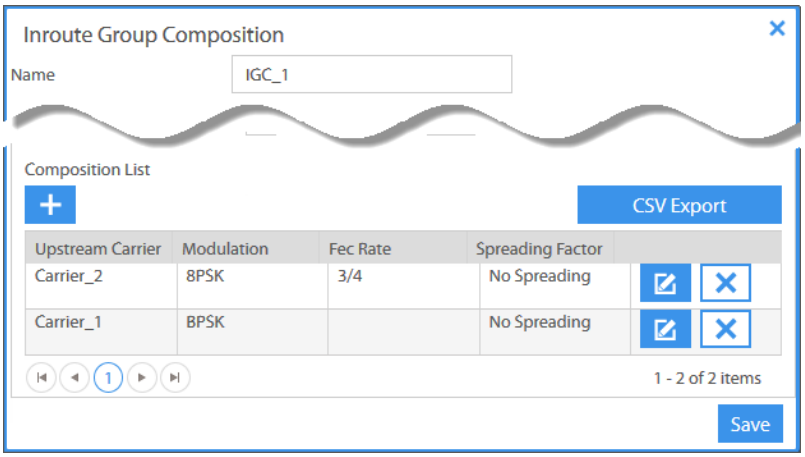

Figure 3-8. Inroute Group Carrier Composition List Records

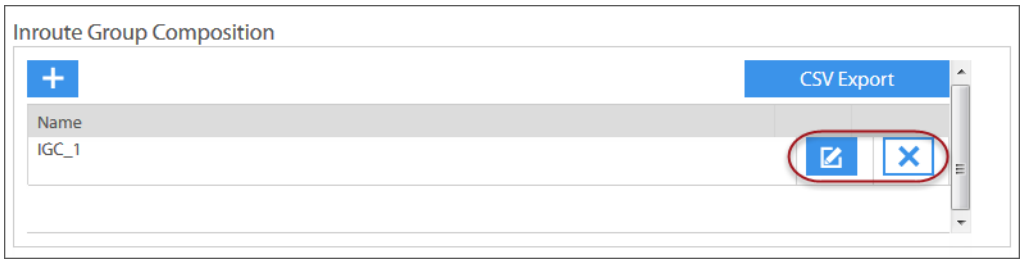

Figure 3-9. Inroute Group Composition (IGC) Records

3.4 Network Domain Browse Actions

Using the Pulse **Browse Network Domain** command**,** users can interact with configured Network Domain elements in the Browse Results list to perform a variety of operations. These operations are called “actions.” An action can be performed on a single element, using the **Action** button for that element, or simultaneously on multiple selected elements, by using the browse window **Group Actions** button.

Only the actions which are possible, based on the element type, are displayed when an element type is selected. All actions are not possible with all elements.

The Network Domain element actions are listed and briefly described as follows:

Table 3-1. Network Domain — Browse Actions

Action	Brief Description
View Details	View configured information for a selected element.
Copy	Create a copy of the selected element, which can be modified as required, renamed, and saved as a new element.
Modify Element	Modify the configured information for the selected element, and re-submit with changes.
Delete Element	Remove the selected element from the NMS.
Apply Configuration	Apply the configured NMS changes to the selected element, using the pending option file configured for the element.
Impact Analysis	View impact on other elements, if changes are applied to the selected element.
Progress Report	View a summary report of update manager progress since applying changes to the selected element. For details.
Retrieve Pending Option File	Load from the NMS database, and display the pending copy of the options file for the selected element.
Retrieve Active Option File	Load and display the options file currently active for the selected element.
Compare Configurations	Compare the pending options file and the active options file for the selected element.
Modify Engineering Debug Keys	Modify custom key associated with a specific feature to enable or disable, add or modify functionality.

4 Configuring Service Domain Elements

The *service domain* includes elements like group service plans, subscriber service plan profiles, subscriber plan components, and geographic regions. Through the creation of service domain elements, available bandwidth is procured and allocated, as well as managed through the implementation of the bandwidth management and Quality of Service (QoS) operations.

The following topics briefly introduces each Service Domain element and provides step-by-step procedures for configuring each element and its associated parameters.

4.1 Service Domain Configuration Sequence

The NMS tools for defining, configuring, and modifying service domain elements are accessed from the **Service Domain** operations menu on the NMS **Configuration** tab. Each service domain element, before it can be deployed in an iDirect Velocity™ Network, must first be created and the associated parameters configured in the NMS.

Depending on assigned user group membership and access permissions, the NMS supports creating, viewing, modifying, and deleting of Service Domain Element configurations.

A general sequence for configuring Service Domain elements in the NMS, is shown in here.

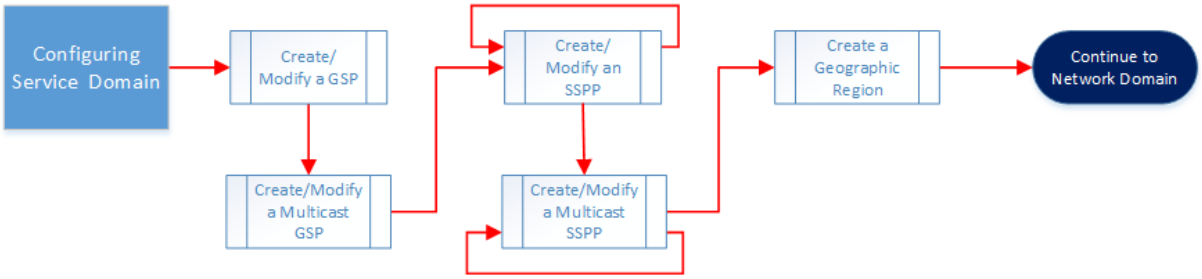

Figure 4-1. Building a Basic Network — Creating Service Domain Elements

4.2 Creating Geographic Regions

A *geographic region* is defined as a combination of beams or service areas that constitutes an area of coverage. When it comes to configuring the geographic scope of a service plan, multiple regions may be assigned to a plan. These regions, however, may only be assigned as part of the geographic scope if they have already been defined in the NMS.

Generally, a Satellite Operator creates geographic regions, however a Service Provider can also create a geographic region using service areas from an SA Group for which permission to use has been assigned by the Satellite Operator.

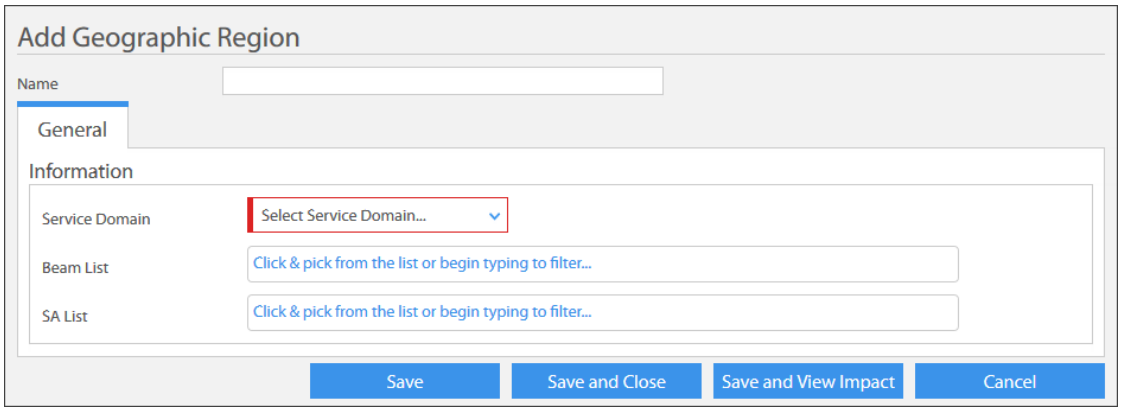

Figure 4-2. Creating a New Region

To add a new geographic region:

1. Click the **Configuration** tab **> Service Domain** > **Add > More Options > Geographic Region.**
2. Type the **Name** of the new geographic region.
3. Use the **Service Domain** drop-down to select the parent domain for this region.
4. Use the **Beam List** multi-select box to select two or more beams to define the region; or use the **SA List** multi-select box to select two or more Service Areas to define the region. Both beams and service areas combined cannot be selected to form a region.
5. Click **Save** to save the new geographic region to the NMS and continue in the **Modify** mode; or click **Save and Close** to save and open the **Browse Service Domain** window.

4.3 About GSP MODCOD Scaling

The Velocity system, in order to o address the non-homogeneity of beam combinations in a GSP, implements GSP MODCOD scaling. MODCOD scaling applies an appropriate scaling factor to each beam in order to normalize the performance between stronger and weaker beams. With MODCOD scaling, the CIR/MIR for any given beam is either scaled up or down based on the ratio of the spectral efficiencies of the Nominal MODCOD and the Average MODCOD in the beam.

In Pulse, depending on the number of GSPs and beams to be configured for MODCOD scaling, either a manual or profile-based method of configuration can be used. The manual method of configuring the parameters for MODCOD scaling is performed directly on the **Geographic Scope** tab of the GSP dialog; and although the MODCOD scaling profile is applied on the **Geographic Scope** tab, the *GSP Service Plan Profile* must have already been configured. If the profile-based method is used the fields used for the manual configuration are disabled.

4.4 Creating a GSP Service Plan Profile

In networks with large numbers of beams and GSPs, configuring a *GSP Service Plan Profile* for MODCOD scaling, provides an efficient way to configure scaling factor values to be applied on a per beam basis for specific beams, and a default to be applied to the remaining beams. The profile will contain a per beam **Average MODCODs** to be applied to specific beams, and a **Default Average MODCOD** to be applied to all other beams. Once the profile is configured, it can be applied to the geographic scope of multiple GSPs, on the GSP **Geographic Scope** tab.

A GSP Service Plan Profile is applied when configuring the GSP Geographic Scope.

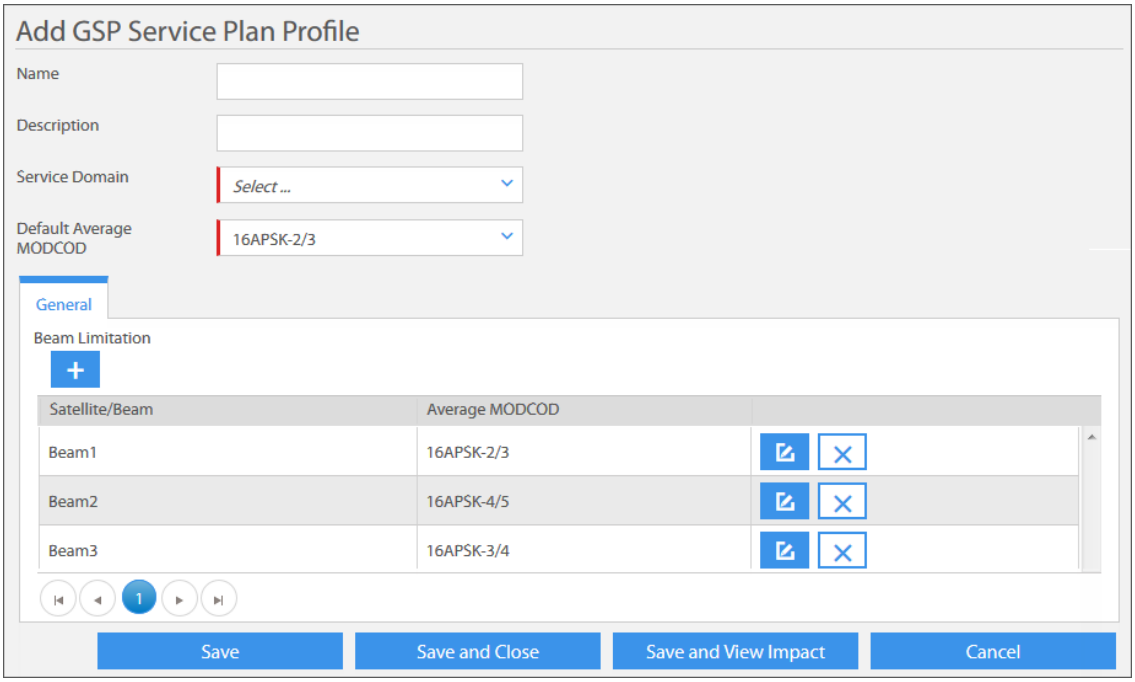

Figure 4-3. Creating a GSP Service Plan Profile for MODCOD Scaling

To add a new GSP Service Plan Profile for MODCOD scaling:

1. Click the **Configuration** tab > **Service Domain** > **More Options** > **GSP Service Plan Profile.**
2. Type the **Name** of the new MODCOD profile.
3. Enter a **Description** of the new MODCOD profile.
4. Use the **Service Domain** drop-down to select the parent domain for this profile.
5. Use the **Default Average MODCOD** drop-down to select the default average MODCOD to be apply to all beams of the GSP to which the profile is applied.
6. Under the **Beam Limitations** section, click the **Add Record** button, to define one or more specific beam MODCOD scaling records for this profile.
7. Click the **Satellite/Beam** drop-down and select a desired **Satellite/Beam** to configure.
8. Specify the **Average MODCOD** for the beam.
9. Click the **Update** icon to accept the entry as a new specific beam profile record.
10. Repeat the above steps to specify an additional specific beam record for the profile.
11. Click the **Edit** icon to modify a record; click the **Delete** icon to remove a record.
12. Click **Save** to save configuration to the NMS and remain in modify mode; or click **Save and Close** to save the configuration and open the **Browse Service Domain** window.
13. If applicable, find the GSPs to which this new profile will be applied. The profile is applied on the GSP **Geographic Scope** tab.

4.5 Creating Group Service Plans

A *Group Service Plan (GSP),* which may be defined by the Network Operator or by a Service Provider, is a plan of service that represents an acquisition of satellite bandwidth capacity on the Velocity Network. By defining GSPs, the available capacity is allocated to groups rather than to individual terminals. As a result of defining GSPs for the various VNO/VNO or VNO/Dealer relationships, available bandwidth is allocated and the structure for bandwidth management is thereby defined.

A VNO may procure multiple GSPs, each of which may support a different application. For example — one GSP may provide a data service — another a voice service. Each plan may also have a different priority and geographic scope — for example one has global scope and is assigned Priority of 1; another has regional scope and is assigned Priority of 2. In such a scenario, subscribers of the GSP with a data component would receive capacity from the data GSP, and subscribers with a voice component would receive capacity from the voice GSP.

Later, when a VNO creates a subscriber service plan profile (SSPP), subscriber service plan components (SSPCs) that are derived from the SSPP are linked to a parent GSP. Association with the GSP identifies the SSPC as a QoS node that receives bandwidth from the GSP.

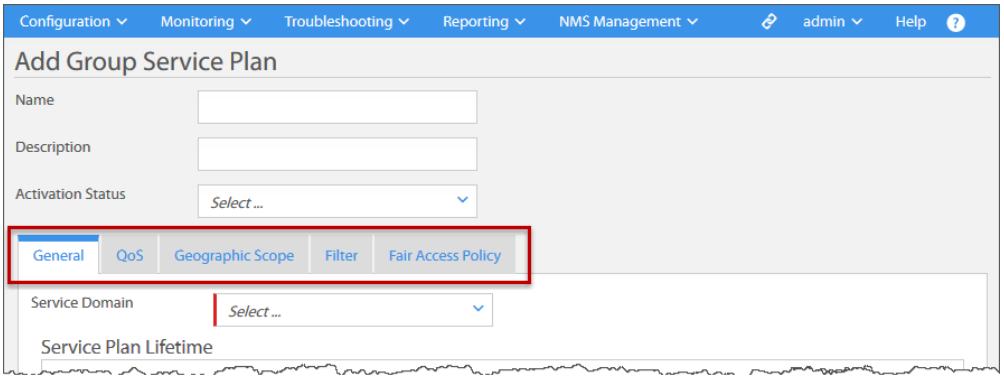

Figure 4-4. Add Group Service Plan Configuration Tabs

4.5.1 Add GSP — General Parameters

The GSP **General** tab is for defining basic settings like the GSP **Name** and **Description**. It also includes sections for configuring the **Service Plan Lifetime**, a **Recurrence Pattern**, **Limits** if applicable, and an **Information** section for specifying other items supported by the GSP.

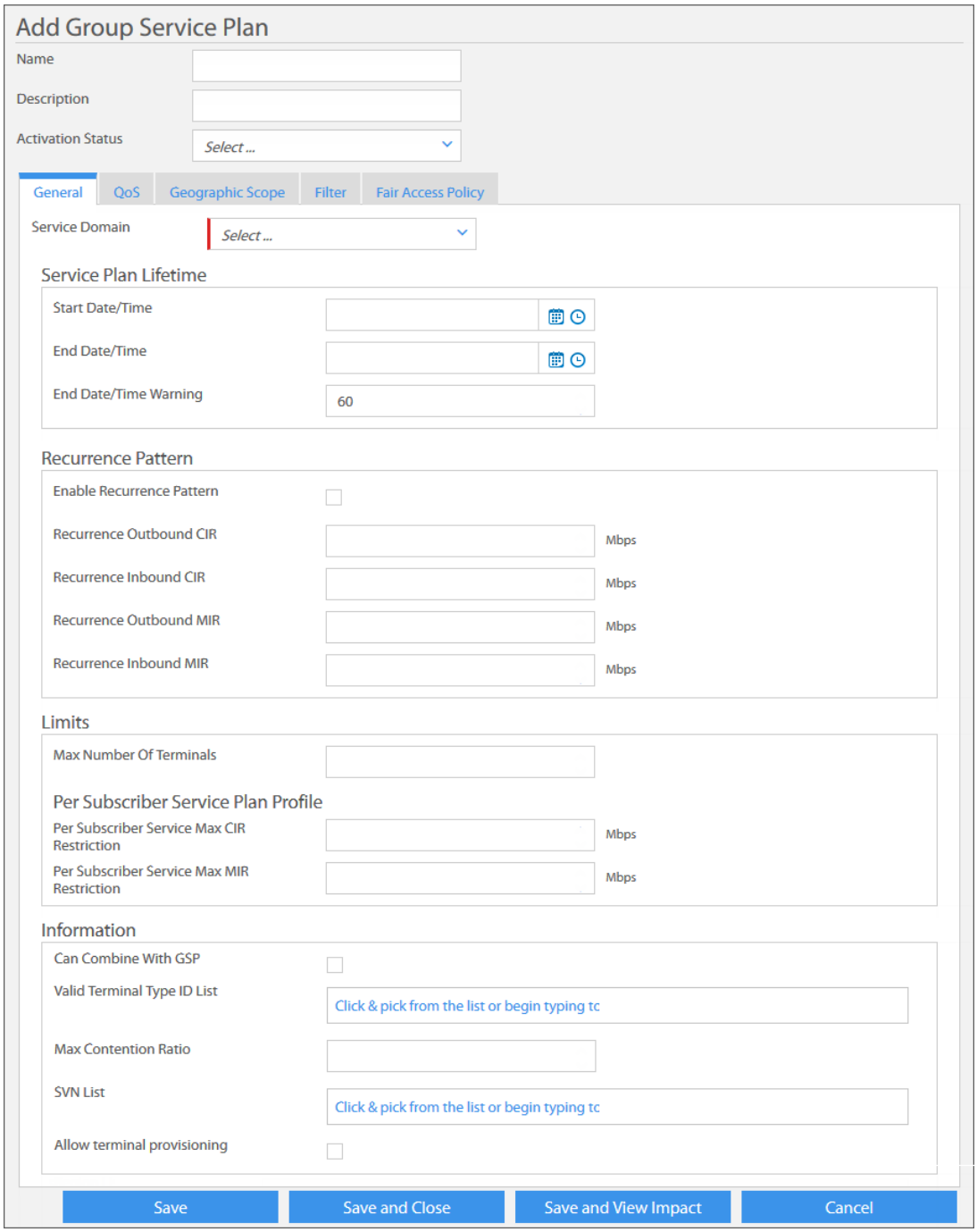

Figure 4-5. Add GSP — General Parameters

To create a Group Service plan:

1. Click the **Configuration** tab > **Service Domain** > **Add > Group Service Plan.**
2. On the **General** tab, enter a **Name** and **Description** of the new group service plan (GSP).
3. Use the **Activation Status** drop-down to specify whether the GSP should be **activated** or **de-activated** when saved to the NMS.
4. Use the **Service Domain** drop-down to select the parent GQoS node for this GSP.
5. Under the **Service Plan Lifetime** section, select a **Start Date/Time** and an **End Date/Time** to define the valid duration for this GSP.
6. Enter the **End Date/Time Warning** as the number of days prior for issuing a warning.
7. Under the **Recurrence Pattern** section, select **Enable Recurrence Pattern**, to display fields for entering a service recurrence pattern for the GSP, if this is applicable.
8. Select a **Recurrence Type** of **Daily**, **Weekly**, or **Monthly,** if a recurrence is enabled, then from the list below, use the appropriate instructions based on the recurrence type:
   a. **Daily** — Specify a **Recurrence Start Time** and **Recurrence End Time** for the GSP.
   b. **Weekly** — Use the **Recurrence Weekdays** multi-select box, to select weekdays.
   c. **Monthly** — Use the **Recurrence Month Days** multi-select box, to select the days.
9. Enter a **Recurrence Outbound CIR** and **Recurrence Inbound CIR** for the GSP.
10. Enter a **Recurrence Outbound MIR** and **Recurrence Inbound MIR** for the GSP.
11. Under the **Limits** section, enter a **Maximum Number of Terminals** the GSP will support.
12. Enter the **Per Subscriber Service Max CIR Restriction** (not to be exceeded), to allocate to subscribers to this GSP.
13. Enter the **Per Subscriber Service Max MIR Restriction** (not to be exceeded), to allocate to subscribers to this GSP.
14. Under the **Information** section, select **Can Combine With GSP** if this GSP may be combined with other GSPs.
15. Use the **Valid Terminal Type ID List** multi-select list box, to choose one or more terminal types that can support this new GSP.
16. Specify the **Maximum Contention Ratio** that the GSP will support. This value is calculated by dividing the aggregate CIR of all terminals in a group by the group CIR.
17. Use the **SVN List** multi-select list box, to choose the SVNs to support traffic for this GSP.
18. Select **Allow Terminal Provisioning**, to support this feature for this GSP.
19. Click **Save and Close** to save the configuration to the NMS; or click **Save** to continue in the modify mode to *Add GSP — QoS Parameters*.

4.5.2 Add GSP — QoS Parameters

QoS or *Quality of Service,* refers to the classification and priority given to IP traffic in order to optimize and control the delivery of packets as they flow through a Velocity Network. Managing the distribution of available bandwidth, in the face of contention among demanding subscribers, is also the subject of the QoS implementation. Each GSP is specified in terms of Mbps, at a nominal MODCOD, which translates directly to bandwidth.

The GSP *QoS* is defined by parameters such as *Committed Information Rate (CIR)*, *Maximum Information Rate (MIR)*, *Nominal MODCOD*, *Priority*, and *QoS Cost*. These parameters, which determine the level of service or bandwidth allocation, are configured for both the Inbound and Outbound service.

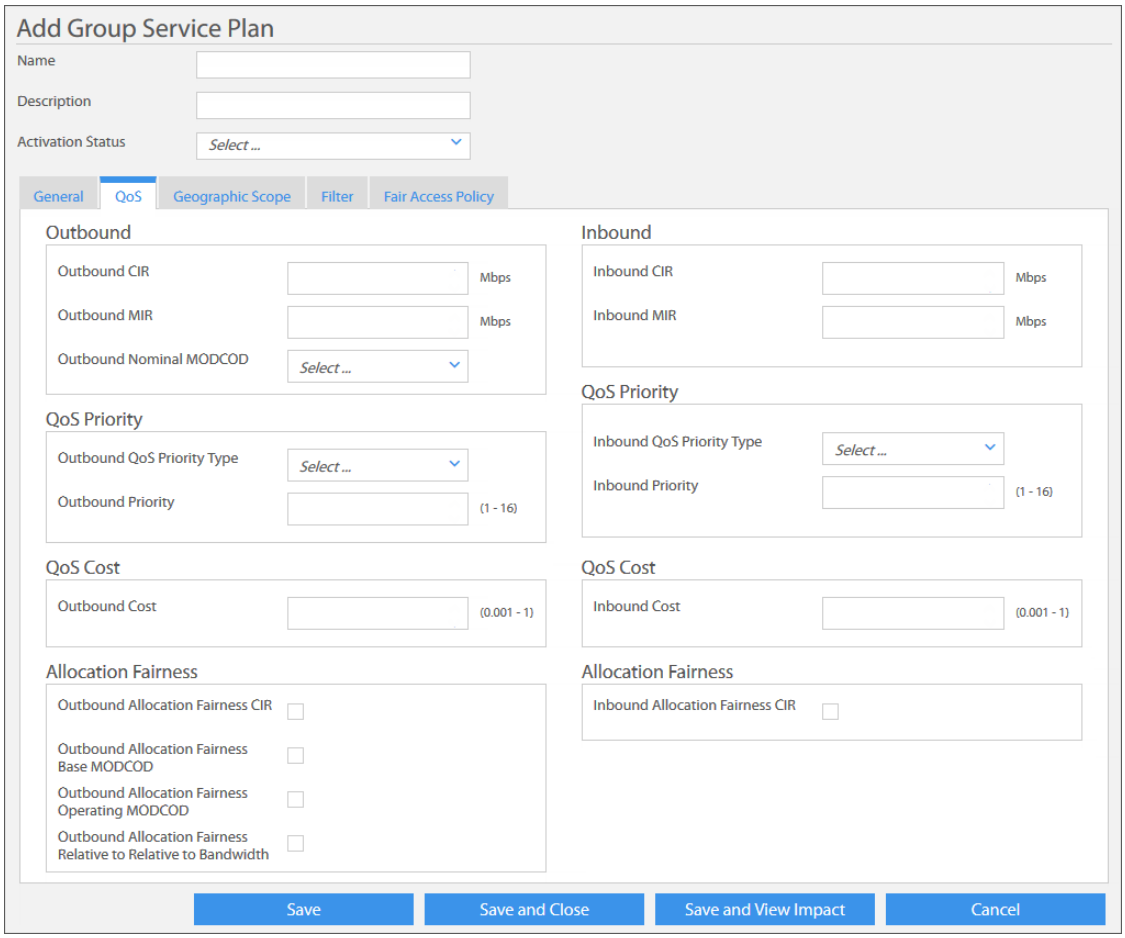

Figure 4-6. GSP QoS Parameters Dialog

To define the GSP Quality of Service (QoS):

1. Click the **QoS** tab, to open the QoS parameters dialog for the Group Service Plan.
2. Specify the **CIR** and **MIR**, in Mbps, for both **Inbound** and **Outbound** traffic of this GSP.
3. Select the **Outbound Nominal MODCOD**.

4. Select the **QoS Priority Type** as **Absolute** or **Pre-Allocation Round**, for both the **Outbound** and **Inbound**.
5. Enter the **QoS Priority** (1 = highest; 16 = lowest); and the **QoS Cost**, as a value between 0.001 and 1, for the **Outbound** and **Inbound**.
6. Select the desired **Allocation Fairness** options to be applied to applications under this GSP, for both the **Outbound** and **Inbound** traffic.
7. Click **Save and Close** to save the configuration to the NMS; or click **Save** to continue in the modify mode to *Add GSP — Regional Geographic Scope*.

4.5.3 Add GSP — Global Geographic Scope

To configure a GSP with global geographic scope, means that the coverage includes all geographic regions. When the **Scope Type** is set to **Global** on the GSP **Geographic Scope** dialog, default **Beam Restrictions**, that apply to all beams, may be defined for the Inbound and Outbound. Also, specific **Beam Limitations** may be specified on a per beam basis.

On the Outbound, a **Default Average MODCOD** value, which must be specified, is used in determining the default MODCOD scaling factor to be applied to all beams. As an alternative, a GSP Profile, which specifies a **Default Average MODCOD** and a per beam **Average MODCOD**, which applies to specific beams can be applied to the GSP.

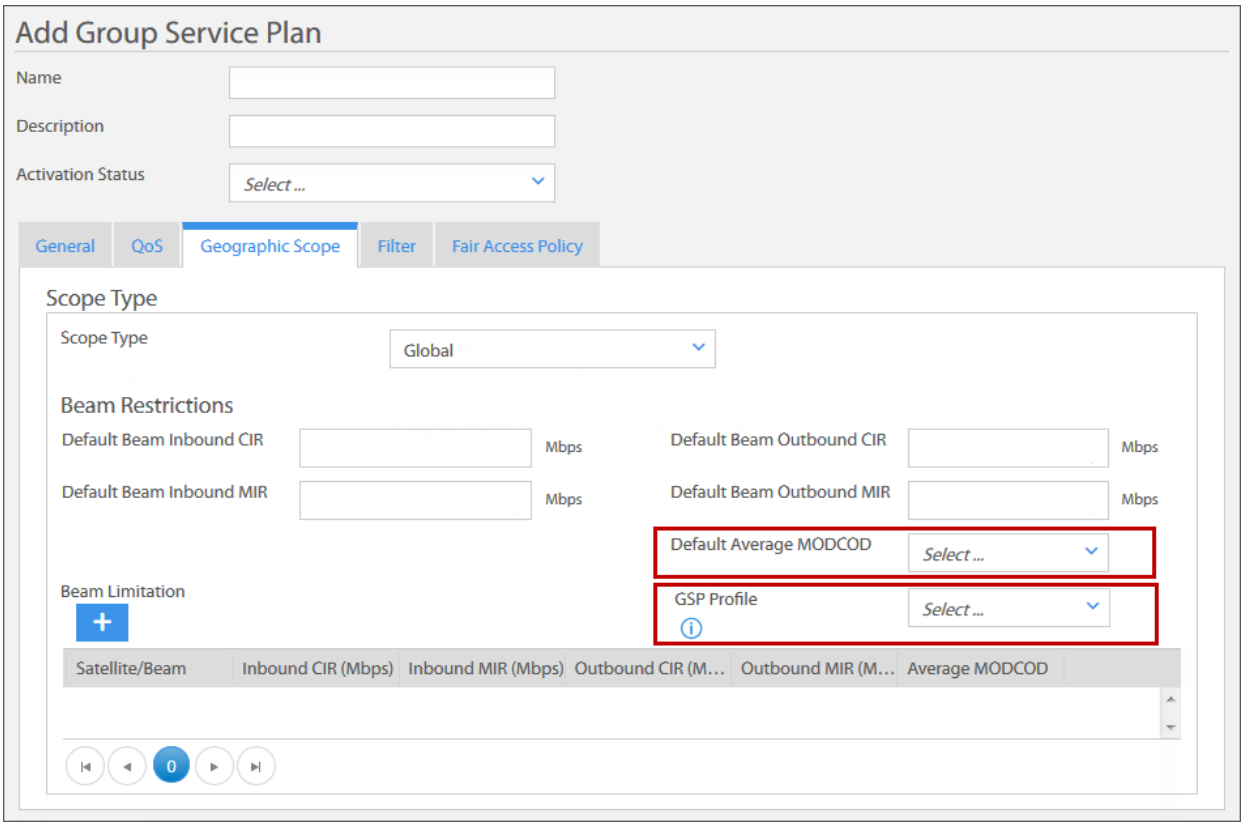

Figure 4-7. GSP Regional Geographic Scope

To configure global geographic scope for a GSP:

1. From the **Add Group Service** plan page, click the **Geographic Scope** tab.
2. Use the **Scope Type** drop arrow to select **Global** to configure a global coverage.
3. Under **Beam Restrictions**, specify the **Default Beam Inbound CIR** and the **Default Beam Inbound MIR.** These default values apply to all beams.
4. Specify the **Default Beam Outbound CIR** and **Default Beam Outbound MIR.** These default values apply to all beams.
5. Specify the **Default Average MODCOD.** This value is used to determine the MODCOD scaling factor that will apply to all beams, unless a GSP Service Plan profile is applied.
6. If applicable, use the **GSP Profile** drop-down and select a MODCOD scaling profile to apply to this GSP.
7. Click **Save** to continue to *Configuring GSP Single Beam Limitations*, if applicable.

4.5.4 Add GSP — Regional Geographic Scope

When the **Scope Type** is set to **Regional** on the GSP **Geographic Scope** dialog, multiple regions may be selected from a list of regions. These regions may include SAs or Beams that have already been defined in the NMS. The configuration includes default **Beam Restrictions**, that apply to all beams, and is defined for the Inbound and Outbound. Also, specific **Beam Limitations** may be specified on a per beam basis.

On the Outbound, a **Default Average MODCOD** value, which must be specified, is used in determining the default MODCOD scaling factor to be applied to all beams. As an alternative, a GSP Profile, which specifies a **Default Average MODCOD** and a per beam **Average MODCOD**, which applies to specific beams can be applied to the GSP.

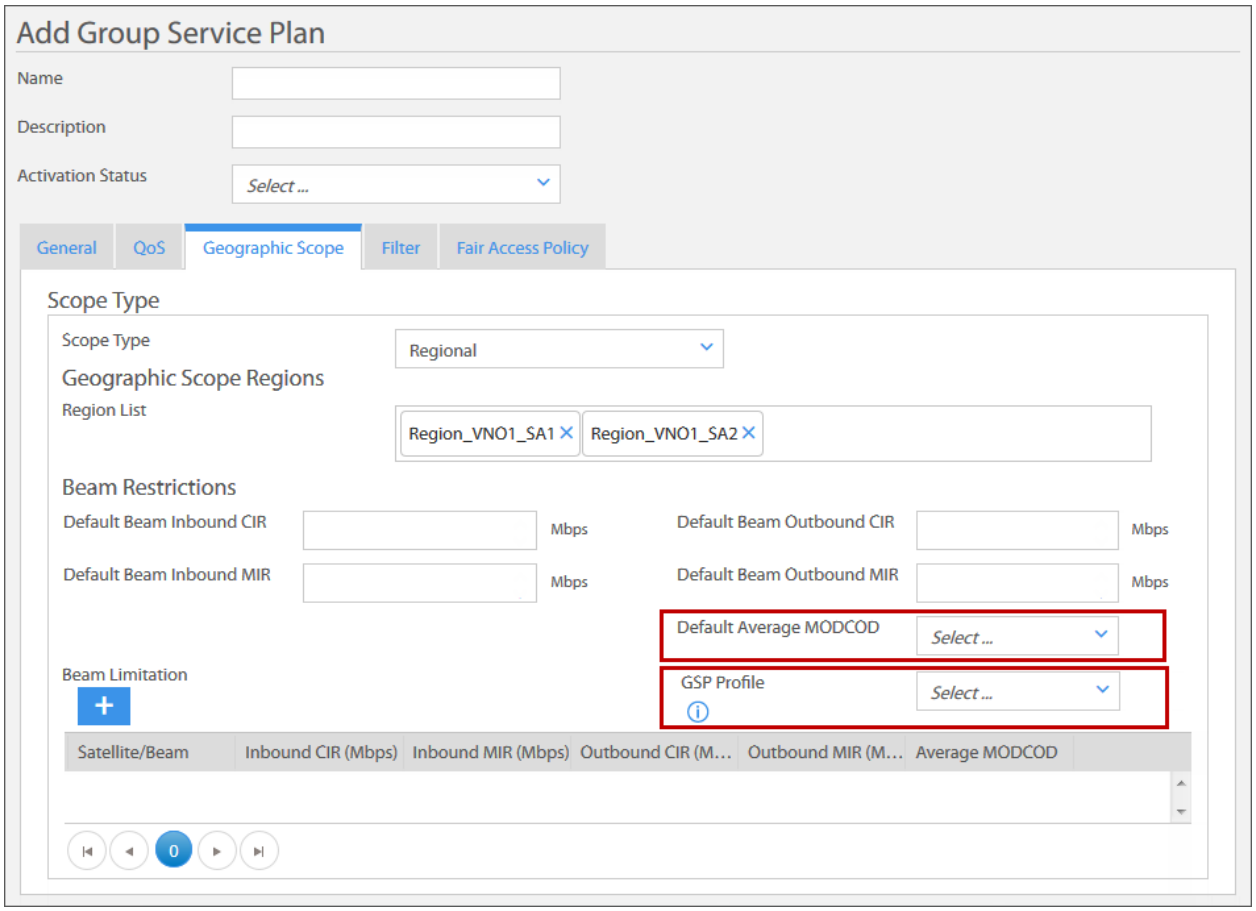

Figure 4-8. GSP Regional Geographic Scope

To specify regions to a GSP regional scope:

1. Click the **Geographic Scope** tab > **Scope Type** > **Regional** to add GSP regional coverage.
2. Under the **Geographic Scope Region**, use the **Regions List** multi-select list box and select one or more predefined regions to add to the geographic scope of the GSP.
3. Use the **Scope Type** drop arrow to select **Regional** to configure a regional coverage.

4. Under **Beam Restrictions**, specify the **Default Beam Inbound CIR** and the **Default Beam Inbound MIR.** These default values apply to all beams.
5. Specify the **Default Beam Outbound CIR** and **Default Beam Outbound MIR.** These default values apply to all beams.
6. Specify the **Default Average MODCOD.** This value is used to determine the MODCOD scaling factor that will apply to all beams, unless a GSP Service Plan profile is applied.
7. If applicable, use the **GSP Profile** drop-down and select a MODCOD scaling profile to apply to this GSP.
8. Click **Save** to *Configuring GSP Single Beam Limitations*, if applicable.

4.5.5 Configuring GSP Single Beam Limitations

If required, users can define the maximum CIR/MIR allowed for a GSP in a specific (single) beam. Single beam limitations may be specified when defining global or regional geographic scopes. For example, a single beam CIR/MIR limit of 5 Mbps/10 Mbps is configured for 3 beams that define a region. By specifying restrictions for specific beams, it is possible to avoid placing a disproportionate demand on any one beam relative to the global CIR/MIR.

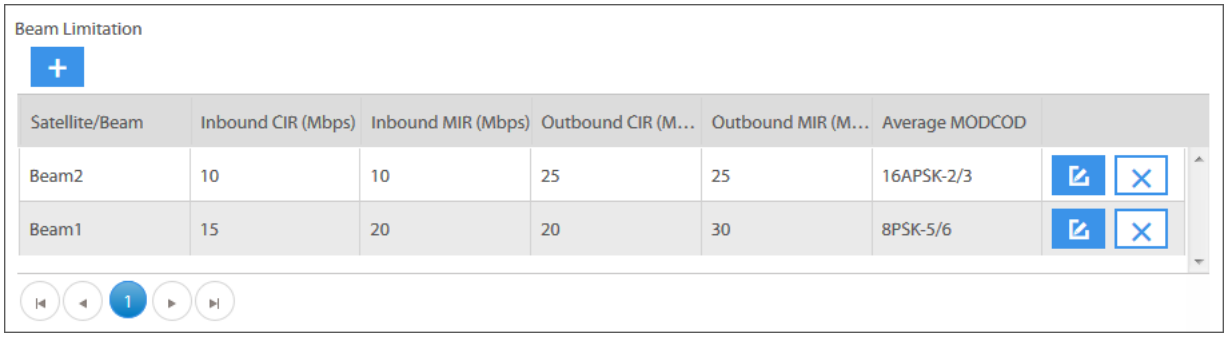

Figure 4-9. GSP Single Beam Specific Limitations Records

To add GSP beam specific restrictions for global or regional scope:

With the **Add Group Service Plan** page open to the **Geographic Scope** tab, and with the **Scope Type** drop arrow set for **Global** or **Regional**, per beam restrictions are defined under the **Beam Limitation** section.

1. Under the **Beam Limitation** section, click the **Add Record** button, to define a new single beam limitation. The **Beam Limitation** record fields are enabled.
2. Click the **Satellite/Beam** drop-down and select a beam to which MIR/CIR limits are to be defined for both the Inbound and Outbound.
3. Specify the **Outbound CIR** (Committed Information Rate) and the **Outbound MIR** (Maximum Information Rate), in Mbps, for the beam outbound.
4. Specify the **Inbound CIR** (Committed Information Rate) and the **Inbound MIR** (Maximum Information Rate)**,** in Mbps, for the beam inbound.
5. Specify the **Average MODCOD** for the beam record. This value is used in determining the MODCOD scaling factor to be applied to the specified beam.

6. Click the **Update** icon to accept the entries as a new single beam limitation record, listed under the **Beam Limitation** section.
7. Repeat the above steps to add another beam restriction record to the geographic scope.
8. Click the **Edit** icon on a given **Beam Restriction** record, to modify the record; click the **Delete** icon to remove the selected record.
9. Click **Save and Close** to save the GSP configuration.

4.6 Creating Multicast Group Service Plans

A *Multicast Group Service Plan (MGSP)* is a GSP is much like the previously described unicast GSP, except that it provides a data transmission service in which the data stream is simultaneously transmitted to multiple recipients, rather than sending separately to each recipient. Each multicast stream is identified by the destination multicast address and a network ID of the SVN to which the stream is targeted.

The MGSP requires that a plan priority, which is typically higher than other service plans, be specified. A low priority can also be specified for non-real-time applications. Typically, the multicast MODCOD is configured to apply to all beams within the coverage, but can be selectable by beam. Like the unicast GSP, the multicast GSP also supports a Fair Access Policy.

Finally, as with the GSP, the Multicast GSP is created only by authorized VNOs under the **Service Domain** of the **Configuration** page. Each Multicast GSP is configured using a **General**, **Geographic Scope**, **Quality of service** (**QoS**), **Filter**, and a **Fair Access Policy** tab.

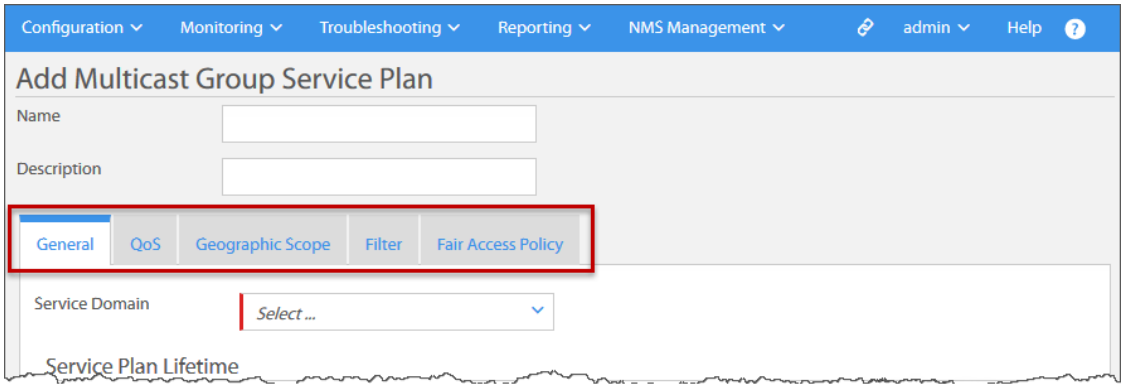

Figure 4-10. Add Multicast Group Service Plan Configuration Tabs

4.6.1 Add Multicast GSP — General Parameters

The **General** tab is for defining basic settings like the **Name** and **Description** of the Multicast GSP. It also includes sections for configuring the **Service Plan Lifetime**, a **Recurrence Pattern**, if applicable, and a section for other general **Information** including any specific allowances, limitations, or restrictions that may be imposed on the Multicast GSP.

This latter section supports configuration of items such as supported SVNs, allowed terminal types, maximum number of terminals, a maximum CIR/MIR per subscriber, maximum contention ratio, supported regions, and the option to allow or restrict terminal provisioning.

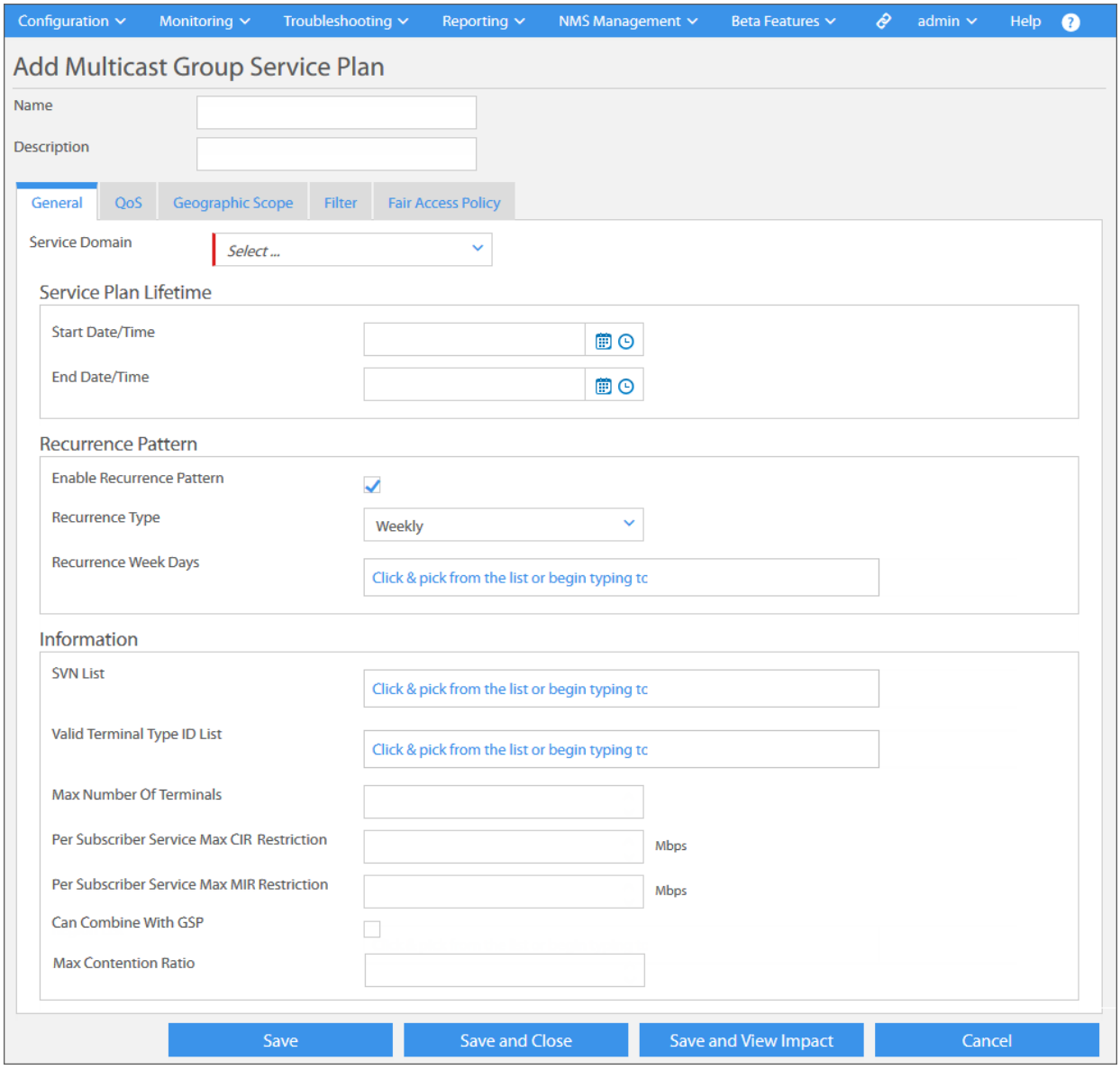

Figure 4-11. Multicast GSP — General Parameters

To create a multicast GSP:

1. Click the **Configuration tab > Service Domain** > **Add > More Options > Multicast Group Service Plan. The Add Multicast Group Service Plan** dialog opens.
2. On the **General** tab, enter a **Name** and **Description** of the new Multicast GSP.
3. Use the **Service Domain** drop-down to select the parent GQoS node for this MGSP.
4. Select a **Start Date/Time** and an **End Date/Time**, under the **Service Plan Lifetime** section, to define the valid duration for this MGSP.
5. Select **Enable Recurrence Pattern**, under the **Recurrence Pattern** section, to display fields for entering a service recurrence pattern for the GSP, if this is applicable.
6. Select a **Recurrence Type** of **Daily**, **Weekly**, or **Monthly,** if a recurrence is enabled, then from the list below, use the appropriate instructions based on the recurrence type:
   a. **Daily** — Specify a **Recurrence Start Time** and **Recurrence End Time**.
   b. **Weekly** — Use the **Recurrence Weekdays** multi-select box, to select the weekdays.
   c. **Monthly** — Use the **Recurrence Month Days** multi-select box, to select the days.
7. Use the **SVN List** multi-select list box to specify the SVNs (VLANs) for which traffic for this MGSP is supported.
8. Use the **Valid Terminal Type ID List** multi-select list box, to select one or more terminal types that supports this new MGSP.
9. Specify the **Maximum Number of Terminals** that the MGSP will support.
10. Enter the **Per Subscriber Service Max CIR Restriction** (not to be exceeded), to allocate to subscribers to this MGSP.
11. Enter the **Per Subscriber Service Max MIR Restriction** (not to be exceeded), to allocate to subscribers to this MGSP.
12. Choose from the **Region List** multi-select list box, the regions in which to allow traffic for this MGSP.
13. Select **Can Combine With GSP** if this MGSP may be combined with other GSPs.
14. Specify the **Maximum Contention Ratio** that the Multicast GSP will support. This value is calculated by dividing the aggregate CIR of all terminals in a group by the group CIR.
15. Click **Save and Close** to save the configuration to the NMS; or click **Save** to continue in the modify mode with *Add Multicast GSP — QoS Parameters*.

4.6.2 Add Multicast GSP — QoS Parameters

The quality of service (QoS) for the Multicast GSP is defined by parameters such as *committed information rate (CIR)*, *maximum information rate (MIR)*, QoS *priority* and *QoS cost*, *multicast MODCOD*, and *allocation fairness method*. These parameters, which determine the level of service, are configured for Outbound traffic only.

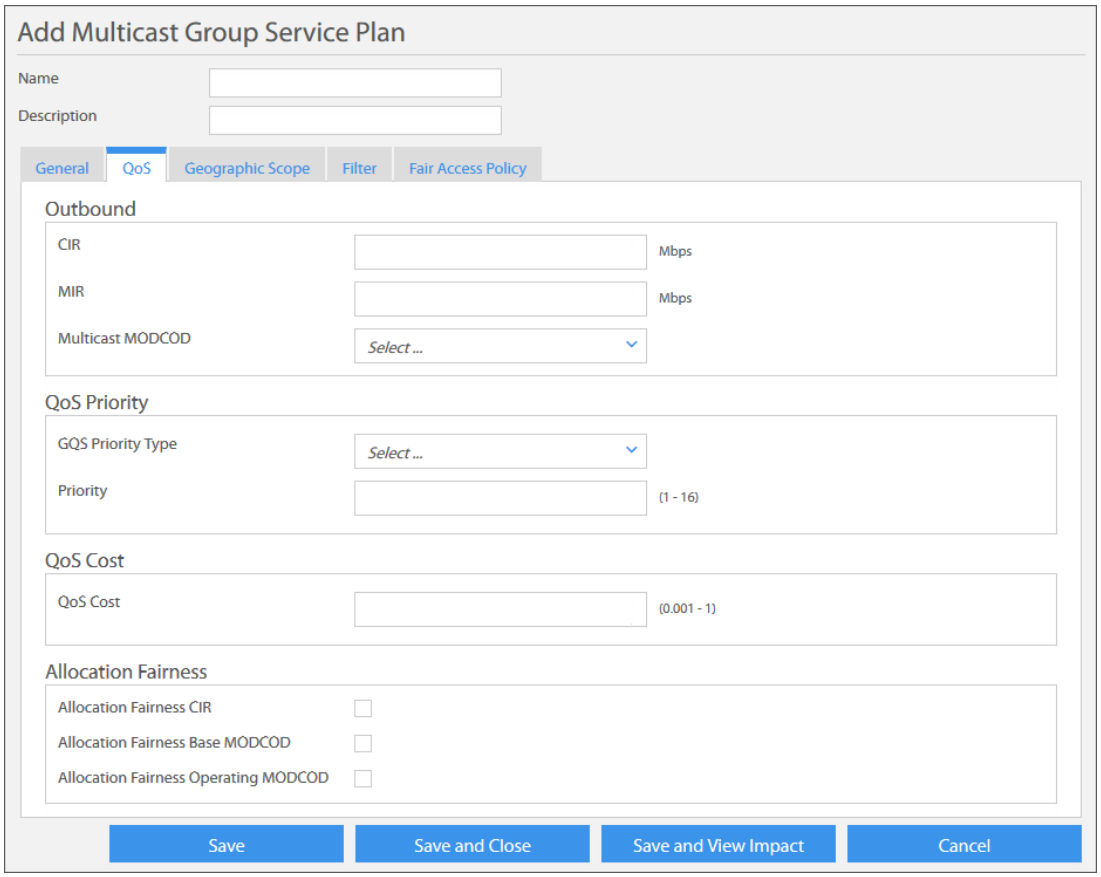

Figure 4-12. Multicast GSP — QoS Parameters

To define the Multicast GSP Quality of Service (QoS):

1. From the **Add MGSP** page, click the **QoS** tab.
2. Specify the **Outbound** traffic **CIR** and **MIR**, in megabits per second (Mbps).
3. Use the drop-down to select the appropriate **Multicast MODCOD**.
4. Under **QoS Priority**, select the **GQoS Priority Type** as **Absolute** or **Pre-Allocation Round**.
5. Select the **QoS Priority** for this Multicast GSP (1 = highest; 16 = lowest).
6. Under **QoS Cost**, specify a **QoS Cost** for the MGSP, as a value between 0.001 and 1.
7. Select the desired **Allocation Fairness** method for applications under this MGSP.
8. Click **Save and Close** to save the configuration to the NMS; or click **Save** to continue in the modify mode with *Add Multicast GSP — Geographic Scope*.

4.6.3 Add Multicast GSP — Geographic Scope

The geographic **Scope Type** for the MGSP may be specified as either global or regional. Global scope is composed of all satellites and beams. When regional is selected as the **Scope Type**, one or more pre-defined regions may be specified. This configuration allows for the Multicast GSP to be restricted to a collection of beams or service areas.

Before geographic regions may be specified as part of the geographic coverage of the Multicast GSP, the regions must have already been defined in the NMS.

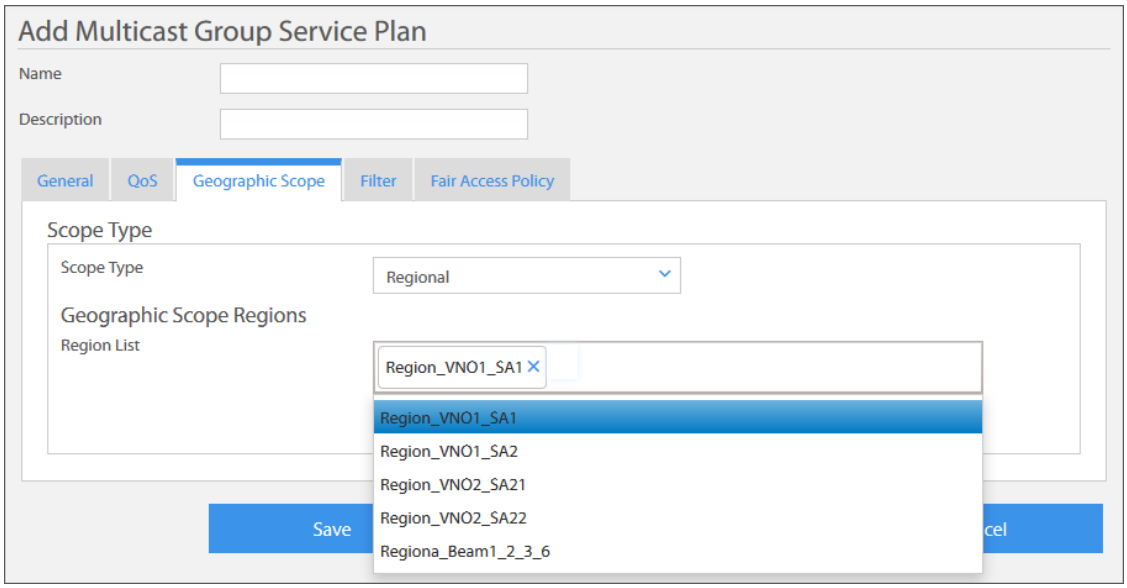

Figure 4-13. Multicast GSP — Geographic Scope Tab

To add regional geographic scope to a Multicast GSP:

1. From the **Add MGSP** page, click the **Geographic Scope** tab.
2. Use the **Scope Type** drop-down to select **Regional** to define the regional coverage.
3. Use the **Region List** multi-select list box to select the regions required as part of the regional geoscope for the MGSP.
4. Click **Save and Close** to save the MGSP configuration; or click **Save** to continue in the **Modify** mode with *Configuring Traffic Filter Parameters*, if applicable.

4.7 Creating Subscriber Service Plan Profiles

A *Subscriber Service Plan Profile (SSPP)* is a set of service plan parameters configured for use in creating a Terminal Service Plan. When an SSPP is selected as part of a Terminal Service Plan (TSP), an instance of the SSPP is created in the NMS. That instance of the SSPP is called a *Subscriber Service Plan Component (SSPC).* A Terminal Service Plan configuration may consist of multiple SSPCs, where each component is an instance of either a Unicast or Multicast SSPP.

When a Terminal Service Plan is created, each component of the plan is linked to a specific GSP or MGSP, using a Service Group ID. This association identifies the subscriber plan as a QoS node that receives its bandwidth allocation from the identified GSP/MGSP. The components of an SSPP, which may include voice, data, or multicast data components, may be derived from the same or different GSPs/MGSPs, and may be provided by the same or different VNOs.

The creation of a Subscriber Service Plan Profiles (SSPP) is only supported in the NMS by authorized VNOs, under the **Service Domain** of the **Configuration** page. An SSPP, which is acquired by other VNOs or client dealers, is in turn used to define service plans to which individual Satellite Terminals or a group of Satellite Terminals may subscribe. Dealers may procure SSPPs from any number of VNOs, including the Network Service Provider.

Each SSPP uses configuration tabs for **General**, **Geographic Scope**, **QoS** (quality of service), **Application/Service**, **Filter**, and a **Fair Access Policy** (FAP) parameters.

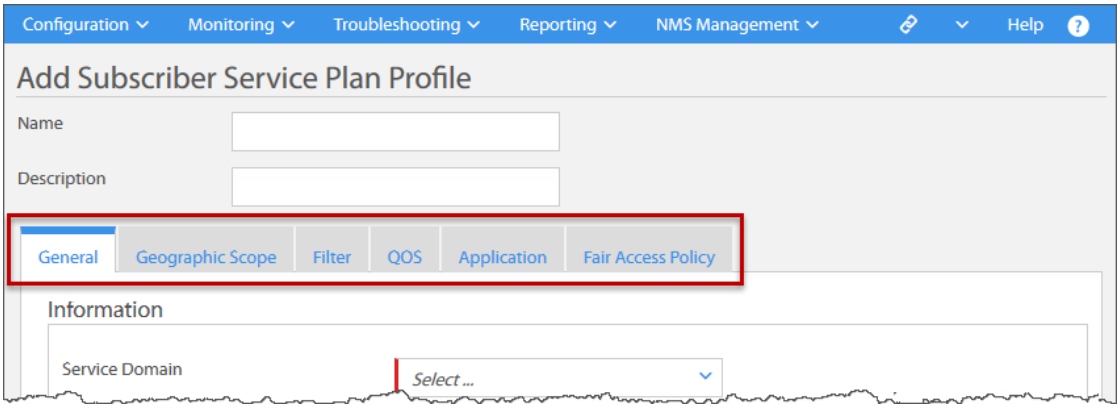

Figure 4-14. Add Subscriber Service Plan Profile Configuration Tabs

4.7.1 Add an SSPP — Configure General Parameters

In addition to specifying the **Name** for this SSPP, the SSPP **General** parameters configuration tab, requires that the following be specified:

- The Service Domain — the root domain to which the SSPP is associated
- **Valid Terminal Type ID List** — a list of supported terminal types
- **SVN List** — a list of SVNs for which the SSPP is supported
- **Parent GSP List** — a list of GSPs from which the SSPP may be allocated bandwidth

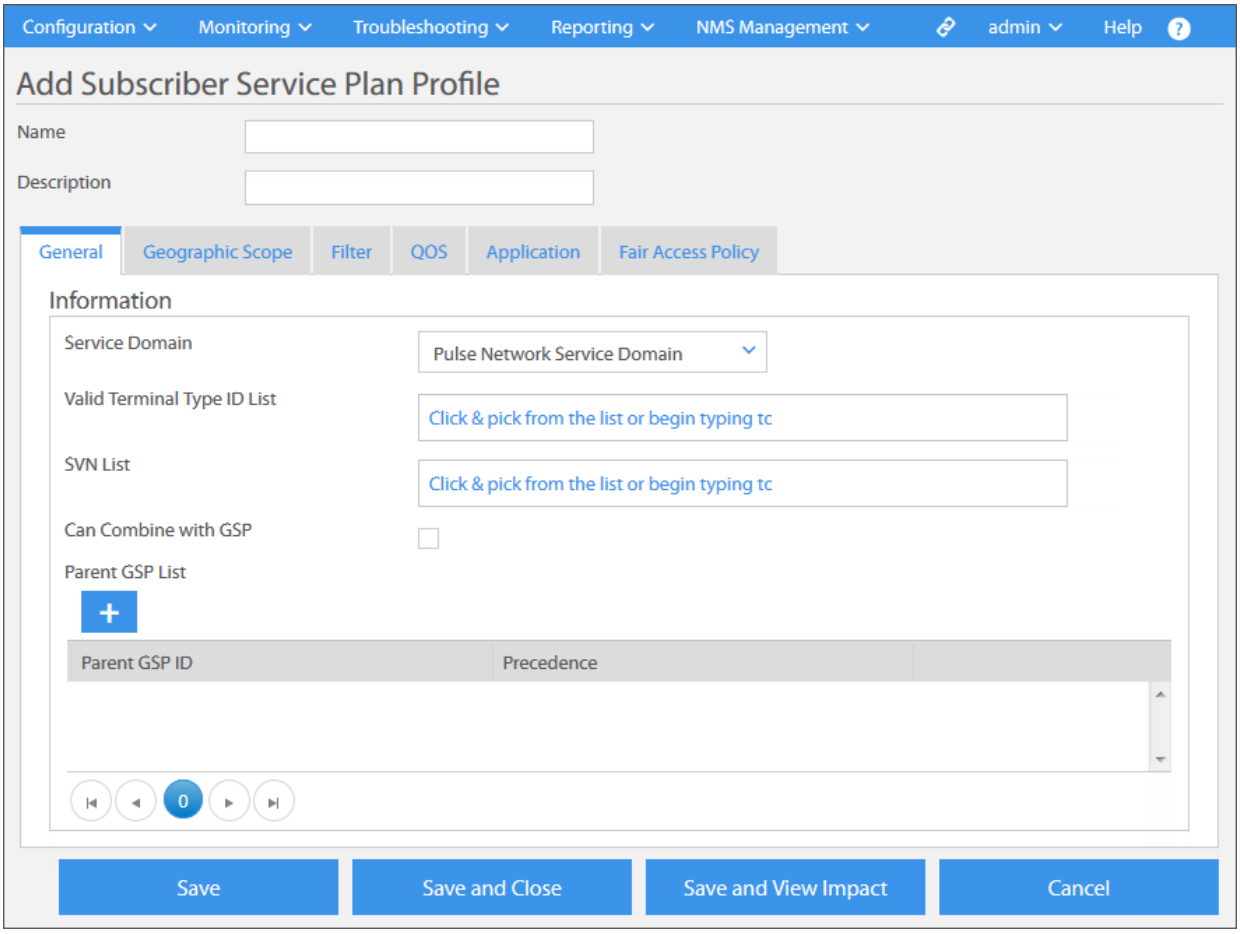

Figure 4-15. Add SSPP — General Parameters

To add a subscriber service plan profile:

1. Click the **Configuration** tab > **Service Domain** > **Add > Subscriber Service Plan Profile.**
2. Enter a **Name** and **Description** (for example "Video Plan").
3. Use the **Service Domain** drop-down to select the root node to which this SSPP is associated. This field must be entered.
4. Use the **Valid Terminal Type ID List** multi-select box, to the terminal types that are supported by this new SSPP.
5. Use the **SVN List** multi-select box, to pick the VLANs where this SSPP is supported.
6. Select **Can Combine With GSP** to allow this SSPP to be combined with one or more Group Service Plans in a given bandwidth pool or bundle.
7. Under **Parent GSP List**, click the **Add Record** button to specify the GSP records from which this SSPP will receive bandwidth. Repeat this step to insert additional records.
8. Click **Save and Close** to save the configuration to the NMS; or click **Save** to continue in the modify mode with *Add an SSPP — Global Geographic Scope*.

4.7.2 Add an SSPP — Global Geographic Scope

A global geographic scope is composed of all satellites and beams.

If both global and regional coverage are defined, the inbound/outbound CIR/MIR values are independent for each scope. As an example, a voice SSPP, which specifies a global CIR/MIR, may configure a different CIR/MIR for a high-demand service area. Also, SSPP traffic filtering rules may be defined to block certain traffic types in a specific region.

The following can be configured for the global SSPP geoscope:

- Global QoS upstream and downstream configuration
- QoS Per Recurrence Pattern

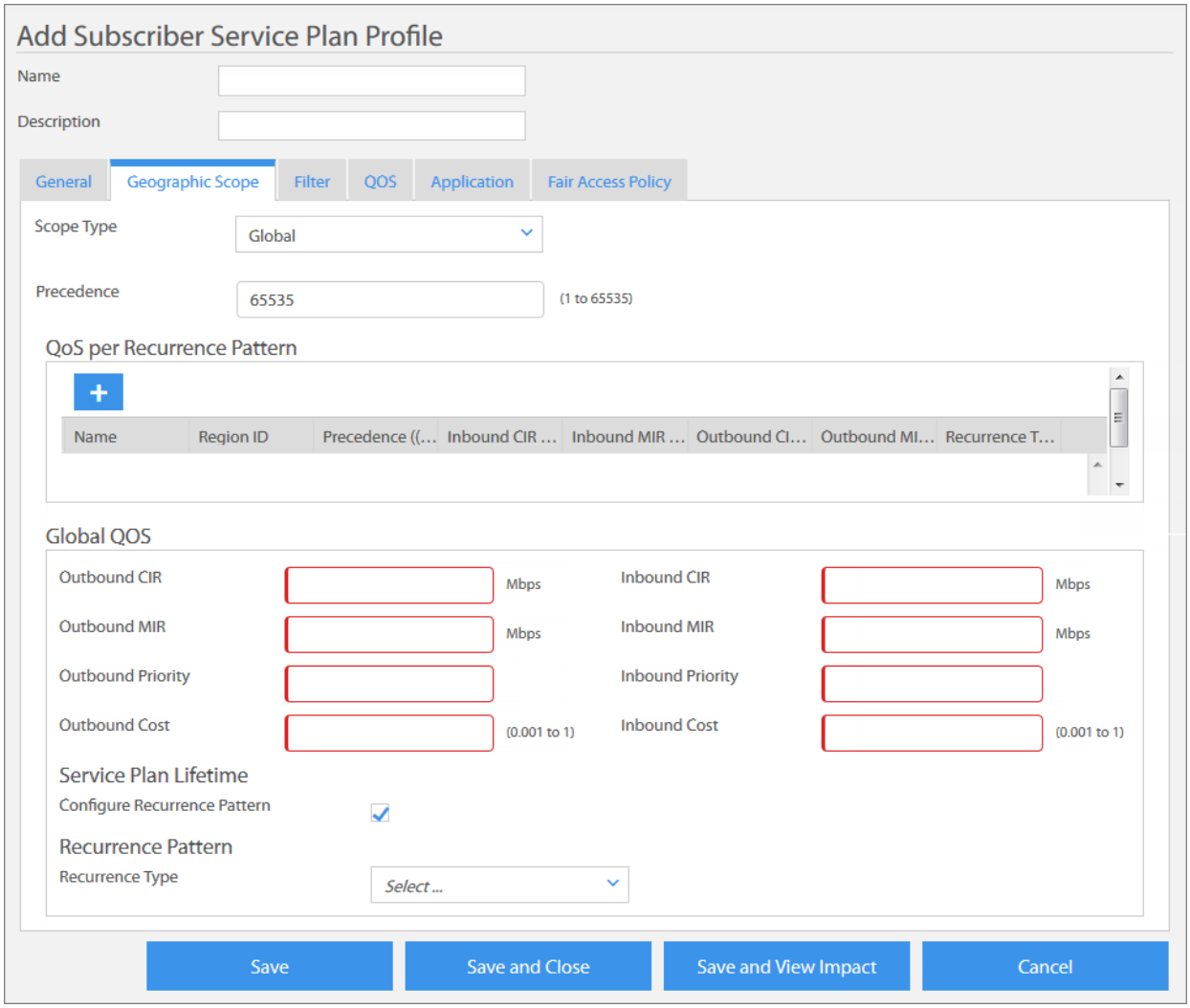

Figure 4-16. SSPP — Add Global Geographic Scope

To define a global geographic scope for the SSPP:

1. Click the **Geographic Scope** tab of the **Add Subscriber Service Plan Profile** dialog.

2. Use the **Scope Type** drop-down and select **Global**. The page is populated with the **Global QoS** dialog and a QoS Per Recurrence Pattern dialog for the global geographic scope.
3. Enter a **Precedence** value to this global scope.
4. Under the **Global QoS**, enter the following QoS parameters for the global scope:
   a. Specify an **Outbound CIR** and **Inbound CIR**, as a data rate in Mbps.
   b. Specify an **Outbound MIR** and **Inbound MIR**, as a data rate in Mbps.
   c. Specify an **Outbound Priority** and **Inbound Priority**.
   d. Specify an **Outbound Cost** and **Inbound Cost**.
5. If applicable, select **Configure Recurrence Pattern** to configure a Service Plan Lifetime.
6. If a recurrence pattern is enabled, select a **Recurrence Type** of **Daily**, **Weekly**, or **Monthly,** then use the appropriate instruction below, based on the recurrence type:
   a. **Daily** — Specify a **Recurrence Start Time** and **Recurrence End Time** for the SSPP.
   b. **Weekly** — Use the **Recurrence Weekdays** multi-select box to add the desired days.
   c. **Monthly** — Use the **Recurrence Month Days** multi-select box to add the desired days.
7. Click **Save and Close** to save the SSPP configuration to the NMS; or click **Save** to continue

To define a QoS Per Recurrence Pattern for the SSPP:

8. If applicable, under **QoS Per Recurrence Pattern**, click the **Add Record** icon to define one or more regional scope records.
9. Enter a **Name** for the region, and use the drop-down to select the **Region ID**; then enter the following QoS parameters for the regional scope record:
   a. Assign a **Precedence** to this SSPP region. If two configured regions have overlapping area, the region with the lowest precedence CIR/MIR will take effect.
   b. Specify an **Outbound CIR** and **Inbound CIR**, as a data rate in Mbps.
   c. Specify an **Outbound MIR** and **Inbound MIR**, as a data rate in Mbps.
   d. Specify an **Outbound Cost** and **Inbound Cost**.
   e. Specify an **Outbound Priority** and **Inbound Priority**.
10. Under **Recurrence Pattern**, select a **Recurrence Type** of **Daily**, **Weekly**, or **Monthly,** then from the list below, use the appropriate instructions based on the recurrence type:
    a. **Daily** — Enter a **Recurrence Start Time** and **Recurrence End Time** for the SSPP.
    b. **Weekly** — Use the **Recurrence Weekdays** multi-select box to add the desired days.
    c. **Monthly** — Use the **Recurrence Month Days** multi-select box to add the desired days.
11. Click **Save** to save the Geoscope QoS configuration and the new region record.
12. Click **Save and Close** to save the SSPP configuration to the NMS; or click **Save** to continue in the modify mode with *Add an SSPP — Configure QoS Parameters*.

4.7.3 Add an SSPP — Regional Geographic Scope

Whereas global geographic scope is composed of all satellites and beams, regional scope is defined by adding one or more defined regions to the configuration. The SSPP geoscope can be added either by a Service Provider or a VNO.

The following can be configured for the regional SSPP geoscope:

- QoS Per Recurrence Pattern

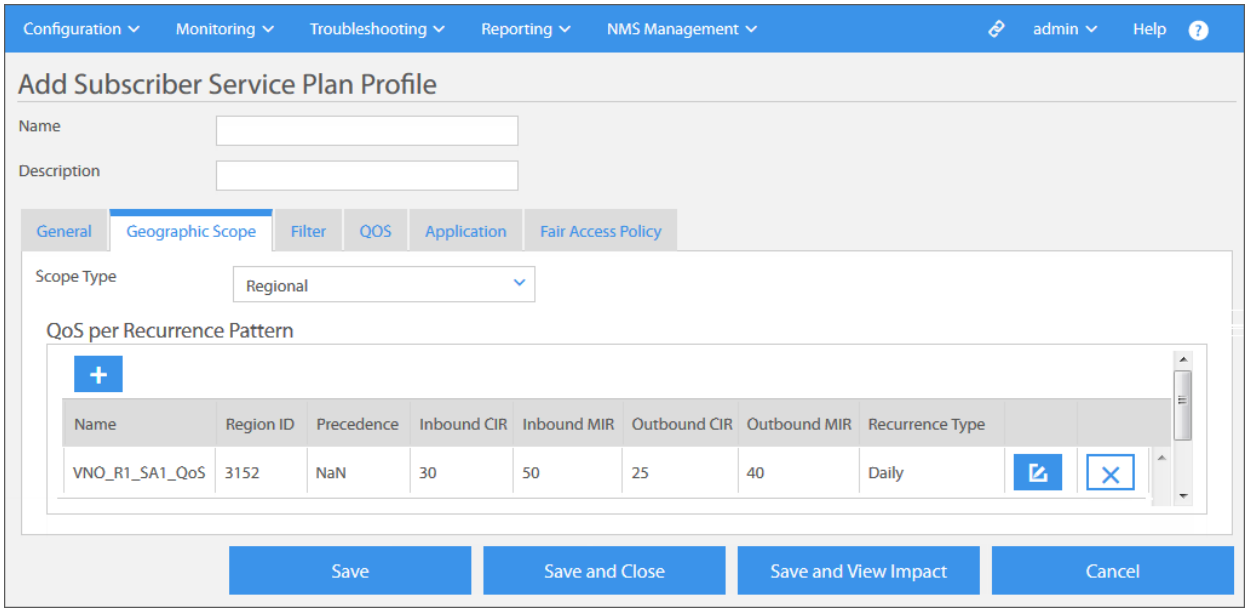

Figure 4-17. SSPP — Add Regional Geographic Scope

NOTE: The regional coverage may consist of both Service Areas and beams.

To define an SSPP regional scope and QoS per Recurrence Patterns:

1. Click the **Geographic Scope** tab of the **Add Subscriber Service Plan Profile** dialog.
2. Use the **Scope Type** drop-down and select **Regional**.
3. Under **QoS Per Recurrence Pattern**, click the **Add Record** icon to define one or more regional scope records. The region **GeoScope QoS** dialog opens.
4. Enter a **Name** for the region, and use the drop-down to select the **Region ID**; then enter the following QoS parameters for the regional scope record:
   a. Assign a **Precedence** to this SSPP region. If two configured regions have overlapping area, the region with the lowest precedence CIR/MIR will take effect.
   b. Specify an **Outbound CIR** and **Inbound CIR**, as a data rate in Mbps.
   c. Specify an **Outbound MIR** and **Inbound MIR**, as a data rate in Mbps.

d. Specify an **Outbound Cost** and **Inbound Cost**.

e. Specify an **Outbound Priority** and **Inbound Priority**.

5. Under **Recurrence Pattern**, select a **Recurrence Type** of **Daily**, **Weekly**, or **Monthly,** then from the list below, use the appropriate instructions based on the recurrence type:

a. Daily — Enter a **Recurrence Start Time** and **Recurrence End Time** for the SSPP.

b. Weekly — Use the **Recurrence Weekdays** multi-select box to add the desired days.

c. Monthly — Use the **Recurrence Month Days** multi-select box to add the desired days.

6. Click **Save** to save the Geoscope QoS configuration and the new region record.

7. Click **Save and Close** to save the SSPP configuration to the NMS; or click **Save** to continue in the modify mode with *Add an SSPP — Configure QoS Parameters*.

4.7.4 Add an SSPP — Configure QoS Parameters

The following parameters are specified when defining the SSPP QoS (quality of service):

- Outbound (Downstream) Base MODCOD
- Inbound (Upstream) Fairness Base Bit Rate (Kbps)
- Inbound and Outbound CIR Fulfillment Evaluation Time

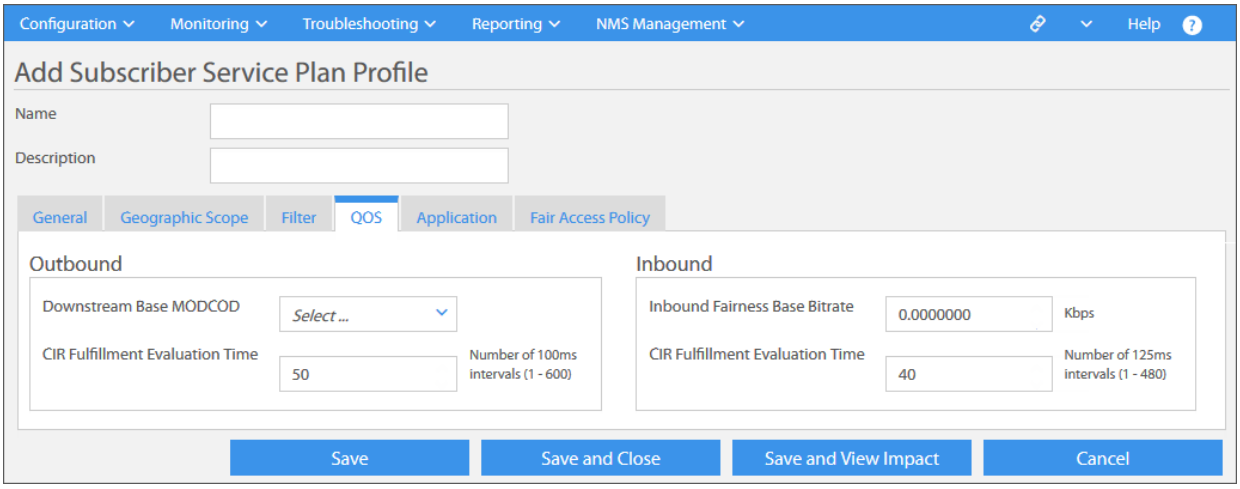

Figure 4-18. Add SSPP — QoS Parameters

To define the SSPP Quality of Service (QoS):

1. From the **Add Subscriber Service Plan Profile** page, click the **QoS** tab.
2. Use the drop-down to select the **Downstream Base MODCOD** for this SSPP**.**
3. Enter the **Outbound CIR Fulfillment Evaluation Time**.
4. Select the **Outbound Priority** from 1 to 16 (1 = highest; 16 = lowest).
5. Specify the **Outbound Cost** as a value between 0 and 1.
6. Enter the **Inbound Fairness Base Bitrate**.
7. Select the **Inbound Priority** from 1 to 16 (1 = highest; 16 = lowest).
8. Specify the **Inbound Cost** as a value between 0 and 1.
9. Click **Save and Close** to save the SSPP configuration to the NMS; or click **Save** to continue in the modify mode.

4.8 Creating Multicast Subscriber Service Plan Profiles

Like the unicast SSPP, the *Multicast Subscriber Service Plan Profile (MSSPP)* is defined by authorized VNOs and used in creating a subscriber service plan - particularly, a multicast component of a service plan, to which individual terminals or a group of terminals may subscribe. Each MSSPP, when created, is linked to a specific Multicast Group Service Plan.

When an MSSPP is selected as part of a Terminal Service Plan, an instance of the MSSPP is created in the NMS. The terminal service plan configuration may consist of multiple components, where each component is an instance of a Unicast SSPP or Multicast SSPP. For the subscriber, the multicast component of its service plan is a subscription to multicast audio or video channels, or perhaps to a file distribution service.

When configuring the geographic scope of a Multicast Subscriber Service Plan Profile the scope type may be specified as global or regional coverage.

The Add MSSPP page is accessed from the **Service Domain** menu of the **Configuration** page. The Multicast SSPP is configured using tabs for **General**, **Geographic Scope**, **Filter**, and **Fair Access Policy** parameters.

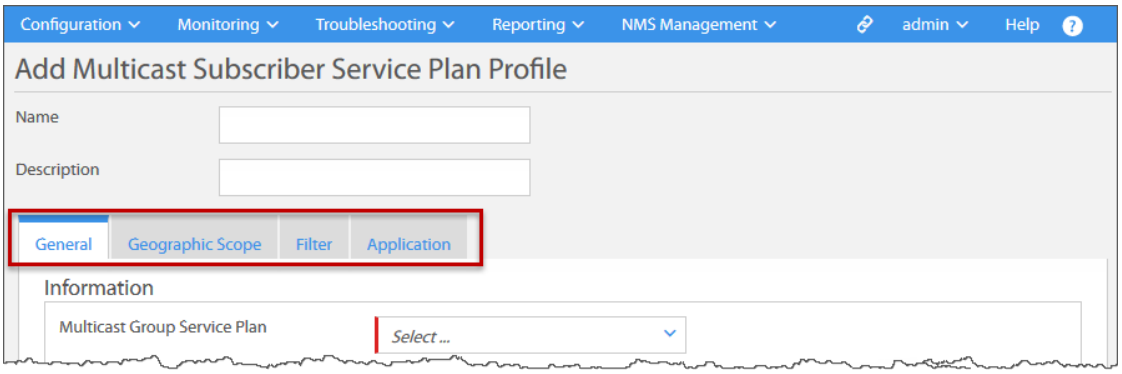

Figure 4-19. Add Multicast Subscriber Service Plan Profile Configuration Tabs

4.8.1 Add Multicast SSPP — Configure General Parameters

The **General** parameters tab of the Multicast SSPP configuration page, defines the Multicast SSPP **Name** and **Description**; the **Multicast GSP** bandwidth pool to which the Multicast SSPP is associated; **Valid Terminal Types**; and a **Blocked RA list**. The following QoS parameters are also specified for the Multicast SSPP downstream QoS configuration:

- Committed Information Rate (CIR) in Mbps/Maximum Information Rate (MIR) in Mbps
- Multicast MODCOD/QoS Priority/Downstream QoS Cost

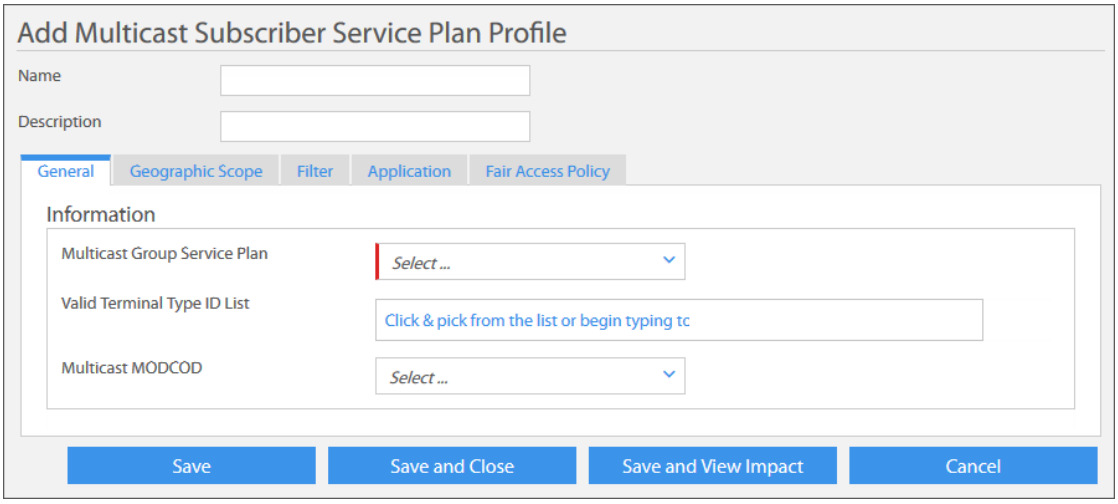

Figure 4-20. Multicast SSPP — General Parameters Dialog

To add a multicast subscriber service plan profile:

1. Click the **Configuration** tab **> Service Domain** > **Add > More Options > Multicast Subscriber Service Plan Profile.**
2. Enter a **Name** and **Description** of the new Multicast SSPP on the **General** tab.
3. Use the **Multicast Group Service Plan** drop-down to select the parent Multicast GSP, from which this Multicast SSPP is allocated bandwidth.
4. Use the **Valid Terminal Type ID List** multi-select box to pick the terminal types that supports this new Multicast SSPP.
5. Use the **Multicast MODCOD** drop-down to select the modulation and coding value to use with this Multicast SSPP.
6. Click **Save and Close** to save the Multicast SSPP configuration to the NMS; or click **Save** to continue in the modify mode.

4.8.2 Add Multicast SSPP — Global Geographic Scope

A global geographic scope is composed of all satellites and beams.

If both global and regional coverage are defined, the inbound/outbound CIR/MIR values are independent for each scope. As an example, a video MSSPP, which specifies a global CIR/MIR, may configure a different CIR/MIR for a high-demand service area. Also, MSSPP traffic filtering rules may be defined to block certain traffic types in specific regions.

The following can be configured for the global Multicast SSPP geoscope:

- Global QoS Parameters

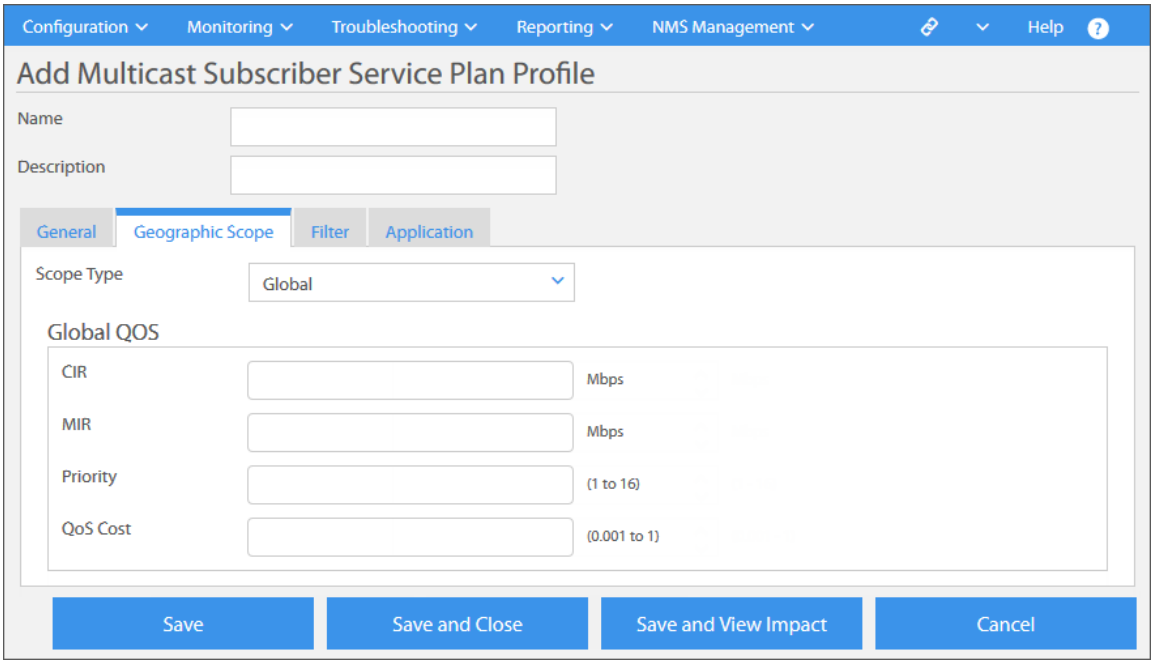

Figure 4-21. SSPP — Add Global Geographic Scope

To define a global geographic scope for the multicast SSPP:

1. Click the **Geographic Scope** tab of the **Add Multicast Subscriber Service Plan Profile** dialog.
2. Use the **Scope Type** drop-down and select **Global**.
3. Enter the total **CIR**, as a data rate in Mbps, for the multicast SSPP.
4. Enter the total **MIR**, as a data rate in Mbps, for the multicast SSPP.
5. Enter the QoS **Priority** and **Qos Cost** for the multicast SSPP.
6. Click **Save and Close** or **Save** to save the configuration to the NMS; or click **Save** to continue in the modify mode.

4.8.3 Add Multicast SSPP — Regional Geographic Scope

Whereas global geographic scope is composed of all satellites and beams, regional scope is defined by adding one or more defined regions to the configuration.

The multicast SSPP geoscope can be added by either a Network Operator or a Service Provider. The regional configuration involves specifying the QoS parameters for one or more regions.

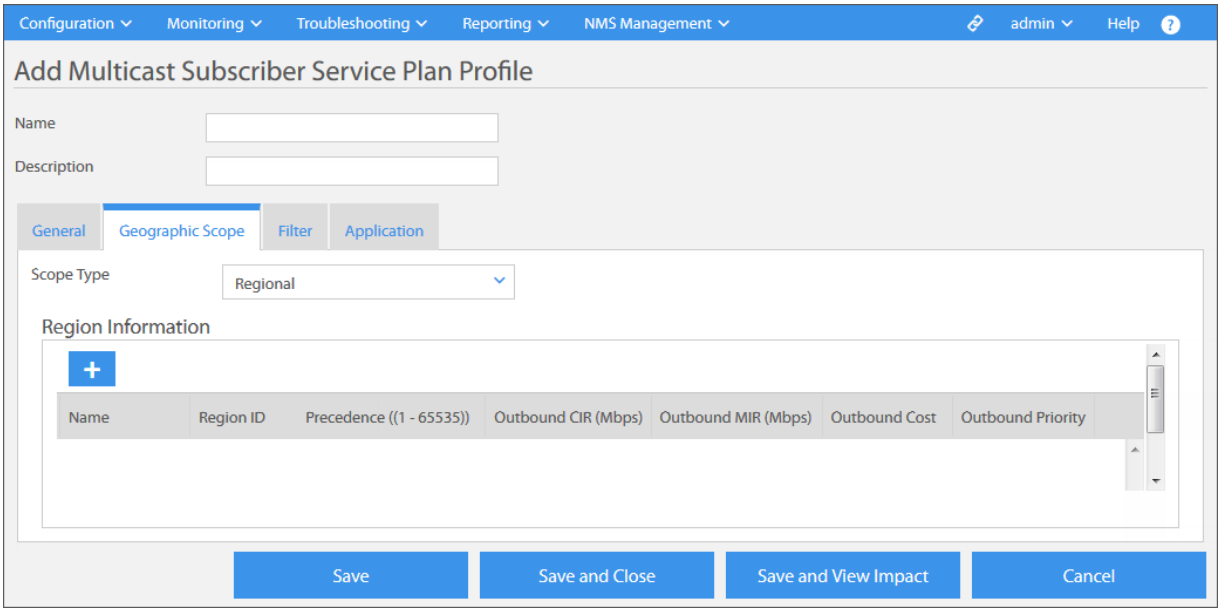

Figure 4-22. Multicast SSPP — Add Regional Geographic Scope

NOTE: The regional coverage may consist of both Service Areas and beams.

To define a regional geographic scope for the Multicast SSPP:

1. Click the **Geographic Scope** tab of the **Add Multicast Subscriber Service Plan Profile** dialog.
2. Use the **Scope Type** drop-down and select **Regional**.
3. Under **Region Information**, click the **Add Record** icon to define one or more regional scope records. The **Region Information** dialog opens.
4. Enter a **Name** for the region, and use the drop-down to select the **Region ID**; then enter the following parameters for each regional scope record:
   a. Assign a **Precedence** to this SSPP region. If two configured regions have overlapping area, the region with the lowest precedence CIR/MIR will take effect.
   b. Specify an **Outbound CIR** and an **Outbound MIR** and **Inbound MIR**, as the data rate.

c. Specify an **Outbound Cost** and an **Outbound Priority**.

5. Click **Save** to save the Geoscope QoS configuration and the new region record.
6. To specify additional regional records for the MSSPP, repeat the procedure from Step 3. Multiple regions may be added to the MSSPP Geoscope.
7. Click **Save and Close** to save the Multicast SSPP configuration to the NMS; or click **Save** to continue in the modify mode.

NOTE: All regions use the same **Outbound CIR**, **MIR**, **Cost** and **Priority**. Changing any existing values for these parameters will apply to existing regions upon saving.

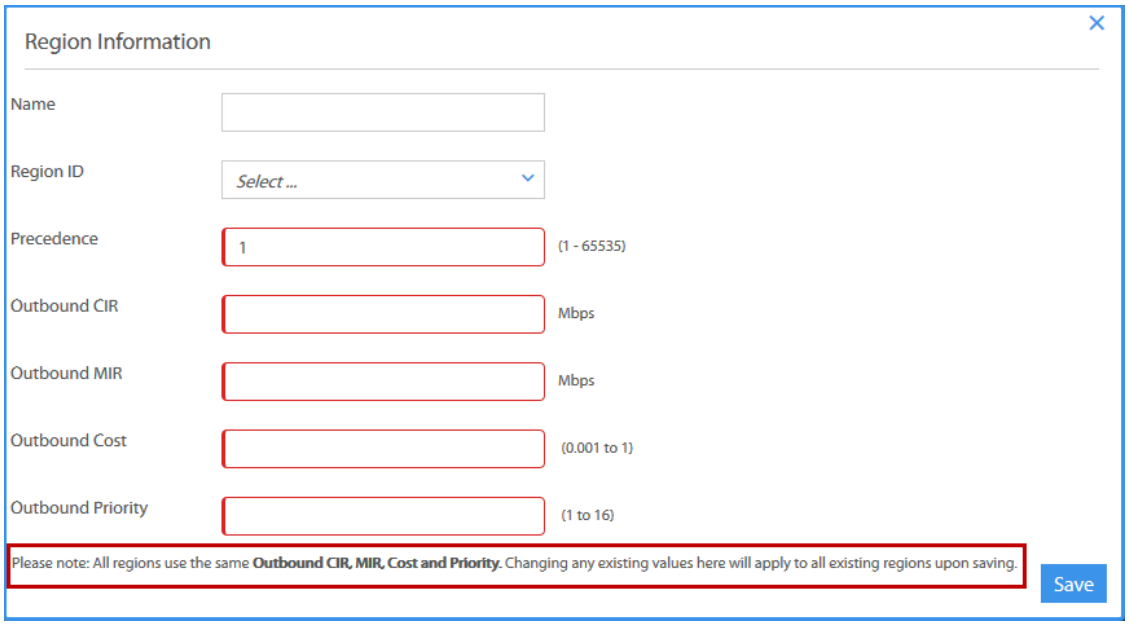

Figure 4-23. Multicast SSPP - Region Information Dialog

4.9 Configuring Application Service Levels

An *application service level* defines a set of QoS properties and classification rules for a given application.

The Service Level (SL) configuration dialog is accessed from the **Application** tab of either the **Subscriber Service Plan Profile** page or the **Multicast SSPP page.** From the Application that constab, one or more Service Levels can be configured, where each SL can specify one or more Classification Rules. Each SL has a unique name, is configured with specific QoS properties and a set of rules that determines how packets are filtered and prioritized.

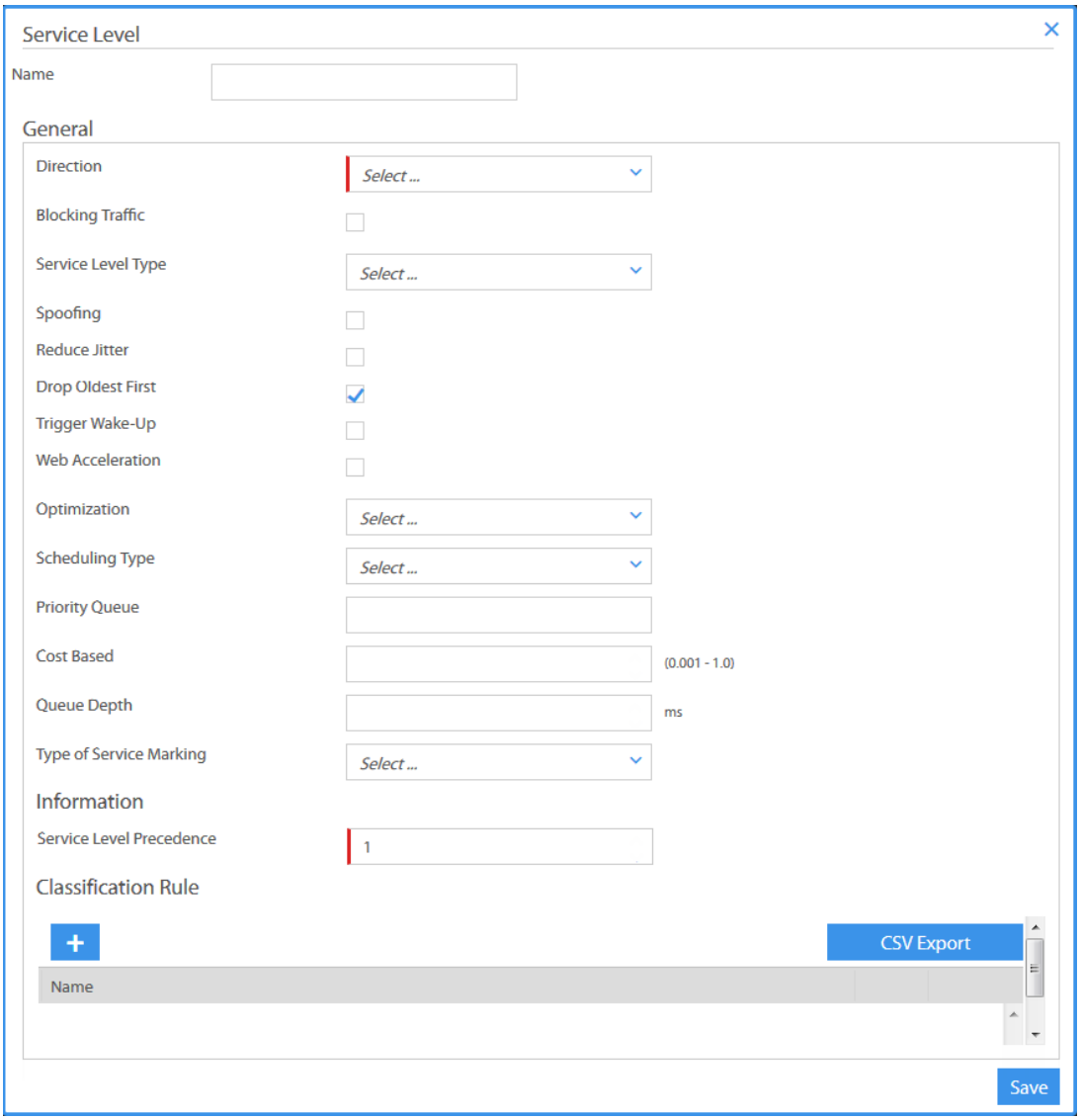

Figure 4-24. Add SSPP — Application/Service Level Dialog

To add an Application/Service Level:

1. Click the **Application** tab from the **Add Subscriber Service Plan Profile** page, or from the **Add Multicast Subscriber Service Plan Profile** page.
2. Click the **Add Record** record icon, to define a new service level. The **Service Level** dialog is opened. The dialog consists of a tab for **General** parameters, which also includes a **Classification Rule** section that supports definition of multiple traffic rules.
3. Enter a **Name** for the new Service Level that is being added to the **Application** profile.
4. Select the **Direction** as **Inbound** or **Outbound** to indicate whether the service level will apply to inbound or outbound traffic.
5. Select **Blocking Traffic** if a specific type of traffic should be blocked.
6. Select the **Service Level Type** as **Reliable** or **Unreliable**. Use **Reliable**, if the Service Level is to match TCP traffic; select **Unreliable** for all other traffic — for example, UDP traffic.
7. Select **Spoofing** to enable TCP Acceleration between the hub and Satellite Terminals. This selection does not apply to **Unreliable** traffic.
8. Select **Reduce Jitter** for VoIP applications. By default, TDMA slots used by an application are grouped together in the transmission frame. The system attempts to distribute slots evenly over the frame when this option is enabled. Do not enable for non-jitter applications.
9. Select or un-select **Drop Oldest First**.
10. Select **Trigger Wakeup** to cause terminals to automatically exit Sleep Mode in order to transmit incoming LAN packets on the upstream carrier when packets match the Service Level definition. **Trigger Wakeup** applies only to upstream profiles, and affects only terminals that have Sleep Mode enabled.
11. Select or clear **Web Acceleration** to enable or to disable Web acceleration.
12. Use the **Optimization** drop-down to select an option for determining how matching traffic for this Service Level should be optimized:
    a. Select **Maximum Efficiency** to allocate bandwidth as efficiently as possible.
    b. Select **Minimum Latency** to not hold partially filled TDMA bursts, but instead release them immediately. This option should only be specified where required.
13. Select the **Scheduling Type** as based on **Best Effort**, **Cost Based**, or **Priority Queue**. An appropriate **Cost Based** value or **Priority Queue** value must be entered if one of these scheduling types is selected.
14. Enter a **Queue Depth** value in milliseconds.
15. Choose the **Type of Service Marking** as **None**, **DSCP**, or **Max DSCP Value**.
16. Click **Save and Close** or **Save** to save the Application Service level configuration to the NMS; or click **Save** to continue in the modify mode with *Configuring Service Level Classification Rules*.

4.9.1 Configuring Service Level Classification Rules

Classification rules determine how packets are filtered and prioritized. Each Service Level can have multiple *rules*, each of which is composed of matching criteria designed to handle a specific type of traffic. The criteria of each rule is compared, in order, to each IP packet until a match is found. Once a packet matches a Rule, no further comparisons are made.

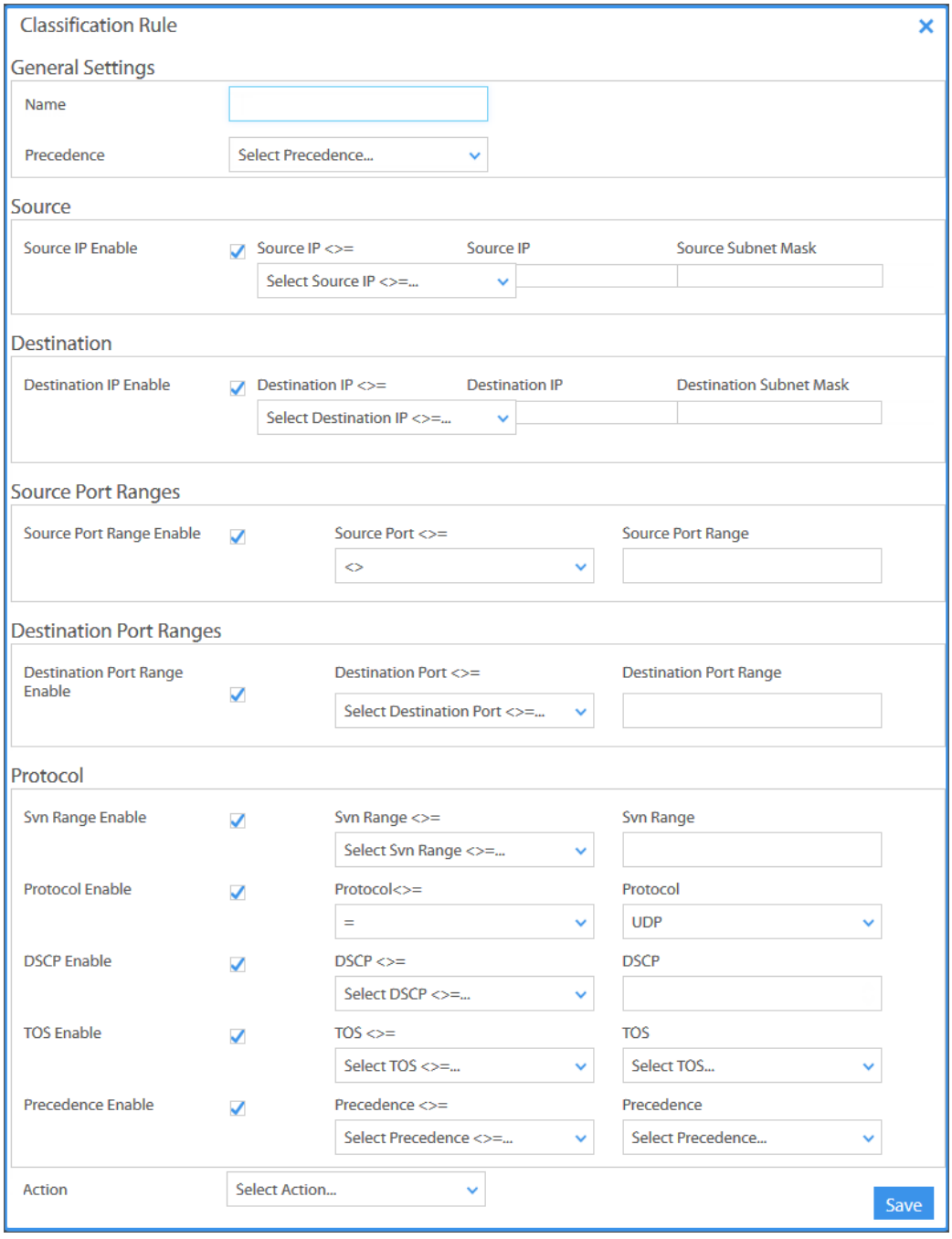

Figure 4-25. Add Service Level Classification Rule Dialog

To add Classification Rules to a Service Level:

1. Click the **Add Record** button, under the **Classification Rule** section of the **Service Level** dialog, to insert a new Classification Rule to the service level. The **Classification Rule** dialog opens.
2. Under **General Settings**, type a **Name** of the new filter rule; and use the **Direction** drop-down and select **Inbound** (Upstream) or **Outbound** (Downstream) as the traffic direction that the new traffic rule will affect.
3. Selectively enable the check boxes for **Source IP Enable**, **Destination IP Enable**, **Source Port Range Enable**, and **Destination Port Range Enable**, as required, to construct the compare clauses for IP source/destination addresses and port ranges; then, complete each clause as follows:
   a. Use the associated drop-down to select *equal to* (=) or *not equal to* (<>) as the compare operator.
   b. Specify a value to complete each compare clause.
4. Selectively enable the check boxes for **Protocol Enable**, **DSCP Enable**, **TOS Enable**, **SVN Range Enable**, and **Precedence Enable,** as required, to construct the compare clauses for the IP Protocol parameters; then complete the clause as follows:
   a. Use the associated drop-down to select *equal to* (=) or *not equal to* (<>) as the compare operator.
   b. Specify a value to complete each compare clause.
5. Finally, select the **Action** drop-down to select an action to perform based on a TRUE outcome of the enabled compare clauses. The options are to **Deny** the packet, or to **Allow** the packet, which is the default action and is indicated by a blank or no entry.
6. Click **Save** to update the classification rule to the Service Level. The new rule is inserted as a new record, listed by Name, under the **Classification Rule** section.
7. Repeat this procedure to insert another classification rule record for the Service Level.
8. For a given **Classification Rule** record, click the **Edit** icon to modify the record; and click the **Delete** icon to remove the selected Rule.
9. Click **Save** to save the Service Level configuration and return to the Application tab. The service level is inserted as a new record, listed by Name, under the **Service Level and Classification Rules** section of the **Application** tab.
10. Repeat this procedure to insert another Service Level record for the service plan.
11. Click **Save** to save the configuration to the NMS and continue in the **Modify** mode, or click **Save and Close** to save and open the **Browse Service Domain** window.

4.10 Configuring Traffic Filter Parameters

Traffic filters are created to classify and manage packets presented on the Upstream or Downstream. Each filter contains one or more f*ilter rules, each of which* is configured with one or more logical compare clauses. Each clause compares a specific IP header field with a user specified value. IP header filtering options include source/destination IP address and port number ranges, protocol, SVN IP Address Range, as well as other IP header fields.

As each packet is presented, configured rules are each checked in sequential order, as each of rule clauses are applied. Each rule comparison must match the user-specified value for the rule to match and for the packet to be classified. A packet is classified according to the first rule that matches, and must match at least one rule to be further classified. All configured rules are applied to each packet before any other QoS processing is performed.

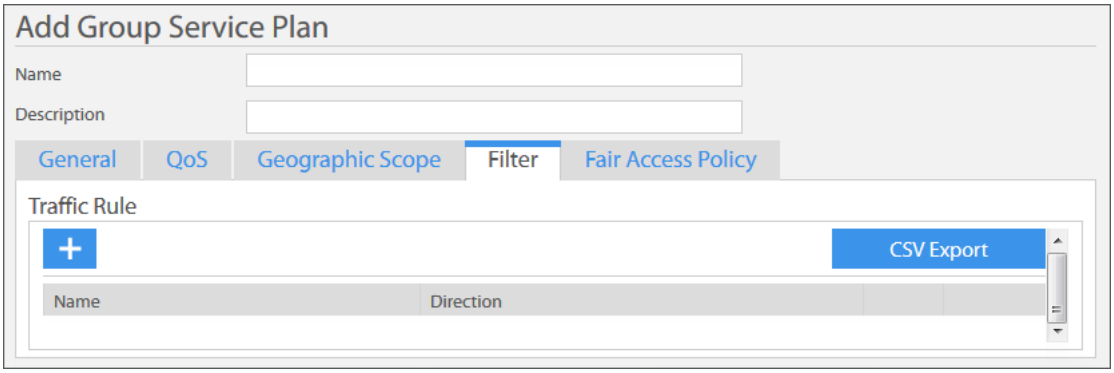

Figure 4-26. Add Group Service Plan — Filter Tab

To configure a QoS Filter traffic rules, perform the following steps:

1. From the **Filter** tab of the **Add Group Service Plan** or **Add Multicast GSP** dialog, click the Add Record button, to open the **Traffic Rule** dialog.
2. Under **General Settings**, type a **Name** of the new filter rule; and select the **Direction** as **Inbound** (Upstream) or **Outbound** (Downstream) to indicate the traffic direction that the new traffic rule will affect.
3. Selectively enable the check boxes for **Source IP Enable**, **Destination IP Enable**, **Source Port Range Enable**, and **Destination Port Range Enable**, as required, to construct the rule compare clauses for IP source/destination addresses and port ranges; then, complete each clause as follows:
   a. Use the drop-down to select *equal to* (=) or *not equal to* (<>) as the operator.
   b. Specify a value to complete each compare clause.
4. Under the **Protocol** section, selectively enable check boxes **SVN Range Enable**, **Protocol Enable**, **DSCP Enable**, **TOS Enable**, and **Precedence Enable,** as required, to construct the compare clauses for the IP Protocol parameters; then complete the clause as follows:
   a. Use the drop-down to select *equal to* (=) or *not equal to* (<>) as the operator.
   b. Specify a value or range, as needed, to complete each compare clause.

5. Select the **Action** drop-down to select an action to perform based on a "True" outcome of the enabled compare clauses. The options are to **Deny** the packet, or to **Allow** the packet, which is the default action and is represented by a blank or no entry.
6. Click **Save** to update the rule and return to the **Filter** tab. The new rule is inserted into under the **Traffic Rule** section as a new record, listed by **Name**.
7. Repeat the above steps to insert additional traffic rule records.
8. For a given **Traffic Rule** record, click the **Edit** icon to modify the record; or click the **Delete** icon to remove the selected record.
9. Click **Save** to save the configuration to the NMS.

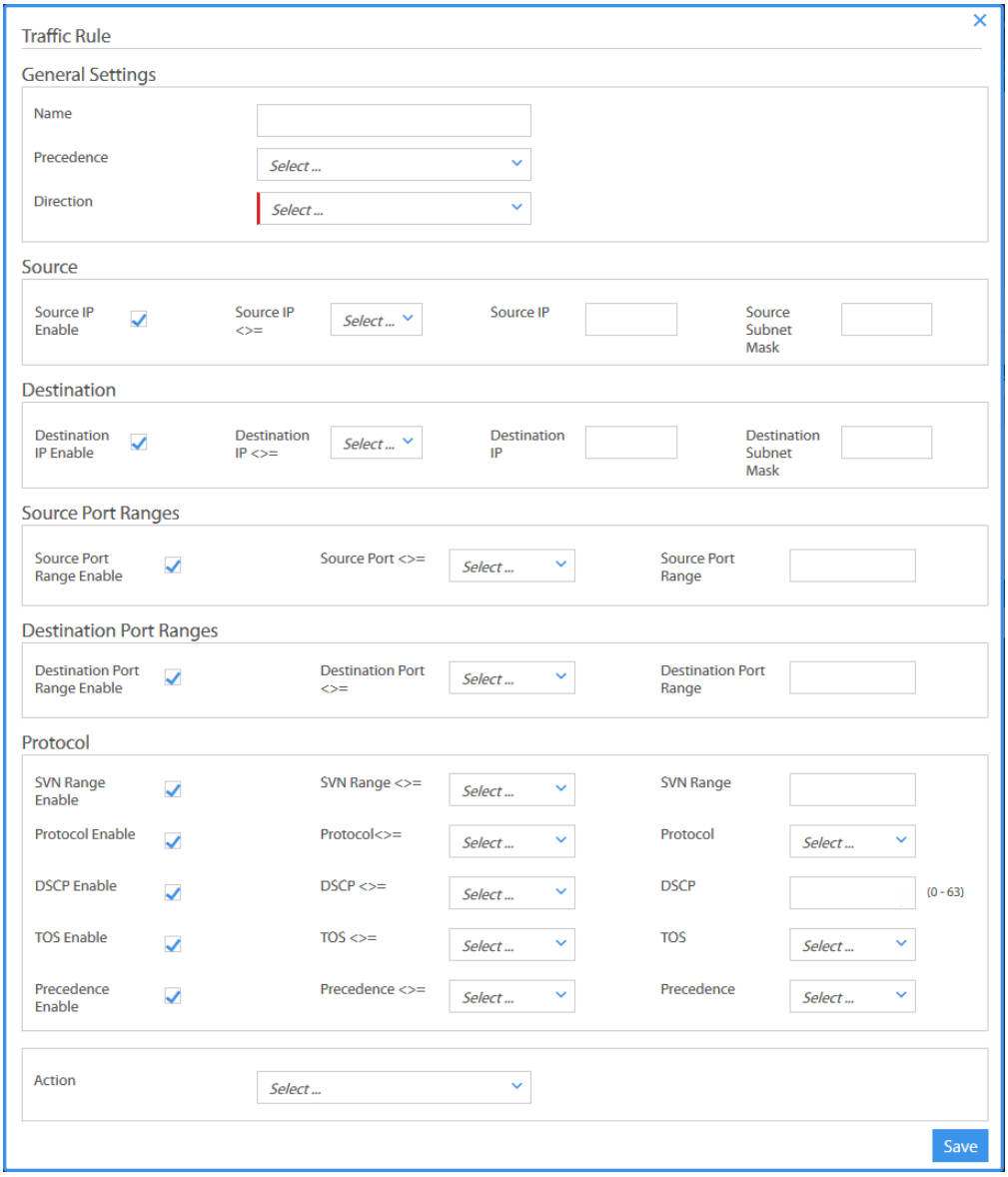

Figure 4-27. Add Filter Rules Dialog

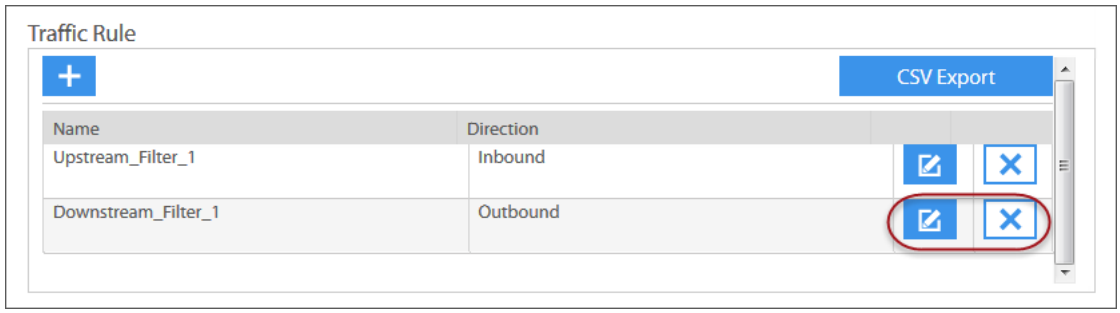

Figure 4-28. Filter Records

4.10.1 Filter Application Guidelines

- **Source/Destination IP** addresses may be specified with **Subnet Masks**. The subnet mask is first applied to the IP address in the packet, and then to the filter specified IP address. As such, **Source** and **Destination Ranges** of subnet masks may be made to match the rule.
- Each header field value, for example — IP address, IP Port Number, or Protocol) that is specified, is checked against the presented packet for *equal to* (=) or *not equal to* (<>).
- All specified comparisons, as indicated by the associated enable check box of each parameter, must match in order for the rule to match a packet that is presented.
- **SVN Range:** Specify compare equal to (=) or not equal to (<>) a specified value.
- **Protocol:** Select a Protocol that may be equal to (=) or not equal (<>) a specified value.
- **DSCP, TOS, Precedence:** If DiffServ **DSCP** is selected, then **TOS** or **Precedence** may not be selected. If **TOS** or **Precedence** is selected, then **DSCP** must not be selected.
- A traffic filter that is created or modified under a GSP or MGSP does not take effect until the changes are applied to the SSPCs associated with the GSP or MGSP.

4.11 Configuring a Fair Access Policy

A *Fair Access Policy (FAP)* is implemented to ensure fair usage of bandwidth and access to the network service by all subscribers. The FAP implementation governs the amount of data that is downloaded or uploaded within a specific period by a subscriber or group. If set limitations are exceeded, the CIR and MIR restrictions take effect during a "*Recovery Period*," in which service is still usable, although speeds may be reduced or some other penalty is applied.

4.11.1 Defining FAP Volume Allowance

The FAP controls the upstream/downstream *volume allowance*, in terms of Mbytes, over a specified period. A FAP may be configured separately for downstream and upstream traffic, or as an aggregate, which is a combined allowance for both upstream and downstream traffic. If the allowance is exceeded for the period, a per-megabyte overage charge may be assessed.

The policy may also be configured to use *throttling options,* which activate when the volume allowance is reached during the specified period; or to allow rollover of unused volume of the current period, for use by the next period. The *maximum rollover volume* can be defined as an absolute value or as a percentage of the total allowance. Rollover of unused volume can also be applied separately, for downstream and upstream, when separate volume allowances are specified; or combined when an aggregate allowance is specified.

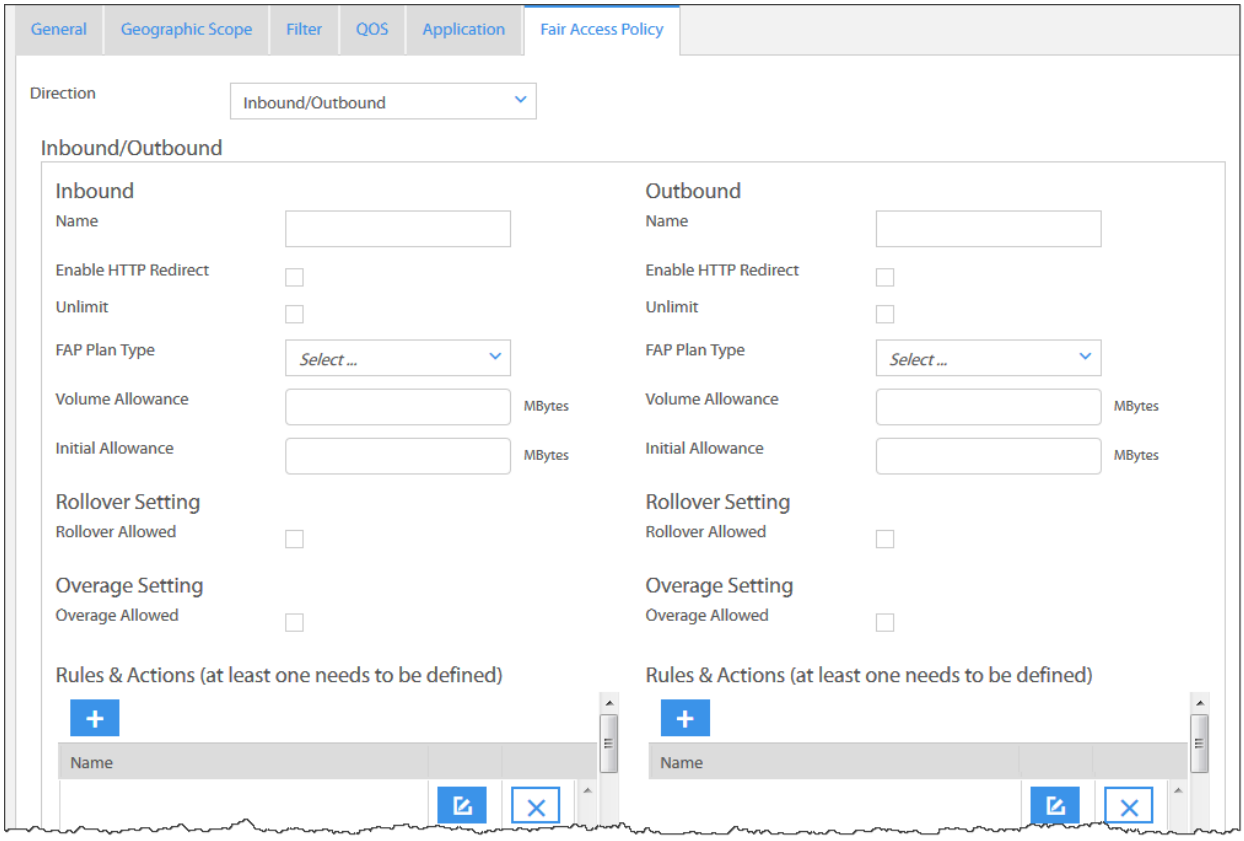

Figure 4-29. Fair Access Policy — Separate Inbound/Outbound Volume Allowances

The volume allowance dialog set for **Inbound FAP/Outbound FAP**, allows definition of a separate FAP for upstream and downstream traffic. Choosing **Aggregate Inbound & Outbound**, allows a combined inbound/outbound FAP to be configured.

When configuring the FAP for Multicast GSP or Multicast SSPP, only the downstream (outbound) configuration is applicable.

To configure FAP for separate Inbound/Outbound or aggregate Inbound/Outbound:

1. For the open GSP, Multicast GSP, SSPP, or Multicast SSPP, click the **Fair Access Policy** tab.
2. Use the **Direction** drop-down and choose **Aggregate** to specify a combined upstream/downstream allowance; or **Inbound/Outbound** to specify separate allowances.
3. Configure the following parameters for **Inbound** and **Outbound** or for the **Aggregate**.
4. Select **Enable HTTP Redirect**, to redirect requests to a destination URL address. The field **Http Redirect Address** is enabled for address entry.
5. Select **Overage Pre-Approval**, if approval is required in advance.
6. Enter the **Rolling Restoration** amount in megabytes.
7. Select the **Rolling Allowance Period Type** as **Daily**, **Weekly**, or **Monthly**.
8. Select the **Throttle Action Upon Top-Up** as **Add Top-Up to Quota** or **Throttle Until End of Regular Allowance**.
9. Select **Unlimit** to indicate an unlimited volume allowance for Inbound/Outbound traffic. If **Unlimit** is selected, the **FAP Plan Type** and **Volume Allowance** fields are disabled. Continue to next step if **Unlimit** is not selected.
10. Select the **FAP Plan Type** as **Fixed**, to indicate that the entire periodic allowance is renewed at the end of the period; or as **Rolling**, to indicate that the periodic allowance is replenished on a gradual incremental basis over the period.
11. Type the **Volume Allowance**, in total Megabytes, for the Upstream transfer volume.
12. Type the **Initial Allowance**, in total Megabytes, for the Upstream transfer volume. This value may be the same as the **Volume Allowance**, but may also differ.
13. Continue with the appropriate procedure for **Fixed Plan Type** or **Rolling Plan Type**:

    Configure the allowance period for a Fixed Plan:

    a. Use the clock icon to select a **Fixed Start Time** for the plan.
    b. Use the **Fixed Recurrence Type** drop-down to set a **Daily**, **Weekly**, or **Monthly** recurrence period.
    c. Select a **Fixed Week Day** at which the FAP should commence.
    d. Select the number of **Fixed Month Days** for which the FAP should be in force.
    e. Continue with Step (11).

    Configure the allowance period for a Rolling Plan:

    a. Use the calendar and clock icons and select a **Rolling Start Date/Time** for the plan.
    b. Use the **Fixed Recurrence Type** drop-down to set **Daily**, **Weekly**, or **Monthly** period.

c. Enter a **Rolling Update Interval**, which in conjunction with the value selected from the **Rolling Update Interval Unit** drop-down (**Days, Hours, or Months**) establishes how the volume allowance is gradually restored.

d. Select the number of **Fixed Month Days** for which the FAP should be in force.

e. Continue with Step (12).

14. Select the **Rollover Allowed** check box if the policy should support allowance rollover, and, if allowed, type the **Maximum Rollover** of the transfer volume, in Megabytes.

15. Select **Overage Allowed** if the FAP should allow the rollover allowance to be exceeded, and if allowed, enter a **Maximum Overage** of rollover allowance in Megabytes.

16. Click **Save and Close** or **Save** to save the Fair Access Policy to the NMS; or click **Save** to continue in the modify mode with *Defining FAP Rules and Actions*.

4.11.2 Defining FAP Rules and Actions

FAP rules and actions govern the actions taken when the volume allowance is exceeded. Multiple FAP rules may be defined, for which specific triggers and actions may be specified. Triggers determine when a rule is applied, and actions determine the measures taken when a rule is triggered. FAP rules are defined independently for each GSP, MGSP, SSPP, or MSSPP. Rules and actions are configured using the Fair Access Policy — **Add Rules & Actions** dialog. At least one rules and action records must be defined.

When a *throttling* option is configured, a FAP violation causes any terminal governed by the service plan to be placed in a "*recovery zone*" for a specified duration. Time spent in the recovery zone is called a *recovery period*. *Restoration rules,* which specify conditions that must be met prior to restoring a service to its initial CIR/MIR, may also be configured.

To add FAP Rules and Actions:

1. From the **Fair Access Policy** tab, under **Rules & Actions**, click the **Add Record** button. The **Add Rule** dialog opens.

2. Use the following steps to define Rules and Actions for separate **Inbound** and **Outbound**, or for the **Aggregate** Inbound/Outbound. At least 1-rule must be configured.

3. Under **General Settings**, type a **Name** of the new FAP rule.

4. Under **FAP Trigger Rule**, use the **Rule Type** drop-down to select **Percentage of Volume Allowance** or **Volume Usage**, as the rule type.

5. Based on the selected **Rule Type**, enter the **Percentage of Volume Allowance** that will trigger the rule; or specify the **Volume Usage**, in gigabytes, which will trigger the rule.

6. Specify the **Time From Start of Period** as the number of **Days**, **Hours**, or **Months** after which the rule will be triggered.

7. Specify the **Time From Start of Period Unit** as **Days**, **Hours**, or **Months**.

8. Under **FAP Actions**, use the **Action Type** drop-down to select **Notify** or **Throttle** as the action to take as a result of exceeding the volume allowance.

9. If the **Action Type** is **Throttle**, specify the **Throttle CIR** (**Committed Information Rate**) **Percentage** and the **Throttle MIR (Maximum Information Rate) Percentage**, by which the service should be reduced.

10. Under **FAP Restoration Rule**, use the **FAP Restoration Rule** drop-down to select **Allowance Balance** or **Percentage Recovered** as the method upon which restoration to normal service or the initial **CIR/MIR** configuration for the service is to be based.
11. If the **FAP Restoration Rule** is based on **Percentage Recovered**, then enter a **Percentage of Volume Allowance** to which the service should be restored.
12. If the **FAP Restoration Rule** is based on **Allowance Balance**, then enter a **Volume Allowance**, in gigabytes, to which the service should be restored.
13. Click **Save** to add the rule to the **Fair Access Policy** tab, with the rule inserted as a **Rules & Actions** record listed by **Name** under **Inbound**, **Outbound**, or **Aggregate**.
14. Repeat the above steps, to insert another FAP **Rules & Actions** record.
15. To modify a given **Rules & Actions** record, click the **Edit** icon, modify as required and click the **Update** icon; to remove the record, click the **Delete** icon.
16. Click **Save and Close** or **Save** or click **Save** to continue in the modify mode.

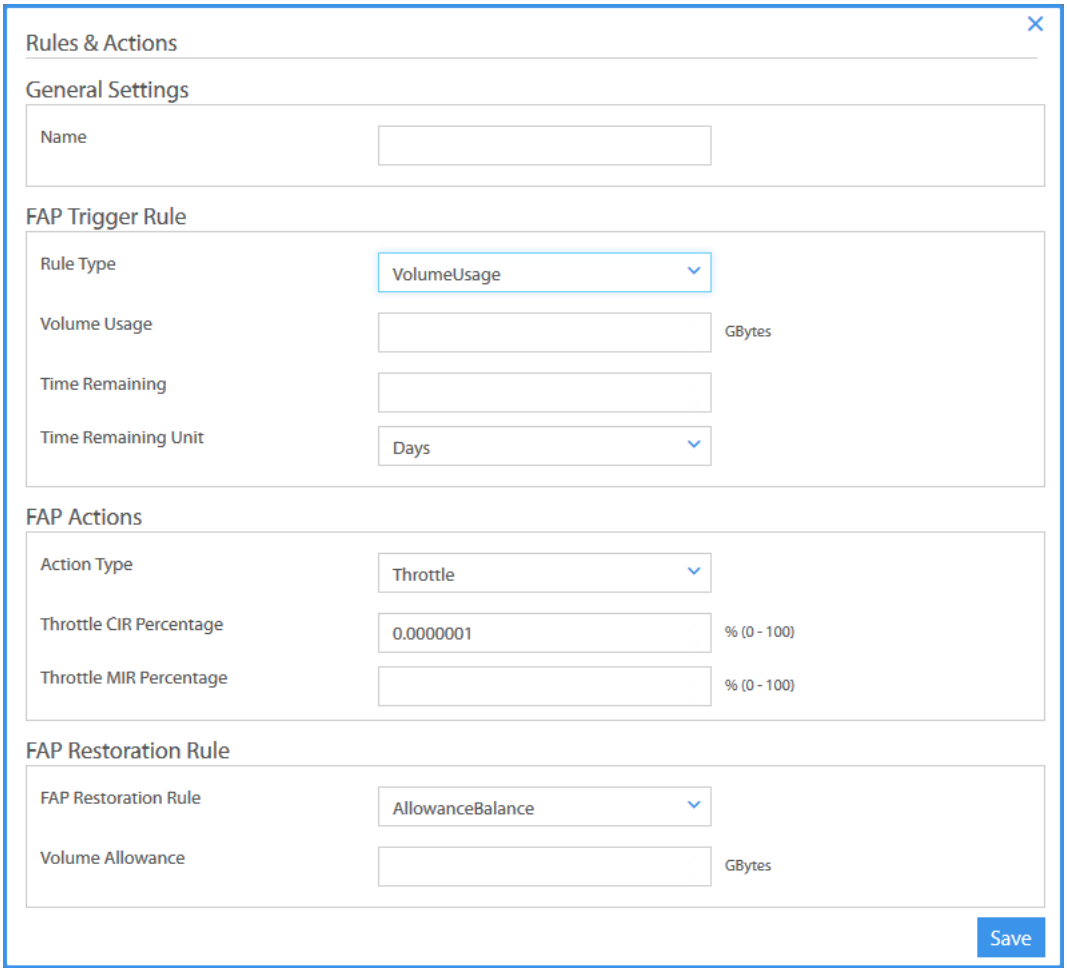

Figure 4-30. Fair Access Policy — Add Rule Dialog

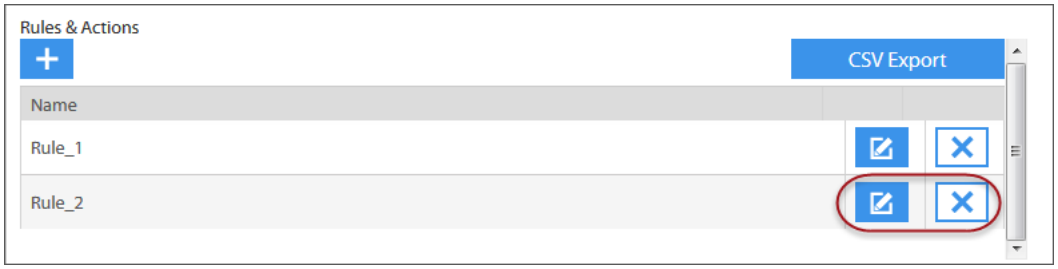

Figure 4-31. Fair Access Policy — Rules and Actions Records

4.11.3 Defining FAP Geographic Scope

Adding *FAP geographic scope* to the configured FAP allows the policy to be enforced within specific regions. When configured to have its own geographic scope and recurrence pattern, the FAP becomes a subset of the GSP geographic scope and recurrence pattern. A GSP service plan with a global scope that is always available, for example, may specify a FAP to apply only in specific high demand beams and during weekdays.

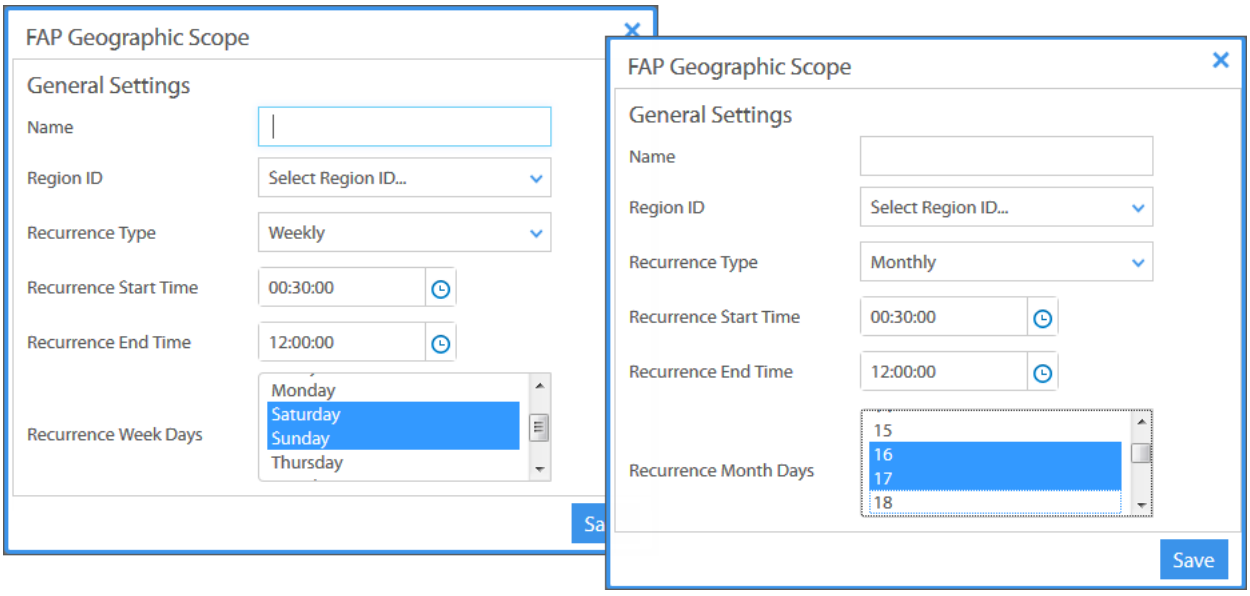

Figure 4-32. Fair Access Policy — Add FAP Region Dialog

To add FAP Rules and Actions:

1. From the **Fair Access Policy** page, under **FAP Geographic Scope**, click the **Add Record** button. The **FAP Geographic Scope** dialog opens.
2. Use the following steps to define **FAP Geographic Scope** records for separate **Inbound** and **Outbound**, or for the **Aggregate** Inbound/Outbound.
3. Click the **Region ID** drop-down and select a region to which the FAP should apply.

4. Select a **Recurrence Type** of **Daily**, **Weekly**, or **Monthly,** then from the list below, use the appropriate instructions based on the recurrence type:

   a. **Daily** — Enter a **Recurrence Start Time** and **Recurrence End Time** for the FAP.

   b. **Weekly** — Use the **Recurrence Weekdays** multi-select box, to select one or more days.

   c. **Monthly** — Use the **Recurrence Month Days** multi-select box, to select one or more days.

5. Click **Save** to update the **FAP Region** and return to the **Fair Access Policy** page. The region is inserted under **FAP Geographic Scope** as a new **FAP Region**.
6. Repeat the previous steps to insert additional FAP Regions.
7. Click the **Edit** icon to modify a record; click the **Delete** icon to remove the record.
8. Click **Save and Close** to save the FAP to the NMS database.

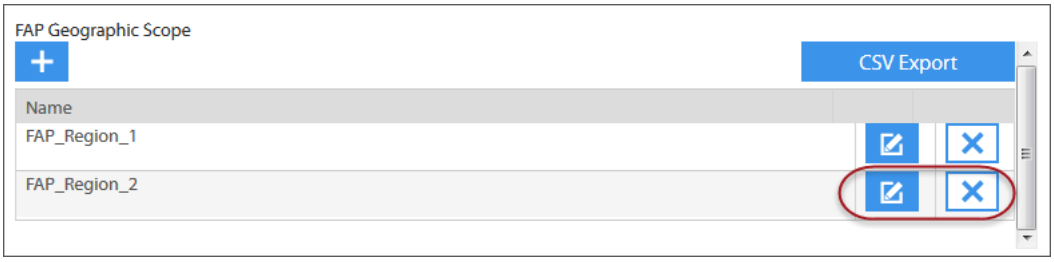

Figure 4-33. Fair Access Policy — FAP Region Records

4.12 Service Domain Browse Actions

Using the Pulse **Browse Service Domain Elements** command, users can interact with configured Service Domain elements in the Browse Results list to perform a variety of specific operations. These operations are called “actions.” An action can be performed on a single element, using the **Action** button for that element, or simultaneously on multiple selected elements, by using the browse window **Group Actions** button.

Only the actions which are possible, based on the element type, are displayed when an element type is selected. All actions are not possible with all elements.

The Service Domain element actions are listed and briefly described as follows:

Table 4-1. Service Domain — Browse Actions

Action	Applicable Elements	Brief Description
View Details	All Service Elements	View configured information for the selected service element.
Copy	All Service Elements	Create a cloned copy of the selected element, which can be modified as required, renamed, and saved as a new element.
Modify Element	All Service Elements	Modify the configured information for the selected element, and re-submit with changes.
Delete Element	All Service Elements	Remove the selected element from the NMS database.
Apply Configuration	All Service Elements - Except Region and SSPP	Apply configured NMS changes to the selected element, using the pending option file configured for the selected element.
Impact Analysis	All Service Elements	View impact on other elements, if changes are applied to the selected element.
Progress Report	All Service Elements	View a summary report of update manager progress since applying changes to the selected element.
Retrieve Pending Option File	All Service Elements - Except Region and SSPP	Load from the NMS database, and display the pending copy of the options file for the selected service domain element.
Retrieve Active Option File	All Service Elements - Except Geographic Region and SSPP	Load and display the options file currently active in the selected service domain element.
Compare Configurations	All Service Elements - Except Geographic Region and SSPP	Compare the pending options file and the active options file for the selected service element.
Modify Engineering Debug Keys	All Service Elements - Except Region and SSPP	Modify custom key associated with a specific feature to enable or disable, add or modify functionality.
Add GSP	Group Service Plan Only	Add a Group Service Plan to the selected GSP.
Add Multicast SSPP	Multicast GSP Only	Add a Multicast SSPP to the selected Multicast GSP

5 Configuring Terminal Domain Elements

iDirect Velocity™ Satellite Terminals provide IP connectivity between each Terminal LAN and the Velocity hub system. The Velocity element domains described thus far have the primary purpose of providing services to the Velocity *terminal domain*. The elements of this domain depend on the resources of the previously configured elements of the Physical, Transport, Network, and Service domains.

The Terminal Domain includes Terminal Components and Terminals.

The following topics briefly introduces each Terminal Domain element and provides step-by-step procedures for configuring each element and its associated parameters.

5.1 Terminal Domain Configuration Sequence

The Velocity Terminal Domain, which consists of **Terminal Components** and **Terminal Elements**, are accessed from the NMS **Configuration** tab, under **Terminals Domain**. Terminal components, which include block up converters (BUC), low noise block down converter (LNB), antenna control unit (ACU), terminal type, and satellite router, must be configured in the NMS database, prior to creating or adding a new terminal that would require these components.

Depending on assigned user group membership and access permissions, the NMS supports creating, viewing, modifying, and deleting of Terminal Domain Element configurations.

A general sequence for configuring Terminal Domain Elements, is shown here.

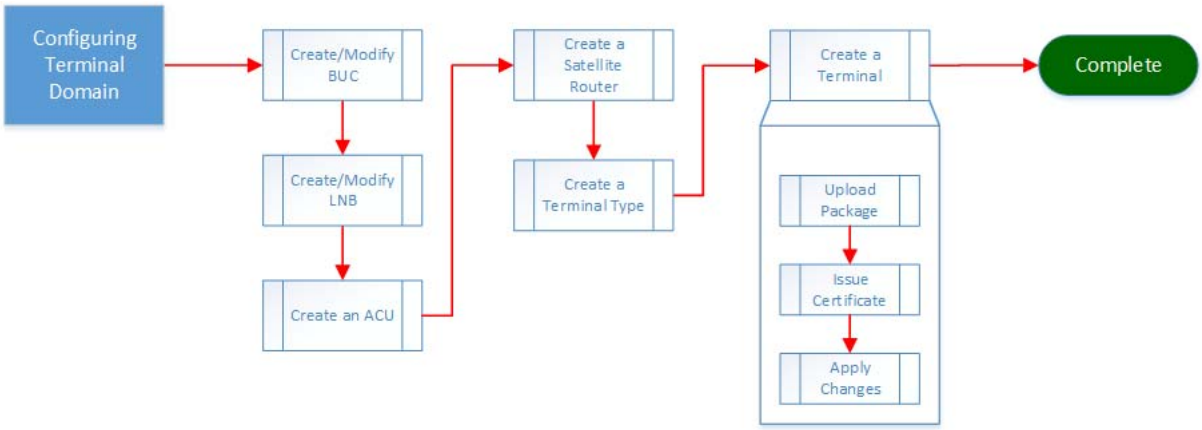

Figure 5-1. Building a Basic Network — Creating Terminal Domain Elements

5.2 Adding a Block Up Converter (BUC)

The *block up converter (BUC)* is used in the transmission of VSAT uplink signals. It converts a band of frequencies from a lower frequency range to a higher range. Several BUC devices that are certified for use with iDirect products are already pre-defined in the NMS. You can Browse Terminal Components and search/filter for these components. New BUC devices may be added, using the **Add BUC** configuration dialog.

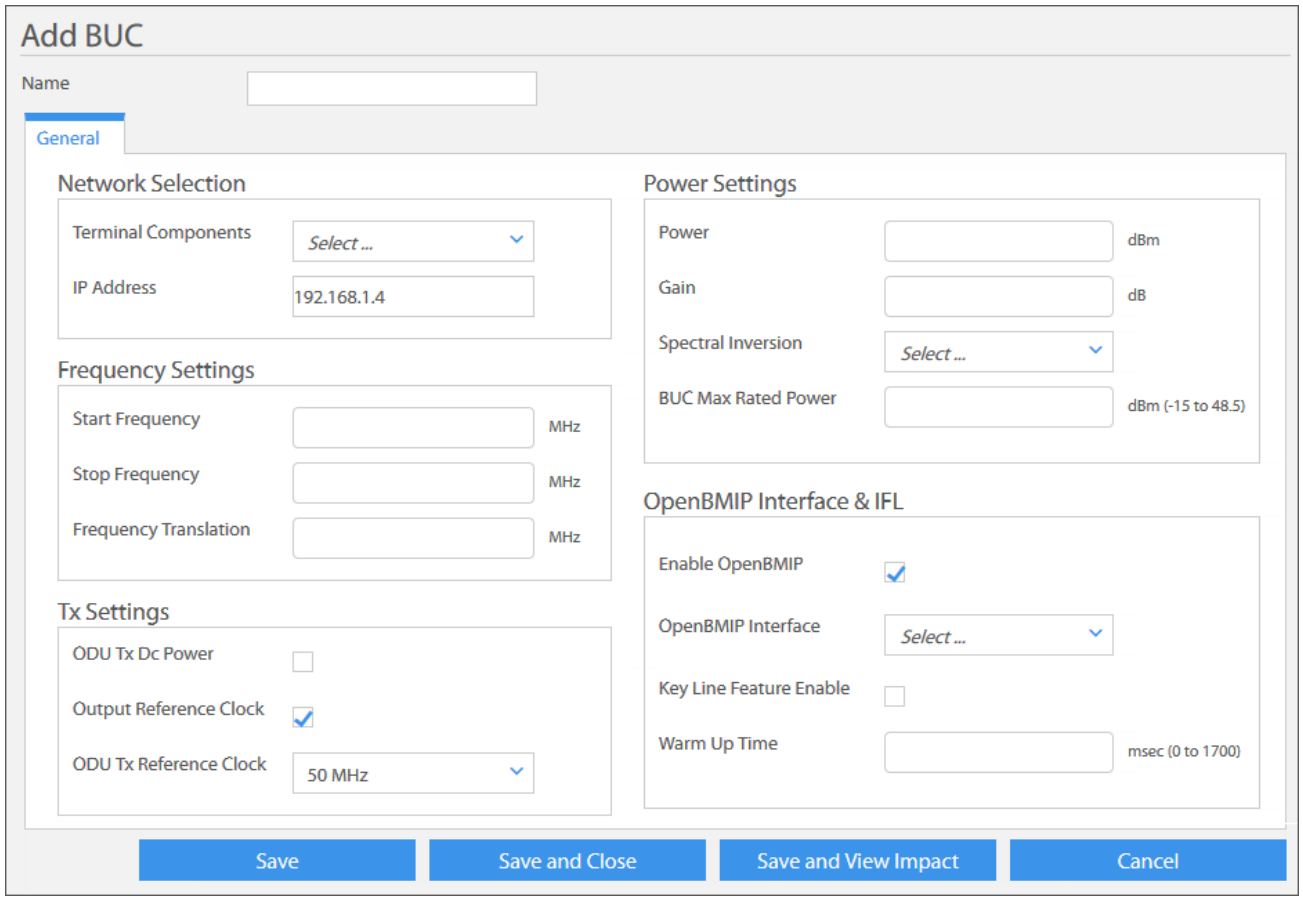

Figure 5-2. Add BUC Dialog

To add a BUC to the NMS:

1. Click the **Configuration** tab > **Terminal Domain > More Options > Add > BUC.**
2. Type the **Name** of the new block up converter.
3. Under the **Network Selection** section, use the **Terminal Components** drop-down and select the root Network node to which the BUC component is associated.
4. Use the default **IP Address** or configure a new IP Address for the new BUC.
5. Under **Frequency Settings**, specify BUC operating parameters **Start Frequency, Stop Frequency**, and **Frequency Translation.**
6. Under **Tx Settings**, use **ODU Tx Power** to enable/disable the ODU Tx DC output power.

7. Select **Output Reference Clock** to enable/disable the terminal reference clock output.
8. If applicable, select a **10 MHz** or **50 MHz** reference clock output; or select **OFF** to switch off the reference clock output.
9. Under **Power Settings**, specify the BUC **Power** and **Gain** operating parameters.
10. As required, select **Normal** or **Inverted** for **Spectral Inversion**. **Spectral Inversion** is used if the BUC local oscillator frequency is higher than the transmitted or received frequency. The **Normal** option is typical for C-band operation.
11. Use **BUC Max Rated Power**, to specify the rated maximum power of this BUC.
12. Select **Enable Open BMIP**, if applicable, and select **Serial** or **Ethernet** as the **OpenBMIP Interface** communication mode.
13. Select **Key Line Feature Enable** to enable the feature when using this BUC**.**
14. If applicable, enter a **Warm-Up Time**, from 0-1700 milliseconds. to allow the BUC (SR) device to reach the recommended temperature.
15. Click **Save and Close** to save the BUC configuration to the NMS.

5.3 Adding a Low Noise Block (LNB) Converter

The *low-noise block (LNB) converter,* is a receiving device that is integrated in the VSAT terminal to convert the signal gathered by the antenna feed circuit. Several LNB devices, already predefined in the NMS, are certified for use with iDirect products.

The **Add LNB** dialog is used to add new LNB devices. Both single-band and multi-band LNBs may be added.

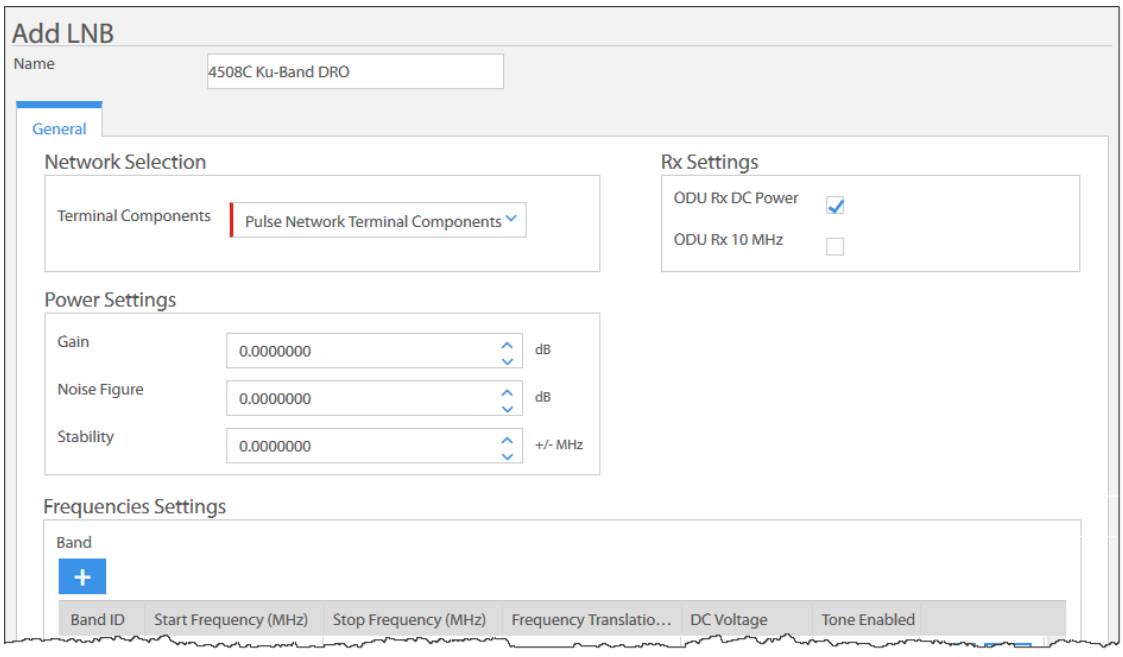

Figure 5-3. Add LNB Component

To add an LNB to the NMS:

1. Click the **Configuration** tab > **Terminal Domain > More Options > Add > LNB**.
2. Type the **Name** of the new low noise block (LNB) component.
3. Under the **Network Selection** section, use the **Terminal Components** drop-down and select the root Network node to which the LNB component is associated — for example, **Pulse Network System Terminal Components**.
4. Under **Power Settings**, enter operating values for **Gain** (dB), **Noise Figure** (dB), and **Stability** (± MHz) for the LNB device.
5. Under **RX Settings**, select **ODU Rx DC Power** and **ODU Rx 10 MHz** to indicate that the iDirect Satellite Terminal must supply the required DC power and 10 MHz clock.
6. Under **Frequency Settings** click the **Add Record** button to add one or more frequency band records, which are supported by the LNB.
7. For each **Band ID**, enter the LNB operating parameters for **Start Frequency**, **Stop Frequency**, and **Frequency Translation,** based on design recommendations for the specific network.
8. Use the **DC Voltage** drop-down to select **X-Polmode(13V)** or **X-Polmode(18V)** to generate DiSEqC compatible voltage to select the LNB band.
9. Use the **Tone Enabled** drop-down to select **ON** or **OFF** to generate DiSEqC compatible tone to select the LNB band.
10. Click **Save and Close** to save the LNB configuration to the NMS.

NOTE: In the preceding procedure, the frequency band records dialog for a multi-band LNB appears only after step 3 is completed. Also note that the Pulse **View LNB** dialog does not show the LNB band configurations. Band configurations are viewed by using the **Modify LNB** command from the LNB Actions menu.

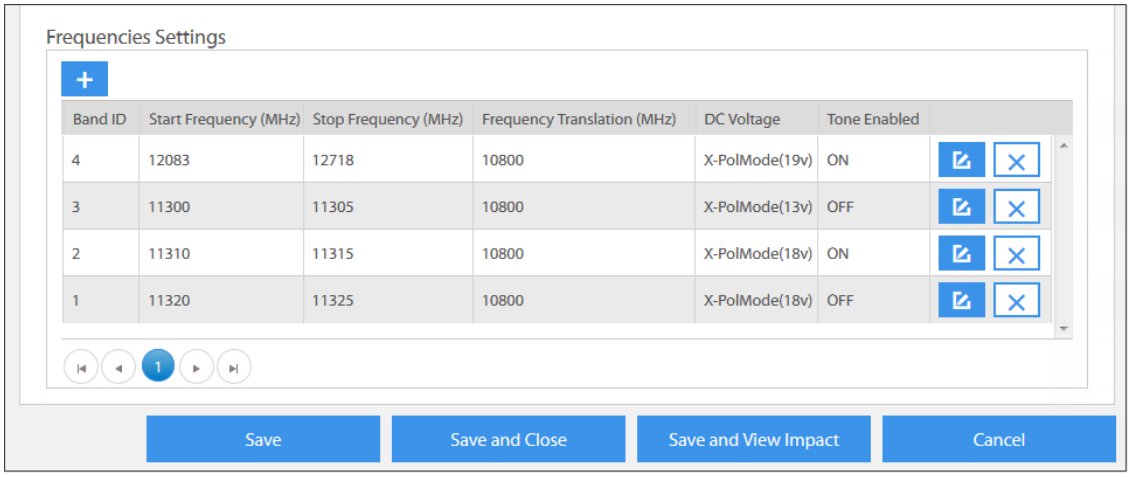

Figure 5-4. LNB Frequency Band Settings

5.4 Adding an Antenna Control Unit

The *antenna control unit,* is an intelligent control device that both monitors and controls the positioning of an VSAT antenna. Several ACU devices that are certified for use with iDirect products, are predefined in the NMS. ACU devices may also be added using the **Add ACU** configuration dialog.

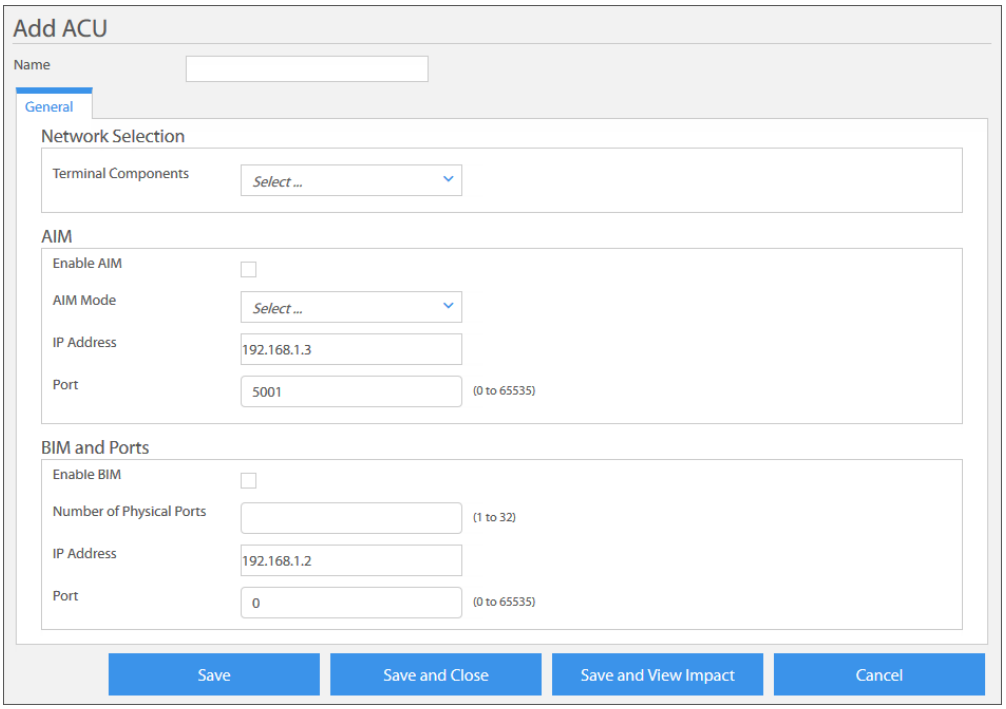

Figure 5-5. Add Antenna Control Unit Component

To add an Antenna Control Unit (ACU) to the NMS:

1. Click the **Configuration** tab > **Terminal Domain > More Options > Add > ACU.**
2. Type the **Name** of the new antenna control unit (ACU) component.
3. Under the **Network Selection** section, use the **Terminal Components** drop-down and select the root Network node to which the ACU component is associated.
4. Select **Enable AIM** to enable the Antenna control unit Interface Module on the ACU.
5. Use the **AIM Mode** drop-down and specify the mode of communications**.**
6. Use the AIM default **IP Address** and **Port** or specify a new IP address and port number.
7. Enter the **Number of Physical Ports** available on the switch.

To enable the BIM (Broadband Interface Module) component:

1. Select the **Enable BIM** check box.
2. Enter the **Number of Physical Ports** available on the switch.
3. Use the BIM default **IP Address** and **Port** or specify a new IP address and port number.

4. Click **Save and Close** to save the ACU configuration to the NMS.

5.5 Adding a Terminal Type

The **Add Terminal Type** dialog is used to create and configure a new Terminal Type in the NMS. A *terminal type* is a unique element in the NMS that has a unique Name, is composed of specific satellite components (**LNB**, **BUC**, and **ACU**), a specific **Satellite Router Type**. This baseline Terminal Type is also referred to as the NMS Terminal Type.

A Terminal Type may also have associated RF parameters that are not configured explicitly, with the NMS Terminal Type configuration, but instead the RF parameters associated with a Terminal Type are specified on the **Terminal Type** tab of the **Add Channel** dialog or from the Add Regulatory Area page where the RF limits are associated with the NMS Terminal Type.

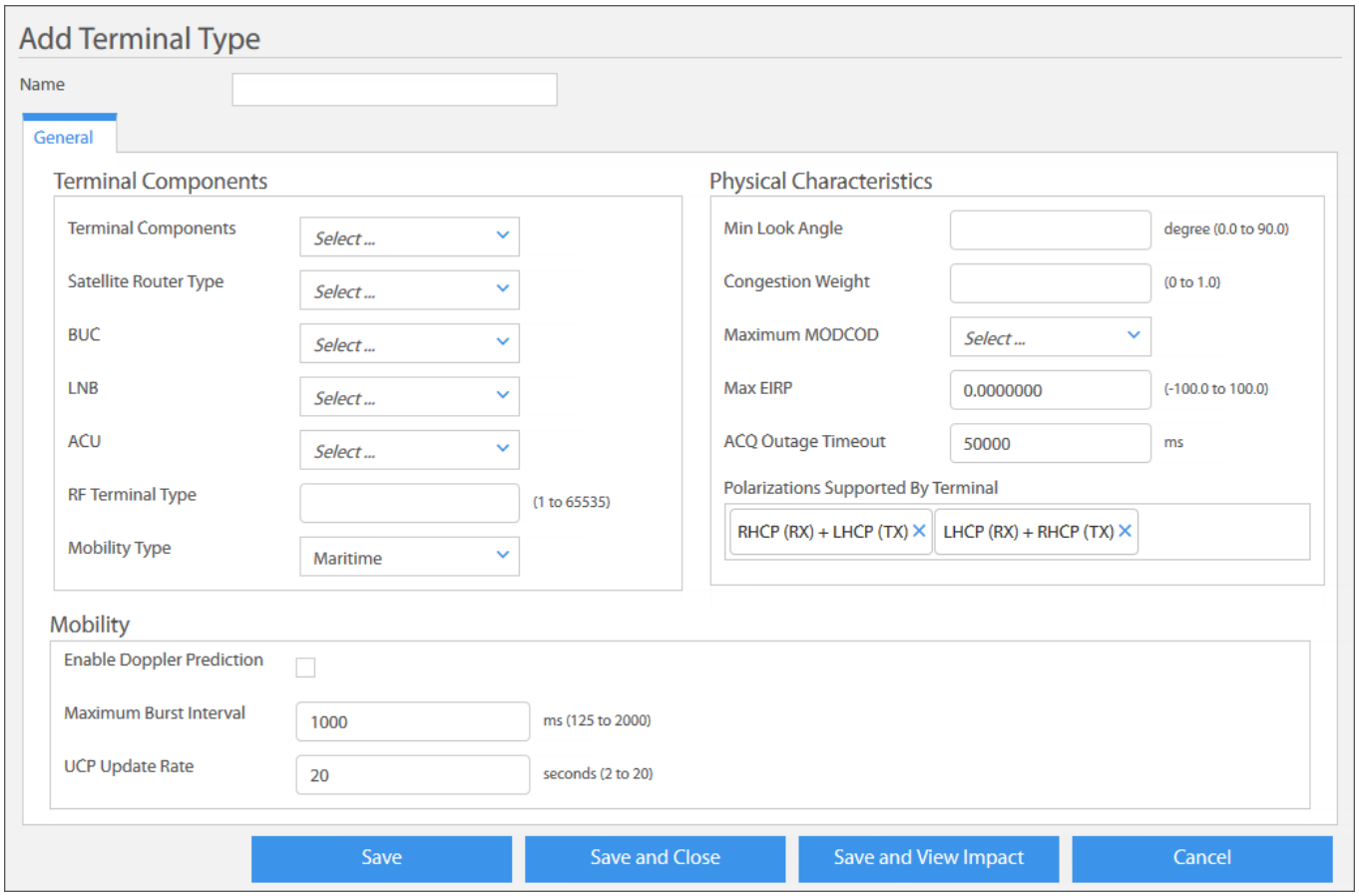

Figure 5-6. Add Terminal Type

To add a Terminal type:

1. Click the **Configuration** tab > **Terminal Domain > More Options > Add > Terminal Type.**
2. Type the **Name** of the new terminal type.

3. Use the **Terminal Components** drop-down and select the root Network node to which the Terminal Type is associated — for example **Pulse Network Terminal Components**.
4. Select the **Satellite Router Type** to be used for the new Terminal Type.
5. Use the appropriate drop-down list to select the appropriate **BUC, LNB,** and **ACU** devices to be used for the new Terminal Type.
6. Enter **RF Terminal Type** as a unique value of 1-65535, to represent this terminal type.
7. Select the **Mobility Type** as **Aeronautical, Fixed**, or **Maritime**.
8. Under **Mobility**, select **Enable Doppler Prediction** to enable/disable the feature on this Terminal Type.
9. Enter the **Maximum Burst Interval** or use the 1 second default.
10. Enter the **UCP Update Rate** or use the 20 seconds default for this terminal type.
11. Under **Physical Characteristics**, enter the **Minimum Look Angle** of the Terminal Type.
12. In **Congestion Weight** enter a weighted-value between 0.0 and 1.0, which gives the relative weight of the figure of merit versus the congestion metric. This factor is applied to terminals of this terminal type, during periods of congestion.
13. Use **Maximum MODCOD** to select the highest modulation code for the Terminal Type.
14. Enter a **Maximum EIRP** between -100.0 and 100.0, supported by this terminal type.
15. Enter the **ACQ Outage Timeout** value or use the default value of 50,000 milliseconds.
16. Use **Polarizations Supported By Terminal** to specify one or more polarizations supported by this Terminal Type. Mixed linear/circular combinations are not supported.
17. Click **Save and Close** to save the new terminal type configuration to the NMS.

5.6 Adding a Satellite Router

The satellite router component is the intelligence of the Satellite Terminal. It provides IP connectivity and communications with other network elements. The **Add Satellite Router** dialog is used to create and configuring the satellite Router in the NMS.

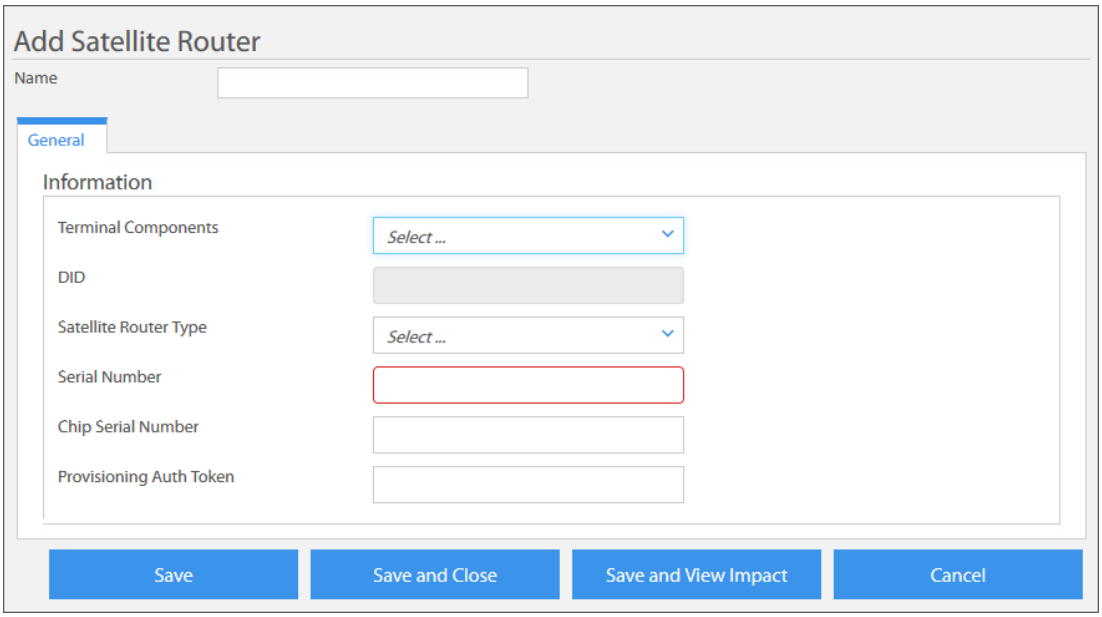

Figure 5-7. Add Satellite Router

To add a Satellite Router:

1. Click the **Configuration** tab > **Terminal Domain > More Options > Add > Satellite Router.** The **Add Satellite Router** dialog opens.
2. Type a **Name** for the new Satellite Router.
3. Use the **Terminal Components** drop-down and select the root Network node to which the Satellite Router is associated — for example **Pulse Network Terminal Components**.
4. Select the correct **Satellite Router Type** for the new satellite router.
5. Enter the **Serial Number** of the Satellite Router. The **Derived ID (DID)** number, which is system generated, is automatically displayed in the **DID** field.
6. Enter the **Chip Serial Number** of the new Satellite Router.
7. Enter the appropriate **Provisioning Auth Token** for the satellite router.
8. **Click Save and Close** to save the satellite router configuration to the NMS database.

5.6.1 Confirming the Satellite Terminal Derived ID (DID)

Using the **Terminal Provisioning Tool**, the encrypted string for the satellite router DID (derived ID) of a Satellite Terminal can be confirmed from the NMS. This dialog is accessed from the **Terminal Domain** menu of the **Configuration** tab.

Provisioning is a task that is performed by a Service Provider System Administrator. Each satellite router, when shipped from the manufacturer, has an attached label of the encrypted DID. The only requirement now, is to open the Terminal Provisioning Tool and enter the DID provided on the device label. Through use of the provisioning tool, visibility of the satellite routers that were encrypted during the staging process can now be obtained.

Once the provisioning task is completed, the information needed to create and configure Satellite Terminals in the NMS is available.

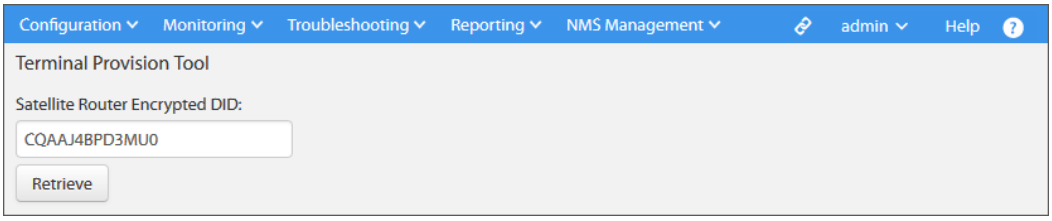

Figure 5-8. Terminal Provisioning Tool Dialog

To use NMS provisioning tool:

1. Click the **Configuration** tab > **Terminal Domain** > **More Options** > **Confirm Satellite Router DID.** The **Terminal Provision Tool** dialog opens.
2. In the **Satellite Router Encrypted DID** field, enter the **Provisioning Key** code (13-character string), encrypted DID found on the label attached to the satellite router packaging.
3. Click the **Retrieve** button. The Satellite Router can now gain visibility to the Satellite Router information for successfully completing the Satellite Terminal provisioning. The confirmed DID is required for entry into the Satellite Terminal configuration dialog.
4. Repeat the previous step for each Satellite Router, until done.

5.7 Satellite Terminal Component Browse Actions

Using the Pulse **Browse Satellite Terminal Components** command, users can interact with configured Satellite Terminal Components in the Browse Results list to perform a variety of specific operations. These operations are called “actions.” An action can be performed on a single element, using the **Action** button for that element, or simultaneously on multiple selected elements, by using the browse window **Group Actions** button.

Only the actions which are possible, based on the element type, are displayed when an element type is selected. All actions are not possible with all elements.

The Terminal Component element actions are listed and briefly described as follows:

Table 5-1. Terminal Components — Browse Actions

Action	Applicable Elements	Brief Description
View Details	All Satellite Terminal Components	View configured information for the selected satellite component.
Copy	All Satellite Terminal Components	Create a cloned copy of the selected component, which can be modified, renamed, and saved as a new component.
Modify Component	All Satellite Terminal Components	Modify the configured information for the selected satellite terminal component, and re-submit with changes.
Delete Component	All Satellite Terminal Components	Remove the selected satellite terminal component from the NMS database.
Apply Configuration	All Satellite Terminal Components	Apply configured NMS changes to the selected service, using the pending option file for the element.
Progress Report	All Satellite Terminal Components	View a summary report of update manager progress since applying changes to the selected element.
Provision Satellite Router	Satellite Router Only	See *Confirming the Satellite Terminal Derived ID (DID)*.

5.8 Add Terminal — General Parameters

NMS pages for creating a Satellite Terminal are provided using individual tabs for **General**, **Performance Optimization**, **SVN**, **Switch Configuration**, **Geo Location**, **Terminal Service Plan**, and **Advanced** configuration parameters.

.

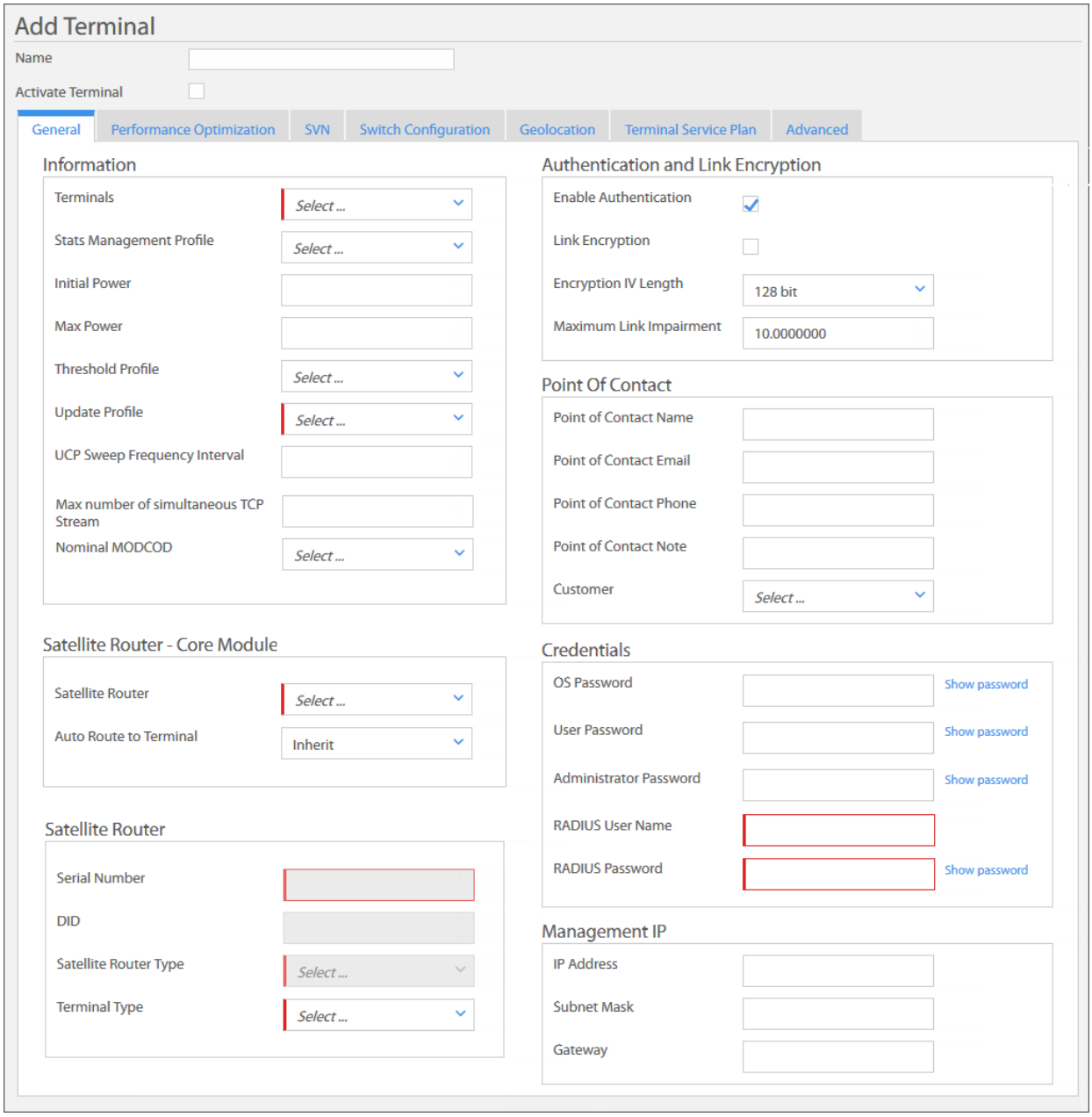

Figure 5-9. Add Terminal — General Parameters Dialog

To configure Satellite Terminal general parameters:

1. Click the **Configuration** tab > **Terminal Domain > Add Terminal.**
2. On the General tab, enter a **Name** for the new Satellite Terminal and select **Activate Terminal** to activate the terminal in the network. By default, terminals are deactivated, and must be activated to be seen by the NMS update manager.
3. Under **Information**, use the **Terminals** drop-down**,** to choose the network terminals group to which the new satellite terminal should be assigned.
4. Select the **Stats Management Profile** to be assigned to this terminal— for example **Standard, Bronze**, **Silver**, or **Gold**.
5. In **Initial Power**, enter an initial TDMA transmit power level for this Satellite Terminal; and in **Max Power**, enter the maximum TDMA transmit power level, in dBm, as determined for this terminal during remote commissioning.
6. Use the **Threshold Profile** drop-down and select the appropriate threshold profile for this terminal — for example, **Terminal Default Thresholds.**
7. Use the **Update Profile** drop-down and select the appropriate update profile for this terminal — for example, **Default Terminal Update Profile**. The selected update profile represents a group of Update Manager rules to apply to this satellite terminal.
8. Enter the **UCP Sweep Frequency Interval**. This value, typically in kHz, represent the frequency window (- frequency to + frequency) used to trying to lock on to the upstream/downstream carrier. This interval is either added to or subtracted from the carrier center frequency in order to receive an upstream or downstream carrier lock.
9. Enter a **Max Number of Simultaneous TCP Streams** supported by this terminal.
10. Enter the **Nominal MODCOD** supported by this terminal.
11. Use the **Satellite Router** drop-down to select the satellite router on which the new Satellite Terminal is based. The fields **Serial Number**, **DID (Derived ID)**, and **Satellite Router Type** under the **Satellite Router** section, are automatically populated.
12. Use the **Auto Route To Terminal** drop-down to choose **Enable**, **Disable**, or **Inherit**.
13. Use the **Terminal Type** drop-down and choose the pre-configured Terminal Type to use in creating the new satellite terminal.
14. Under **Credentials**, enter an **OS Password** to allow access to the terminal operating system; enter a **User Password** to allow access to the terminal user console; and enter an **Administrator Password** to access to the terminal configurations.
15. Type the **RADIUS User Name** and **RADIUS Password**, for accessing the RADIUS Server associated with this terminal.
16. Under the **Management IP** section, enter the **IP Address**, **Subnet Mask**, and **Gateway** addresses by which the NMS communicates with this terminal.
17. Under the **Authentication and Link Encryption** section, select **Enable Authentication** to require authentication by this terminal on acquisition.
18. Select **Link Encryption** to require OTA encryption of the connection of this terminal.
19. Use the **Encryption IV Length** drop-down to specify 12-bit or 128-bit encryption. Link Encryption should only be enabled if it is supported by the Satellite Terminal type.

20. Under the **Point of Contact** section, use **Name**, **E-mail** address, and **Phone** number, to specify point of contact information for the owner of the new terminal.
21. Use the **Customer** drop-down**,** to assign a specific customer owner of the terminal. Names of customers or Service Providers already added to the NMS database, will appear in the list.
22. **Click Save and Close** to save the terminal configuration, or click **Save** to continue in the modify mode with the terminal configuration.

5.9 Add Terminal — Performance Optimization

The **Performance Optimization** tab contains parameters for enabling and configuring TCP acceleration and compression, UDP compression, RTP compression, and optimization settings for Transmit Properties on a Satellite Terminal**.** Each of these parameter sections must be enabled to allow the supported feature to be enabled and configured.

iDirect terminals generally supports both *payload compression* and *header compression*. Enabling header or payload compression allows the terminal to optimize the use of the over-the-air bandwidth. In operation, upstream packets that are compressed by the terminal, are restored by the Protocol Processor decompression process. In the downstream direction, compressed packets are decompressed by the terminal.

Optimization characteristics can also be configured on a per-SVN basis, from the SVN configuration tab.

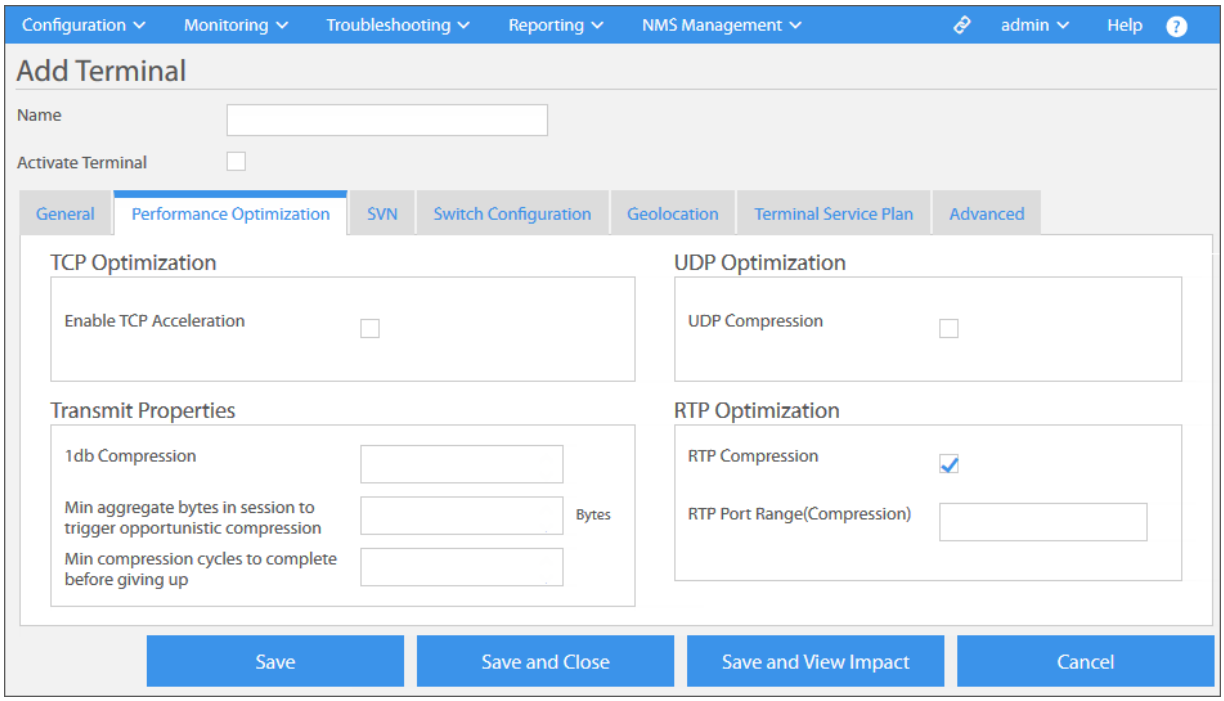

Figure 5-10. Add Terminal — Configuring Performance Optimization Parameters

To configure TCP Acceleration and Compression:

1. From the **Add Terminal** page click the **Performance Optimization** tab.
2. Select **Enable TCP Acceleration** to enable TCP acceleration on this terminal.
3. Select **Enable Connection Acceleration** to enable TCP acceleration on this terminal to Teleport connection.
4. In **TCP Port Range (Acceleration)**, use comma separation to specify port numbers — for example 2001, 2005; or use a hyphen to specify a port range — for example 2001-2003. TCP traffic is accelerated for the specified ports.
5. Use **Max Acceleration Session** to specify the maximum number of accelerated sessions allowed on this Satellite Terminal. This value must be >=0.
6. Select **Enable TCP Compression** to enable TCP payload compression on this terminal.
7. In **TCP Port Range (Compression)**, use comma separation to specify port numbers — for example 2001, 2005; or use a hyphen to specify a port range — for example 2001-2003. TCP payload packets are compressed for the specified ports.
8. Select **Enable TCP Header Compression** to enable the compression of the TCP header on this Satellite Terminal for the specified ports or port range.
9. In **TCP Port Range (Header Compression)**, use comma separation to specify port numbers — for example 2001, 2005; or use a hyphen to specify a range — for example 2001-2003. TCP header packets are compressed for the specified ports.

To configure UDP Optimization:

1. Select **UDP Compression** to enable the UDP compression on this Satellite Terminal.
2. Select the compression method using the **UDP Compression Method** drop-down.
3. In **UDP Port Range (Compression)**, use comma separation to specify port numbers — for example 2001, 2005; or use a hyphen to specify a port range — for example 2001-2003.
4. Select **UDP Payload Compression** to enable UDP payload packet compression on this Satellite Terminal.
5. In **UDP Port Range (Payload Compression)**, use comma separation to specify port numbers — for example 2001, 2005; or use a hyphen to specify a range — for example 2001-2003.

To configure RTP Optimization:

6. Select **RTP Compression** to enable the feature on this Satellite Terminal.
7. In **RTP Port Range (Compression)**, use comma separation to specify port numbers — for example 2001, 2005; or use a hyphen to specify a port range — for example 2001-2003.

To configure Optimized Transmit Properties:

1. In **1db Compression**, specify the 1dB Compression Point determined for this Satellite Terminal, at the time of Satellite Terminal commissioning.
2. Specify the **Minimum Aggregate Bytes** that the terminal must receive in a session, before opportunistic compression is started.

3. In **Compression Cycle Timeout**, specify the maximum number of compression cycles that should be completed before compression is considered to have failed.
4. **Click Save and Close** to save the terminal configuration, or click **Save** to continue in the modify mode with the terminal configuration.

5.10 Add Terminal — Switch Configuration

An iDirect Satellite Terminal, depending on the type, may have up to 8 Ethernet ports located on the terminal back panel. The ports that are used and the parameters for each port are configured from the **Switch Configuration** tab.

The **Switch Configuration** tab supports the following:

- Assignment of a port to one or more VLANs
- Specification of Duplex Mode (full/half)
- Enable tagged packets on designated VLANs
- Specification of port speed (10/100 Mbps/Auto-Negotiate)
- Configure a port as trunk (allowing pass-through traffic from designated VLANs)

When a port is defined as a trunk, all traffic from designated VLANs is able to pass through the port — this includes both Customer VLANs and default VLANs (Admin, and Tunnel). All Customer-defined VLAN frames on trunk ports are tagged to explicitly identify the source VLAN. Default VLAN traffic passing through a trunk port is not tagged.

As an alternative to allowing a port to act as a trunk, a port can also be dedicated to any user-defined VLAN or to the default VLANs. In such a case, only traffic for those designated VLANs pass through the port. There is no VLAN tagging on a port dedicated to an VLAN, regardless of whether the port is dedicated to a default VLAN or to a Customer VLAN.

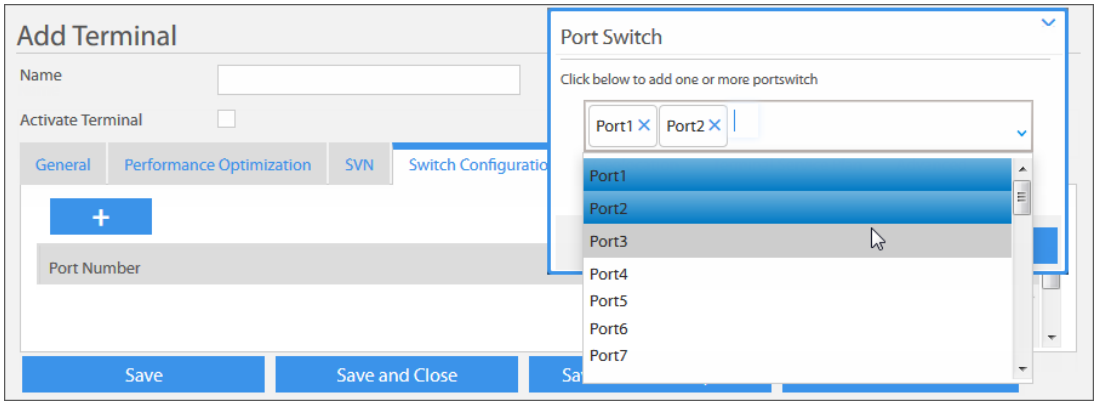

Figure 5-11. Add Terminal — Switch Configuration Tab and Port Switch Selection Dialog

To configure a Satellite Terminal switch assignment:

1. Click the **Switch Configuration** tab, from the **Add Terminal** page.
2. Click the **Add Record** icon to add one or more ports to the terminal. The **Port Switch** select dialog opens as shown in the foreground.

3. Select up to eight ports to configure for the Satellite Terminal, and click **Save** to accept the selected ports and return to the **Switch Configuration** tab. The port switches are listed as individual records under **Port Number**.
4. Click the **Delete** icon of a selected port, to remove the port; click the **Edit** icon to configure the port parameters. If edit is selected, the **Port Switch** configuration dialog opens, as shown in the foreground image.
5. Select **Auto Negotiation**, on the **Port Switch** dialog, if the port speed should be automatically determined. The **Speed** and **Mode** fields are disabled, with this selection.
6. Disable **Auto Negotiation** to manually enter the port **Speed** and **Mode**, then use the **Speed** drop-down to set the port for **10 Mbps** or **100 Mbps**; use the **Mode** drop-down to set **Full-Duplex** or **Half-Duplex** communication.
7. Use the **SVN List** multi-select box to assign one or more configured SVNs to the selected port switch. Use the **CTRL** key to select multiple SVNs.
8. Select **Tag Enable** to indicate that packets should be tagged with the VLAN ID.
9. Select **Trunk** to configure the port as a trunk; and use the **Trunk SVN List** multi-select box to pick one or more configured VLANs whose traffic should pass through the trunk. Click **Save Switch Configuration** to update the edited port parameters in memory.
10. Click **Save and Close** to save the configuration to the NMS or click **Save** to continue in the modify mode with *Add Terminal — Geo-Location Parameters*.

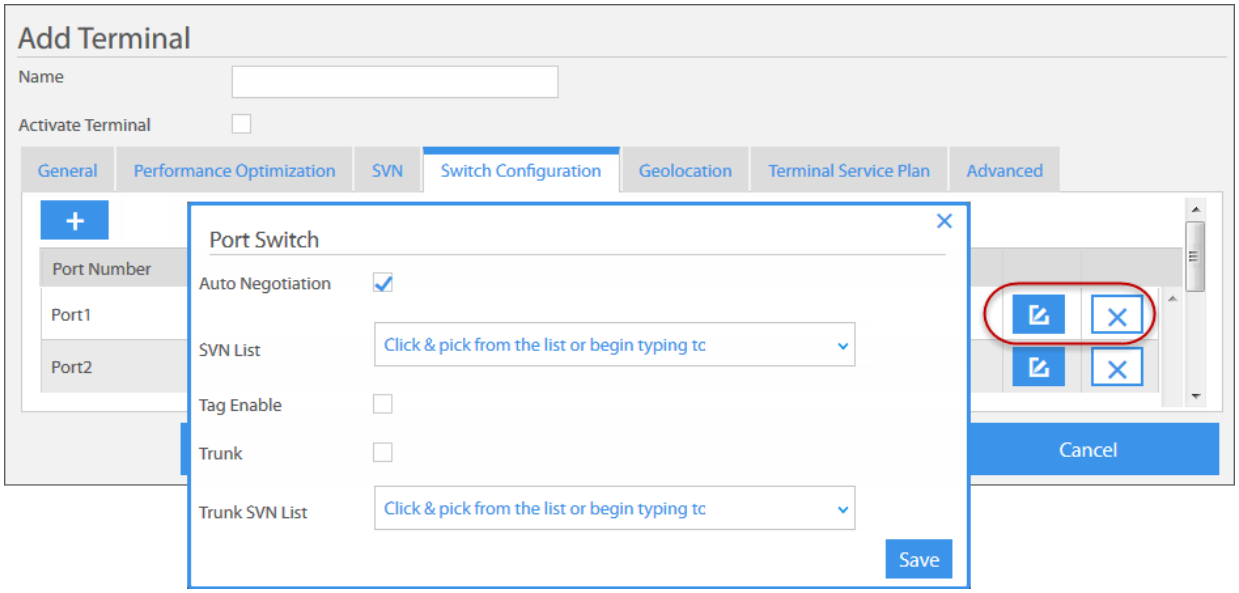

Figure 5-12. Selected Port Switch Records

5.11 Add Terminal — Geo-Location Parameters

When commissioning a Satellite Terminal, the **Terminal Geo Location** tab is used to specify geographic location of the installation site. The Geo location can be determined by using a GPS receiver. The dialog provides a choice of specifying the Latitude and Longitude in decimal degrees format; or by specifying the direction, degrees, minutes, and seconds format.

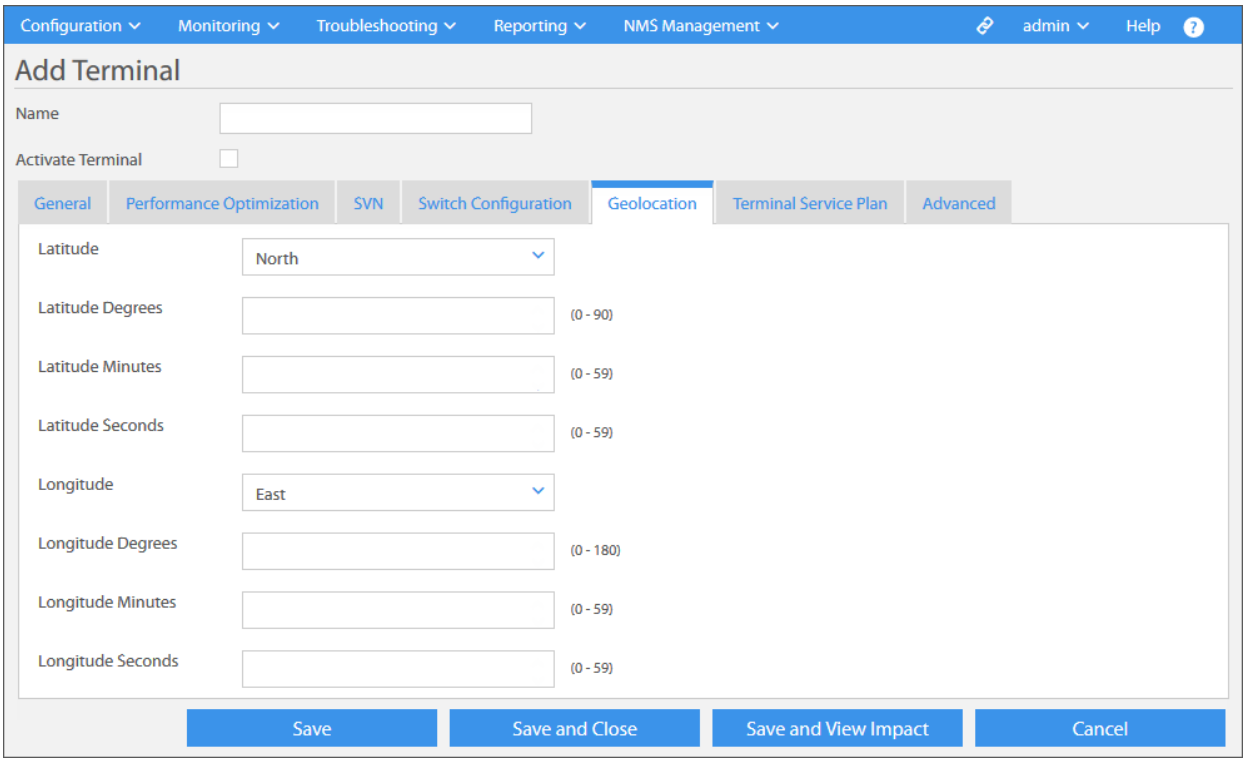

Figure 5-13. Add Terminal — Geo Location Parameters Dialog

To configure Satellite Terminal Geo Location Parameters:

1. From the **Add Terminal** page click the **Terminal Geo Location** tab.
2. Use the **Latitude** drop-down and select the direction as **North** or **South**.
3. Enter the **Latitude** coordinates using the fields **Latitude Degrees** (0-90), **Latitude Minutes** (0-59), and **Latitude Seconds** (0-59).
4. Use the **Longitude** drop-down and select the direction as **East** or **West**.
5. Enter the **Longitude** coordinates using the fields **Longitude Degrees** (0-180), **Longitude Minutes** (0-59), and **Longitude Seconds** (0-59).
6. **Click Save and Close** to save the Satellite Terminal configuration.

5.12 Add Terminal — Service Plan

A *Terminal Service Plan (TSP)* or *Subscriber Service Plan*, is the configured service plan of an individual terminal. The TSP is defined by the Network Operator or by a Service Provider. As briefly introduced in the discussion of Group Service Plans, a Subscriber Service Plan generally consist of one or more subscriber service plan components, where each component is an instance of a specific unicast or multicast Subscriber Service Plan Profile (SSPP/MSSPP).

The components that make up a TSP may represent different applications — for example, a data component, provided by a data SSPP; a voice component, provided by a voice SSPP, or a multicast component, such as audio or video, provided by a multicast SSPP. Each component may be associated with a different Service Provider; have a different scope, such as regional or global; or different traffic priority.

The TSP may be configured to consist only of the parameters pre-configured in the SSPP or multicast SSPP, which are added as part of the plan; or the dealer may further define the service plan by adding the following:

- Modify a Service Plan Component to Overwrite the Default Plan Lifetime
- Modify a Service Plan Component to add Terminal Specific Service Applications (VRs)

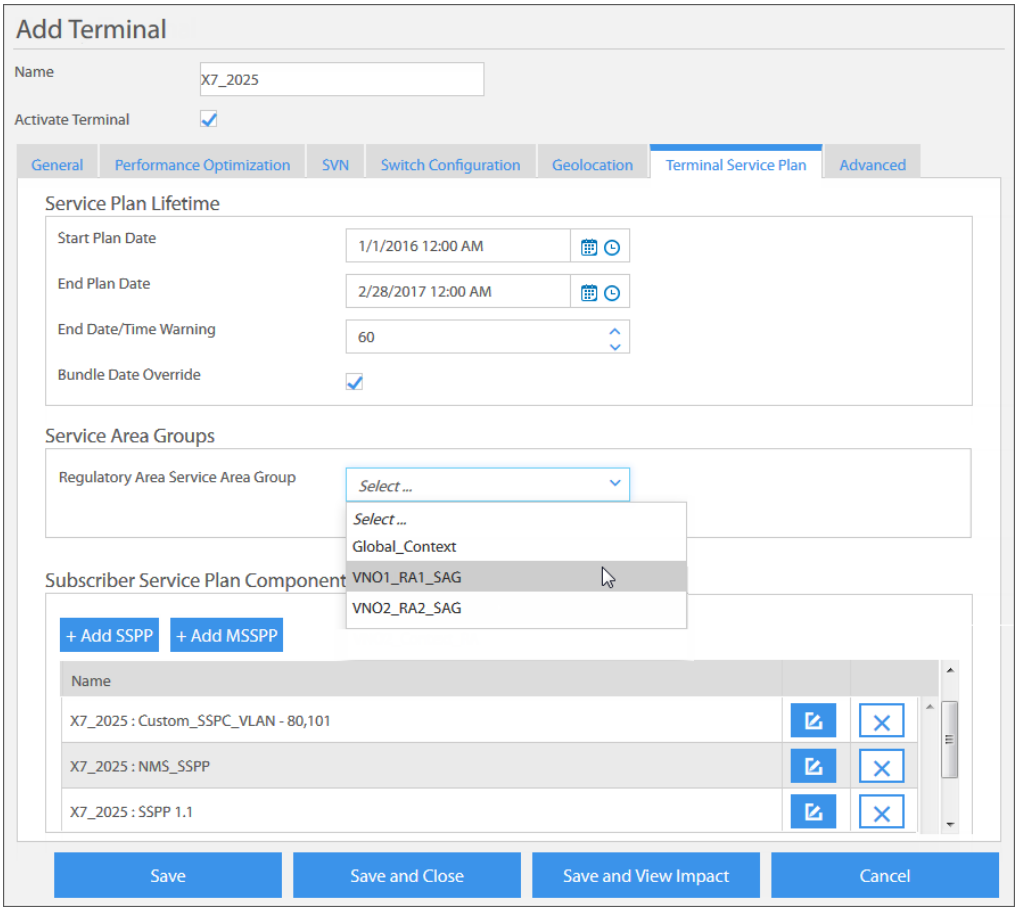

Figure 5-14. Add Terminal — Terminal Service Plan Tab

To create a Terminal Service Plan (TSP):

1. From the **Add Terminal** page click the **Terminal Service Plan** tab.
2. Under **Service Plan Lifetime**, enter a **Start Plan Date/Time** and **End Plan Date/Time**.
3. Use **End Date/Time Warning** to specify a warning time, in days, prior to the plan end.
4. Select **Bundle Date Override** to specify that all of the **Start Date/End Date** periods specified as the default for the TSP should override the **Start Date/End Date** periods specified for the individually configured TSP components (SSPC/MSSPC).
5. Use the **Regulatory Area Service Group** drop-down to select the SA Group that applies to this terminal.
6. Click **+Add SSPP** to select one or more unicast components to add to the TSP, or click **+Add MSSPP** to select one or more multicast components to add to the TSP. In either case, the associated **Subscriber Service Plan Component** selection dialog opens.
7. Select each unicast or multicast component to add to the TSP, and click **Save** to accept the selected components and return to the **TSP** tab. The components are listed by **Name**, as individual records under **Subscriber Service Plan Components**.
8. Click the **Edit** icon, on a specific SSPP or MSSPP to modify the component. If an edit icon is selected, the appropriate **Subscriber Service Plan Component** dialog opens.
9. **Click Save and Close** to save the Satellite Terminal configuration or click **Save** to continue in the modify mode with configuring the terminal service plan.

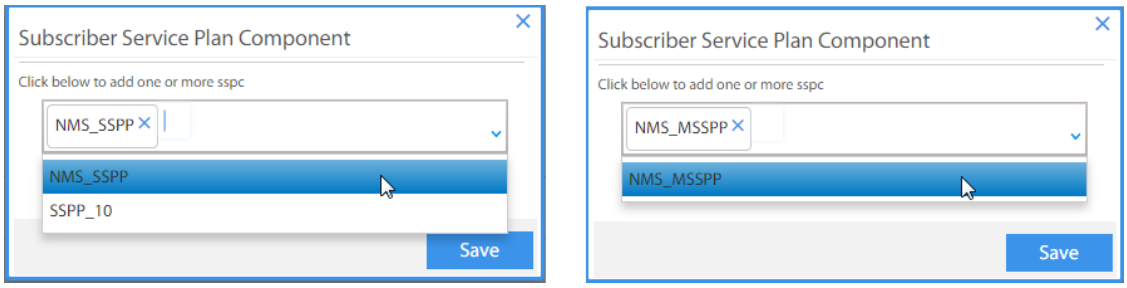

Figure 5-15. Add Terminal — Unicast and Multicast Service Plan Components Selection

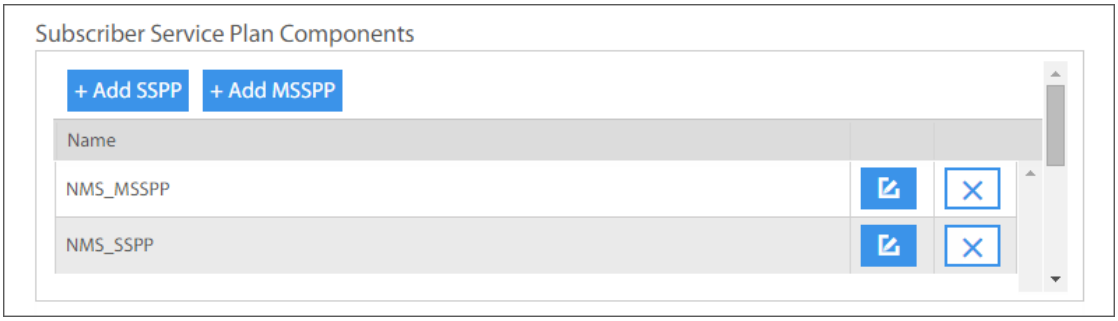

Figure 5-16. Terminal Service Plan Component Records

5.12.1 Configure Terminal SSPC General Parameters

Any unicast or multicast SSPCs added as terminal service plan components, may be left unmodified as the originally added to the terminal service plan or they may be modified.

Using the **General** tab, it is possible to activate the terminal service plan component, to overwrite the default terminal service plan **Start/End Date and Time**, and to specify a **Priority Type** for applying the QoS processing for this service plan component.

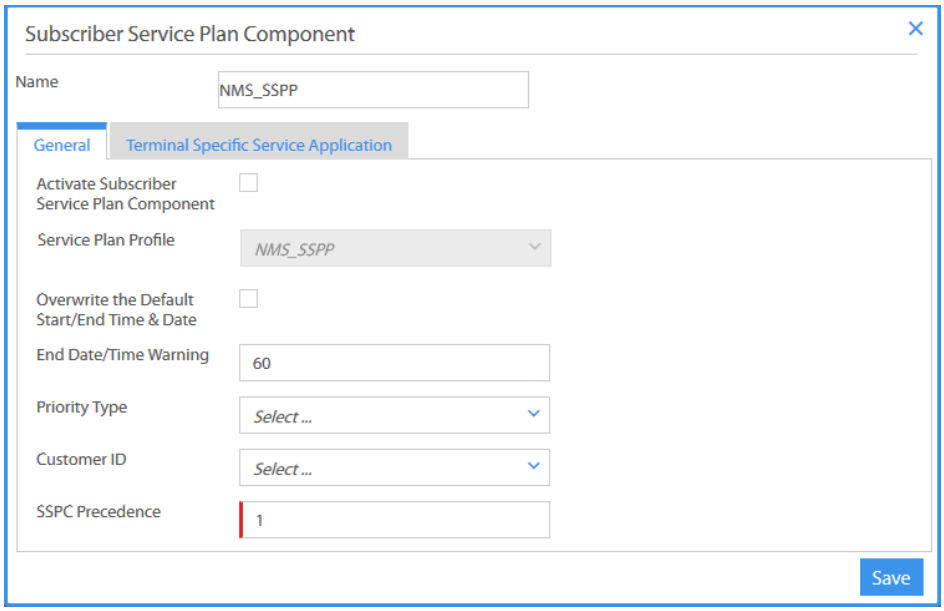

Figure 5-17. Subscriber Service Plan Component — General Configuration Tab

To modify a TSP component to override the default plan lifetime:

1. From the **Add Terminal** page, with TSP components listed under the **Subscriber Service Plan Components** section, click the **Edit** icon on a TSP component. The **Subscriber Service Plan Component** page opens to the **General** tab.
2. Select **Activate Subscriber Service Plan Component** to activate the terminal component.
3. Select **Overwrite the Default Start/End Time & Date** if the default Start/End Date and Time for the component should be overwritten with a new Start/End Time and Date.
4. Enter the parameters **Start Date/Time** and an **End Date/Time**, if **Overwrite the Default Start/End Time & Date** is enabled:
5. Enter a **End Date/Time Warning** to specify a warning time, in days, to issue a warming prior to the expiration of the terminal plan component.
6. Use the **Priority Type** drop-down to select **Absolute** or **Pre-Allocation Round** as the priority type for QoS processing for this terminal service plan component.
7. Select the **Customer ID** for this component.
8. Click **Save and Close** to save the configuration to the NMS; or click **Save** to continue in the modify mode with *Configure Terminal-Specific Service Application*.

5.12.2 Configure Terminal-Specific Service Application

Using the **Terminal Specific Service Application** tab, individual inbound or outbound application profile records can be created. Each application service specifies the **Name** of the profile, traffic **Direction**, a **CIR** (Committed Information Rate), a **MIR** (Maximum Information Rate), and a QoS **Priority** and **Cost**.

In the Group QoS Structure, at the Satellite Terminal level, a terminal specific service application is referred to as a *Virtual Remote (VR)*. Each VR is an SSPC that is responsible for the management of a specific type of traffic.

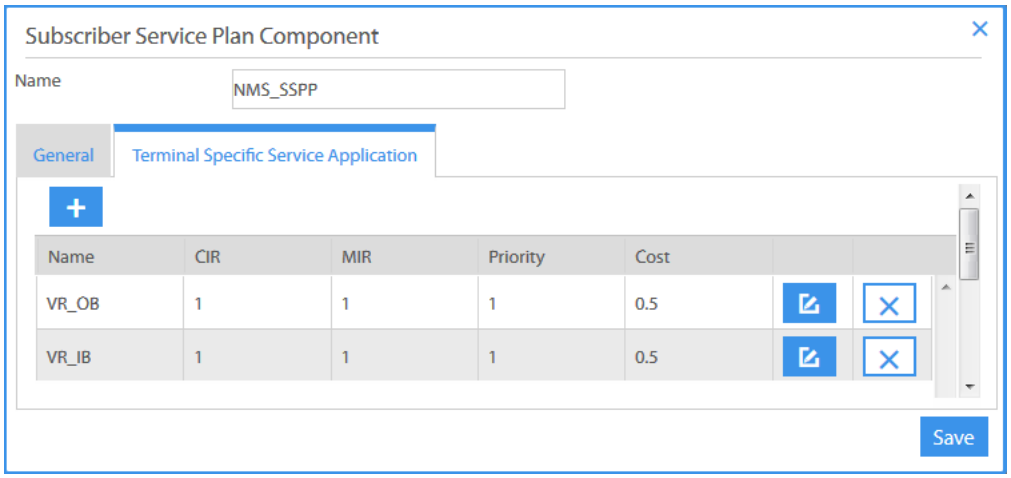

Figure 5-18. Terminal SSPC — Terminal Specific Service Application Tab

To modify a TSP component to create terminal specific service applications:

1. From the **Add Terminal** page, with TSP components listed under the **Subscriber Service Plan Components** section, click the **Edit** icon on a TSP component.
2. On the **Subscriber Service Plan Component** page click the **Terminal Specific Service Application** tab.
3. Click the **Add Record** icon to open the **Terminal Specific Application** dialog for inserting new applications (VRs) to this TSP component.
4. Enter a **Name** for the new Application, for example **VR_IB** or **VR_OB.**
5. Select **Inbound** or **Outbound** as the traffic direction, using the **Direction** drop-down.
6. Enter a **CIR** (Committed Information rate) and **MIR** (Maximum Information Rate) for QoS servicing of this application.
7. Enter a **Priority** (1-16), where 1 is the highest priority; and a **Cost** (0.001- 1.0), where 1.0 is the lowest cost. These values are applied in determining the QoS servicing of this application (VR).
8. In **Service Levels** pane, select the service levels and traffic rules to inherit from the configured SSPP or multicast SSPP. New classification rules can be added to the terminal SSPC from the **Terminal Traffic Rule** tab, if required.
9. Click the **Terminal Traffic Rule** tab, to insert a new Classification Rule.

10. Click **Save**, to save the application as a new Application Service record, listed on the **Terminal Specific Service Application** tab.
11. Repeat the previous steps, from Step (3), to insert additional terminal specific service application records.
12. Click the **Edit** icon on a record to be modified, make the required changes and again click **Save**; click the **Delete** icon of a record to remove the record.
13. Click **Save** to save the **Subscriber Service Plan Component**, and return to the **Terminal Service Plan** tab.
14. Click **Save and Close** to save the terminal configuration, or click **Save** to continue in the modify mode with *Add Terminal — Advanced Configuration*.

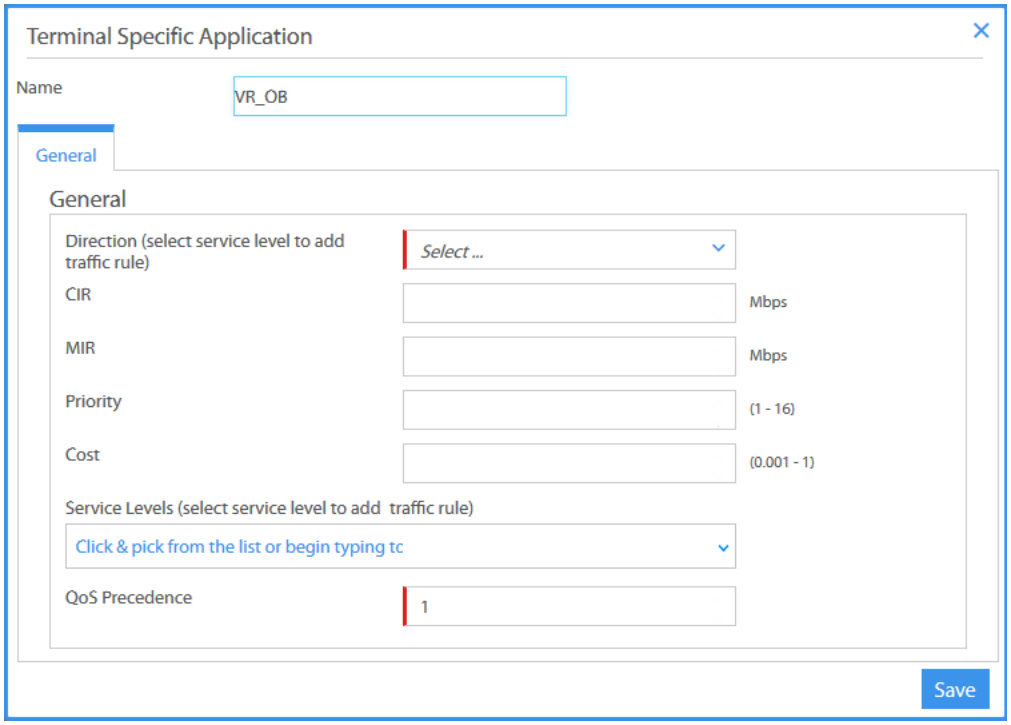

Figure 5-19. Terminal SSPC — Terminal Specific Application Dialog

5.13 Add Terminal — Advanced Configuration

The Satellite Terminal **Advanced Configuration** tab consists of three configuration components, as listed below:

- Terminal Information — Defining general parameters for the terminal
- Terminal Access Bitmask — Defining the terminal access class value

5.13.0.1 Terminal Information

Using the Terminal **Information** tab, the Satellite Terminal can be configured for specific behavior with respect to acquisition and authentication.

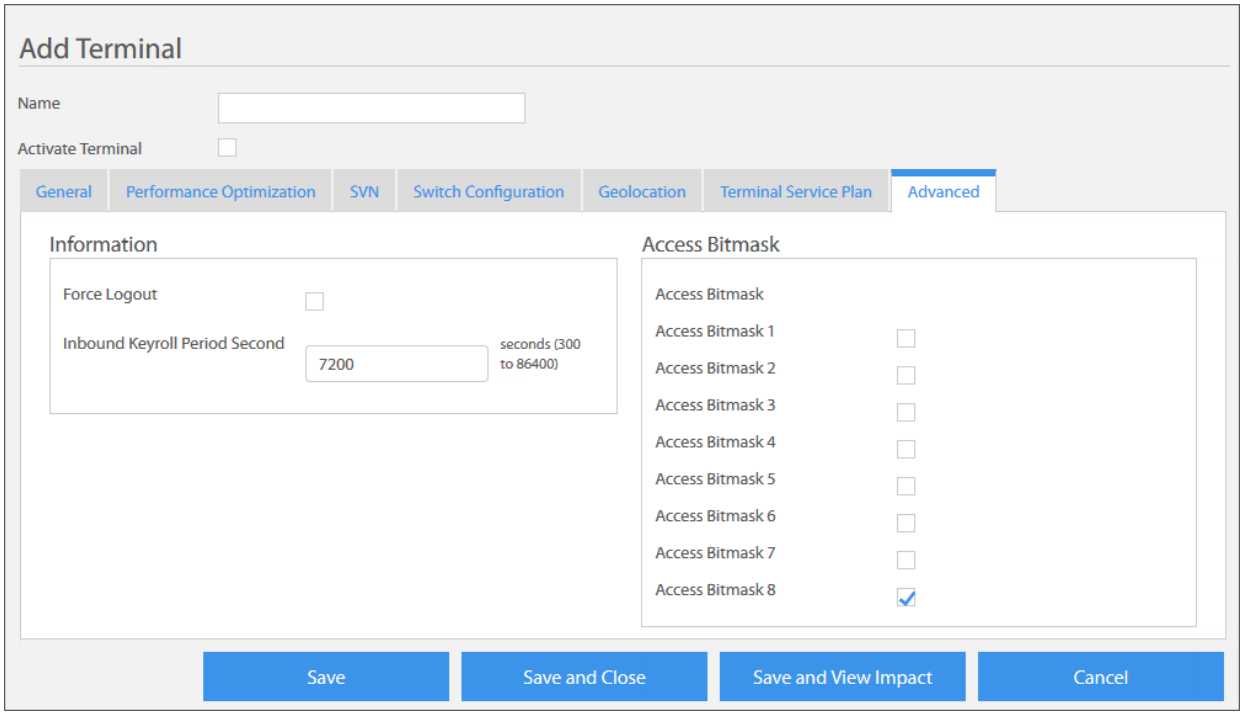

Figure 5-20. Add Terminal Advanced Tab - Access Bitmask Dialog

To define a Satellite Terminal access value:

1. From the **Add Terminal** page click the **Advanced Configuration** tab.
2. Select **Forced Logout** if the this terminal should be forced from the network based on the severity of a terminal identification mismatch.
3. In **Inbound Keyroll Period Second**, use the default value of 2 hours (7200), or enter a value in seconds that represents the period at which the Key Roll process is initiated.
4. Click **Save** and Close or click Save to continue in the Modify mode.

5.13.0.2 Defining the Terminal Access Class Value

Each Satellite Terminal has an *access class value* that is used during acquisition to control whether it is allowed or denied access to a specific iNet — particularly during periods of high demand. Assignment of access classes to a terminal is applied by the Primary Service Provider.

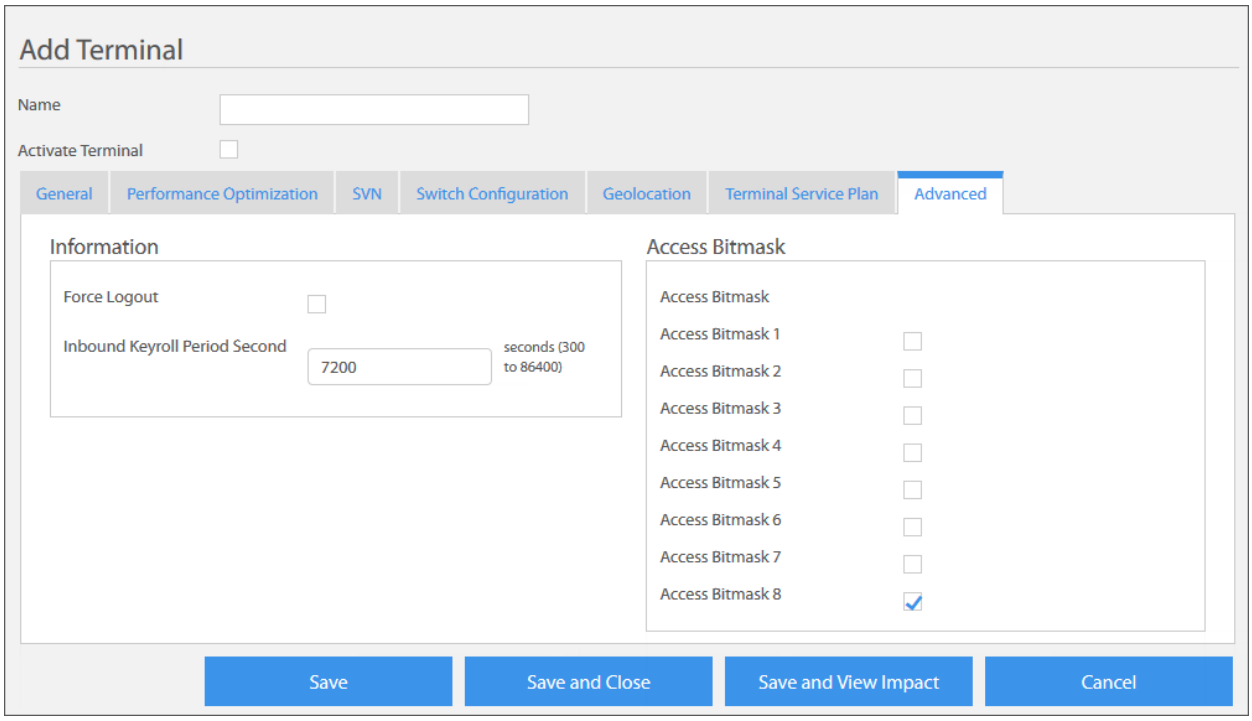

Figure 5-21. Add Terminal Advanced Tab - Access Bitmask Dialog

The access class value is composed of eight bits, where the most significant bit is reserved. By default, the access class of each terminal when it is created is "1" or 00000001_2. This arrangement allows for up to 7 different access classes that may be assigned to a terminal. A terminal may be assigned one or more access classes, where each class is represented by one of the 7 available bits. The value of the assigned access classes, is stored in the terminal configuration file as a decimal value, which can range from 1-127.

An access class value is also defined at the iNet or channel level, for each iNet. During the Satellite Terminal acquisition, the iNet's access class value is logically combined with the terminal access class value, using the AND operation. If the result is non-zero the Satellite Terminal is allowed into the channel. If a terminal access class is manually changed to 00000000_2, the Terminal is excluded from acquiring into any network.

To define a Satellite Terminal access value:

1. From the **Add Terminal** page click the **Advanced Configuration** tab.
2. According to access classes to be assigned to this terminal, check mark or uncheck an **Access Bit Mask** number to enable/disable a specific access class. A checked Access Bit Mask number is '1'; an unchecked Access Bit Mask number is '0'.
3. Click **Save** to save the configuration to the NMS.

5.14 Managing Terminal Authentication

The **Manage Terminal Authentication Token** operation, is used to create or generate a one-time use authentication token for one or more terminals. On an attempt to authenticate into the network, the terminal must use the assigned token. Tokens may be created for a single terminal or multiple terminals simultaneously, and may be automatically generated or entered manually by an authorized NMS user.

Once a terminal authenticates, it appears listed by **Terminal Name**, **Terminal DID**, and the **Status** shows as "Authenticated."

In case a terminal authentication token is ever compromised, a new token can be re-issued, which the terminal will use on the next authentication attempt.

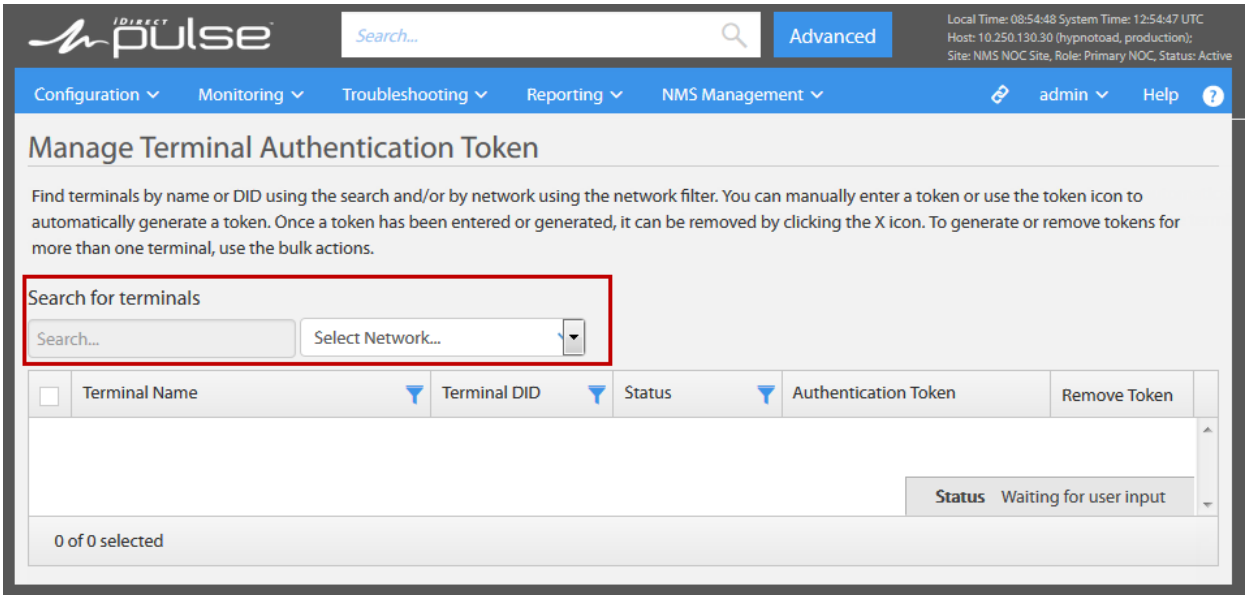

Figure 5-22. Manage Terminal Authentication Dialog

To create an authentication key for a single terminal:

1. Click the **NMS Management** tab > **Manage Terminal Authentication**.
2. Use the **Select Network** drop-down to select the network to which the terminals are associated. The terminals found in the NMS, under this network, are returned.
3. To specify one time token for use by a single terminal select the desired terminal and do one of the following:
   a. Click the **Generate Key** icon to automatically populate the **Authentication Key** field with a 156-bit key (64 HEX characters); or use the following as an alternative:
   b. In the **Authentication Key** field, manually enter a Hex string of 64 characters maximum or an ASCII string of 32 characters maximum. For example iDirect123.
4. Click the **Remove Key** icon to remove the terminal authentication key at any time.
5. Click **Save**. A green message indicates that the token was created successfully.

To create an authentication key for multiple terminals:

1. Click the **NMS Management** tab > **Manage Terminal Authentication**.
2. Use the **Select Pulse Network** drop-down to select the network to which the terminals are associated. The terminals found in the NMS, under this network, are listed in a browse like window.
3. To specify a one time common token for use by multiple terminals select the desired terminals and do one of the following:
   a. Click the **Generate Key** icon adjacent to the **Bulk Actions** field to populate the **Authentication Key** field of the selected terminals with the common generated key.
   b. In the **Bulk Action** field, manually enter a Hex string of 64 characters maximum or an ASCII string of 32 characters maximum - for example iDirect123; then click the adjacent **Generate Key** icon.
4. Click the **Remove Key** in-line with a terminal to remove the terminal authentication key; or click the **Remove Key** adjacent to the **Bulk Action** field to remove the terminal authentication key for several selected terminals.
5. Click **Save**. A green message indicate that the token was created successfully.

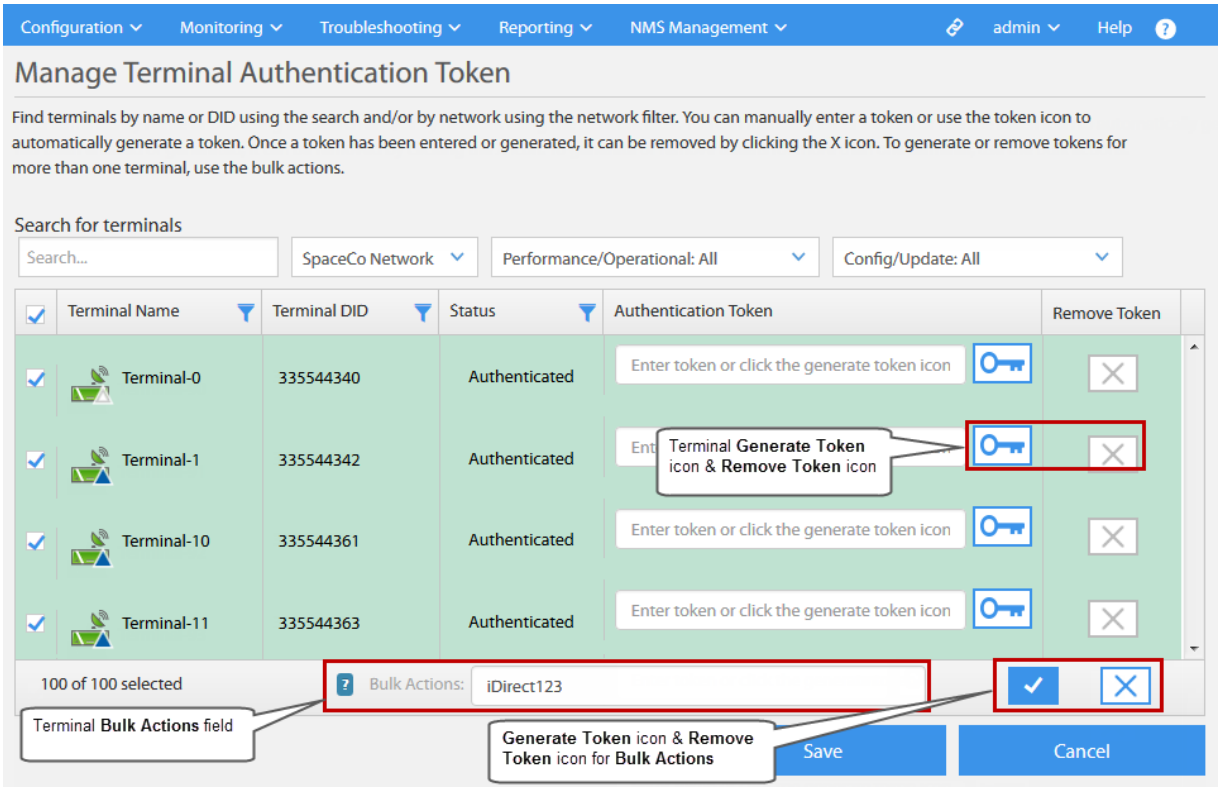

Figure 5-23. Manage Terminal Authentication Dialog

5.15 Terminal Element Browse Actions

Using the Pulse **Browse Terminal Elements** command, users can interact with configured Satellite Terminals and SSPP Components to perform a variety of specific operations. These operations are called “actions.” An action can be performed on a single element, using the **Action** button for that element, or simultaneously on multiple selected elements, by using the browse window **Group Actions** button.

Only the actions which are possible, based on the element type, are displayed when an element type is selected. All actions are not possible with all elements.

The Terminal Domain element actions are listed and briefly described as follows:

Table 5-2. Terminal Domain — +Browse Actions

Action	Applicable Elements	Brief Description
View Details	Terminals, and SSPP Components	View configured information for the selected Satellite Terminal.
Copy	Satellite Terminals, and SSPP Components	Create a cloned copy of the selected Satellite Terminal, and save as a new Satellite Terminal.
Modify	Satellite Terminals	Modify the configured information for the selected Satellite Terminal, and re-submit with changes.
Delete	Satellite Terminals	Remove the selected Terminal from the NMS database.
Apply Configuration	Satellite Terminals, and SSPP Components	Apply configured NMS changes to the selected Satellite Terminal, using the pending option file configured for the selected terminal.
Retrieve Pending Option File	Satellite Terminals, and SSPP Components	Load from the NMS database, an‘-+++++++d display the pending copy of the options file for the selected terminal.
Retrieve Active Option File	Satellite Terminals, and SSPP Components	Load and display the options file currently active in the selected Satellite Terminal.
Compare Configurations	Satellite Terminals, and SSPP Components	Compare the pending options file and the active options file for the selected Satellite Terminal.
Modify Engineering Debug Keys	Satellite Terminals, and SSPP Components	Modify custom key associated with a specific feature to enable or disable, add or modify functionality.
Manage Software Version	Satellite Terminals	View software packages available the on NMS, and install appropriate software package as required.
Manage Blob File	Satellite Terminals	View software BLOB files available on the NMS, and install appropriate BLOB as required.
Progress Report	Satellite Terminals, and SSPP Components	View a summary of update manager progress after applying changes to the selected element.

6 Configuring Terminal SVNs

In an iDirect Velocity network, the *Terminal SVN* provide IP connectivity between each Terminal LAN and the Velocity hub system. The terminal SVN represents that segment of the SVN that is located in the remote network behind a Satellite Terminal.

The following topics briefly introduces satellite terminal SVNs and provides step-by-step procedures for configuring the various SVN components.

6.1 About Configuring a Terminal SVN

NMS tools for creating and accessing existing Terminal SVNs are accessed from the **SVN** tab of the **Add Terminal** configuration page.

Satellite Terminals support a wide range of configurations, including IP addressing schemes, routing protocols; and many configurable SVN parameters that are defined on a per SVN basis for each Satellite Terminal. The first step in configuring terminal SVNs is to assign one or more SVNs to the terminal. After an SVN is assigned to the terminal it can then be configured using the following sub-tabs.

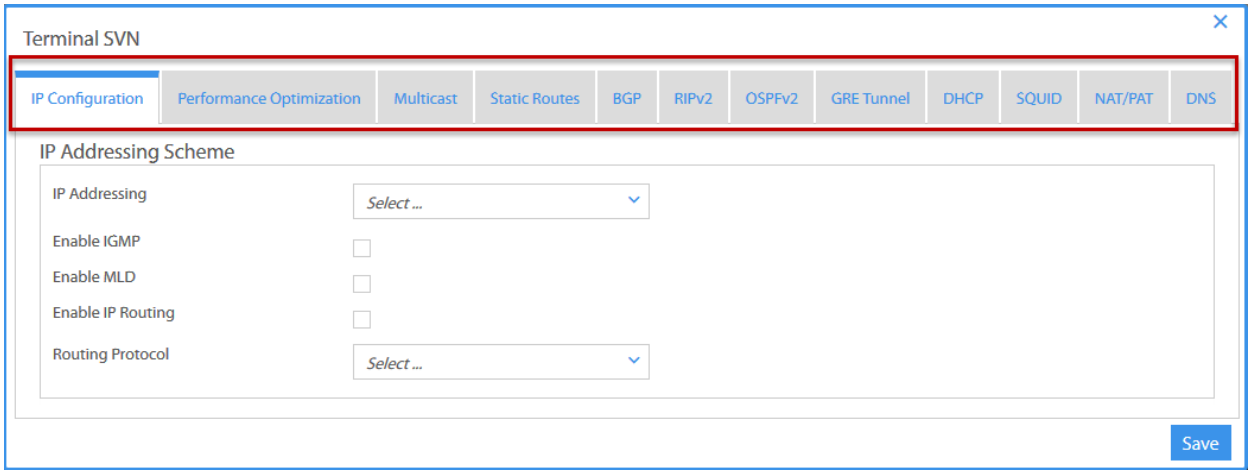

Figure 6-1. Add Terminal — SVN Configuration Tabs

- IP Address Configuration
- Performance Optimization
- Multicast Configuration
- Static Routes Configuration
- BGP Routing Configuration
- RIPv2 Routing Configuration
- GRE Tunnel Configuration
- DHCP Configuration
- Squid Configuration
- NAT/PAT Configuration
- DNS Configuration

6.2 Adding Terminal SVN Assignments

Prior to configuring any of the SVN configuration pages, the SVN must first be assigned to the Satellite Terminal. Up to 12 SVNs may be configured for a terminal, from the **SVN** tab.

An SVN is assigned to a terminal using the **Terminal SVN** dialog, from which SVNs that are already configured in the NMS may be assigned to the terminal. The presented SVN list represents those SVNs that have already been configured in the NMS. Once an SVN is assigned to the terminal, it can then be configured.

The iDirect Velocity Satellite terminal SVN configuration supports the following operations:

- Assign and configure up to 12 unique SVN definitions per Satellite Terminal
- Assign and configure 1 SVN dedicated to the NMS administrative (**Admin**) traffic
- Assign and configure up to 11 active SVNs dedicated to user traffic

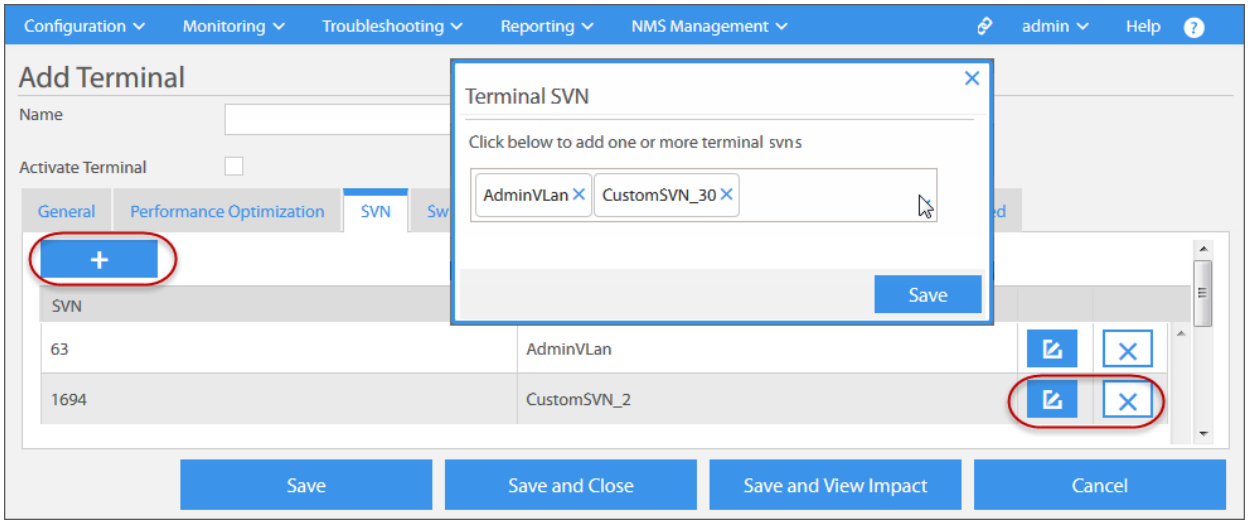

Figure 6-2. Add Terminal — SVN Tab and Terminal SVN Select Dialog

To assign a Satellite Terminal SVN:

1. Click the **SVN** tab on the **Add Terminal** page.
2. Click the **Add Record** icon, to select one or more SVNs to add to the configuration. The **Terminal SVN** select dialog opens.
3. Click the drop-down and select up to 12 SVNs to assign to the Satellite Terminal. The **Management** SVN (**Admin**) must be assigned to each Satellite Terminal.
4. Click **Save** to accept the selected terminal SVNs and return to the **SVN** tab. The selected SVNs are listed as individual records, by **SVN** number and **Name**.
5. Click the **Edit** icon on an SVN record to configure the SVN; click the **Delete** icon to remove an SVN from the list.
6. Click **Save and Close** or click **Save** to continue with SVN configuration.

6.3 Terminal SVN IP Addressing

IP addresses for the two SVN interfaces of a terminal are configured from the IP Configuration tab of the Terminal SVN page. The **ETH0,** or *LAN interface*, is the Ethernet interface to the terminal LAN; and **SAT0** is the terminal *satellite interface*. The **SAT0** interface is also called the *management interface,* when referring to the Admin SVN. SAT0 is always configured by the operator.

The **IP Configuration** tab supports **Static Addressing**, whereby IP addresses are operator configured for the **SAT0** and **ETH0** interfaces; or **Radius addressing**, in which case **SAT0** is still operator configured and the same whether using static or radius addressing.

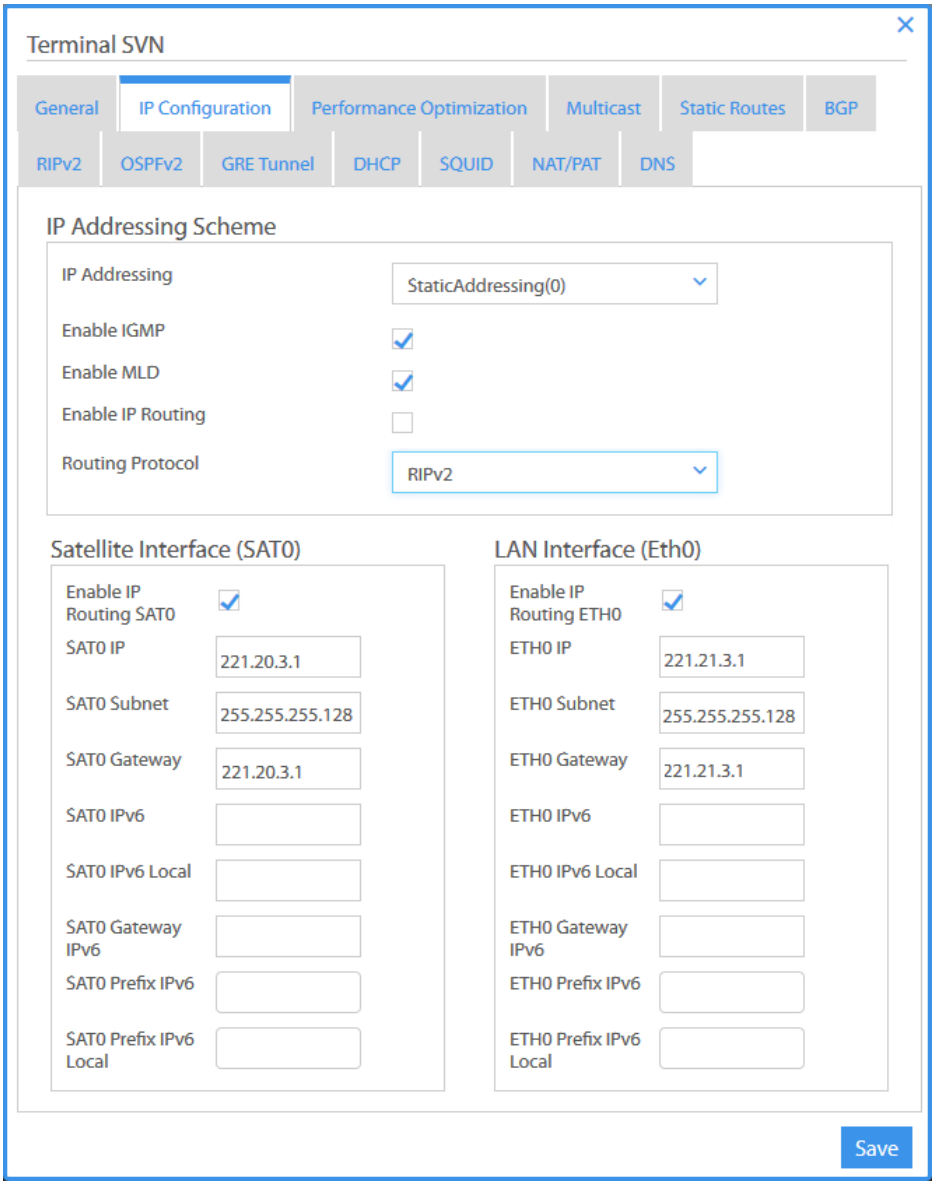

Figure 6-3. Terminal SVN — Static IP Addressing Parameters Dialog

To configure the Satellite Terminal SVN for Static IP Addressing:

1. Click the **Edit** icon on an assigned SVN for which static IP address parameters are to be configured. The SVN configuration dialog opens to the **IP Configuration** tab.
2. Under **IP Addressing Scheme**, use the **IP Addressing** drop-down and select the desired addressing method (Radius addressing only applies to ETH0):
3. Select **Enable IGMP** (Internet Group Management Protocol), if applicable, to allow the terminal and adjacent routers to establish IPv4 multicast group memberships.
4. Select **Enable MLD** (Multicast Listener Discovery), if applicable, to allow this terminal and adjacent routers to establish IPv6 multicast group memberships.
5. Select **Enable IP Routing** to enable this option on the SVN.
6. Select the applicable **Routing Protocol**, using the drop-down.
7. Use the following procedure to configure **SAT0 IP addressing**:
   a. Select **Enable IP Routing SAT0**.
   b. If applicable, enter IPv4 addresses using **SAT0 IP**, **SAT0 Subnet**, and **SAT0 Gateway.**
   c. If applicable, enter IPv6 addresses using **SAT0 IPv6**, **SAT0 IPv6 Local**, **SAT0 Gateway IPv6**; and enter prefixes using **SAT0 Prefix IPv6**, and **SAT0 Prefix IPv6 Local**.

NOTE: The SAT0 interface cofiguration is always operator configured, and is the same whether using Static addressing or Radius addressing.

8. For **Static Addressing**, use the following to configure the **LAN Interface ETH0**:
   a. Select **Enable IP Routing ETH0**.
   b. If applicable, enter IPv4 addresses using **ETH0 IP**, **ETH0 Subnet**, and **ETH0 Gateway.**
   c. If applicable, enter IPv6 addresses using **ETH0 IPv6**, **ETH0 IPv6 Local**, **ETH0 Gateway IPv6**; and enter prefixes using **ETH0 Prefix IPv6**, and **ETH0 Prefix IPv6 Local**.
9. For **Radius Addressing** use the following to configure the **LAN Interface ETH0**:
   a. Under the **Radius Configuration** dialog, select **Enable Radius**, to enable IP addressing to be requested by the RADIUS server on this SVN.
   b. Specify the **RADIUS Server Type** as **RoundRobin**, **LastKnown,** or **Fixed**.
   c. Enter an **ACK Timeout**, or use the default acknowledgment timeout value of 2 seconds.
   d. Enter an **AcctUpdate Time-out**, in seconds, or use the default value of 1800 seconds as the update timeout.
   e. Specify a **Disconnect Time-out**, in seconds, or use the default value of 1 second.
   f. Enter a **Send Limit** value, in seconds, or use the default value of 3 seconds.
10. Click **Save** to save the SVN **IP Configuration** and return to the **Add Terminal SVN** tab, or continue with *RADIUS Server IP Addresses and Shared Secret* configuration.

6.3.1 RADIUS Server IP Addresses and Shared Secret

With **RADIUS Addressing**, both IP addressing and authentication are dynamically handled by a RADIUS Server. The dialog for the Radius IP addressing supports configuration of the RADIUS Proxy process, which serves as a client on behalf of the Terminal to request IP addressing configuration on a per-SVN basis.

Up to four RADIUS Server IP Address records can be configured, and a **RADIUS Server Secret Key** can be defined. This secret is a shared by the proxy client and server.

Transactions between the RADIUS client and server are authenticated through the use of a shared secret that is never sent un-encrypted over the network. In addition, user passwords are encrypted between the RADIUS client and server to avoid being captured over an unsecured network.

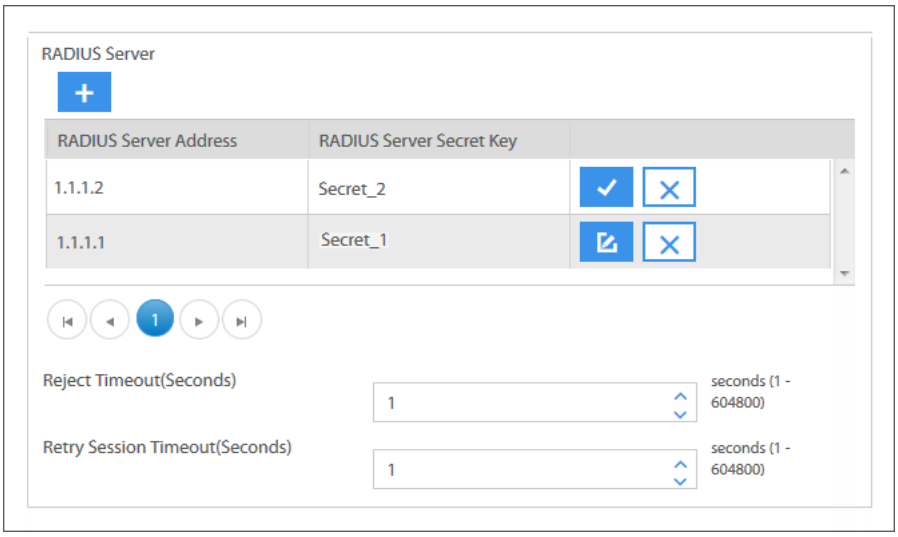

Figure 6-4. Terminal SVN — RADIUS Server IP Address and Secret Key Dialog

To configure the Satellite Terminal SVN RADIUS Server IP Addresses:

1. Click the **Add Record** icon, under the **Radius Server** section of the **Radius Configuration dialog**, to insert a Radius Server IP address record. The fields for entering a **RADIUS Server Address** and a **Radius Server Secret** are enabled.
2. Enter the **RADIUS Server Address**, as the IP address of the RADIUS server.
3. Enter a **RADIUS Server Secret Key**, as the shared secret between the NMS authenticator and the RADIUS server.
4. Click the **Update** icon to save the **RADIUS Server Address** record. The new entry is inserted as a new record, listed under **RADIUS Server**. Multiple records may be entered.
5. Repeat the previous steps to insert another **RADIUS Server Address** record for this SVN.
6. For a given **RADIUS Server Address** record, click the **Edit** icon to modify the record, and again click the **Update** icon. Click the **Delete** icon, to remove a record.
7. Click **Save** to save the **IP Configuration** and return to the **Add Terminal** page **SVN** tab.

6.4 Terminal SVN Performance Optimization

The terminal SVN **Performance Optimization** tab, presents a dialog that contains optimization parameters for **Transmit Properties**, **TCP Acceleration and Compression**, and **UDP** and **RTP Compression.** Each of the acceleration and compression sections must be enabled to allow the supported feature to be enabled and configured on a per-SVN basis.

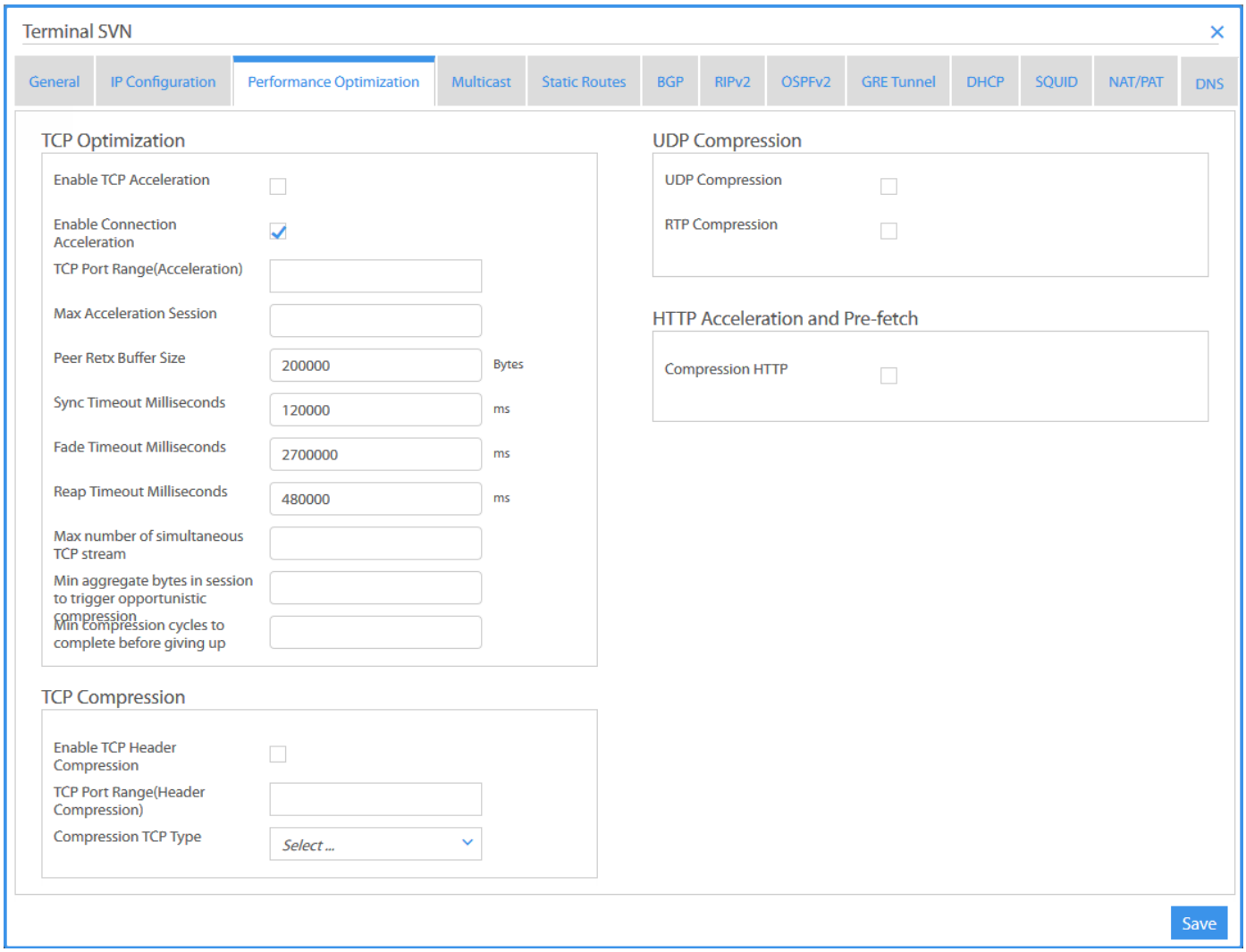

Figure 6-5. Terminal SVN — Performance Optimization Configuration Dialog

To configure Terminal SVN TCP Acceleration and Compression:

1. With the **SVN** tab selected, and with SVN records displayed, click the **Edit** icon on the assigned SVN for which **Performance Optimization** parameters are to be configured.
2. Click the **Performance Optimization** tab.
3. Select **Enable TCP Acceleration** to enable TCP traffic acceleration on this SVN.

4. Select **Enable Connection Acceleration** to enable TCP acceleration between the Satellite Terminal and the Teleport, for a specified port or port range.
5. In **TCP Port Range (Acceleration)**, use comma separation to specify port numbers to which acceleration should be applied. For example 2001, 2005; or use a hyphen to specify a port range — for example 2001-2003.
6. Use **Max. Acceleration Session** to specify the maximum number of TCP accelerated sessions allowed on this SVN. This value must be greater than 0.
7. Under the **TCP Compression** section, select **Enable TCP Compression** to enable TCP data compression on this SVN for a specified port or port range.
8. In **TCP Port Range (Compression)**, use comma separation to specify port numbers to which compression should be applied. For example enter 2001, 2005; or use a hyphen to specify a port range — for example 2001-2003.
9. Select **Enable TCP Header Compression** to enable the compression of the TCP header on this SVN for a specified port or port range.
10. Click **Save** to save the SVN **Performance Optimization** and close the **Terminal SVN** page.

To configure Terminal SVN UDP Compression:

1. Select **UDP Compression** to enable this option on the SVN. The fields are enabled.
2. Under the **UDP Compression** section, use the **UDP Compression Method** to select the header compression type as **None(0)** or no compression; as **ECRTP(1) —** enhanced compressed RTP or; or as **ROHC(2) —** RObust header compression.
3. In **UDP Port Range**, use comma separation to specify port numbers to which UDP compression should be applied. For example 2001, 2005; or use a hyphen to specify a port range — for example 2001-2003.
4. Click **Save** to save the SVN **Performance Optimization** and close the **Terminal SVN** page.

To configure Terminal SVN RTP Compression:

1. Select **RTP Compression** to enable this option on the SVN. The fields are enabled.
2. In **RTP Port Range**, use comma separation to enter one or more port numbers to which RTP compression should be applied. For example 2001, 2005; or use a hyphen to specify a port range — for example 2001-2003.
3. Select **UDP Payload Compression** to enable the compression of the TCP payload packets for the specified port or port range.
4. In **UDP Port Range Payload Compression**, use comma separation to specify port numbers — for example 2001, 2005; or use a hyphen to specify a range — for example 2001-2003.
5. Click **Save** to save the SVN **Performance Optimization** and close the **Terminal SVN** page.

6.5 Terminal SVN Multicast Configuration

The Velocity system supports downstream IPv4 multicasting within any SVN. Any customer equipment on the terminal network may subscribe to multicast streams in its SVNs.

The satellite router is an IGMP proxy and implements IGMPv3 and IGMPv2. For dynamic multicast, the satellite router software accepts IGMPv2 or IGMPv3 join and leave messages

from hosts on the terminal network, and requests the multicast streams on behalf of the hosts from the SAS site using IGMPv3. The PP also is an IGMPv3 proxy, and similarly requests the multicast streams from the upstream multicast source. The access router is expected to use Protocol Independent Multicast (PIM).

For static multicast streams, the network operator enters the multicast IP address of the streams into the satellite router configuration. After it enters the iNet, the satellite router generates IGMPv3 requests to the SAS site for those statically configured multicast IP addresses on behalf of the hosts on the terminal network..

From the Multicast Stream dialog, which is accessed from the SVN Multicast tab, one or more static multicast groups may be configured based on assigned permission.

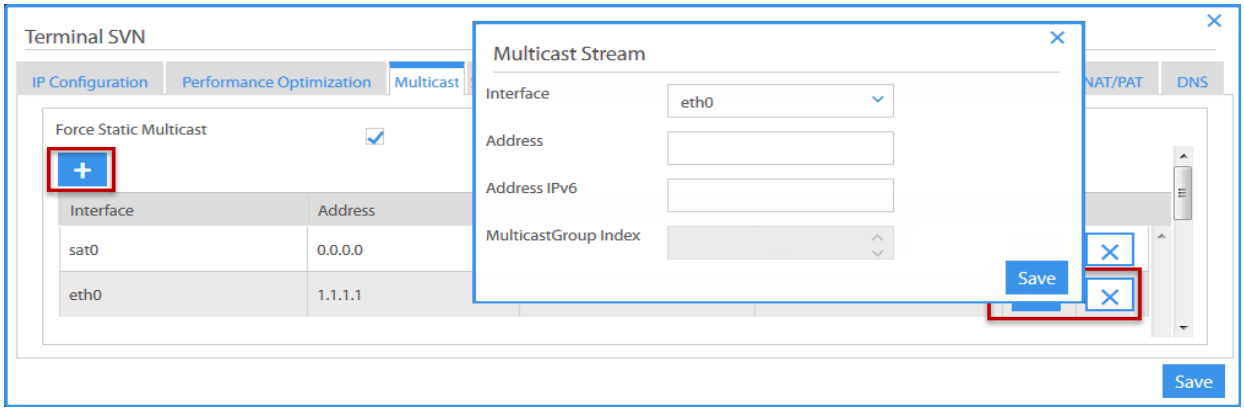

Figure 6-6. Terminal SVN — Multicast Stream Tab and Configuration Dialog

To configure the Satellite Terminal SVN TCP Multicast Stream parameters:

1. With the **SVN** configuration tab selected, and with SVN records displayed, click the **Edit** icon on the assigned SVN for which **Multicast** parameters are to be configured.
2. Click the **Multicast** tab.
3. Click the **Add Record** icon to open the **Multicast Stream** configuration dialog.
4. Use the **Interface** drop-down and select the **SAT0** or **ETH0** interface.
5. In the **Address** (IPv4) or the **Address (IPv6**) field, appropriately enter an **IPv4** or IPv6 multicast address for the multicast group.
6. Click **Save** to accept the **Multicast Stream** record. The new entry is inserted into the configuration as a new record, listed by **Interface** and **Address**.
7. Repeat the previous steps, to insert additional **Static Multicast** records.
8. Click the **Edit** icon on a **Static Multicast** record, to modify the record; click the **Delete** icon to remove the record.
9. Click **Save and Close** to save the terminal configuration, or click **Save** to continue in the modify mode with the Terminal SVN configuration.

6.6 Terminal SVN Static Routes Configuration

Static routes in a Velocity network may be defined on a per SVN, per satellite terminal basis, from the Static Routes tab of the Terminal SVN page. Each SVN supports configuration of IPv4 and IPV6 forwarding tables. Configured static routes, connected routes and learned routes are added to the per-SVN forwarding tables.

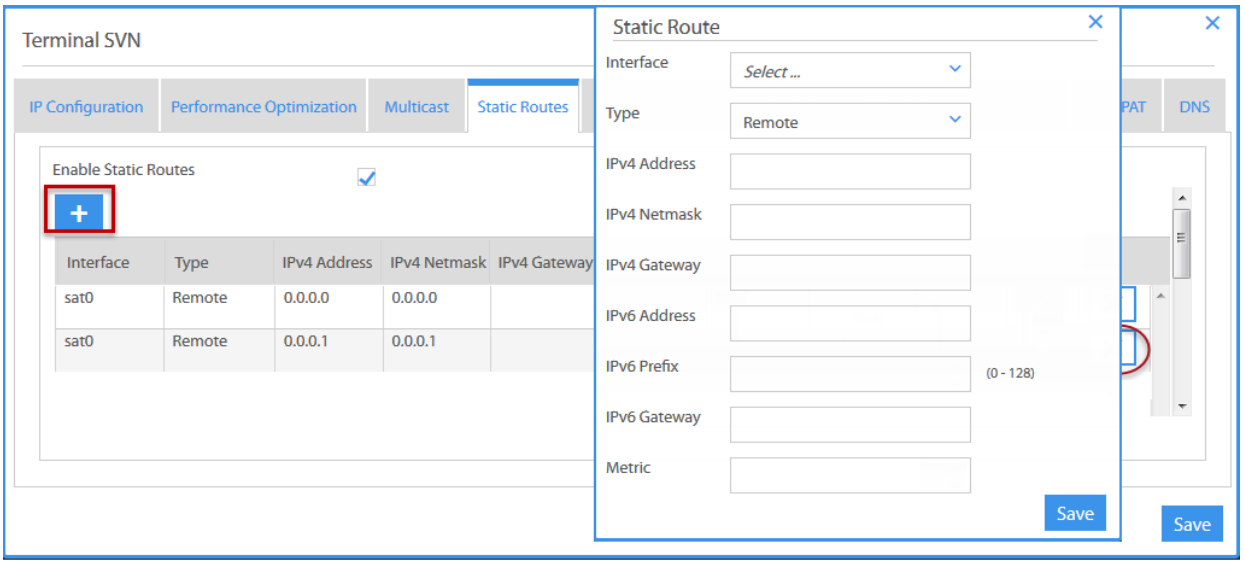

Figure 6-7. Terminal SVN — Static Routes Tab and Configuration Dialog

To configure the Satellite Terminal SVN Static Routes:

1. With the **SVN** configuration tab open, and with SVN records displayed, click the **Edit** icon on the SVN for which **Static Routes** are to be configured, and click the **Static Routes** tab.
2. Click the **Add Records** icon to open the **Static Route** configuration dialog (foreground).
3. Click the **Static Routes** tab, and select **Enable Static Routes** to enable the configuration.
4. Use the **Interface** drop-down and select either the **SAT0** or **ETH0** interface.
5. Use the **Type** drop-down and select the route type as **Hub**, if the **SAT0** interface was selected; and as **Remote**, if the **ETH0** interface was selected.
6. Enter an **IPv4 Address**, **IPv4 Netmask**, and **IPv4 Gateway** address for the static route, if applicable; or enter **IPv6 Address**, **IPv6 Prefix**, and **IPv6 Gateway** address, if applicable.
7. Use the **Metric** field to specify the number of hops to be used by this route.
8. Click **Save** to update the **Static Route** in memory and return to the Terminal SVN **Static Routes** tab. The Static Route is inserted as a new record, listed by **Interface** and **Type**. Each route is added either to the IPv4/IPv6 forwarding table.
9. Repeat the previous steps to insert another **Static Route** record.
10. Click the **Edit** icon to modify a record; and click the **Delete** icon to remove the record.
11. Click **Save** to save the **Static Routes** configuration and close the **Terminal SVN** page.

6.7 Terminal SVN BGP Configuration

The BGP tab is used to enable and configure parameters for the operation of the *Border Gateway Protocol (BGP)* routing on the terminal SVN. The BGP protocol option, by default is disabled, and is only available when it is enabled on the SVN.

BGP configuration starts with enabling the feature, specifying an Autonomous System (AS) number, and selecting the IP address family as IPV4, IPV6 or both. The BGP General parameters dialog is also used to enable and configure BGP Outbound Route Filtering options.

Also in this general dialog, it is possible to enable redistribution of specific route types into BGP. This feature allows BGP to learn or import routes from other routing protocols. Route redistribution options are disabled by default but may be enabled specifically to redistribute static and connected routes into BGP.

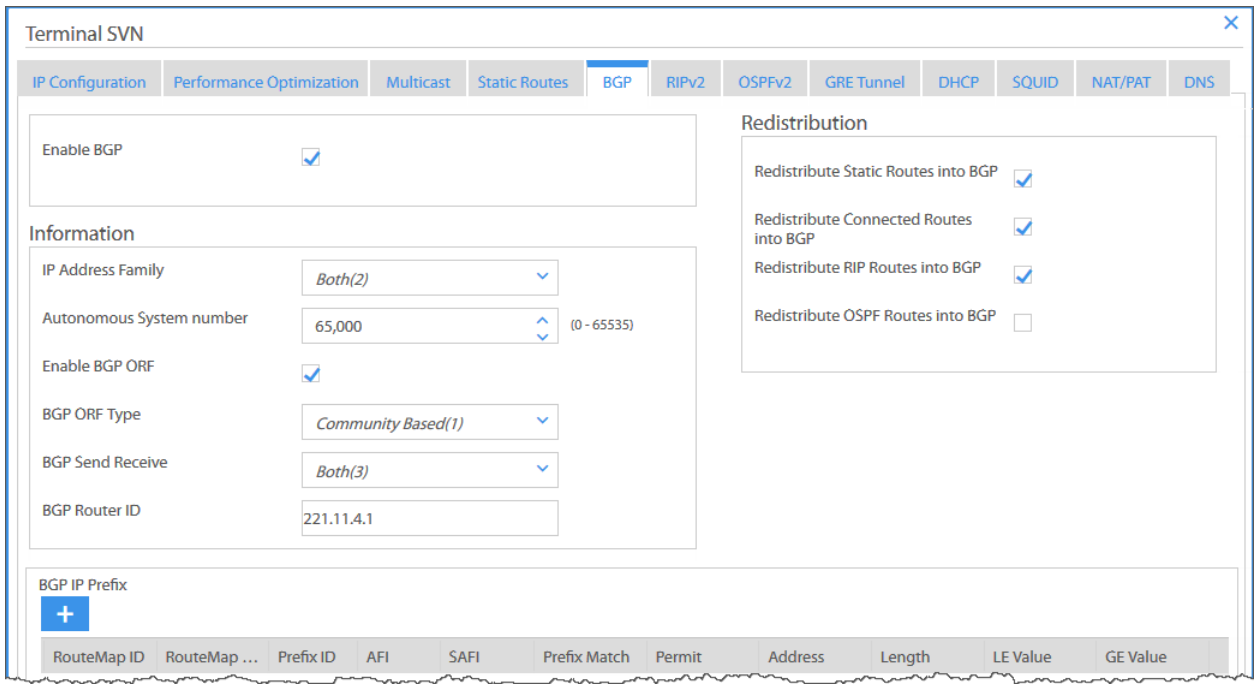

Figure 6-8. Terminal SVN — BGP General Parameters Dialog

In addition to the general parameters, the BGP tab provides access to BGP configuration dialogs for defining **BGP IP Prefix**, **BGP Peer, BGP Peer Group**, **BGP Configuration Table**, **BGP Aggregate Address**, and **BGP Router Map** records.

To configure Satellite Terminal SVN BGP General parameters:

1. With the **SVN** configuration tab open, and with SVN records displayed, click the **Edit** icon on the SVN for which **BGP** parameters are to be configured; and click the **BGP** tab.
2. Select **Enable BGP** to enable the BGP option on the SVN.
3. Under the **Information** section, use the **IP Address Family** drop-down and select **IPV4(0)**, **IPV6(1)**, or **Both(2)** to indicate the SVN supported IP address family.

4. Specify a unique value between 0-65535, as the **Autonomous System Number** (AS) for the terminal SVN interface. Although BGP is configured in each SVN, the AS must be the same for all SVNs configured on a terminal.
5. Select **Enable BGP ORF** to enable BGP Outbound Route Filtering on this SVN. The prefixes that should be received from BGP peers without local filtering must be specified.
6. Use the **BGP ORF Type** drop-down and select **Community Based(1)**, **Extended Community Based(2)**, or **Prefix Based(3)** as the ORF send/receive filtering method to minimize the number of BGP updates between BGP peers on this SVN.
7. Use the **BGP Send Recv** drop-down to select **Receive(1)**, **Send(2)**, or **Both(3)** to indicate if BGP ORF should be implemented to advertise the capability of send, receive, or both send and receive.
8. Enter the **BGP Router ID** for the Satellite Terminal on this SVN.
9. Under **Redistribution**, appropriately enable **Static Routes**, **Connected Routes**, or **RIP Routes** to indicate which route types to redistribute into BGP.
10. Click **Save** to return to the **Add Terminal** page or continue with the BGP configuration.

6.7.1 BGP IP Prefix Configuration

The *BGP IP Prefix list* is essentially a filter, which may be applied to a specific route map. Filtering by prefix list involves matching the prefixes of routes with those listed in a prefix list. When there is a match, the route is used or imported. Whether a prefix is accepted or denied is based upon the following rules:

- An empty prefix list permits all prefixes.
- A prefix is implicitly denied if it does not match any of the prefix list entries.
- A prefix match to multiple prefix list entries uses the longest, most specific match.

The router initiates the search at the top of the prefix list, with sequence number 1. Once a match or deny occurs, it does not continue with the remainder of the prefix list. To ensure search efficiency, the most common matches or denies should be placed at the top of the list.

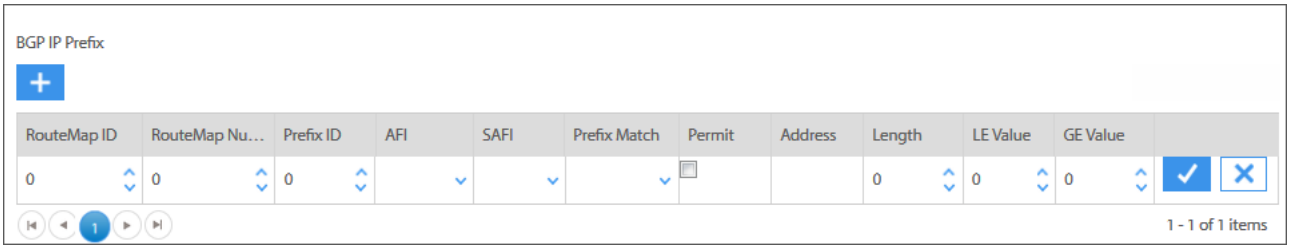

Figure 6-9. BGP IP Prefix Configuration Parameters

To configure Satellite terminal SVN BGP IP Prefix parameters:

1. With the **Terminal SVN** dialog open to the **BGP** tab, click the **Add Record** icon, under the **BGP IP Prefix** section, to define a new BGP IP Prefix record.
2. Use **RouteMap ID** to specify the index of the route map this prefix should use.

3. Enter a **RouteMap Number** that identifies the route map this prefix should use.
4. Use **Prefix ID** to specify the index of this prefix entry. This number is used to reference more than one filter per route map index.
5. Use the **AFI** drop-down to specify **IPv4(0)** or **IPv6(1)** as the Address Family Identifier of this prefix entry.
6. Use the **SAFI** drop-down, to enter the Subsequent Address Family Identifier of this prefix entry, as **MPLS_BGP_VPN(1)**, **Multicast(2)**, **Unicast(3)**, or **Both(0)**. This parameter supplies additional data on the type of the Network Layer Reachability Information that is carried in the prefix—for example, unicast forwarding or multicast forwarding.
7. Use the **Prefix Match** drop-down to select the match criteria to be used by the Route Map that belongs to this Prefix. Select **Match the NLRI Address(1)**, **Match the Source Address(2)**, or **Match the NextHop Address(3).**
8. Select **Permit** if this prefix is linked to a Route Map that has an ORF association and allows the entry to override the action of the Route Map.
9. In **Address**, enter a valid IPv4 address if **AFI** was specified as '0' or a valid IPv6 address if **AFI** was specified as '1'.
10. Use **Length** to specify the length of the prefix.
11. **Use LE Value** to specify the upper value of the range of the prefix length to be matched. **GE** and **LE** allow the range of the matching prefix length to be variable. The range is assumed to span from the **LE**-value to the address length of the family only if the **LE** attribute is specified. A specified **GE**-value and/or **LE**-value must be specified such that: len < GE-value <= LE-value <= address length of family.
12. **Use GE Value** to specify lower value of the range of the prefix length to be matched. **GE** and **LE** allow the range of the matching prefix length to be variable. The range is assumed to span from the GE-value to the address length of the family only if the **GE** attribute is specified. A specified **GE**-value and/or **LE**-value must be specified such that: len < GE-value <= LE-value <= address length of family.
13. Click the **Update** icon to save the **IP** prefix record. The new IP entry is inserted into the BGP configuration as a new record, listed under **BGP IP Prefix**.
14. Repeat the previous steps to insert another **BGP IP Prefix** record for this SVN.
15. For a given **BGP IP Prefix** record, click the **Edit** icon to modify the record, and again click the Update icon. Click the **Delete** icon, to remove the record.
16. Click **Save** to return to the **Add Terminal** page or continue with the BGP configuration.

NOTE: it is recommended that the number of BGP prefixes advertised to and received from BGP peers be controlled, using the maximum prefix and route filtering options to reduce memory usage and overall processing load.

6.7.2 BGP Peer Configuration

BGP Peers refer to any two routers that maintain a TCP connection, via BGP, for the purpose of exchanging BGP route table information. As these BGP peers are configured, they may be assigned to a previously configured BGP peer group.

To configure the Satellite Terminal SVN BGP Peer parameters:

1. With the **Terminal SVN** dialog open to the **BGP** tab, click the **Add Record** icon, under the **BGP Peer** section, to define a new BGP Peer record.
2. Designate this peer as an **LAN Peer** or an **OTA Peer** using the **BGP Peer Type** drop-down.
3. Use **Remote Address** to enter the IP address of the new BGP peer.
4. Use **Remote Port** to enter the port number on which this BGP peer connects.
5. In **Remote AS**, enter the AS number of the Remote BGP peer. If a value of "0" is entered, the hub will use the AS of the Satellite Terminal to configure a peer.
6. Use **ConfigTable ID** to enter the number that identifies the table where peer-specific BGP configuration items may be set for this peer.
7. Select **Hop Self** (set to TRUE), to indicate that this peer should advertise its own peer address as the next hop.
8. Select **Reflector Client** (set to TRUE), to cause the peer to act as a BGP route reflector.
9. In **Connect Retry** enter a time, in seconds, for which the PP can attempt to reconnect to this BGP peer.
10. In **Hold Time** enter a time, in seconds, after which the peer is declared dead if no keep-alive message is received by the protocol processor.
11. In **Keep Alive** enter a value, in seconds, in which a keep-alive message should be sent to the PP by this BGP peer. The range of this value is 0 to 65535; the default value is 60 seconds. A maximum value of 1/3 of the Hold Time value is recommended.
12. Enter a **PeerGroup ID** to identify the peer group to which this BGP peer is a member.
13. Select **Passive** to designate this peer as passive, and will only accept incoming connections. If disabled, the peer will attempt outbound connections in addition to accepting incoming connections.
14. Use **Max Router Peer** to specify the maximum number of prefixes that may be accepted from this peer.
15. Use the **DropWarn** drop-down to select **Drop(1)** if the peer should be dropped when the configured value for **Max Router Peer** is reached; or select **Warn(2)** if a warning should be set when the configured value for **Max Router Peer** is reached.
16. Use **MD5Auth Password** to enter the MD5 password for authentication of this peer. Leave blank if MD5 authentication is not in use.
17. Click the **Update** icon to save the **BGP Peer** record. The new entry is inserted into the BGP configuration as a new record, listed under **BGP Peer**.
18. Repeat the previous steps to insert another **BGP Peer** record for this SVN.
19. Click the **Edit** icon to modify a BGP Peer record, and again click the **Update** icon. Click the **Delete** icon to remove a record.

20. Click **Save** to return to the **Add Terminal** page or continue with the BGP configuration.

6.7.3 BGP Peer Group Configuration

A a *BGP Peer Group* is composed of member BGP peers that share common update policies, in order to simplify routing configuration and management. These common policies are applied to the group instead of to individual peers, to avoid configuration replication and to promote efficient updating. Instead of performing policy checks during updates to individual peers, the check take place once for the group, and is then sent to group members.

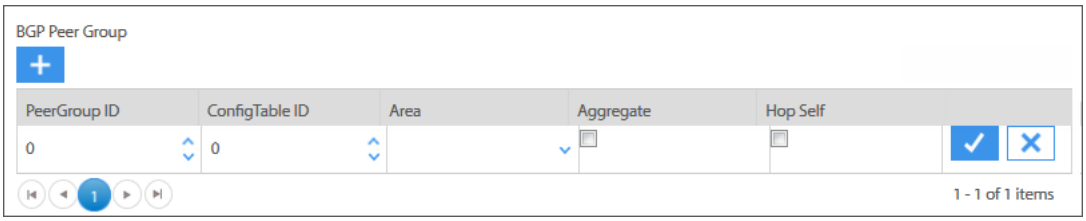

Figure 6-10. BGP Peer Group Configuration Parameters

Peer groups have the following requirements:

- A peer group must be identified as either internal, and having internal (iBGP) members; or as external, and having external (eBGP) members; or as a confederated BGP group, where two or more autonomous systems are combined as a single AS.
- Members of an external peer group have different autonomous system (AS) numbers.
- All members must share identical outbound announcement policies — for example, redistribute-list, filter-list, and route-map, except for default-originate, which is handled on a per-peer basis, even for peer group members.
- The inbound update policy for any group member may be customized.

To configure the Satellite Terminal SVN BGP Peer Group parameters:

1. With the **Terminal SVN** dialog open to the **BGP** tab, click the **Add Record** icon, under the **BGP Peer Group** section, to define a new BGP Peer Group record.
2. Enter a **PeerGroup ID** number that uniquely identifies the group.
3. Enter a **ConfigTable ID** that uniquely identifies the BGP configuration table used by this group, and where various peer-specific BGP configuration items may be set for the entire peer group. An entry of '0' indicates that there is no **Config Table** association.
4. Use the **Area** drop-down to designate the peer group membership type. **IBGP(1)** specifies internal members**; EBGP(2)** specifies external members; and **Confederated EBGP(3)** specifies confederated external members (a group of autonomous systems under a single AS designation).
5. Select **Aggregate**, to enable the aggregate-address or summarization option. This option is disabled by default, and member peers do not understand aggregated confederation AS_PATH information.
6. Select **Hop Self**, to indicate that the peer group should advertise itself as the next hop.

7. Click the **Update** icon to save the **BGP Peer Group** record. The new entry is inserted into the BGP configuration as a new record, listed under **BGP Peer** Group.
8. Repeat the previous steps to insert another **BGP Peer Group** record for this SVN.
9. For a given **BGP Peer Group** record, click the **Edit** icon to modify the record, and again click the Update icon. Click the **Delete** icon, to remove the record.
10. Click **Save** to return to the **Add Terminal** page or continue with the BGP configuration.

6.7.4 BGP Config Table Configuration

The *BGP configuration table* dialog supports the entry of one or more configuration records may be created, where each record contains a **ConfigTable ID**, an **Import Map ID**, an **Export Map ID**, an **Advertise Map ID**, and a **Non Exist Map ID**.

The Advertise-map specifies match statements that the route must pass before it is passed to the next route map; in the case of a Non-Exist-map, a route is not advertised unless a prefix in the BGP table does not match a prefix in the prefix lists.

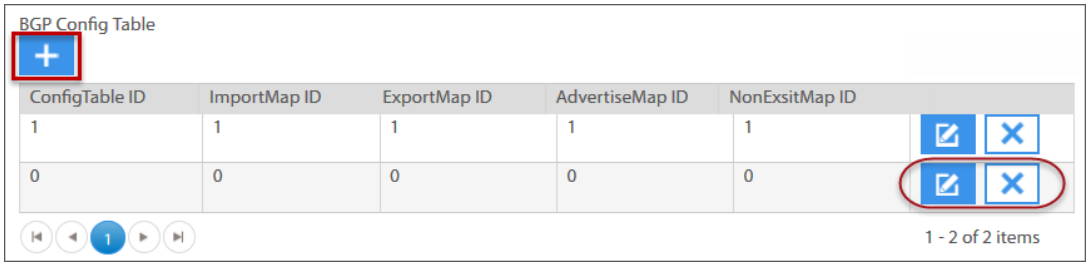

Figure 6-11. Add BGP Config Table Dialog/Records

To configure the Satellite Terminal SVN BGP Config Table parameters:

1. With the **Terminal SVN** dialog open to the **BGP** tab, click the **Add Record** icon, under the **BGP Peer Config Table** section, to define a new BGP Peer Group record.
2. Use **ConfigTable ID** to enter a numeric identifier for this configuration table.
3. Under **ImportMap ID**, enter an index that identifies a BGP map to use as the import map.
4. Under **ExportMap ID**, enter an index to identify a BGP map to use as the export map.
5. Under **AdvertiseMap ID**, enter an index that identifies a BGP route map to use as the advertise map. Both the **Advertise Map ID** and **Non-Exist Map ID** must be configured for the correct operation of the conditional advertisement feature.
6. Use **Non-ExistMap ID** to enter an index that identifies a BGP route map to use as a non-exist map. Both the **Advertise Map ID** and **Non-Exist Map ID** must be configured for the conditional advertisement feature to function correctly.
7. Click the **Update** icon to save the **BGP Config Table** record. The new entry is inserted into the configuration as a new record, listed under **BGP Config Table**.
8. Repeat the previous steps to insert another **BGP Config Table** record for this SVN.
9. For a given **BGP Config Table** record, click the **Edit** icon to modify the record, and again click the Update icon. Click the **Delete** icon, to remove the record.

10. Click **Save** to return to the **Add Terminal** page or continue with the BGP configuration.

6.7.5 BGP Aggregate Address Configuration

By configuring a BGP *aggregate-address,* a number of IP addresses can be replaced with a single address that represents a set of included addresses. The aggregate is used to simplify and minimize the size of routing tables. Aggregate networks are configured before being advertised to external peers.

The router's IP routing table must contain networks that represent a subset of the aggregate in order for the aggregate to be advertised; only the aggregate, and not the individual routes, are advertised to external BGP peers. Internal BGP peers receive the individual routes if they originated outside the AS; and do not exchange internal routes via BGP.

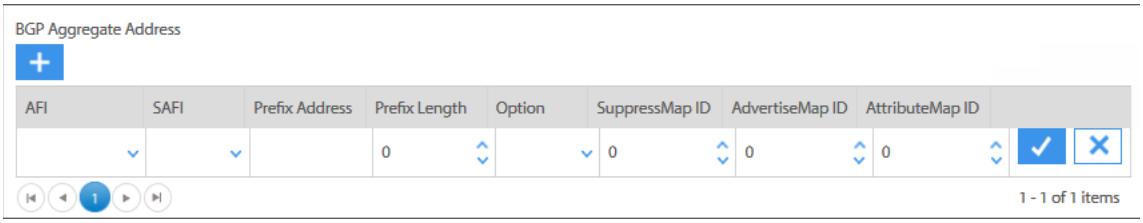

Figure 6-12. Satellite Terminal SVN BGP Aggregate Configuration Parameters

To configure the Satellite Terminal SVN BGP Aggregate Address parameters:

1. With the **Terminal SVN** dialog open to the **BGP** tab, click the **Add Record** icon, under the **BGP Aggregate Address** section, to define a new Aggregate Address.
2. Use the **AFI** drop-down to specify **IPv4** or **IPv6** as the Address Family of this aggregate address record.
3. Use the **SAFI** drop-down, to enter the Subsequent AFI of this aggregate address, as **MPLS_BGP_VPN(1)**, **Multicast(2)**, **Unicast(3)**, or **Both**. This parameter supplies additional data on the type of the Network Layer Reachability Information that is carried in the prefix—for example, unicast forwarding or multicast forwarding.
4. Under **Prefix Address,** enter the prefix address of this Aggregate Address.
5. Under **Prefix Length**, enter the length of the prefix of this Aggregate Address.
6. Use the **Option** drop-down to select one of the options to be applied to the configured Aggregate Address. If **None (1)** is chosen, more specific routes are installed in the routing table, but the AS_PATH will lose information as it no longer contains AS_SETs.
7. Use **SuppressMap ID** to specify the index of the Route Map used to suppress routes. The match clauses of this Route Map are used to selectively suppress specific routes from being advertised. No entry should be made if the **Option** field is configured with either **Summary(2)** or **Summary with AS Set(4)**.
8. Use **Advertise Map ID** to specify the index of the Route Map used to advertise routes. The match clauses of this Route Map are used to select routes which, although they match the aggregate address, they should not be aggregated.

9. Use **Attribute Map ID** to specify the index of the Route Map used to set the attributes of aggregated routes. The set clauses of this Route Map are use to set the path attributes of the aggregated route.
10. Click the **Update** icon to save the **BGP Aggregate Address** record. The new entry is inserted into the configuration as a new record, listed under **BGP Aggregate Address**.
11. Repeat the previous steps to insert another **BGP Aggregate Address** record for this SVN.
12. For a given **BGP Aggregate Address** record, click the **Edit** icon to modify the record, and again click the Update icon. Click the **Delete** icon, to remove the record.
13. Click **Save** to return to the **Add Terminal** page or continue with the BGP configuration.

6.7.6 BGP Route Map Configuration

A *route map* defines the routing policies that are considered before a router examines its forwarding table. The BGP route map configuration is, therefore, a way of defining specific routing policy that takes precedence over the different route processes. In other words, these policies support the filtering of the routing updates that are forwarded by BGP.

To configure the Satellite Terminal SVN BGP Route Map parameters:

1. With the **Terminal SVN** dialog open to the **BGP** tab, click the **Add Record** icon, under the **BGP Route Map** section, to define a new BGP Route Map record for this Terminal SVN.
2. Enter an alphanumeric **RouterMap ID** that identifies the new Route Map, which is used by BGP neighbors to reference the Route Map.
3. Enter the **Router Map Number** that identifies a secondary index of this Route Map entry, which is used to reference more than one filter per Route Map index.
4. Select **Permit** to enable the action that is applied to a route that matches the route map entry. This parameter is ignored for a Route Map used for aggregation.
5. Use the **ORF Association** drop-down to choose the type of association, if any, this route map has with the Outbound Route Filtering (ORF) protocol. Specify **Local (1)** if the filtering information contained in this route map is advertised to peers with appropriate ORF support; specify **Remote (2)** if this route map is created to respond to ORF(s) received from a peer; otherwise choose **None(0)**.
6. In **Continue**, enter a value to indicate the Route Map clause at which processing should continue. The entry is only valid for Route Maps of permit type and used for policy filtering.
7. Use the **AFI** (Address Family Identifier) drop-down to select the address index as **IPv4(0)** or **IPv6(1)**, to match against the AFI type.
8. Use the **SAFI** drop-down, to enter the *Subsequent Address Family Identifier* of this prefix entry, as **MPLS_BGP_VPN(1)**, **Multicast(2)**, **Unicast(3)**, or **(None (0)**, to match against the AFI type.
9. In **MaMed**, enter a value that the *Multiple Exit Discriminator* attribute must match.
10. In **MaAs-Path**, enter the regular expression to use when matching the "**AS-Path**" for a route. "**AS**" numbers are matched as decimal numbers.
11. In **MaCommunity**, use one of the following entries:

g. **If representing non-ORF entries:** enter the regular expression to use when matching elements of the *Community* list for a route.

h. **If representing ORF entries:** enter a comma separated list of communities that are logically "OR-ed" when matching.

12. In **MaExCommunity**, use one of the following entries:

    i. **If representing non-ORF entries:** enter the regular expression to use when matching elements of the *Extended Community* list for a route.

    j. **If representing ORF entries:** enter a comma separated list of extended communities that are logically "OR-ed" together when matching.

13. In **SeMed**, enter a value to which the *Multi Exit Discriminator (MED)* is set, if there is a match. A value of '0' indicates that the **MED** should be removed.

14. Use the **SeCommunity Action** drop-down to select the action to be taken on the Community List if this Route Map matches the route.

15. In **SeCommunity**, enter the regular expression to use when executing the action specified by the **SeCommunity Action** parameter.

16. Use the **SeExCommunity Action** drop-down to select the action to be taken on the Extended Community list if this Route Map matches the route.

17. In **SeExCommunity**, enter the regular expression to use when executing the action specified by the **SeExCommunity Action** parameter.

18. In **SeAsTimes**, enter the number of times the AS number is prefixed to the AS path if there is a match. This value is only valid if the Route Map is used for exporting routes, or for setting attributes for an aggregate route for which the AS_SET option is not set.

19. Use the **SeAs Action** drop-down to select the action taken by the **SeAsTimes** parameter, when this parameter is configured with **SET(1)** or **REM_MATCH_AND_SET(3)** as updating attributes. Other options include **IGNORE(0)** and **REM_MATCH(2)**.

20. In **Se Local Pref**, enter the local preference value to set when a route match occurs.

21. Use the **SeOrigin**, drop-down to select the origin value to set if there is a match. The options include **IBGP(0)**, **EBGP(1)**, or **Incomplete(2)**.

22. In **Se Weight**, enter the weighted value to assign to a path if there is a match.

23. In **SNR Metric Router Map Index**, enter the Route Map index for the SNR metric.

24. In **Se NextHop** enter the value to set for the Next Hop if a match occurs. If the value is set, then the match **AFI** and **SAFI** fields must also be set appropriately to ensure that the address type is being set appropriately to IPv4 or IPv6.

25. Click the **Update** icon to save the **BGP Route Map** record. The new entry is inserted into the configuration as a new record, listed under **BGP Route Map**.

26. Repeat the previous steps to insert another **BGP Route Map** record for this Terminal SVN.

27. For a given **BGP Route Map** record, click the **Edit** icon to modify the record, and again click the **Update** icon. Click the **Delete** icon, to remove the record.

28. Click **Save** to return to the **Add Terminal** page or continue with the BGP configuration.

6.8 Terminal SVN GRE Tunnel Configuration

Each Satellite Terminal can be configured with one or more GRE encapsulation tunnels per SVN. A configured GRE tunnel is only established within the iDirect system, for the designated SVN. GRE endpoints must be established upstream from the Protocol Processor and downstream from the Satellite Terminal. IP addresses for tunnel endpoints of both the Local-side and Hub-side may be configured for IPv4 or IPv6 independently.

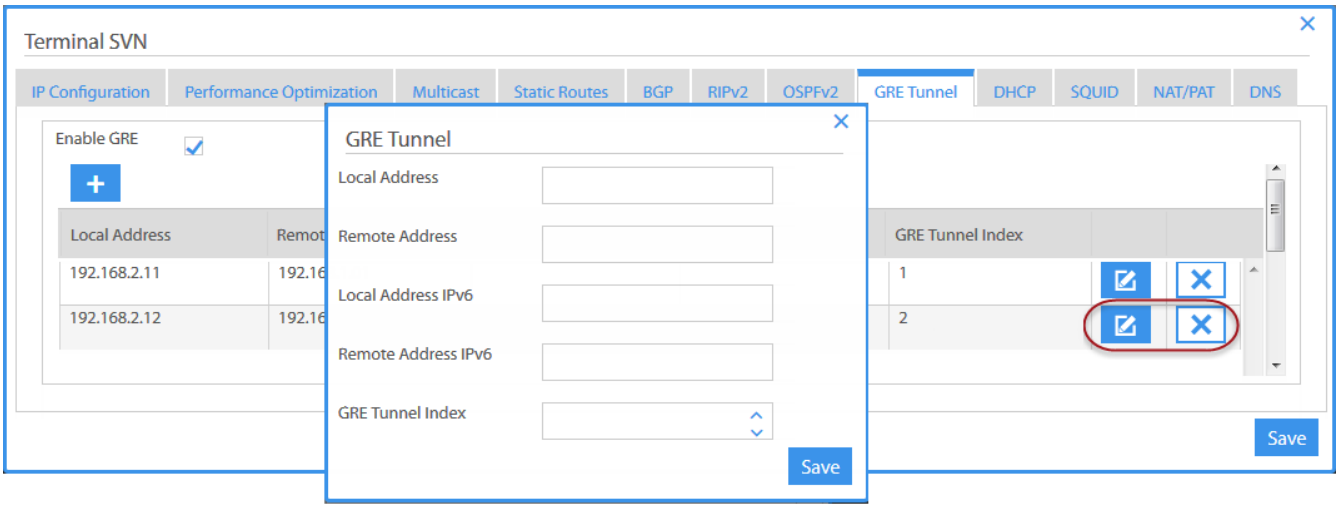

Figure 6-13. Terminal SVN: GRE Tunnel Configuration Tab/GRE Tunnel Dialog

To configure the Satellite Terminal SVN GRE Tunnels:

1. With the **SVN** configuration tab open, and with SVN records displayed, click the **Edit** icon on the SVN for which **GRE Tunnel** parameters are to be configured, and click the **GRE Tunnel** tab. The **GRE Tunnel** dialog opens.
2. Select **Enable GRE** to enable the feature on the terminal SVN.
3. Click the **Add Record** icon to open the **GRE Tunnel** dialog, and to configure a GRE Tunnel record for this SVN configuration.
4. Use **Local Address** and **Remote Address** to enter the Hub Gateway node address and the terminal node address respectively, to establish the IPv4 tunnel endpoints.
5. Use **Local Address IPv6** and **Remote Address IPv6** to enter the Hub Gateway node and the terminal node address respectively, to establish the IPv6 tunnel endpoints.
6. Enter a **GRE Tunnel Index** value to associate with this GRE tunnel record.
7. Click **Save** to accept the GRE tunnel record in memory, and to return to GRE Tunnel tab. The new GRE tunnel is inserted as a new record.
8. Repeat the previous procedure to insert additional GRE Tunnel records.
9. To modify a **GRE Tunnel** record, click the **Edit** icon, make the required changes, and again click **Save**; click the **Delete** icon to remove a record.
10. Click **Save** to close the **Terminal SVN** dialog and return to the **SVN** tab, or with the terminal SVN configuration.

6.9 Terminal SVN DHCP Configuration

iDirect Velocity supports configuration of the *Dynamic Host Configuration Protocol (DHCP)* to allow dynamic address assignment of devices connected to the terminal SVN interfaces. DHCP is configurable on a per SVN basis, and can be enabled separately for IPV4 or IP4v6 networks. iDirect satellites terminals can be configured as a DHCP Relay agent or as a DHCP Server.

6.9.1 IPv4 DHCP Relay Configuration

The Satellite Terminal is configured as a **DHCP Relay** agent, on a particular SVN, if the designated DHCP Server is located at the Teleport site. When configuring the terminal as an IPv4 **DHCP Relay** agent, fields are provided for the **IPv4 Address**, and the **Subnet and NetMask** addresses of a DHCP Server.

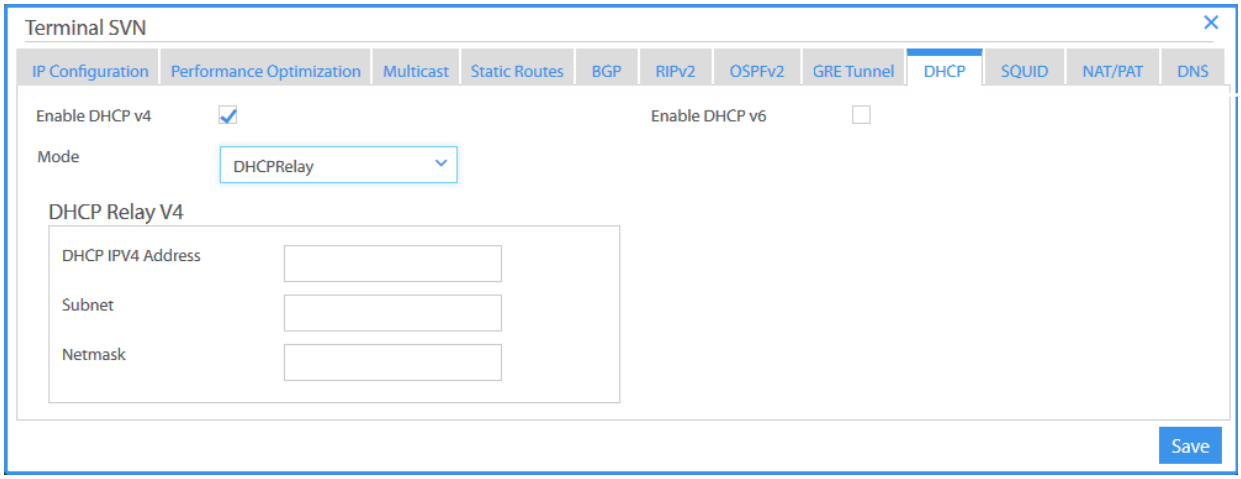

Figure 6-14. Terminal SVN — DHCP Relay (IPv4) Configuration Dialog

To configure the Satellite Terminal as a DHCPv4 relay agent**:**

1. With the **SVN** configuration tab open, and with SVN records displayed, click the **Edit** icon on the SVN for which **DHCP** parameters are to be configured.
2. Click the **DHCP** tab.
3. Select **Enable DHCPv4**.
4. Use the **Mode** drop-down and select **DHCP Relay** to enable the DHCP IPv4 relay configuration parameters. The DHCP Relay configuration dialog opens.
5. In **DHCP IPv4 Address** enter the IP address of the DHCP Server.
6. Enter the IPv4 **Subnet** address of the DHCP Server.
7. Enter the IPv4 **NetMask** address of the DHCP Server.
8. Click **Save** to save the DHCP Relay configuration and close the Terminal SVN dialog.

6.9.2 IPv4 DHCP Server

By enabling DHCP v4, the dialog for configuring the Satellite Terminal as a IPv4 DHCP Server for IPv4 is displayed. By default, DHCP is disabled, and must be enabled to display the associated fields.

The **DHCP Server** dialog supports specification of the **Subnet** and **Netmask** address, **Lease Duration** and **Lease Duration Unit, Primary** and **Secondary DNS** addresses, a **Default Gateway**, and a **Broadcast IP** address. Users may also specify a range of clients to be served, using the **Client Address Range** section of the dialog.

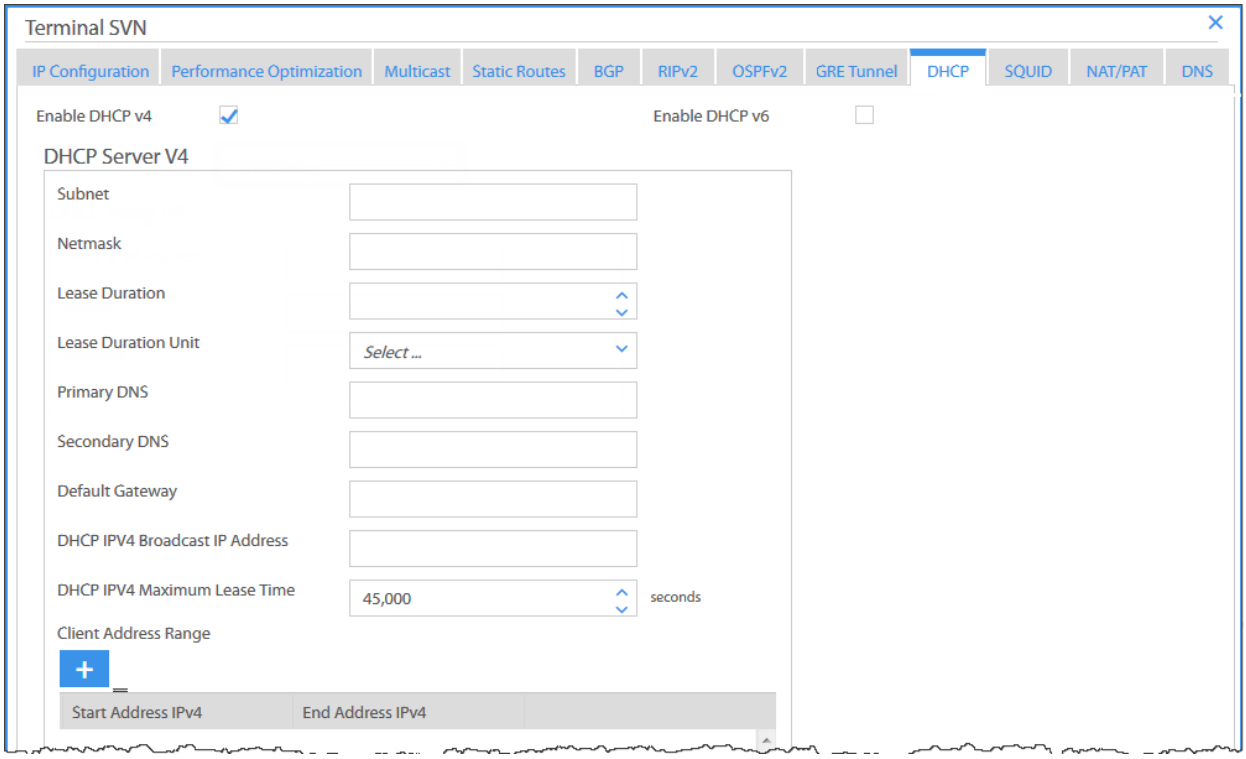

Figure 6-15. Terminal SVN — DHCP (IPv4) Server Configuration Dialog

To configure the Satellite Terminal as a DHCPv4 server:

1. With the **SVN** configuration tab open, and with SVN records displayed, click the **Edit** icon on the SVN for which **DHCP** parameters are to be configured.
2. Click the **DHCP** tab.
3. Select **Enable DHCPv4**.
4. Select **DHCP Server**, using the **Mode** drop-down, to enable the DHCP IPv4 Server configuration parameters.
5. Enter the **Subnet** and **NetMask** addresses of the DHCP Server.
6. Enter the **Lease Duration** or the amount of time before the address must be renewed.
7. Use the **Lease Duration Unit** drop-down to select a unit of **Days**, **Hours**, or **Weeks**.

8. Enter the **Primary DNS**, **Secondary DNS**, and **Default Gateway** server addresses in the appropriate IPv4 fields.
9. Enter the **DHCP IPv4 Broadcast IP Address**.
10. Under **Client Address Range**, click the **Add Record** icon to enter a range of assignable addresses, as required. The **Client Address Range** dialog is enabled.
11. Enter a **Start Address IPv4** and an **End Address IPv4** of the address range and click the **Update** icon to accept the entry. An accepted address range is entered as a new record under **Client Address Range**.
12. Repeat the previous steps, from Step (10), to add client address range records.
13. To modify a configured client address range, click the **Edit** icon on the record to be modified; click the **Delete** icon to remove a record.
14. Click **Save** to save the DHCP Server configuration and close the Terminal SVN dialog.

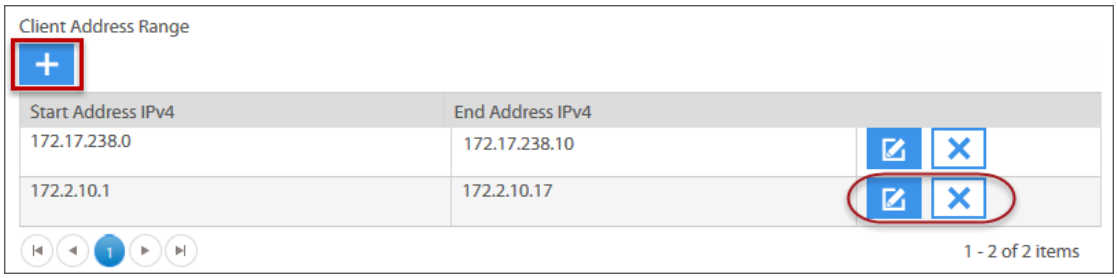

Figure 6-16. Terminal SVN — IPv4 Client Address Range Records

6.9.3 IPv6 DHCP Relay Configuration

The Satellite Terminal is configured as a IPv6 **DHCP Relay** agent, on a particular SVN, if the designated DHCP Server is located at the Teleport site. When configuring the terminal as an IPv6 **DHCP Relay** agent, fields are provided for the **IPv6 Address** and **IPv6 Address Prefix** of the DHCP Server, the **Subnet** and **Subnet Prefix**.

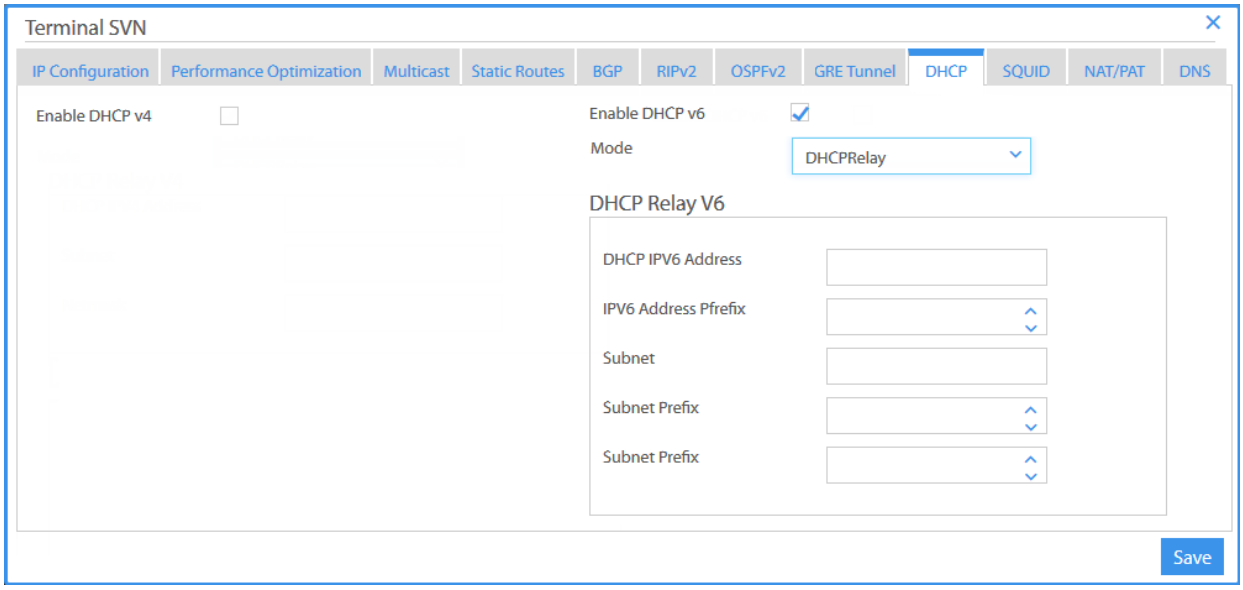

Figure 6-17. Terminal SVN — DHCP Relay (IPv6) Configuration Dialog

To configure the Satellite Terminal as a DHCPv6 relay agent**:**

1. With the **SVN** configuration tab open, and with SVN records displayed, click the **Edit** icon on the SVN for which **DHCP** parameters are to be configured.
2. Click the **DHCP** tab.
3. Select **Enable DHCPv6**.
4. Use the **Mode** drop-down and select **DHCP Relay** to enable the DHCP IPv6 relay configuration parameters. The configuration dialog opens with fields enabled.
5. Enter the IP address of the DHCPv6 server in **DHCP IPv6 Address**.
6. Enter the IPv6 prefix address of the DHCPv6 server in **DHCP IPv6Address Prefix**.
7. Enter the IPv6 **Subnet** address and **Subnet Prefix** of the DHCPv6 server.
8. Click **Save** to save the DHCPv6 Relay configuration and close the **Terminal SVN** dialog.

6.9.4 IPv6 DHCP Server Configuration

By enabling DHCP v6, the dialog for configuring the Satellite Terminal as an IPv6 DHCP Server is displayed. By default DHCP is disabled, and must be enabled to configure.

The **DHCPv6 Server** dialog supports specification of **Primary** and **Secondary DNS** addresses, a **Default Gateway**, **Lease Duration**, **Lease Duration Unit**, and a **Maximum Lease Time**. Users may also use the **Client Address Range** section, to specify a range of clients to be served.

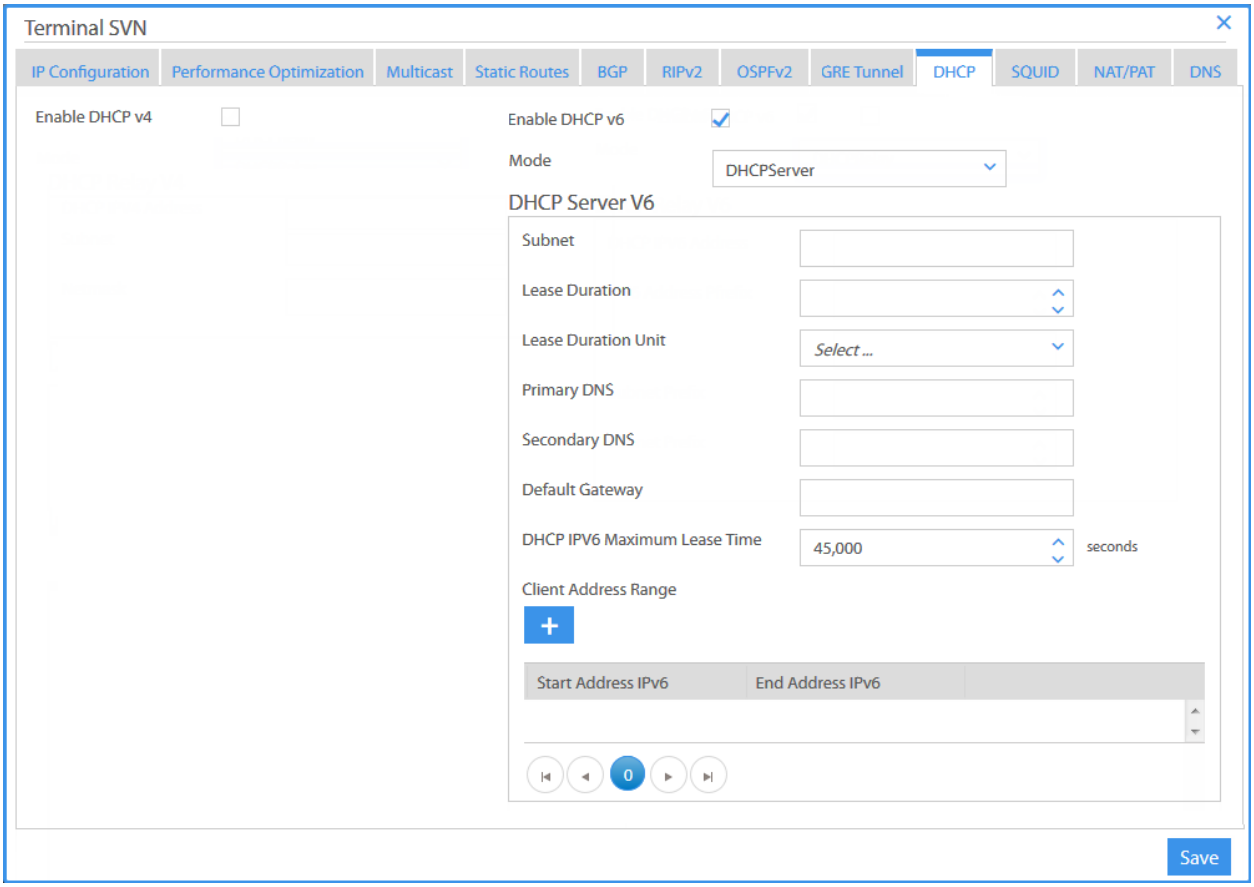

Figure 6-18. Terminal SVN — DHCP (IPv6) Server Configuration Dialog

To configure the Satellite Terminal as a DHCPv6 server:

1. With the **SVN** configuration tab open, and with SVN records displayed, click the **Edit** icon on the SVN for which **DHCP** parameters are to be configured.
2. Click the **DHCP** tab.
3. Select **Enable DHCPv6**.
4. Select **DHCP Server,** using the **Mode** drop-down, to enable the DHCP IPv6 Server configuration parameters. The configuration dialog opens with fields enabled.
5. Enter the **Subnet** address of the DHCP Server.

6. Enter the **Lease Duration**, as the amount of time before the address must be renewed.
7. Use the **Lease Duration Unit** drop-down to select a unit of **Days**, **Hours**, or **Weeks**.
8. Enter the **Primary DNS**, **Secondary DNS**, and **Default Gateway** Server addresses in the appropriate fields.
9. Enter the **DHCP IPv6 Maximum Lease Time**, in seconds.
10. Under **Client Address Range**, click the **Add Record** icon to enter a range of assignable addresses, as required. The **Client Address Range** dialog is enabled.
11. Enter a **Start Address IPv4** and an **End Address IPv4** of the address range and click the **Update** icon to accept the entry. An accepted address range is entered as a new record under the **Client Address Range** section.
12. Repeat the previous steps, from Step (10), to add client address range records.
13. To modify a configured client address range, click the **Edit** icon on the record to be modified; click the **Delete** icon to remove a record.
14. Click **Save** to save the DHCP Server configuration and close the Terminal SVN dialog.

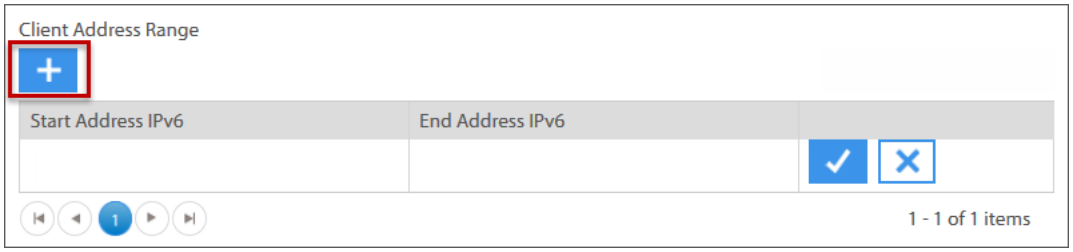

Figure 6-19. Terminal SVN — IPv6 Client Address Range Dialog

6.10 Terminal SVN HTTP Aceleration Configuration

The Satellite Terminal accelerates web traffic and caches data locally to avoid long satellite delays for frequently accessed pages. The Velocity Network implementation employs a *Squid* proxy server and web cache software component. When enabled, this option reduces the time required to load a web page by caching objects that the browser will eventually need.

In addition to web page caching and acceleration, DNS caching is also necessary to speed up web access. The DNS cache works in conjunction with the Squid to enhance lookups of web page objects without going over the air for each lookup.

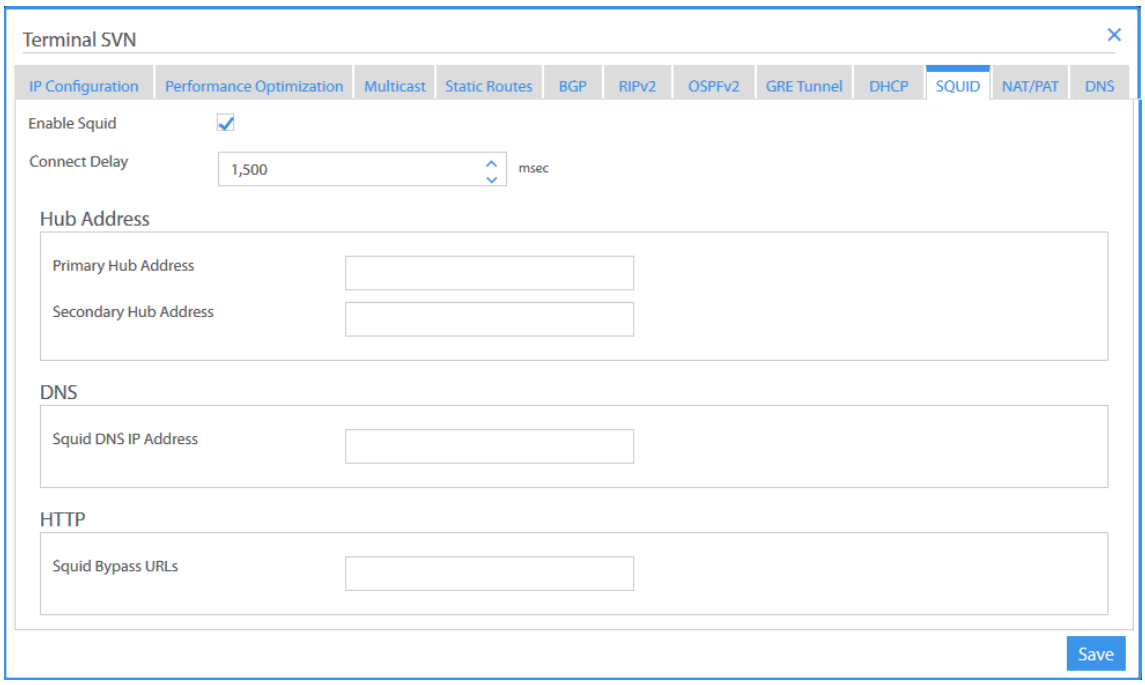

Figure 6-20. Add Terminal SVN — Squid Configuration Dialog

To configure the Satellite Terminal SVN Squid parameters:

1. With the **SVN** configuration Tab selected, and with SVN records displayed, click the **Edit** icon on the assigned SVN to which **Squid** configuration parameters are to be added.
2. Click the **Squid** tab, to open the configuration dialog.
3. Select **Enable Squid** to enable this HTTP acceleration option on the SVN.
4. Enter the **Connect Delay** in milliseconds. This value represents delay between each attempt to connect.
5. Enter a **Primary Hub Address** and **Secondary Hub Address** for this Squid Server.
6. Enter the **Squid DNS IP Address**. This is the IPv4 address of the DNS server that the Squid uses to resolve domain names.
7. Enter **Squid Bypass URLs**. These entries are URLs to be bypassed by the Squid.
8. Click **Save** to save the Squid configuration and close the **Terminal SVN** dialog.

6.11 Terminal SVN NAT/PAT Configuration

Network Address/Port Translation (NAT/PAT or NAPT) is a process of modifying IP addresses as well as TCP/UDP port numbers so that nodes residing on a private network can share a public IP address for communication with the outside world. Address/port translation and IPv4/IPv6 protocol translation on up to 8 SVNs is independently provided on a per-SVN basis.

The Satellite Terminal NAT implementation for an iDirect Velocity Network is known as Symmetric NAPT. In operation, requests from internal IP address and port pairs targeted to different external IP address and port pairs are mapped to an external NAT address on a unique port. The same applies to all requests from the same host to different destinations.

The terminal SVN NAT/PAT configuration uses three dialogs: the **NAT Session**, **NAT Firewall**, and the NAT **SIPALG Table**, all of which are only displayed if the **NAT/PAT** option is enabled.

6.11.1 Configuring the NAT Session

The NAT session dialog supports the definition of multiple NAT/PAT session record entries. Each record allows specification of a single port or a range of ports (**Local Port Range**), **NAT Port Range**, the supported protocol, and the IP address (**Local Address**) to which traffic is forwarded.

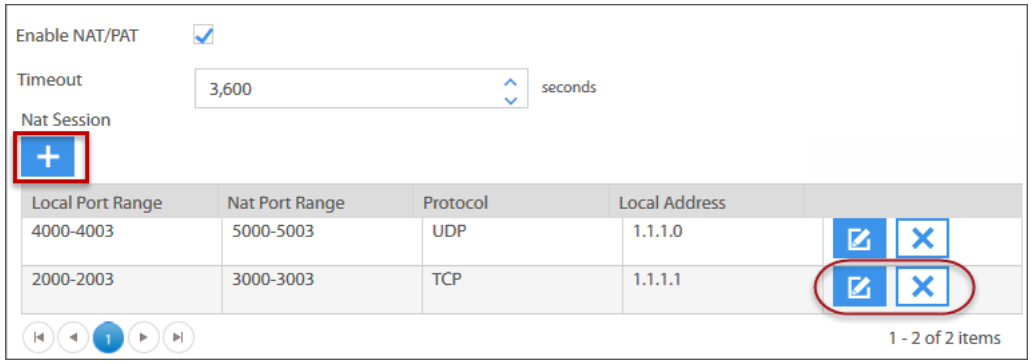

Figure 6-21. Terminal SVN — NAT/PAT Session Configuration Dialog/Records

To configure the Satellite Terminal SVN NAT/PAT Session:

1. With the **SVN** configuration tab selected, and with SVN records displayed, click the **Edit** button on the assigned SVN for which **NAT/PAT** parameters are to be configured.
2. Click the **NAT/PAT** tab, to open the configuration dialog.
3. Select **Enable NAT/PAT** to enable the feature on this SVN.
4. Enter a **Session Timeout** value, in seconds, or use the default of value of 1hour.
5. Under the **NAT Session** section, click the **Add Record** icon to enable the fields for inserting a **NAT Session** record.
6. In **Local Port Range**, enter a single port number or a range of ports — for example **2300-2305**, on which NAT session can be made.
7. In **NAT Port Range**, enter a single port number or a range of ports — for example **2300-2305**, on which NAT firewall connection may be made.

8. Use the **Protocol** drop-down and select the appropriate protocol for this session.
9. Enter the IP address of the NAT **Local Address**.
10. Click the **Update** icon to accept the entry. An accepted entry is entered as a new record under **Nat Session**.
11. Repeat the previous step to insert additional **NAT Session** records.
12. Click the **Edit** icon on a **NAT Session** record to modify the record; make the required changes, and again click the **Update** icon; click the **Delete** icon to remove the record.
13. Click **Save** to save the NAT/PAT Session configuration and close the **Terminal SVN** dialog, or continue with the Terminal SVN NAT/PAT configuration.

6.11.2 Configuring the NAT Firewall

The NAT firewall is an optional feature that acts as an additional protective filter between the local SVN and external VPN providers that offer a NAT firewall service.

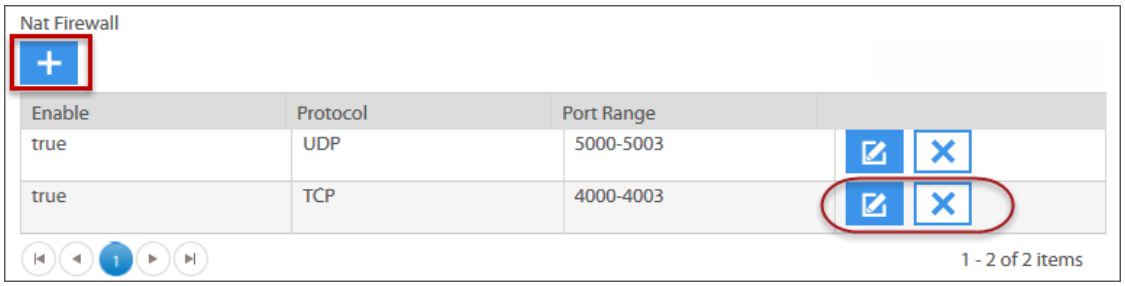

Figure 6-22. Terminal SVN — NAT/PAT Firewall Configuration Dialog/Records

To configure the Satellite Terminal SVN NAT Firewall:

1. With the **SVN** configuration tab selected, and with SVN records displayed, click the **Edit** button on the assigned SVN for which **NAT/PAT** firewall parameters are to be configured.
2. Click the **NAT/PAT** tab, to open the configuration dialog.
3. Select **Enable NAT/PAT** to enable the feature on this SVN.
4. Enter a **Session Timeout** value, in seconds, or use the default of value of 1hour.
5. Click the **Add Record** icon under the **NAT Firewall** section, to enable the fields for inserting a NAT Firewall record.
6. Select the **Enable** check box, to enable the NAT Firewall record.
7. Use the **Protocol** drop-down and select the appropriate protocol to allow through the firewall. A configured firewall record can be disabled at any time.
8. In the **Port Range** field, enter a range of ports — for example **2300-2305**, or a single port number on which NAT firewall connection may be made.
9. Click the **Update** icon to accept the entry. An accepted entry is entered as a new record under **Nat Firewall**.
10. Repeat the previous step to insert additional **NAT Firewall** records.

11. Click the **Edit** icon on a **NAT Firewall** record to modify the record; make the required changes, and again click the **Update** icon; click the **Delete** icon to remove the record.
12. Click **Save** to save the NAT/PAT Firewall configuration and close the **Terminal SVN** dialog, or continue with the Terminal SVN NAT/PAT configuration.

6.11.3 Configuring the NAT SIPALG Table

The Signaling Protocol (SIP) Application Layer Gateway (**SIPALG**) works in conjunction with the NAT implementation on the Satellite Terminal, and can be enabled or disabled independently on each SVN. The NAT implementation supports dynamic addition and deletion of ports based on SIP traffic, which is monitored by the SIP application layer gateway (ALG).

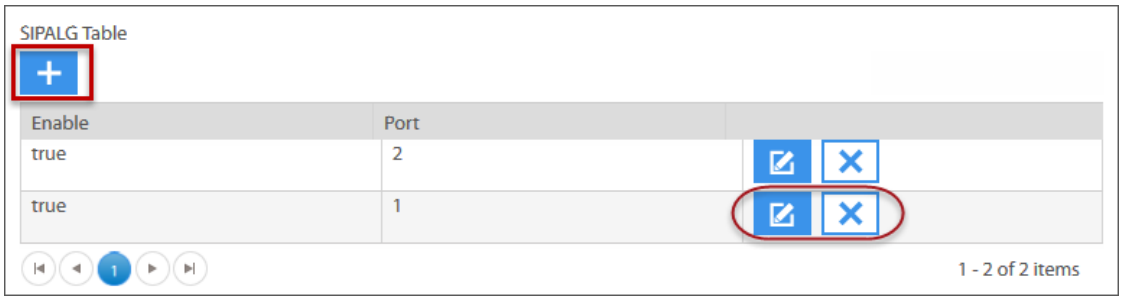

Figure 6-23. Terminal SVN — NAT/PAT SIPALG Table Configuration Dialog

The **SIPALG** parameter should be enabled only if **NAT** is also enabled on the Satellite Terminal, since it is not relevant in the absence of **NAT**. However, the **SIPALG** parameter may be disabled even if **NAT** is enabled.

The dynamic buildup and tear-down of the transport streams, is managed by the SIP. The SIP application layer gateway also identifies the ports that need to be opened up by the NAT/PAT implementation in order for VoIP calls to operate seamless on the Satellite Terminal.

To configure the Satellite Terminal SVN NAT SIPALG Table configuration:

1. Click the **Add Record** button under the **SIPALG Table** section, to enable the fields of a NAT SIPALG Table record.
2. Select **Enable** to enable the SIP Application Gateway on the Satellite Terminal for this SVN. A configured **SIPALG** record can be disabled at any time.
3. Enter a **Port** number on which the **SIPALG** should make a connection.
4. Click the **Update** icon to accept the entry. An accepted entry is entered as a new record under **SIPALG Table**.
5. Repeat the previous steps to insert additional **SIPALG Table** records.
6. Click the **Edit** icon on a **SIPALG Table** record to modify the record; make the required changes, and again click the **Update** icon; click the **Delete** icon to remove the record.
7. Click **Save** to save the NAT SIPALG Table configuration and close the **Terminal SVN** dialog, or continue with the Terminal SVN configuration.

6.12 Terminal SVN DNS Configuration

In Velocity, the Terminal SVN is configured for **DNS (Domain Name System)** from the Terminal SVN DNS tab. The DNS feature may be enabled/disabled on a per-SVN basis. If the DNS option is enabled the SVN, by default, acts as the DNS server for all nodes present on its local LAN.

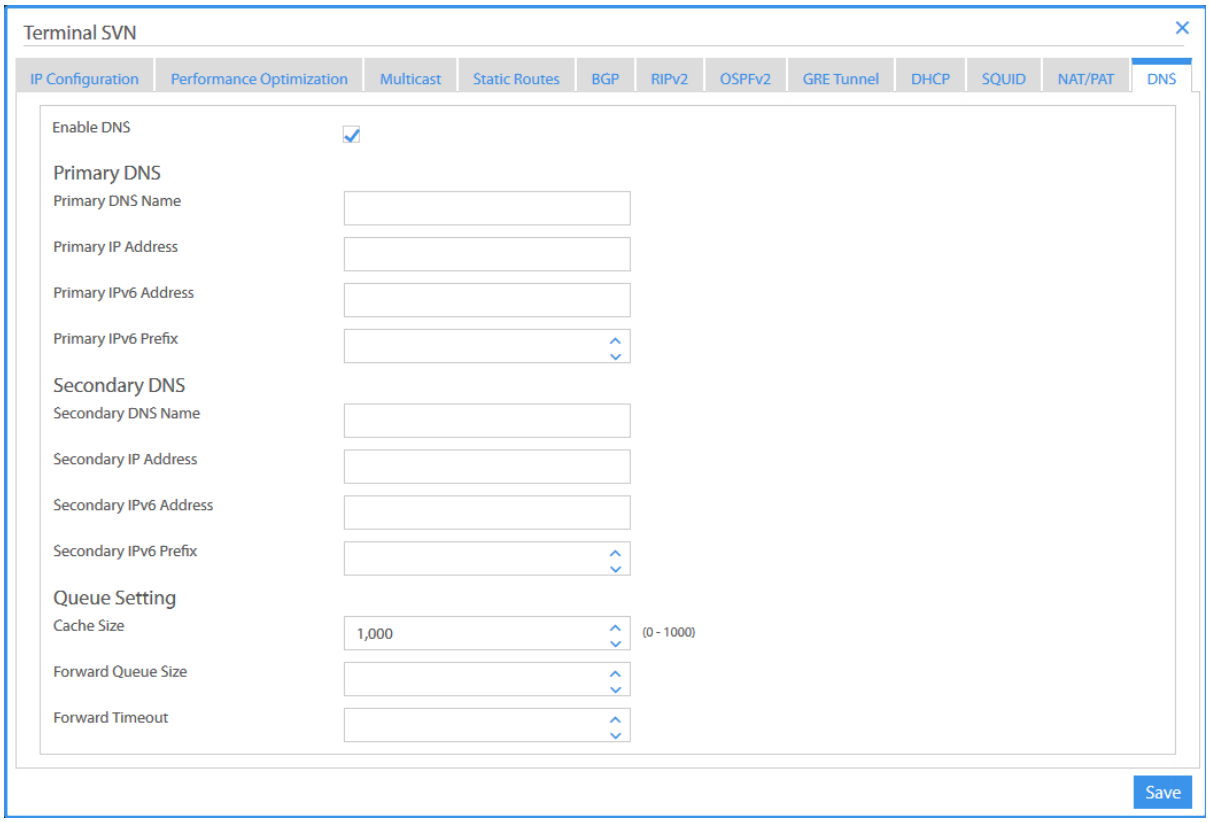

Figure 6-24. Terminal SVN — DNS Configuration Parameters Dialog

To configure the Satellite Terminal SVN DNS parameters:

1. With the **SVN** configuration tab selected, and with SVN records displayed, click the **Edit** button on the assigned SVN for which **DNS** parameters are to be configured.
2. Click the **DNS** tab to open the configuration dialog.
3. Select **Enable DNS** to configure the DNS parameters for **IPv4**, **IPv6**, or both.
4. Specify **Primary** and **Secondary IP address**, for IPv4 if applicable.
5. Specify the **Primary DNS Name** and **Secondary DNS Name** for IPv4, if applicable.
6. Enter the local **Cache Size**, **Forward Queue Size** and **Forward Time-out** values. Default values, if shown, may be modified.
7. Specify **Primary IPv6** and **Secondary IPv6 Address**, for IPv6, if applicable.
8. Specify **Primary IPv6** and **Secondary IPv6 Prefix**, for IPv6, if applicable.
9. Click **Save and Close** to save the configuration to the NMS database.

7 Monitoring & Reporting Using Pulse

Pulse provide Network Operators with a variety of tools for monitoring the current sate of network physical and logical infrastructure elements, and a of tools for generating a variety of historical reports involving network events, alarms, as well as long term stats and statistical reports of network elements and the overall network.

The following topics present a variety of Velocity network monitoring and reporting use cases using Pulse Monitoring and Reporting tools.

7.1 Use Cases — Alarms Monitoring and Reporting

The following use cases are examples of Pulse Alarms operations executed from either the **Monitoring** or **Reporting** menu.

7.1.1 Use Case: Monitor Current Infrastructure Alarms

Show the current alarms for all network infrastructure elements. For this use case, no Configurator input is required after the appropriate Pulse operation is selected. Since the **Stream** parameter is set to ON, the report is updated with new alarms as they occur.

This report includes the alarms, which exist at the time the report is generated, for all physical infrastructure elements such as Hub Chassis, Line Cards, PP Clusters and PP Servers, NMS Clusters and NMS Servers; as well as for logical infrastructure elements such as Satellites, Beams, Channels, iNets, Signaling Carriers, Upstream and Downstream Carriers.

Table 7-1. Configurator Setup to Monitor Alarms of All Network Infrastructure Elements

Configurator Parameter	User-Required Configurator Input
Simple/Advanced View	N/A
Date Range/Stream	N/A (set by default to Current Date - 30). **Stream** = ON.
View Selection	N/A
Elements	N/A
Severity	N/A
Status View	N/A
Generate Operation	N/A (Auto-generated)

Procedure: To report current alarms of all network infrastructure elements

1. Click the **Monitoring** tab > **Real-Time Alarms** > **All Infrastructure Alarms**. The Configurator is automatically populated and a report of current alarms for all infrastructure elements is displayed.
2. Click on a column heading, for example **Element Name** to sort if necessary. For example, sort by **Severity**, by **Start Time**, or by **State**.
3. Click on a filter icon, for a column, to filter the list of displayed alarms if necessary.
4. Use the browser **Back** arrow to leave the page.

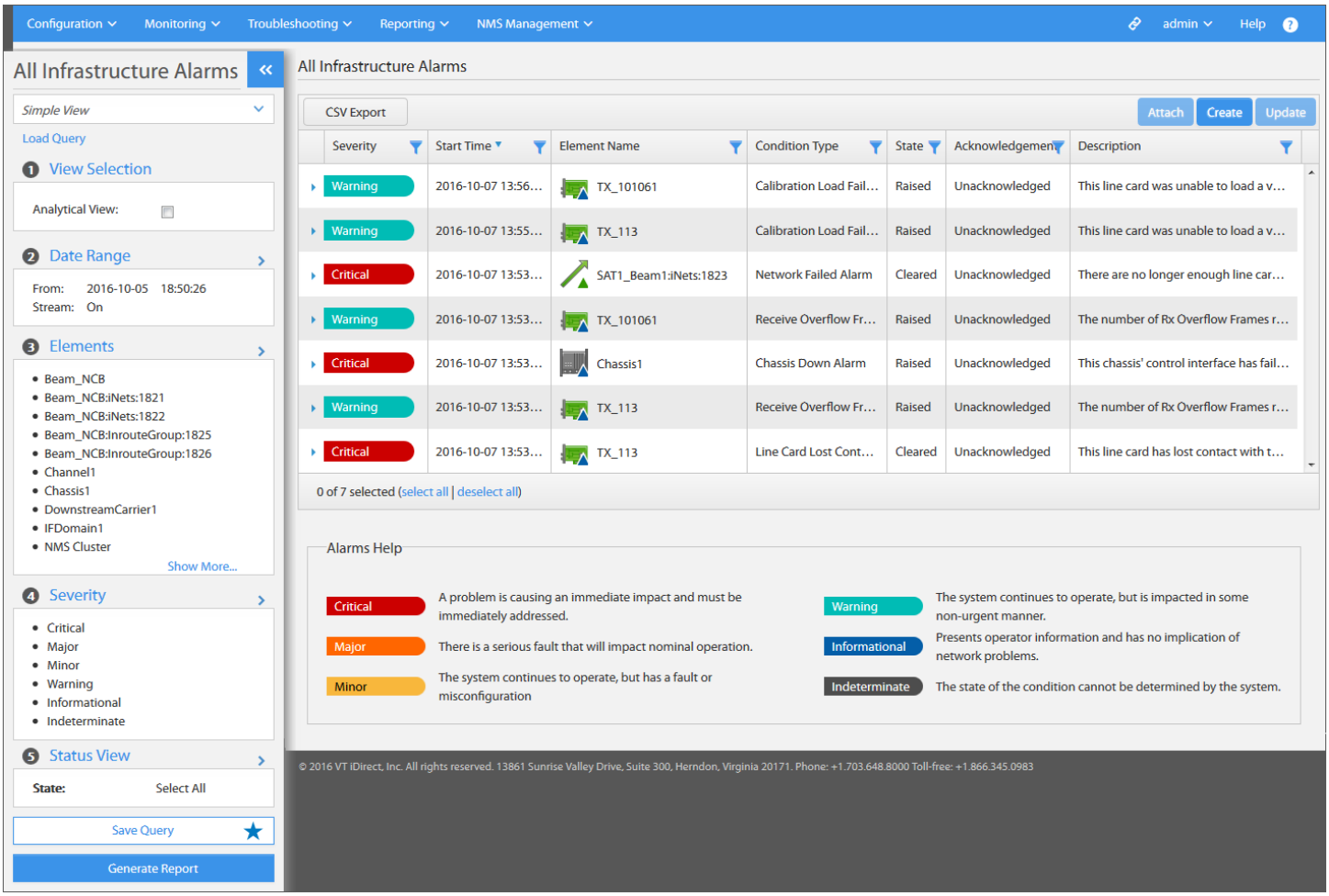

Figure 7-1. Current Network Infrastructure Alarms (Physical and Logical)

7.1.2 Use Case: Monitor Current Logical Infrastructure Alarms

Show the current network alarms of all logical infrastructure elements of the network. For this use case, no Configurator input is required after the Pulse operation is selected. Since the **Stream** parameter is set to ON, the report updates with new alarms as they occur.

This report includes the alarms, which exist at the time the report is generated, for all logical infrastructure elements such as Satellites, Beams, Channels, iNets, Signaling Carriers, Upstream Carriers, and Downstream Carriers.

Table 7-2. Configurator Setup to Monitor Alarms of Logical Infrastructure Elements

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	N/A
Date Range/Stream	N/A (set by default to Current Date - 30). **Stream** = ON.
View Selection	N/A
Elements	N/A
Severity	N/A
Status View	N/A
Generate Operation	N/A (Auto-generated)

Procedure: To report current alarms of all logical infrastructure elements

1. Click the **Monitoring** tab > **Real-Time Alarms** > **Logical Infrastructure Alarms**. The Configurator is automatically populated and the report of current alarms for all logical infrastructure elements is displayed.
2. Click on a column heading, for example **Element Name** to sort if necessary.
3. Click on a filter icon, for a column, to filter the list of displayed alarms if necessary. For example, sort by **Severity**, by **Start Time**, or by **State**.
4. Use the browser **Back** arrow to leave the page.

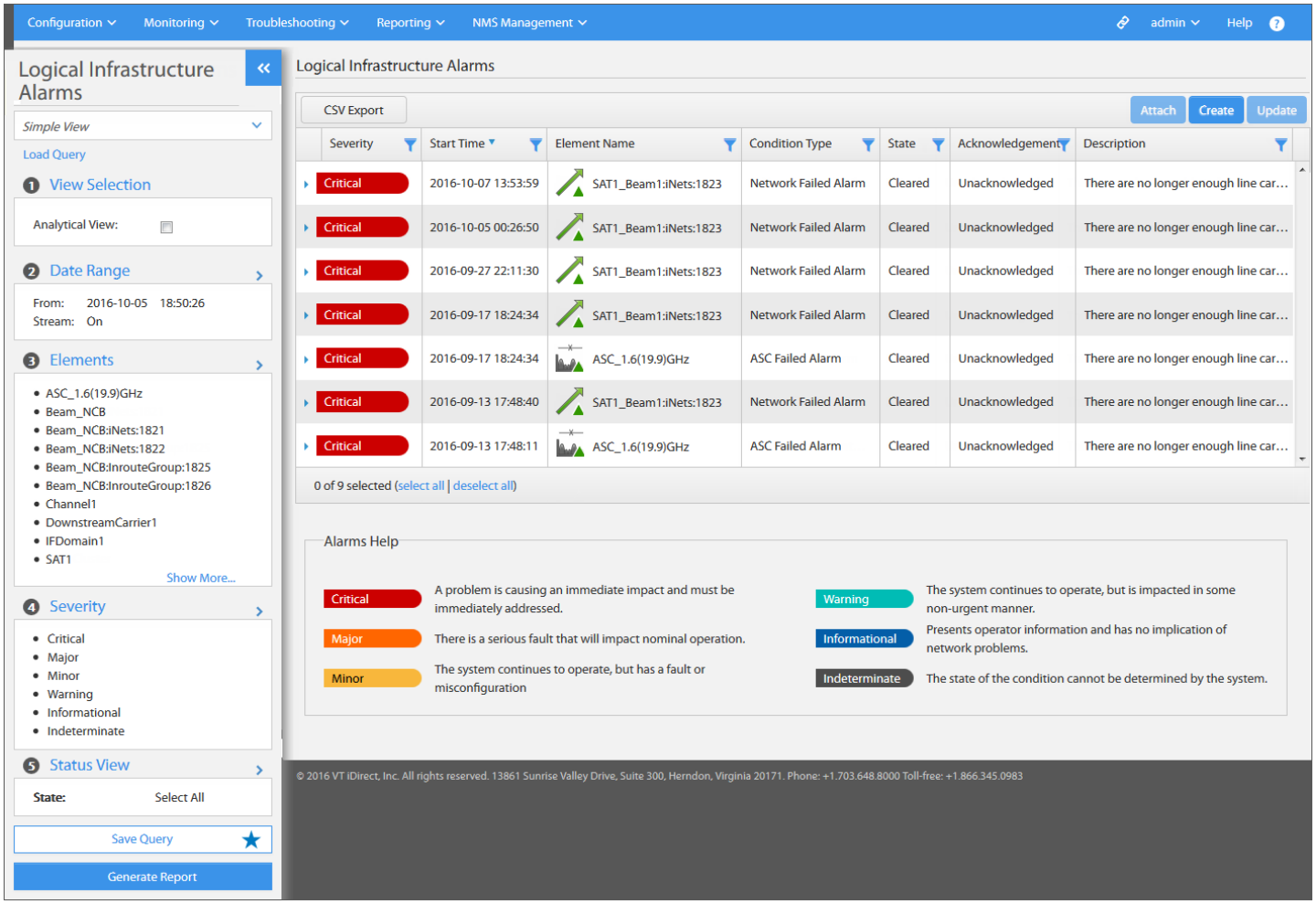

Figure 7-2. Current Logical Infrastructure Alarms

7.1.3 Use Case: Monitor Physical Infrastructure Alarms

Show the current network alarms for all physical infrastructure elements of the network. For this use case, no Configurator input is required after the Pulse operation is selected. Since the **Stream** parameter is set to ON, the report is updated with new alarms as they occur.

This report includes the alarms, which exist at the time the report is generated, for all physical infrastructure elements such as Hub Chassis, Line Cards, PP Clusters and PP Servers, NMS Clusters and NMS Servers.

Table 7-3. Configurator Setup to Monitor Alarms of Physical Infrastructure Elements

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	N/A
Date Range/Stream	N/A (set by default to Current Date - 30). **Stream** = ON.
View Selection	N/A
Elements	N/A
Severity	N/A
Status View	N/A
Generate Operation	N/A (Auto-generated)

Procedure: To report the current alarms of physical infrastructure elements

1. Click the **Monitoring** tab > **Real-Time Alarms** > **Physical Infrastructure Alarms**. The Configurator is automatically populated and the report of current alarms for all physical infrastructure elements is displayed.
2. Click on a column heading, for example **Element Name** to sort if necessary.
3. Click on a filter icon, for a column, to filter the list of displayed alarms if necessary. For example, sort by **Severity**, by **Start Time**, or by **State**.
4. Use the browser **Back** arrow to leave the page.

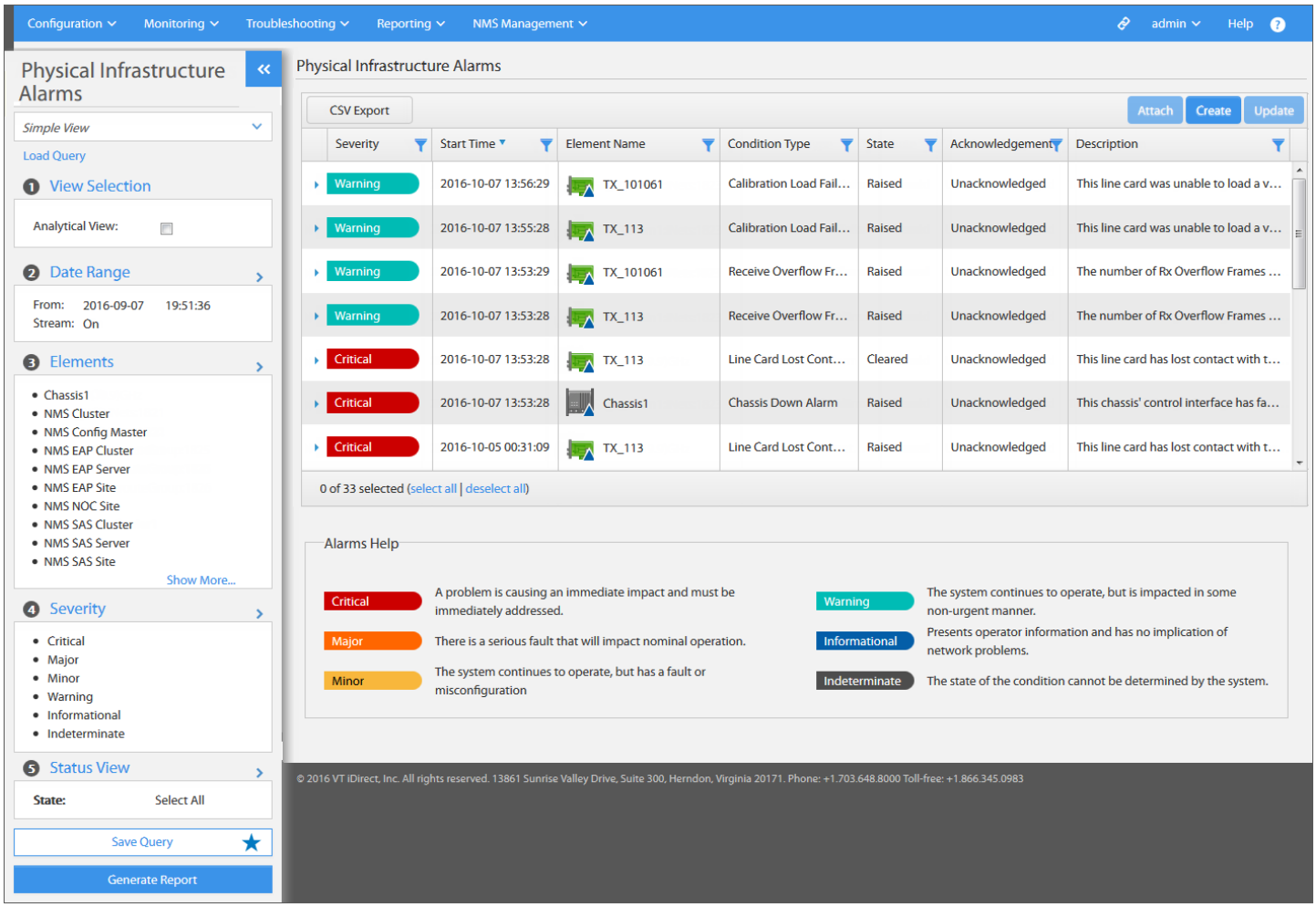

Figure 7-3. Current Physical Infrastructure Alarms

7.1.4 Use Case: Monitor Current Satellite Terminal Alarms

Show the current alarms for all satellite terminals of the network. For this use case, no user input to the Configurator is required after the appropriate Pulse operation is selected. Since the **Stream** parameter is set to ON, the report is updated with new alarms as they occur.

This report includes the alarms, which exist at the time the report is generated, for all Satellite Terminals.

Table 7-4. Configurator Setup to Monitor Alarms of All Satellite Terminals

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	N/A
Date Range/Stream	N/A (set by default to Current Date - 30). **Stream** = ON.
View Selection	N/A
Elements	N/A
Severity	N/A
Status View	N/A
Generate Operation	N/A (Auto-generated)

Procedure: To report the current alarms of all satellite terminals

1. Click the **Monitoring** tab > **Real-Time Alarms** > **Terminal Alarms** sub-menu. The Configurator tool is automatically populated and the report of the current alarms for all satellite terminals is displayed.
2. Click on a column heading, for example **Element Name** to sort if necessary.
3. Click on a filter icon, for a column, to filter the list of displayed alarms if necessary. For example, sort by **Severity**, by **Start Time**, or by **State**.
4. Use the browser **Back** arrow to leave the page.

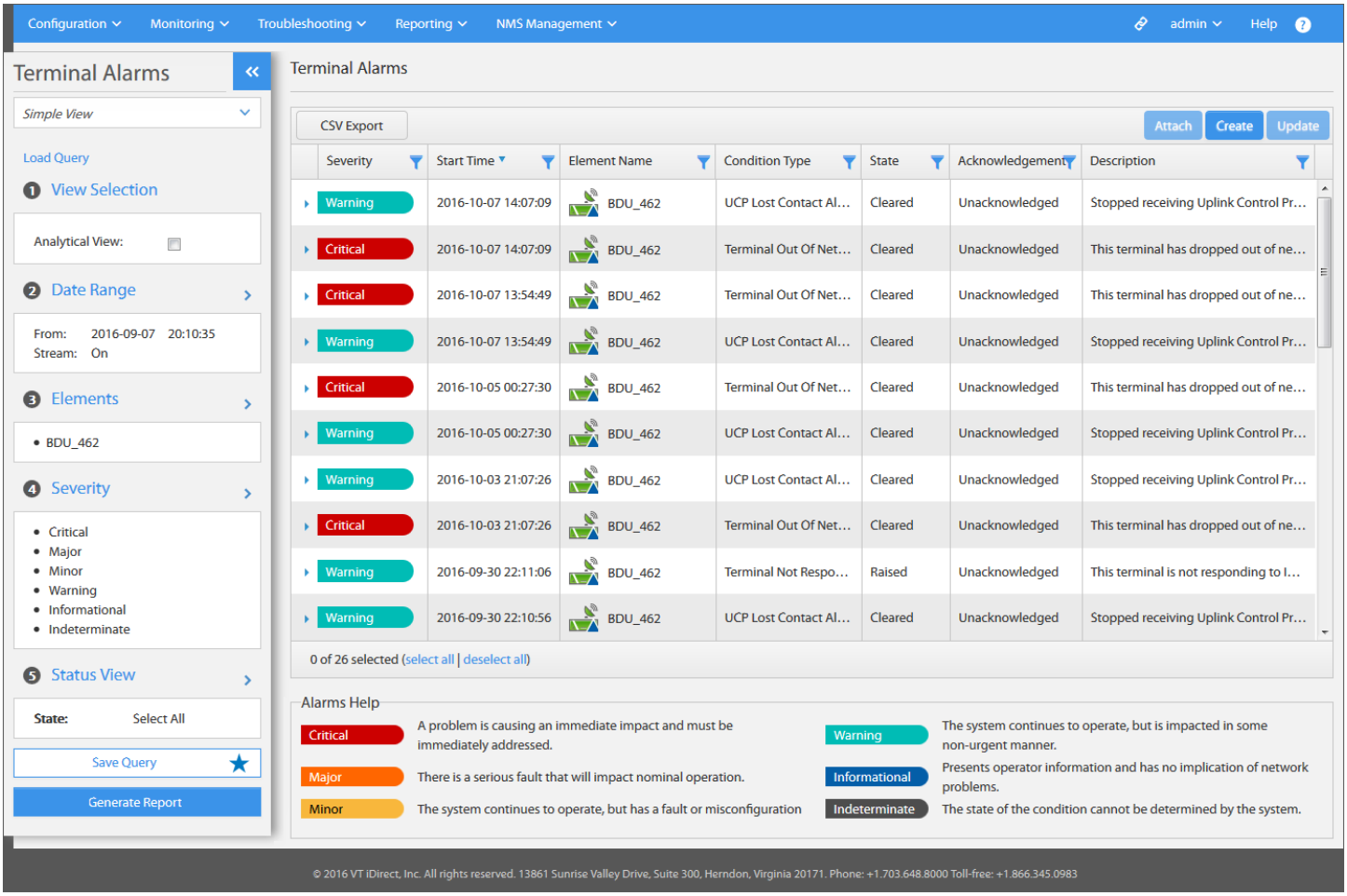

Figure 7-4. Current Satellite Terminal Alarms

7.1.5 Use Case: Generate an Alarms History Report

This report, which is manually configured, is to generate a report of the network alarms that occurred during a specific period. The report can be generated for any one or more elements.

The report may include alarms associated with physical infrastructure elements such as Hub Chassis, Line Cards, PP Clusters and PP Servers, NMS Clusters and NMS Servers; as well as alarms associated with logical infrastructure elements such as Satellites, Beams, Channels, iNets, Signaling Carriers, Upstream and Downstream Carriers.

Table 7-5. Configurator Setup to Generate an Alarms History Report

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	Select **Advanced View** to enable extended report options.
Date Range/ Stream	Use default (Current Date - 30); specify a report period; or select a pre-defined period.
View Selection	Use default; or enable Analytical View to enhance the report display.
Elements	Specify any one or more elements.
Severity	If **Advanced View** selected, alarm **Severity** levels to report can be set.
Status View	If **Advanced View** selected, the alarm **States** to report can be set.
Analytical View	If **Analytical View** is enabled, graphical **Chart** types can be configured.
Generate Operation	Manual

Procedure: To manually generate alarm history report for any element or elements

1. Click the **Reporting** tab > **Report Builder** > **Alarms**.
2. Select **Advanced View** for an extended parameter set.
3. Select **Analytical View** to correlate alarms data using optional bar graphs and pie charts.
4. Click **Date Range** and specify a date range or select any one of the predefined periods.
5. Click the **Elements** to open the Basic Search tool or click **Advanced Search**, to find and specify one or more specific elements or element types to be included in the report.
6. Click the **Severity** selector to specify one or more severity levels to include in the report.
7. Click the **Status View** selector, if desired, to configure the report to only show **Raised**, **Cleared**, or **All** alarm states.
8. Click the **Analytical View** selector and choose the desired **Pie** or **Bar** charts for displaying the report.
9. Click **Generate Report** to generate and view the **Alarm History** report. The Alarm History report is displayed. If configured, analytical charts are also shown.

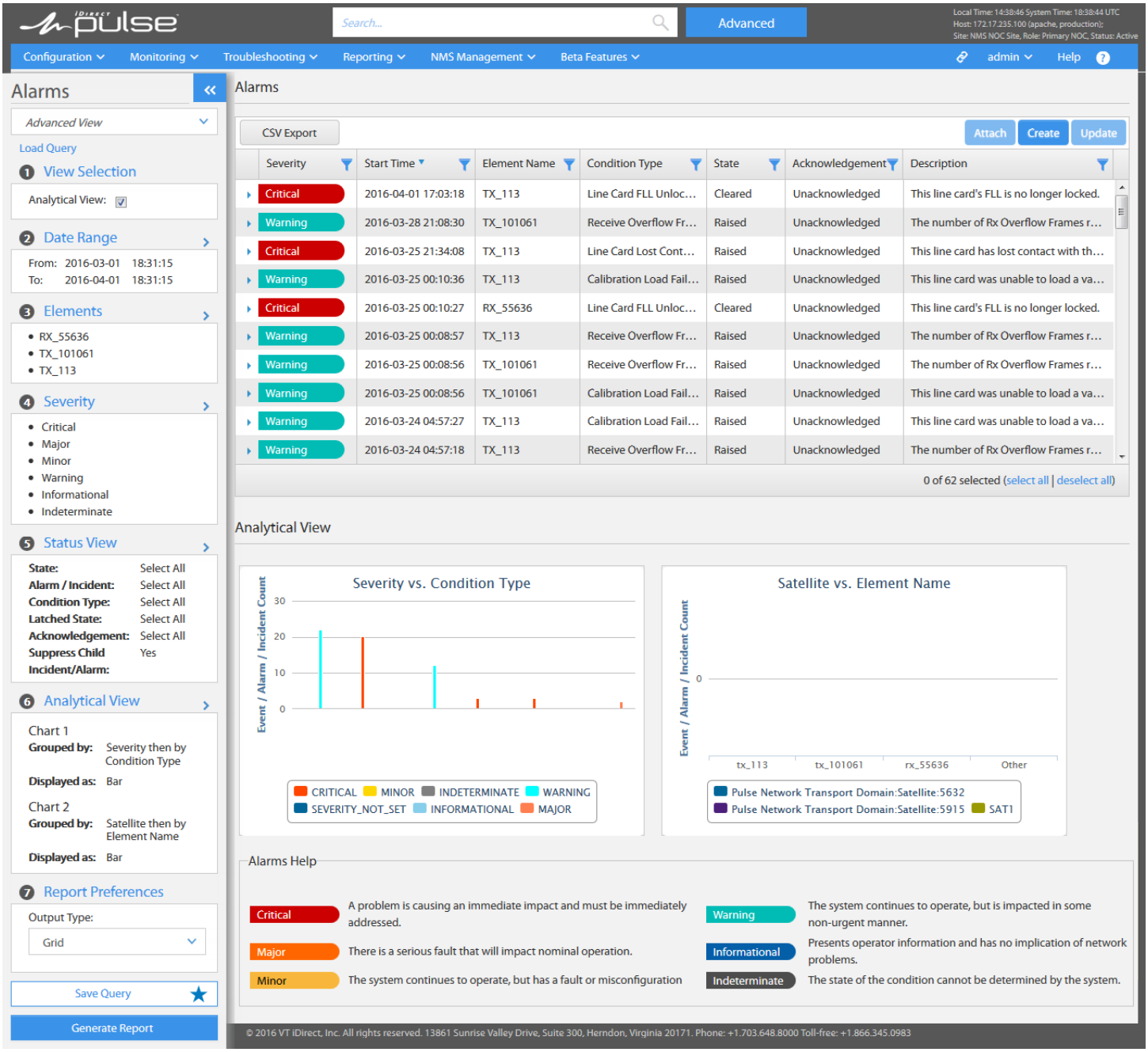

Figure 7-5. History Report of Network Alarms (Physical or Logical, or Both)

7.2 Use Cases — Events Monitoring and Reporting

The following use cases are examples of Pulse Events operations executed from either the **Monitoring** or **Reporting** menu.

7.2.1 Use Case: Monitor Current Logical Infrastructure Events

Show the current events of all logical infrastructure elements of the network. For this use case, no user input to the Configurator panel is required after the appropriate Pulse operation is selected. Since the **Stream** parameter is set to ON, the report is updated with new events as they occur.

This report includes all active events that exist at the time the report is generated, and that are associated with the logical infrastructure elements of the network, such as Satellites, Beams, Channels, iNets, Signaling Carriers, Upstream Carriers, and Downstream Carriers.

Table 7-6. Configurator Setup to Monitor Events of All Logical Infrastructure Elements

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	N/A
Date Range/Stream	N/A (set by default to Current Date/Time). **Stream** = ON.
View Selection	N/A
Elements	N/A
Severity	N/A
Generate Operation	N/A (Auto-generated)

Procedure: To report current events of all logical infrastructure elements

1. Click the **Monitoring** tab > **Real-Time Events > Logical Infrastructure Event Log**. The Configurator is automatically populated and the report of the current events associated with all logical infrastructure elements is displayed.
2. Click on a column heading, for example **Element Name** to sort if necessary.
3. Click on a filter icon, for a column, to filter the list of displayed events if necessary.
4. Use the browser **Back** arrow to leave the page.

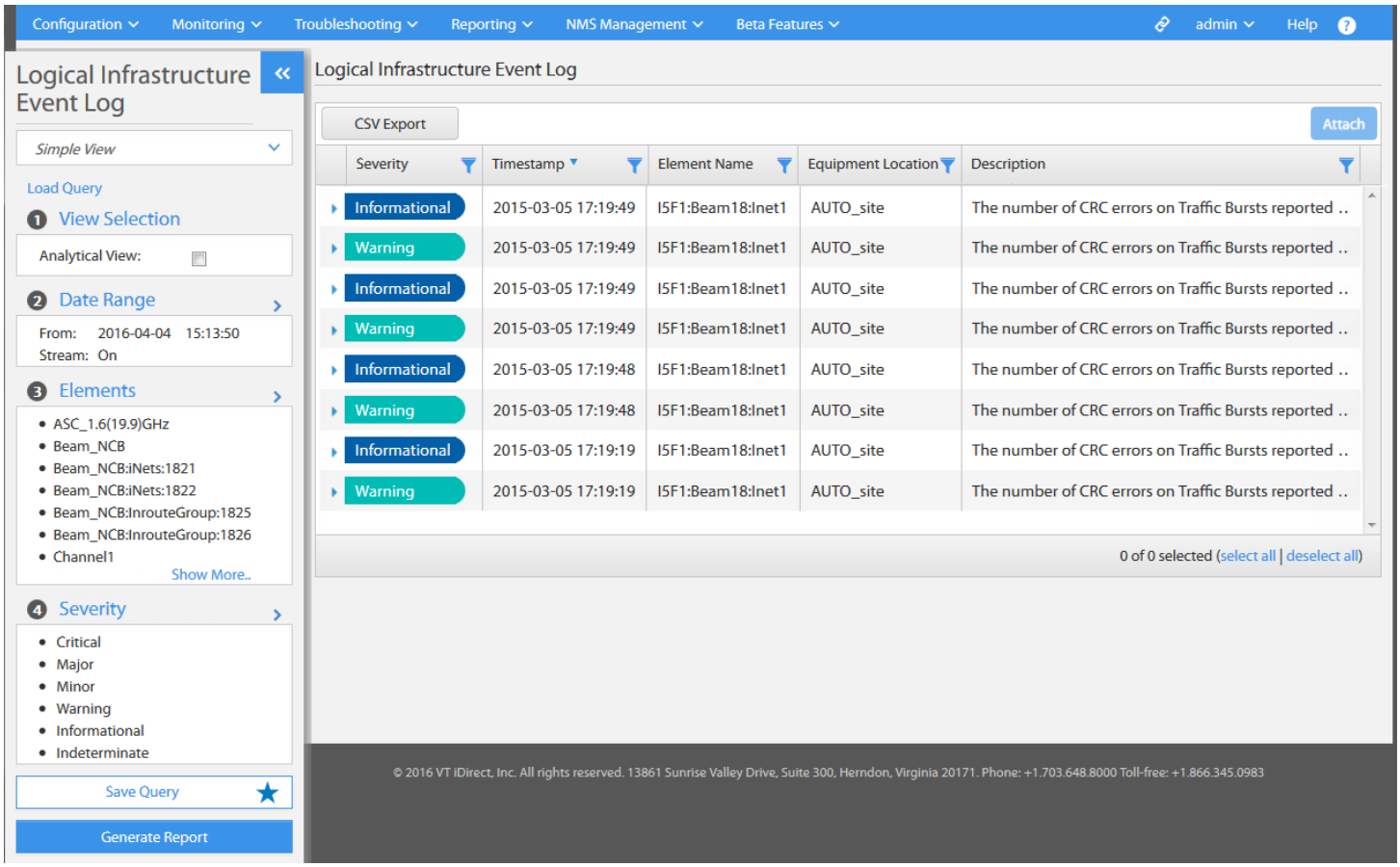

Figure 7-6. Current Logical Infrastructure Event Log

7.2.2 Use Case: Monitor Physical Infrastructure Events

Show the current events for all physical infrastructure elements of the network. For this use case, no user input to the Configurator panel is required after the appropriate Pulse operation is selected. Since the **Stream** parameter is set to ON, the report is updated with new events as they occur.

This report includes all active events that exist at the time the report is generated, and that are associated with the physical infrastructure elements of the network, such as Hub Chassis, Line Cards, PP Clusters and PP Servers, NMS Clusters and NMS Servers.

Table 7-7. Configurator Setup to Monitor Events of Physical Infrastructure Elements

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	N/A
Date Range/Stream	N/A (set by default to Current Date/Time). **Stream** = ON.
View Selection	N/A
Elements	N/A
Severity	N/A
Generate Operation	N/A (Auto-generated)

Procedure: To report the current events of physical infrastructure elements

1. Click the **Monitoring** tab > **Real-Time Events** > **Physical Infrastructure Event Log**. The Configurator tool is automatically populated and the report of current events associated with all physical infrastructure elements is displayed.
2. Click on a column heading, for example **Element Name** to sort if necessary.
3. Click on a filter icon, for a column, to filter the list of displayed events if necessary.
4. Use the browser **Back** arrow to leave the page.

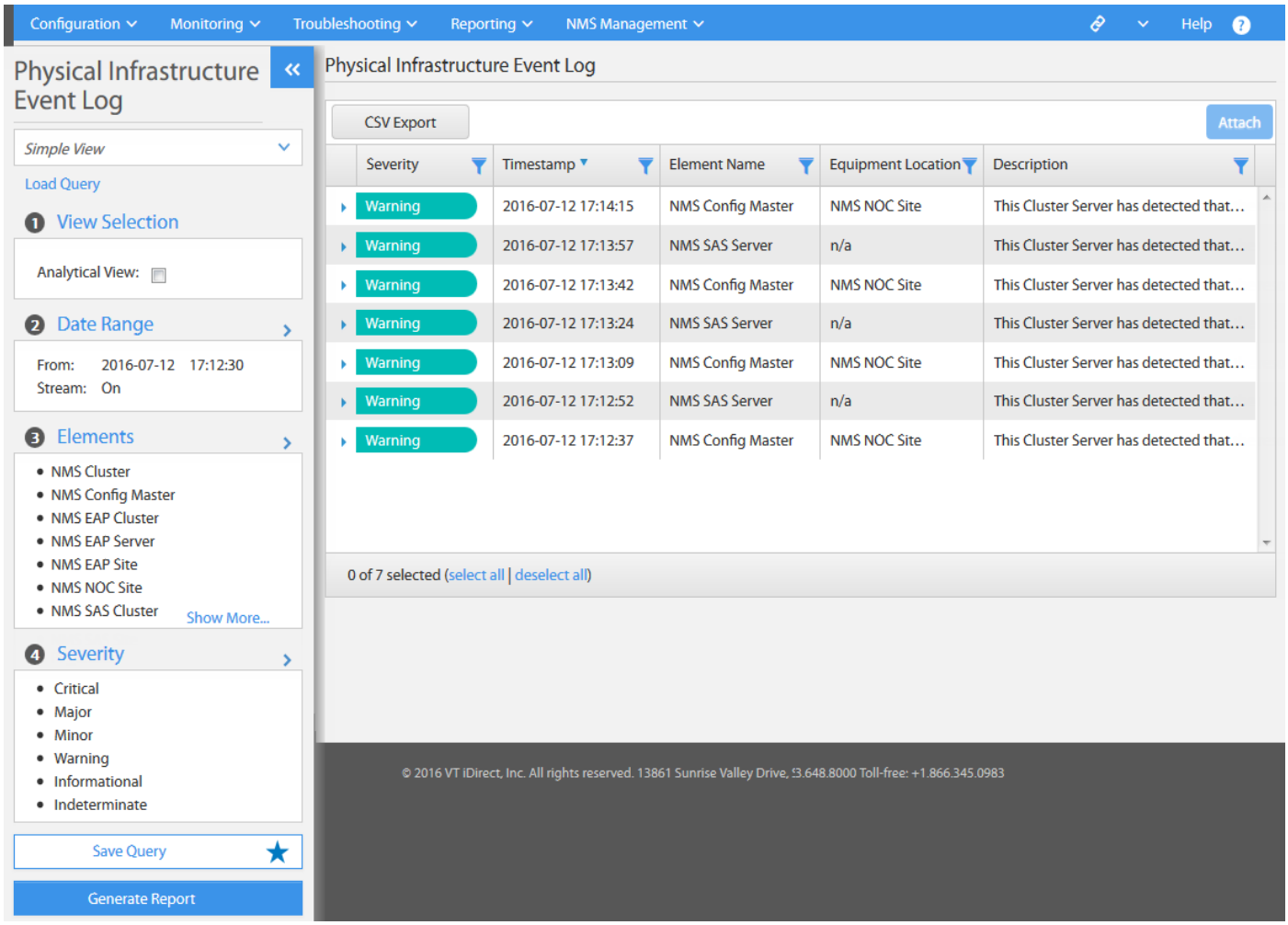

Figure 7-7. Current Physical Infrastructure Events Log

7.2.3 Use Case: Monitor Satellite Terminal Events

Show the current events for all satellite terminals of the network. For this use case, no user input to the Configurator panel is required after the appropriate Pulse operation is selected. Since the Configurator **Stream** parameter is set to ON, the report is updated with new events as they occur.

This report will include all active events at the time the report is generated, and that are associated with the Satellite Terminals in the network.

Table 7-8. Configurator Setup to Monitor Events for All Satellite Terminals

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	N/A
Date Range/Stream On	N/A (**Date Range** set by default to Current Date/Time). **Stream** = ON.
View Selection	N/A
Elements	N/A
Severity	N/A
Generate Operation	N/A (Auto-generated)

To report all of the current satellite terminal events:

1. Click the **Monitoring** tab > **Real-Time Events > Terminal Event Log**. The Configurator tool is automatically populated and the report of current events associated with all satellite terminals is displayed.
2. Click on a column heading, for example **Element Name** to sort if necessary.
3. Click on a filter icon, for a column, to filter the list of displayed events if necessary.
4. Use the browser **Back** arrow to leave the page.

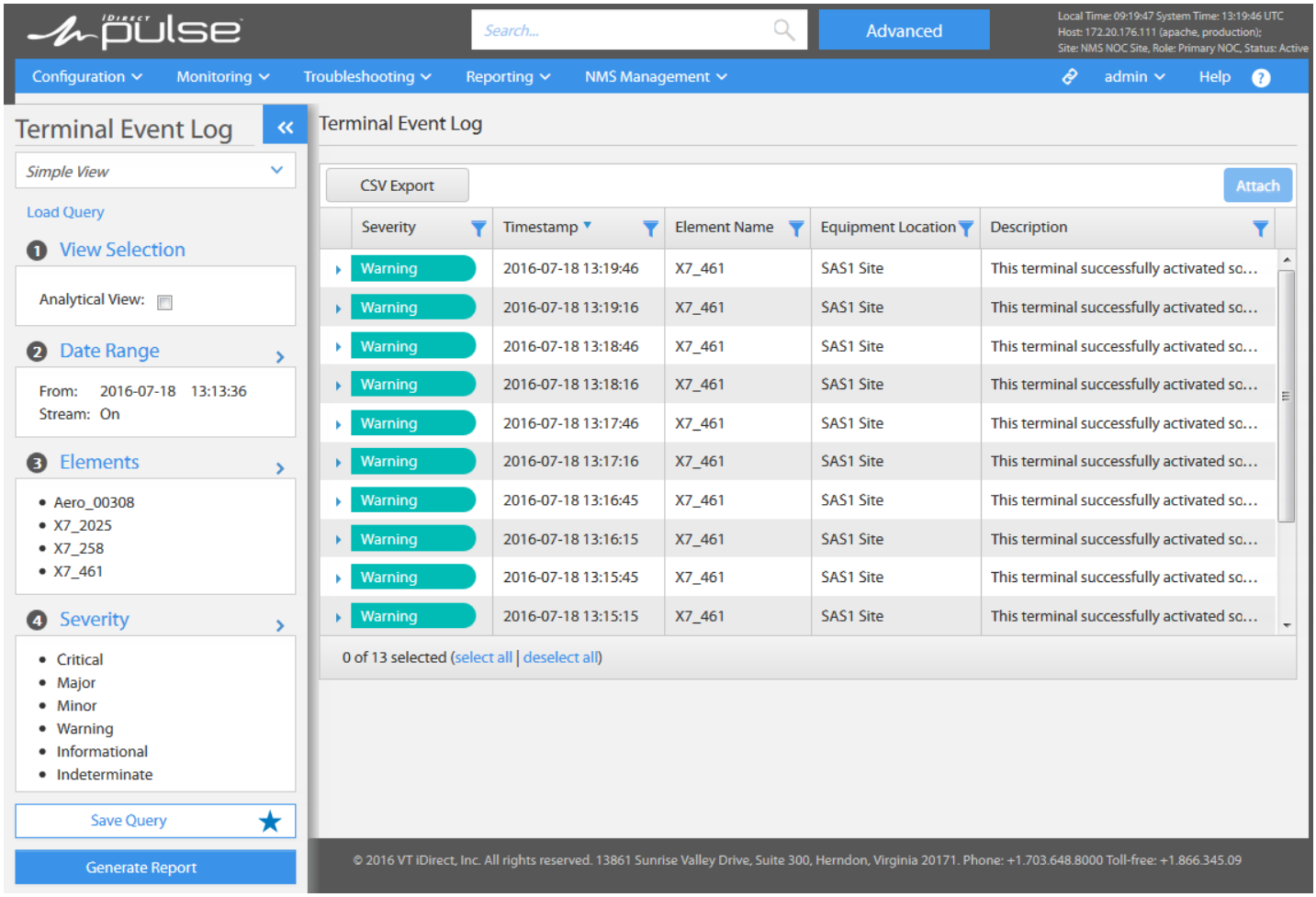

Figure 7-8. Current Satellite Terminal Events

7.2.4 Use Case: Generate an Events History Report

This report, which is manually configured by the user, is to generate a report of network events that occurred during a specific period, for any one or more specified elements.

The report may include events associated with physical infrastructure elements such as Hub Chassis, Line Cards, PP Clusters and PP Servers, NMS Clusters and NMS Servers; as well as events associated with logical infrastructure elements such as Satellites, Beams, Channels, iNets, Signaling Carriers, Upstream and Downstream Carriers.

Table 7-9. Configurator Setup to Generate an Events History Report

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	Select **Advanced View** to enable extended report options.
Date Range/Stream	Use default (Current Time - 24 hrs.); specify a report period; or select a pre-defined period. Set **Stream** = ON to update report with new events.
View Selection	Use default; or enable Analytical View to enhance report display.
Elements	Specify any one or more elements.
Severity	If **Advanced View** is enabled, the **Severity** levels to report can be set.
Log View	If **Advanced View** enabled, the default Log View can be modified.
Report Preferences	If **Advanced View** enabled, the report output type can be changed.
Analytical View	If **Analytical View** enabled, graphical **Chart** types can be configured.
Generate Operation	Manual

Procedure: To manually generate an events history report for one or more elements

1. Click the **Reporting** tab > **Report Builder > Events**.
2. Select **Advanced View** to display an extended set of Configurator parameter options.
3. Select **Analytical View** to correlate events data using optional bar graphs and pie charts.
4. Click **Date Range** and specify a date range or select any one of the predefined periods.
5. Click **Elements** to open the Basic Search tool or click **Advanced Search**, to find and specify one or more specific elements or element types to be included in the report.
6. Click the **Severity** selector to specify one or more severity levels to include in the report.
7. Click the **Log View** selector, if desired, to modify the report default settings. For example, modify **Columns** displayed, the reported event **Severity** levels or **Event Types**.
8. Click the **Analytical View** selector, if shown, to configure report charts — **Chart 1** through **Chart 4**, for **Line**, Area, **Pie,** or **Bar** graphs for displaying the Events Log data.
9. Click **Generate Report** to generate and view the **Event History** report. The Events History report is displayed. If configured, analytical charts are also shown in the report.

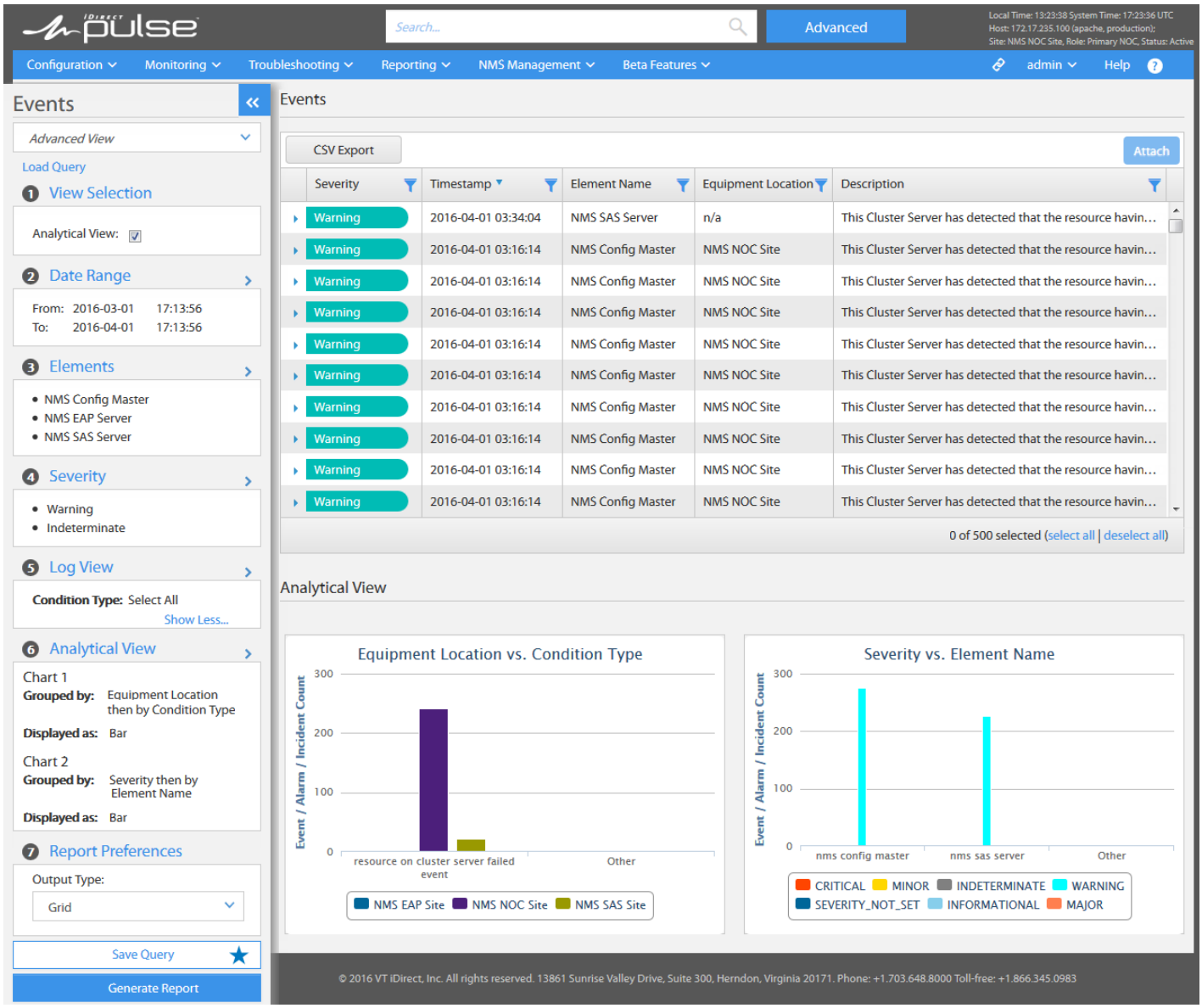

Figure 7-9. History Report of Network Events

7.3 Use Cases — Terminal Statistics

The following use cases are examples of user configurable network statistics reports for satellite terminals, executed from either Pulse **Monitoring** or **Reporting** menus.

7.3.1 Use Case: Terminal Upstream Performance Statistics

This use case, manually configured by the user, is to generate a report of network upstream performance statistics for one or more specified terminals during a specified period.

Table 7-10. Configurator Setup for Terminal Performance Statistics Report

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	Select **Advanced View** to enable extended Configurator report options.
Date Range/Stream	Specify a report period or select a predefined period.
Elements	Specify any one or more terminal elements.
Metrics	Specify the appropriate metrics for upstream performance.
Report Preferences	Specify **Output Type**, **Grouping**, **Chart Type**, and **Chart Size**.
Generate Operation	Manual

Procedure: To generate a terminal upstream performance statistics report

1. Click the **Reporting** tab > **Report Builder** > **Statistics Report.**
2. Select **Advanced View** to display the **Report Preferences** selector bar, to allow configuration of the report **Output Type, Grouping**, **Chart Type**, and **Chart Size**.
3. Click the **Date Range** bar to enter a report period or use one of the pre-defined periods; and specify a **Resolution**. If desired, select **Stream** to display new data as it occurs.
4. Click **Elements** to select one or more specific terminals for which the report should be generated. Each terminal is reported on a different chart.
5. Click the **Metrics** bar, and select the following metrics for generating a terminal upstream performance statistics report:
   a. Acquisition Burst Count
   b. Acquisition Burst CRC Errors
   c. Acquisition Burst Mismatches
   d. Acquisition Bursts Missing
   e. Data Burst Count
   f. Data Burst CRC Errors
   g. Keep-Alive Burst Count
6. Click **Done** to close the dialog and add the metrics to the Configurator.
7. Specify the following parameters under **Report Preferences**:
   a. **Output Type -** choose the output method as **Chart.**

b. **Grouping -** select **Group by Element.**

c. **Chart Type -** choose **Line** as how the data should be plotted.

d. **Chart Size -** choose the chart size as **Large.**

8. Click **Generate Report** to initiate generation of the report output.
9. Click on a specific report metric, on the chart legend, to toggle between showing and hiding the graph for that metric.

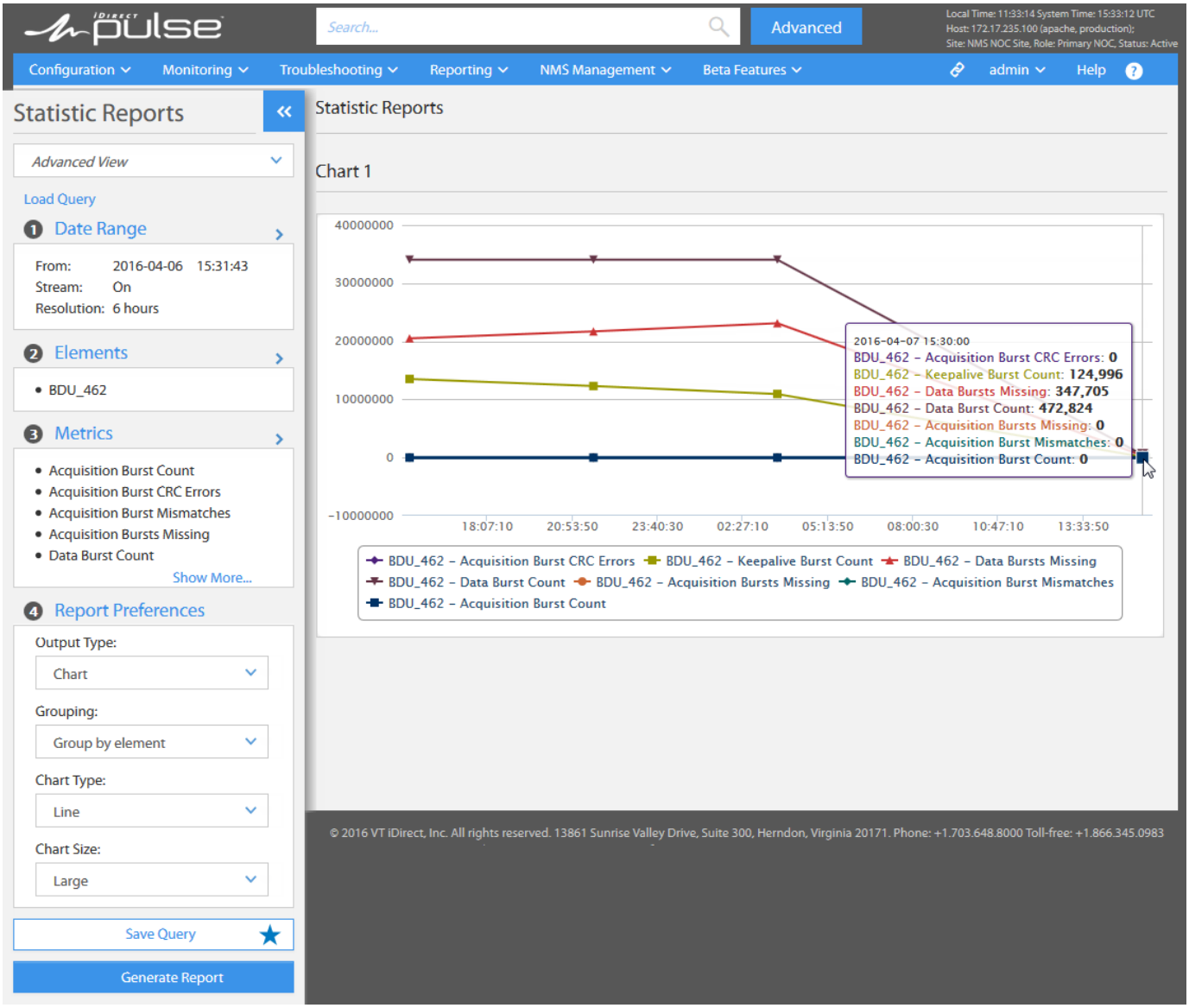

Figure 7-10. Terminal Upstream Performance Statistics Report

7.3.2 Use Case: Terminal Satellite Traffic Statistics

This use case, manually configured by the user, is to generate a report of network satellite traffic statistics for any one or more specified terminals during a specified period.

Table 7-11. Configurator Setup for Events History Report for Any Network Elements

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	Select **Advanced View** to enable extended Configurator report options.
Date Range/Stream	Specify a report period or select a predefined period.
Elements	Specify any one or more terminal elements.
Metrics	Specify data volume for both transmitted and received for HTTP, ICMP, IGMP, TCP, UDP, and Non-categorized traffic for all Other traffic.
Report Preferences	Specify for **Output Type**, **Grouping**, **Chart Type**, and **Chart Size**.
Generate Operation	Manual

Procedure: To generate a terminal satellite traffic statistics report

1. Click the **Reporting** tab > **Report Builder** > **Statistics Report.**
2. Select **Advanced View** to display the **Report Preferences** selector bar, to allow configuration of the report **Output Type, Grouping**, **Chart Type**, and **Chart Size**.
3. Click **Date Range** to enter a report period or use one of the predefined periods; and specify a **Resolution**. If desired, select **Stream** to display new data as it occurs.
4. Click **Elements** to select one or more specific terminals for which the report should be generated. Each terminal will be reported on a different chart.
5. Click the **Metrics** bar, and select the following metrics for generating a terminal satellite traffic statistics report:
   a. Remote HTTP data volume received
   b. Remote HTTP data volume transmitted
   c. Remote ICMP data volume received
   d. Remote ICMP data volume transmitted
   e. Remote IGMP data volume received
   f. Remote IGMP data volume transmitted
   g. Remote TCP data volume received
   h. Remote TCP data volume transmitted
   i. Remote UDP data volume received
   j. Remote UDP data volume transmitted
   k. Remote Non-categorized “other” data volume received
   l. Remote Non-categorized “other” data volume transmitted
6. Click **Done** to close the dialog and add the metrics to the Configurator.

7. Specify the following parameters under **Report Preferences**:
   a. **Output Type -** choose the output method as **Chart.**
   b. **Grouping -** select **Group by Element.**
   c. **Chart Type -** choose **Line** as how the data should be plotted.
   d. **Chart Size -** choose the chart size as **Large.**
8. Click **Generate Report** to initiate generation of the report output.
9. Click on a specific metric, on the chart legend, to toggle between showing and hiding the graph for that metric.

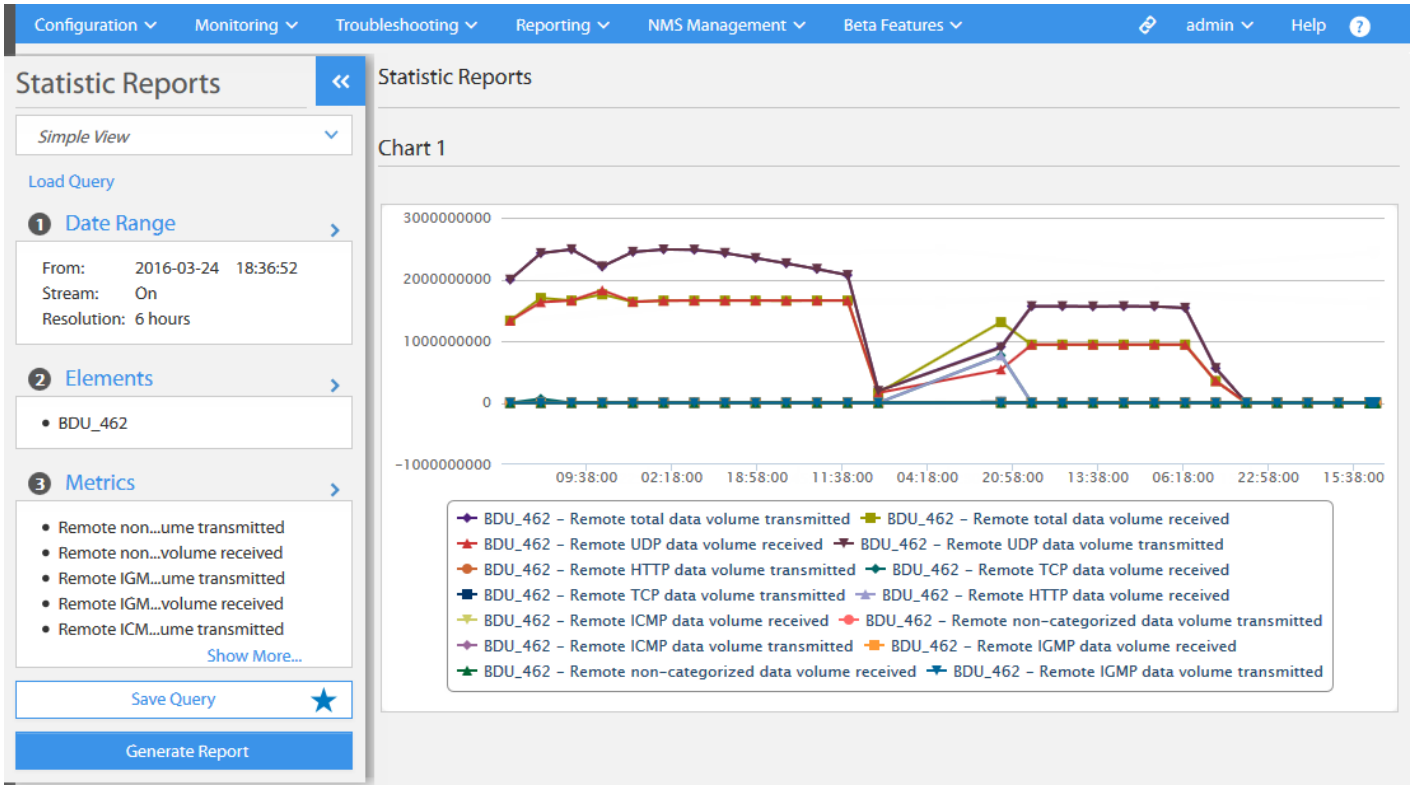

Figure 7-11. Terminal Satellite Traffic Statistics Report

7.3.3 Use Case: Terminal Availability Statistics

This use case, manually configured by the user, is to generate a report of terminal availability statistics for any one or more specified terminals during a specified period.

Table 7-12. Configurator Setup for Terminal Availability Statistics Report

Configurator Parameter	User Required Configurator Settings
Simple/Advanced View	Select **Advanced View** to enable extended Configurator report options.
Date Range/Stream	Specify a report period or select a predefined period.
Elements	Specify any one or more terminal elements.
Metrics	Specify the appropriate metrics for terminal availability statistics.
Report Preferences	Specify for **Output Type**, **Grouping**, **Chart Type**, and **Chart Size**.
Generate Operation	Manual

Procedure: To generate a terminal availability statistics report

1. Click the **Reporting** tab, and under **Report Builder**, select **Statistics Report.**
2. Select **Advanced View** to display the **Report Preferences** selector bar, to allow configuration of the report **Output Type, Grouping**, **Chart Type**, and **Chart Size**.
3. Click the **Date Range** bar to enter a report period or use one of the predefined periods; and specify a **Resolution**. If desired, select **Stream** to stream new data as it occurs.
4. Click the **Elements** selector to select one or more specific terminals for which the report should be generated. Each terminal will be reported on a different chart.
5. Click the **Metrics** bar, and select the following remote traffic metrics for generating a satellite traffic statistics report:
   a. Terminal Online Time
   b. Uptime
6. Click **Done** to close the dialog and add the metrics to the Configurator.
7. Specify the following parameters under **Report Preferences**:
   a. **Output Type -** choose the output method as **Chart.**
   b. **Grouping -** select **Group by Element.**
   c. **Chart Type -** choose **Line** as how the data should be plotted.
   d. **Chart Size -** choose the chart size as **Large.**
8. Click **Generate Report** to initiate generation of the report output.
9. Click on a specific metric, on the chart legend, to toggle between showing and hiding the graph for that metric.

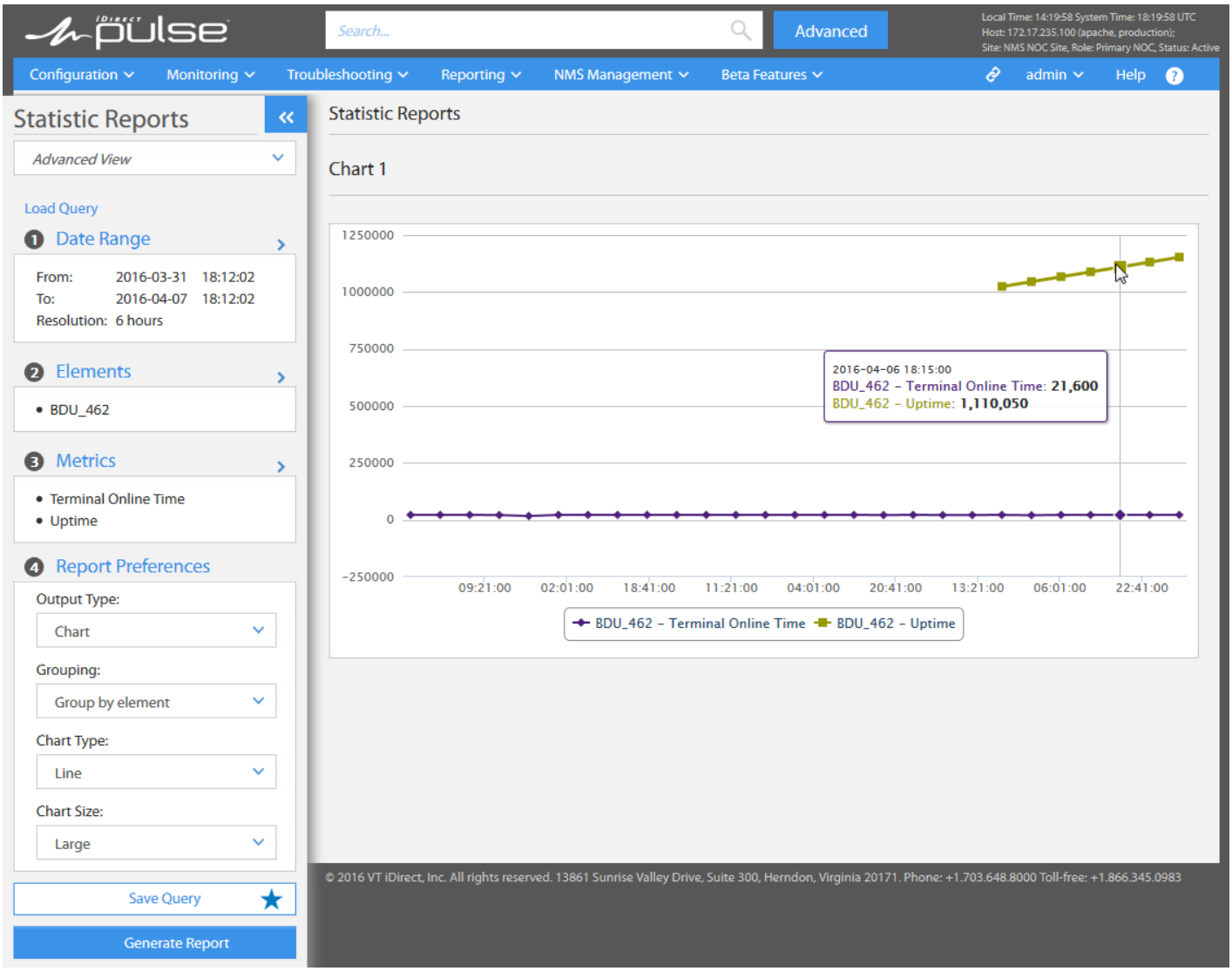

Figure 7-12. Terminal Availability Statistics Report

8 Troubleshooting Operations

Pulse Troubleshooting tools and operations include a variety of network probes that support detailed investigation of network issues. Diagnostic probes are available for infrastructure elements — including line card, cluster, and satellite terminals; and probes for Group Service Plan and Subscriber Service Plan Components.

Pulse Troubleshooting operations are covered in the following topics.

8.1 About Pulse Troubleshooting

Pulse NMS troubleshooting operations, which are accessed from the **Troubleshooting** tab, include the following operations categories:

- Probe Commands
- Engineering Debug Console Operations

The *probe command configurator* supports real-time interaction with the operating system of iDirect Satellite Terminal, Line Card, and Cluster infrastructure elements; as well as support for accessing network service elements including Group Service Plans (GSPs), and Subscriber Service Plan Components (SSPCs). Each of these network elements support a set of commands that allow users with permission to access and manipulate specific operations.

When setting Configurator parameters, the **Command** section of the dialog changes to reflect the selected element type. Each executed command provides feedback to indicate whether the operation was completed.

The *engineering debug console* provides direct access to a selected Satellite Terminal, Line Card, or Cluster server, using a shell window for debugging purposes.

8.2 Satellite Terminal Probe Commands

From the Probe Commands Configurator tool, terminal probe commands can be issued to perform specific tests, or to affect a specific behavior or operation of a satellite terminal.

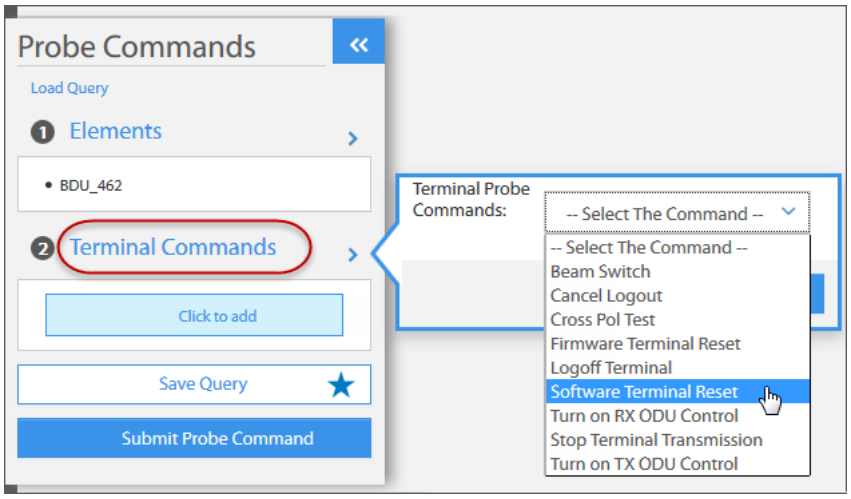

Figure 8-1. Probe Command Configurator - Terminal Commands

To issue satellite terminal probe commands using the configurator:

To issue satellite terminal probe commands using the Configurator:

1. Click the **Troubleshooting** tab > **Probe Commands**.
2. Click **Load Query**, if applicable, to load a saved set of Configurator parameters.
3. Click **Elements** to open the Basic Search tool.
4. Click the **Element Type** drop-down list and select **Terminal** to display terminals found in the NMS.
5. If necessary, use the **Performance/Operational** or **Config/Update** filter to narrow the list.
6. Select one or more terminals to which a probe command will be applied.
7. Click the **Terminal Commands** bar; use the **Terminal Probe Commands** drop-down list to select a command to issue; and click **Done** to add the command to the Configurator.
8. Depending on the command, a **Command Fields** section is displayed with one or more parameters that can be specified. Specify the parameters to be applied to the command.
9. Click **Submit Probe Command**, to issue the command on the selected terminals.

Table 8-1. Satellite Terminal Probe Commands

Probe Command	Brief Description
Beam Switch	Issue command to the satellite terminal, to switch beams based on the specified **IF Domain** and **iNet ID**.
Logoff Terminal	Issue command to the satellite terminal to logoff for a specified period of time. User session with the satellite terminal is logged off.
Cancel Logoff	Cancel previously issued “logoff terminal” command.
Stop Terminal Transmission	Initiate command to satellite terminal to stop transmitting (Mute Tx).
Turn On Tx ODU Control	Turn Tx ODU control (DC power) ON to BUC.
Turn On Rx ODU Control	Turn Rx ODU control (DC power) ON to LNB.
Software Terminal Reset	Initiate reset of the satellite terminal at the iDirect application level.
Firmware Terminal Reset	Initiate reset of the satellite terminal at the OS level.
Cross Pol Test	Supports installer in performing the cross-polarization test. Allows transmission of a modulated or un-modulated CW as part of the test.

8.3 Line Card Probe Commands

From the Probe Commands Configurator tool, users are able to issue commands to either perform specific tests, or to affect a specific behavior or operation of a Hub line card.

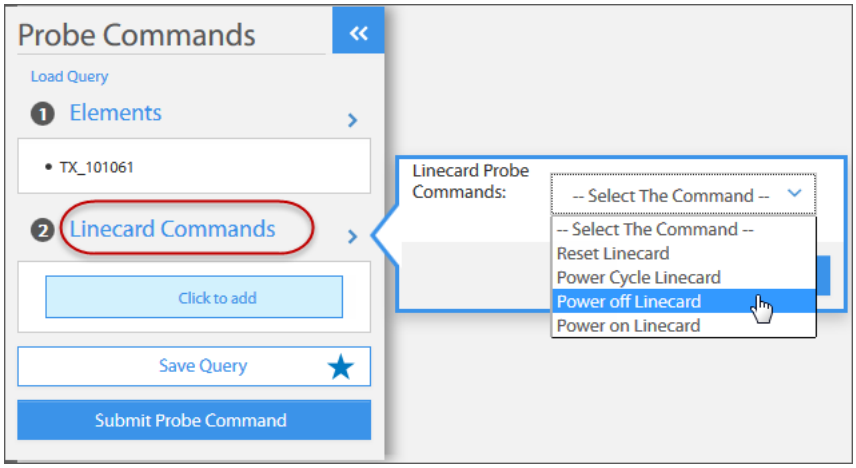

Figure 8-2. Probe Command Configurator - Line Card Commands

To issue line card probe commands using the Configurator:

1. Click the **Troubleshooting** tab > **Probe Commands**.
2. Click **Load Query**, if applicable, to load a saved set of Configurator parameters.
3. Click **Elements** to open the Basic Search tool.
4. Click the **Element Type** drop-down list and select **Line Card** to display a list of all the line cards found in the NMS. Both transmit and receive line cards are listed.
5. If required, use the **Performance/Operational** or **Config/Update** filters to narrow the list of line cards.
6. Select one or more line cards to which a command will be applied and click **Done**.
7. Click the **Linecard Commands** bar; use the **Linecard Probe Commands** drop-down list to select a command to issue; and click **Done** to add the command to the Configurator.
8. With the selected command displayed in the **Linecard Commands** section, click **Submit Probe Command**, to issue the command on the selected line cards.

Table 8-2. Line Card Probe Commands

Probe Commands	Brief Description
Reset Line Card	Initiate reset of the selected line card(s) at the iDirect application level.
Power Cycle Line Card	For the selected line card (s), switch power to OFF-state, and back to ON-state.
Power On Line Card	Switch the power to the selected line card(s) to the ON-state.
Power Off Line Card	Switch the power to the selected line card(s) to the OFF-state.

8.4 Cluster Probe Commands

From the Probe Commands Configurator tool, users are able to issue commands to either perform specific tests, or to affect a specific behavior or operation of a PP or NMS Cluster, located at the Teleport or NOC.

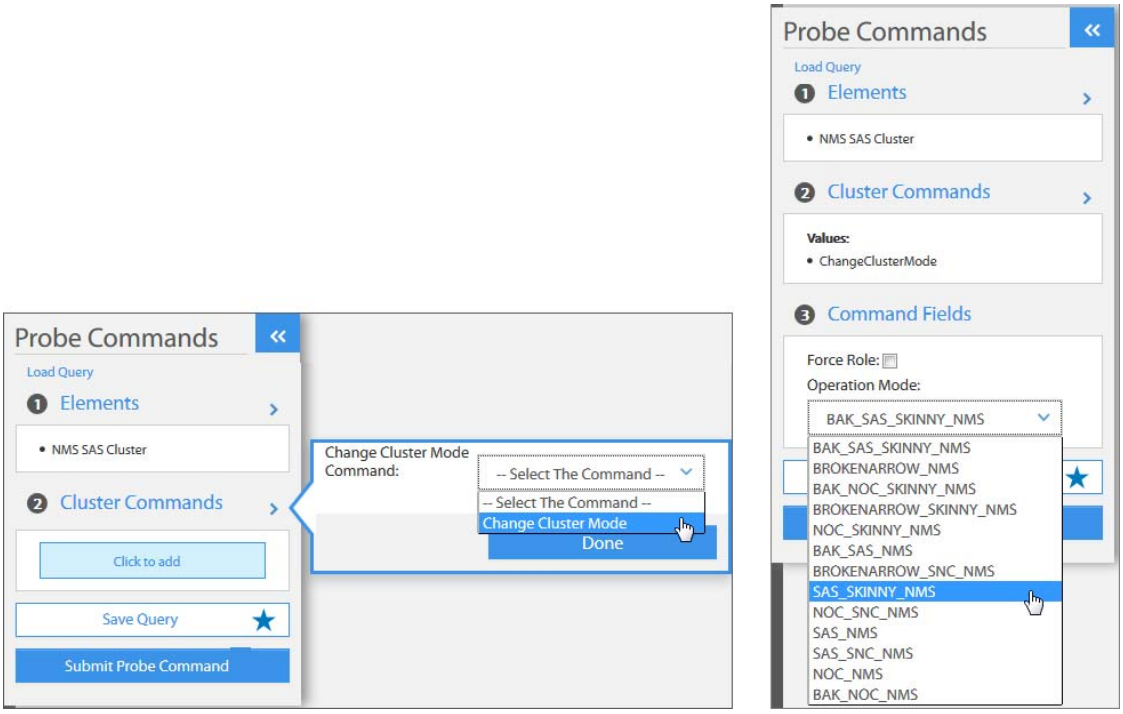

Figure 8-3. Probe Command Configurator - Cluster Commands

To issue cluster probe commands using the Configurator:

1. Click the **Troubleshooting** tab > **Probe Commands**.
2. Click **Load Query**, if applicable, to load a saved set of Configurator parameters.
3. Click **Elements** to open the Basic Search tool.
4. Click the **Element Type** drop-down list and select **NMS Cluster** or **Protocol Processor Cluster** to display a list of configured NMS or PP clusters.
5. Select a desired cluster to which a command will be applied, and click **Done** to add the selected cluster to the Configurator.
6. Click the **Cluster Commands** bar and use the **Change Cluster Mode Command** drop-down list to select **Change Cluster Mode**; and click **Done** to return to the Configurator.
7. The **Command Fields** section displays a set of parameters appropriate to the selected command. Specify the parameters to be applied to the selected Cluster command. The **Force Role** option is only required where there is no backup cluster available and it is necessary to move the current selected cluster into primary mode.

8. Under **Command Fields**, select **Force Role** to enable the command, and use the **Operation Mode** drop-down list to select the operational mode to which the cluster should be switched.
9. Click **Submit Probe Command**, to issue the command on the selected Cluster.

Table 8-3. Cluster Probe Command and Operational Mode Options

Operational Modes	Brief Description
Change Cluster Mode to:	
• BAK_SAS_SKINNY_NMS	5-node Teleport NMS Cluster - No Slave nodes for Regular and Fat Master Nodes
• BROKENARROW_NMS	7-node Teleport NMS Cluster temporarily resumes the authoritative role of NOC NMS Cluster (during NOC to Teleport connection failure)
• BAK_NOC_SKINNY_NMS	5-node Backup NOC NMS Cluster - No Slave nodes for Regular and Fat Master Nodes
• BROKENARROW_SKINNY_NMS	5-node Teleport NMS Cluster resumes the authoritative role of NOC NMS Cluster (during NOC to Teleport connection failure)
• NOC_SKINNY_NMS	5-node NOC NMS Cluster - No Slave nodes for Regular and Fat Master Nodes
• BAK_SAS_NMS	7-node complete operational Backup Teleport NMS Cluster
• BROKENARROW_SNC_NMS	Single node Teleport NMS Cluster temporarily resumes the authoritative role of NOC NMS Cluster (during connection failure to NOC)
• SAS_SKINNY_NMS	5-node Teleport NMS Cluster - No Slave nodes for Regular and Fat Master Nodes
• NOC_SNC_NMS	Single Node NOC NMS Cluster
• SAS_NMS	Node complete operational Primary Teleport NMS Cluster
• SAS_SNC_NMS	Single-node Teleport NMS Cluster
• NOC_NMS	7-node complete operational NOC NMS Cluster
• BAK_NOC-NMS	7-node complete operational Backup NOC NMS Cluster

8.5 Group Service Plan (GSP) Probe Commands

From the Probe Commands Configurator tool, GSP probe commands can be issued to perform specific operations that affect a GSP. For example, to issue a top-up credit, or to approve or decline a FAP overage allowance request. These probe commands may be carried out for both GSP (Group Service Plan) and SSPC (Subscriber Service Plan Component) elements.

The SSPC (Subscriber Service Plan Component) Probe Command procedure is identical to the GSP Probe Command procedure.

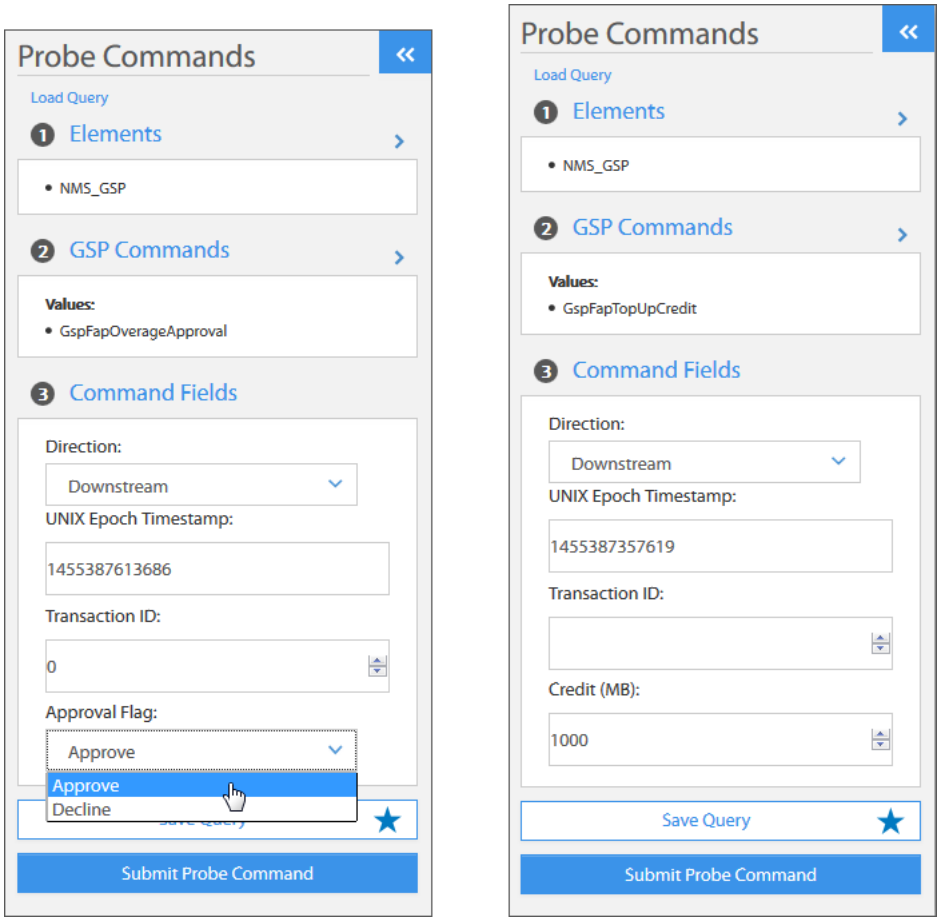

Figure 8-4. Probe Command Configurator - GSP Commands

1. Click the **Troubleshooting** tab > **Probe Commands**.
2. Click **Load Query**, if applicable, to access a saved set of Configurator parameters.
3. Click **Elements** to open the Basic Search tool.
4. Click the **Element Type** drop-down list and select **Group Service Plan** or **Subscriber Service Plan Component** to display a list of configured GSPs or SSPCs found in the NMS.
5. Select a GSP or SSPC from the list, and click **Done** to add the element to the Configurator.

6. Click the **GSP Commands** bar, or the **SSPC Commands** bar and use the **Probe Commands** drop-down list to select a command; click **Done** to add the command value to the Configurator.
7. Depending on the selected command, a **Command Fields** section is displayed with one or more parameters that can be specified.
8. Specify the parameters to be applied to the selected GSP or SSPC command.
9. Click **Submit Probe Command**, to issue the command.

Table 8-4. GSP/SSPC Probe Commands

Probe Commands	Brief Description
GSP FAP Overage Approval or SSPC FAP Overage Approval	Overage charges are per MB charges that are applied when the volume allowance is exceeded during the allowance period. Unless pre-approved, the defined volume allowance, if exceeded, will result in the overage charge. If this command is selected, a FAP Overage Approval can be individually **Approved** or **Declined** for the **Upstream** or **Downstream** Allowance.
GSP FAP Top-Up of SSPC FAP Top-Up	FAP top-up is the process of adding to the current allowance balance, a top-up credit allowance, specified in MBytes. A top-up allowance is a one-time allowance in MB that may be purchased separately at any time. It is typically purchased when the periodic volume allowance is depleted to avoid service interruption. If this command is selected, a FAP Top-up **Credit** can be specified, in MBytes, for the **Upstream** or **Downstream** Allowance.

8.6 Engineering Debug Console

The *engineering debug console* provides direct access to a selected element, using a shell window for debugging purposes. Access to this debug console is via the Configurator tool. Network elements that are accessible using this tool include Line Cards, Satellite Terminals, NMS and PP Servers, and the Chassis Controller.

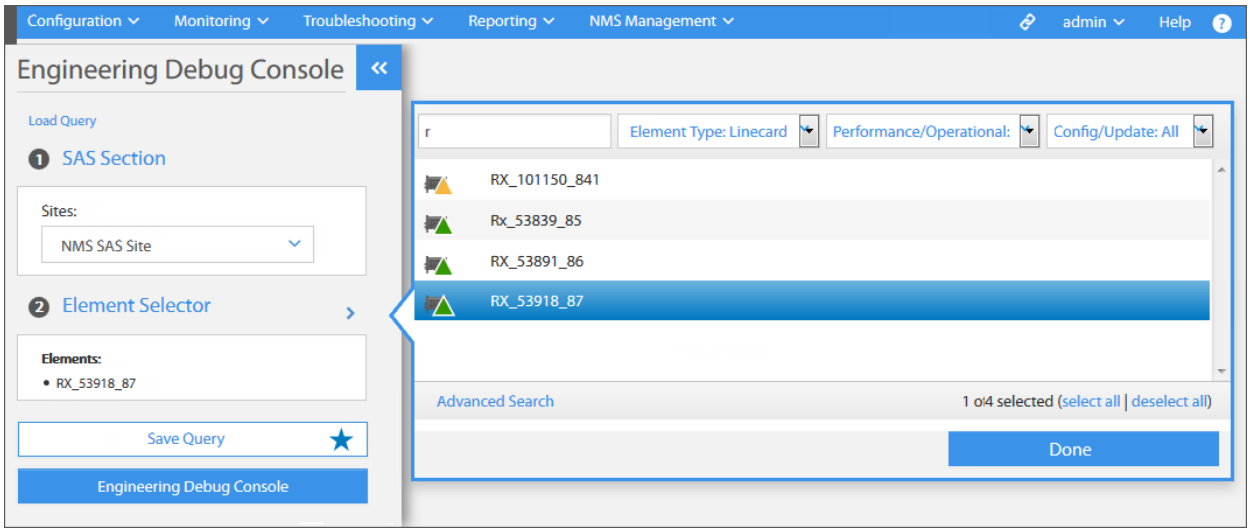

Figure 8-5. Engineering Debug Console

To issue probe commands using the Configurator:

To issue probe commands using the Configurator:

1. Click the **Troubleshooting** tab > **Engineering Debug Console.** The **Engineering Debug Console** dialog is opened.
2. Click **Load Query**, if applicable, to access a saved set of Configurator parameters.
3. Under the **SAS Section**, use the **Sites** drop-down list to select the appropriate site.
4. Click **Element Selector** to open the Basic Search tool.
5. Find and select a specific Terminal, Line Card, or Cluster Server element to which a debug command will be issued.
6. Click **Done** to add a selected element to the Configurator tool.
7. If applicable, click **Save Query**, to save the configuration for future use.
8. Click **Engineering Debug Console**, to open a shell command session directly with the selected element.

Glossary

2D 16-State — Type of Forward Error Correction coding available on iDirect inbound carriers in DVB-S2 networks. 2D 16-State coding can provide better link margins, improved IP throughput and faster acquisition than Turbo Product Coding.

ABS — See Automatic Beam Selection (ABS).

ACM — See Adaptive Coding and Modulation (ACM).

ACM Gain — The ACM Gain represents the increase in performance achieved on a DVB-S2 outbound carrier when the MODCOD used to transmit data is higher than the minimum MODCOD configured for the carrier.

Acquisition — The process whereby the satellite router synchronizes its bursts with the upstream TDMA frame timing and joins an iDirect network.

Access Class Value — On the channel side, a bit mask value that is logically combined, using the AND operation, with the terminal access class value when the terminal attempts to join the channel. If the logical result is non-zero, the terminal is allowed into the sub-channel — otherwise it is not.

Admin SVN — The iDirect administrative data VLAN.

Adaptive Coding and Modulation (ACM) — Adaptive Coding and Modulation. A method of applying coding to a data stream in DVB-S2 networks in which every BBFrame can be transmitted on a different MODCOD.

Allocation Fairness Relative to CIR — An iDirect Group QoS option which, when enabled, causes satellite bandwidth to be allocated in proportion to the configured CIR of the Group QoS node or virtual remote. When this option is disabled, bandwidth is allocated equally to competing nodes until available bandwidth is exhausted.

Allocation Fairness Relative to MODCOD	Applies only to DVB-S2 outbound carriers using Adaptive Coding and Modulation (ACM). An iDirect Group QoS option which, when enabled, causes satellite bandwidth allocation to be based on information rate rather than raw satellite bandwidth. This favors remotes at lower MODCODs, since their satellite bandwidth allocations must increase to achieve the same information rate as remotes at higher MODCODs.
Alternate Downstream Carrier	An iDirect feature that allows a second downstream carrier definition to be associated with an iDirect network in order to facilitate moving the network to a new downstream carrier.
Antenna Control Unit	An intelligent control device that both monitors and controls the positioning of a VSAT antenna.
Application	In iDirect Group QoS (GQoS), the definition of a specific type of service, such as Voice over IP or TCP. An Application is created from an Application Profile. An instance of an Application running on a remote is called a Virtual Remote.
Automatic Beam Selection (ABS)	An iDirect feature that automates the process by which roaming remotes select which network to join and automatically lock on to the associated outbound carrier. Also known as Automatic Beam Switching.
Backup Site	The backup (or secondary) operational site of any one of the Velocity network site pairs, to which operations can be switched if a failure occurs at the primary site. Each site and its optional backup/diversity site can operate as the primary or backup (secondary) site.
Bandwidth Group	An intermediary iDirect Group QoS node. A Bandwidth Pool contains one or more Bandwidth Groups. Each Bandwidth Group Contains one or more Service Groups.
Bandwidth Pool	The root (or top-level node) of an iDirect Group QoS tree. A Bandwidth Pool can be either an iDirect Network (which defines the QoS properties of the Downstream Carrier) or an Inroute Group (which defines the QoS properties of the Upstream Carrier.)
BGP	Border Gateway Protocol.
BGP Peers	Two or more routers that maintain a TCP connection, through BGP, for the purpose of exchanging BGP route table information.
BGP Peer Group	A group composed of member BGP peers that share common update policies, in order to simplify routing configuration and management.
BGP IP Prefix List	A filter list, which may be applied to a specific route map.

Blade	A short name for the Protocol Processor server machine.
Block Up Converter	A device used in the transmission of VSAT uplink signals.
BTP	See Burst Time Plan (BTP).
Burst Time Plan (BTP)	Slot allocation message sent to remote modems to indicate when each remote can transmit on the TDMA upstream carriers.
CA	See Certificate Authority (CA).
CA Foundry	The Certificate Authority (CA) utility that issues the X.509 public key certificates that allow "hosts" to join a secured network.
CCM	See Constant Coding and Modulation (CCM).
Certificate Authority (CA)	An authority in a network that issues and manages security credentials and public keys for message encryption.
Constant Coding and Modulation (CCM)	A method of applying coding in a DVB-S2 data stream in which every BBFrame is transmitted at the same MODCOD.
Channel	A channel is a fixed region of bandwidth on a satellite feeder link that is dynamically mapped onto a beam.
CIR	See Committed Information Rate (CIR).
Classification Rules	Rules and actions that determine how packets are filtered and prioritized.
Committed Information Rate (CIR)	A specified amount of bandwidth that is allocated to a node before additional (non-CIR) bandwidth is allocated to that node for traffic with the same priority.
Comms-on-the-MOVE (COTM)	Communications On-the-Move — an iDirect mobile remote feature.
COTM	See Comms-on-the-MOVE (COTM).
Customer SVN (Data SVN)	A Global SVN that connects customer equipment, located in the terminal network, behind a terminal, through the SAS and across the DCN to a customer network.

Derived ID (DID)	The unique identifier of an iDirect remote satellite router derived from the model type and serial number.
Deterministic TDMA (DTDMA)	A technique used to prevent collisions of remotes transmitting simultaneously in which synchronized burst time plan provides the network timing.
Dedicated Acquisition Signaling Carrier (ASC)	A DVB-S2 signaling carrier in which the hub broadcasts current satellite network configuration information, to terminals, on a single uplink and a single downlink.
Dedicated Acquisition Signaling Carrier (ASC) with fan-out	A single DVB-S2 signaling carrier, in a Velocity network, by which the hub broadcasts the current satellite configuration, on a single up-link that is replicated on multiple downlinks in different beams.
DID	See Derived ID (DID).
Downstream Carrier	Synonymous with Outbound Carrier. The satellite carrier transmitted from the hub to the remote.
DTDMA	See Deterministic TDMA (DTDMA)
DVB-S2	A set of open standards for satellite digital broadcasting. DVB-S2 is an extension to the widely-used DVB-S standard and was introduced in March 2005.
Dynamic Configuration	The terminal configuration information that is passed over the RF interface from the SAS to the remote, using an iDirect over-the-air dynamic configuration exchange protocol.
Dynamic Multicast Stream	When this Velocity multicast option is enabled, the terminal software accepts dynamic configuration of the static streams and configures IGMPv3 or MLD on a per terminal, per SVN basis. Dynamic multicast is the default option on all SVNs, but can be disabled.
Eight-Port Switch	Configurable LAN switch available on some iDirect remote satellite router model types.
EIR	See Enhanced Information Rate (EIR).
Enhanced Information Rate (EIR)	In iDirect's Group QoS (GQoS), the EIR option allows you to configure the system to maintain CIR or MIR during rain fade for the physical remote (Remote-Based Group QoS) or critical applications (Application-Based Group QoS). EIR only applies to networks that use DVB-S2 with Adaptive Coding and Modulation (ACM).

External Access Portal (EAP)	The EAP is an external instantiation of the Pulse NMS that provides limited access to NMS configuration, statistics, and reporting functionality for any users external to the Satellite Network Provider. The EAP also supports configuration capabilities that allow an EAP user with appropriate permissions to create, modify, and delete network elements.
Fast Fade Margin	For iDirect DVB-S2 outbound carriers, the additional margin added to the SNR thresholds measured at hardware qualification to arrive at the operational threshold during a "fast fade" condition.
Feature License	A license purchased from iDirect allowing NMS operators to configure a license-controlled feature.
Filter Profile	A traffic profile configurable in the NMS and assigned to remotes to filter out unwanted packets.
Free Slots	Slots left in the dynamic sub-frame after all stream, guaranteed (CIR) and preemptive bandwidth requests are satisfied. Free slots are allocated to all VSATs (up or down), except the master, in a round-robin fashion.
Frequency Hopping	The ability of iDirect remotes to switch between TDMA carriers within an inroute group when transmitting to the hub.
Full-Trigger CIR	Committed Information Rate (CIR) (CIR) that is always fully-allocated even if demand is less than the configured CIR.
Geographic Region	A geographic region that defined as a combination of satellites/beams, and/or service areas that constitutes an area of coverage.
Global SVN	An SVN type that is at the top of the Velocity SVN object structure and represents a VPN that extends across the Velocity core network (DCN) to another Site.
GQoS	See Group QoS (GQoS).
Group QoS (GQoS)	iDirect's Quality of Service (QoS) solution based on a hierarchical tree structure by which satellite bandwidth allocation flows down the tree from the root node to the leaf nodes. GQoS allows advanced network operators a high degree of flexibility in creating subnetworks and groups of remotes with various levels of service tailored to the characteristics of the user applications being supported.
Group Service Plan	A Group Service Plan (GSP), which may be defined by the Network Service Provider, is a plan of service that represents an acquisition of satellite bandwidth capacity on the Velocity Network.

Header Compression	A Velocity network optimization option that enables the compression of the IP header of each data packet prior to transmission. Two types of header compression are supported in Velocity — RTP header compression (used for RTP packets) and TCP header compression (used for TCP packets).
HLC	See Hub Line Card (HLC).
Hub Line Card (HLC)	An iDirect modem deployed at the hub to transmit and/or receive outroutes and inroutes.
Hub Network Operator (HNO)	An NMS operator with privilege to act as an administrator to Service Providers. An HNO can configure Service Provider users and networks and set Service Provider permissions such as visibility and read/write access.
iDirect Tunnel SVN	A Global SVN that connects Protocol Processors and Line Cards in a Velocity network.
IF Domain	An IF domain is represents a specific group of line cards and IF frequency ranges at which these line cards operate.
Inbound Carrier	Synonymous with Upstream Carrier. The carrier transmitted from the remote satellite router to the hub.
Indoor Unit (IDU)	The satellite modem and indoor devices (in contrast to Outdoor Unit or ODU).
Information Rate	The rate of transmission of user data over an upstream or downstream carrier including IP headers and iDirect overhead.
Inroute	A TDMA Upstream Carrier.
Inroute Group	A group of inroutes shared by a set of remotes in an iDirect network. Typically, a remote can frequency hop among the TDMA carriers within its inroute group.
Inroute Group Composition (IGC)	A set of defined carriers assigned to an inroute group.
LDCP	Low Density Parity Coding. The error correction coding scheme used in DVB-S2 networks.
LEGS	Lightweight Encapsulation for Generic Streams. An iDirect proprietary protocol for encapsulating data in DVB-S2 networks which maximizes the efficiency of data packing into BBFrames.

Low-noise Block (LNB) Converter	A receiving device that is integrated in the VSAT terminal to convert the signal gathered by the antenna feed circuit.
Maximum Information Rate (MIR)	In iDirect's Group QoS, a specification of the maximum bandwidth that will be allocated to a node, regardless of demand generated by the node. A node with MIR set will never be granted more bandwidth than the configured MIR bit rate.
Maximum MODCOD	The highest Modulation and Coding value used in DVB-S2 networks.
MIDAS Controller Board	A controller board used on newer iDirect chassis.
Minimum Information Rate (MIR)	In Group QoS, a specification of the minimum bandwidth that will be allocated to a node, regardless of demand generated by the node.
MIR	See Maximum Information Rate (MIR).
MODCOD	The combinations of Modulation Types and Error Coding schemes supported on a satellite channel. The higher the modulation the greater the number of bits per symbol (or bits per Hz).
Multicast Group Service Plan (MGSP)	A service plan that provides a data transmission service in which the data stream is simultaneously transmitted to multiple recipients, rather than sending separately to each recipient.
Multicast Subscriber Service Plan Profile (MSSPP)	Like the unicast SSPP, the MSSPP is configured in Pulse by authorized VNOs and used in creating a Terminal Service Plan - particularly, a multicast component of a TSP, to which individual terminals or a group of terminals may subscribe. When an MSSPP is selected as part of a TSP, an instance of the MSSPP is created in the NMS. The TSP configuration may consist of multiple components, where each component is an instance of a Unicast SSPP or Multicast SSPP.
Network Domain	In the Pulse hierarchy of network elements, the network domain that is immediately above the transport element domain — it consists of logical infrastructure elements such as iNet Profiles, Inroute Group Profiles, Upstream Carriers, Downstream Carriers, and Inroute Composition Groups.
Network Management System (NMS)	Software used by network operators to configure, control and manage networks.

Network Address/Port Translation (NAT/PAT or NAPT)	A process of modifying IP addresses as well as TCP/UDP port numbers so that nodes residing on a private network can share a public IP address for communication with the outside world.
NMS	See Network Management System (NMS).
NMS Server Cluster	A group of servers that act as a single system to provide the resources required by the Pulse NMS for managing network configuration and control, software version management and updates, as well as for monitoring and reporting on network events and alarms. The NMS server cluster is implemented at both the primary SAS, and optional backup SAS sites where applicable, and at the NOC site.
Nominal MODCOD	In the iDirect DVB-S2 implementation, the Reference Operating Point (ROP) for a remote receiving a downstream DVB-S2 carrier with ACM.
Options File	An iDirect configuration file generated by Pulse. Options files are used to download configuration settings to protocol processors, hub line cards and remote satellite routers.
Outbound Carrier	See Downstream Carrier.
Outroute	See Downstream Carrier.
Payload Compression	A mechanism whereby a datagram is compressed with the intent of reducing the size of data transmitted over congested or slow network connections, thereby increasing the speed of such networks without losing data.
Physical Domain	In the Pulse hierarchy of network elements, the physical domain is at the lowest level of the hierarchy, — it consists of hardware infrastructure network elements such as the NOC and SAS sites, VLANs, hub chassis and line cards, NMS and Protocol Processor (PP) servers, and other ancillary servers.
Primary Site	The main operational site of any one of the Velocity network site pairs. Each site and its optional backup/diversity site can operate as the primary or backup (secondary) site.
Protocol Processor	in a Velocity network, the SAS servers (primary/backup), which are responsible for processing functions, traffic routing, load balancing, automatic fail-over and automatic redistribution of load across the remaining PP servers. A PP cluster also resides at the NOC for handling global bandwidth management operations.
RCM	The Reference Clock Module in an iDirect line card chassis.

Remote Locking An iDirect feature that allows individual remotes to be locked to a particular network. Once a remote is locked with a key, it only functions in a network with the same key.

RTP Real-Time Transport Protocol. A protocol designed to provide end-to-end network transport functions for applications that transmit real-time data, such as audio, video, or simulation data, over unicast or multicast network services. RTP provides such services as payload type identification, sequence numbering, time-stamping, and delivery monitoring to real-time applications.

Route map A map that defines the routing policies that are considered before a router examines its forwarding table.

Satellite Access Station (SAS) The Velocity network terrestrial segment, also referred to as a hub, provides communications between the Service Provider Data communications Network (DCN) and the remote Satellite Terminals. A SAS site contains the SAS LAN, Protocol Processor (PP) servers, NMS servers, Web Cache servers, Chassis and Line Cards, the Radio Frequency Subsystem, and other ancillary equipment.

Satellite Virtual Network (SVN) In a Velocity network, an IP VPN that contains a satellite network segment.

Satellite Terminal Identification Message A terminal identification feature whereby, on each attempt to acquire the network, a terminal is screened, by the SAS, as to whether it should be allowed to acquire the network.

Server (Blade) SVN Each Server SVN is generated automatically as a result of creating a Site SVN and its parent Global SVN.

Service Area Group In Velocity, an SA Group maps to a single active map in the NMS, and represents an identifier pool from which service areas (SAs) can be designated when defining geoscopes or regulatory areas (RAs).

Site A Site, within an iDirect Velocity™ Network, is a collection of processes and equipment at a designated location — for example a *Satellite Access Station (SAS)* or a *Network Operations Center (NOC)*, or *External Access Portal (EAP)*.

Site SVN The Site SVN, just beneath the Global SVN in the Velocity SVN hierarchy, represents the segment of an SVN (VPN) located within a Site — for example within a NOC or SAS.

Sleep Mode An iDirect feature that allows remote modems to conserve power consumption during periods of network inactivity.

Spread Spectrum	A transmission technique in which a pseudo-noise (PN) code is employed as a modulation waveform to "spread" the signal energy over a bandwidth much greater than the signal information bandwidth.
Steady State Margin	In DVB-S2 networks, the margin added to the SNR thresholds measured at hardware qualification to arrive at the operational SNR threshold during steady state operation.
Static Multicast Stream	When this Velocity multicast option is enabled, the NMS provides the terminal with the static multicast configuration.
Static Configuration	The terminal configuration information that is stored in the configuration file, and is the minimum required by the terminal software for the terminal to acquire into a specific iNet.
Squid proxy	A Squid proxy, is a web proxy cache server application that provides caching services to a variety of network protocols, such as HTTP or FTP.
Symbol Rate	The number of symbols that are transmitted in one second. From the symbol rate, calculate the bandwidth (total number of bits per second) by multiplying the bits per symbol by the symbol rate.
Subscriber Service Plan Profile (SSPP)	In Pulse, a set of service plan parameters, configured in Pulse, for use in creating a Terminal Service Plan.
Subscriber Service Plan Component (SSPC)	When an SSPP is selected as part of a Terminal Service Plan (TSP), an instance of the SSPP is created in the NMS. That instance of the SSPP is called a Subscriber Service Plan Component, as it could be one of several components of the TSP.
TAC	See Technical Assistance Center (TAC).
TDMA	See Time Division Multiple Access (TDMA).
Technical Assistance Center (TAC)	iDirect's customer service and technical support center, at http://tac.idirect.net or 703-648-8151. iDirect Government customer service and technical support center, at http://tac.idirectgov.com.
Teleport	A Teleport, for example, contains elements hub equipment such as the Protocol Processor servers, line cards, and chassis; and the NMS and associated servers, and connecting SVNs. Also called SAS.
Terminal Domain	In the Pulse hierarchy of network element domains, the element domain that comprises terminals and terminal components.

Terminal SVN	That segment of an SVN that is located in the remote network behind a Satellite Terminal.
Terminal Type	A terminal type is a unique element type in the NMS that has a unique Name, is composed of specific terminal components (LNB, BUC, and ACU), a specific Satellite Router Type, and specific RF parameters. A terminal type is used in creating a terminal.
Terminal Service Plan (TSP)	It is the configured service plan of an individual terminal.
Time Division Multiple Access (TDMA)	A type of over-the-air multiplexing by which two or more channels of information are transmitted simultaneously over the same link by allocating different time slots within TDMA frames for the transmission of each channel.
Traffic Filters	Traffic filters are created to classify and manage packets presented on the Upstream or Downstream.
Transmission Rate	A measure of the speed of all over-the-air data. This includes the user data (Information Rate), iDirect overhead, and FEC encoding bits.
Transport Domain	In the Pulse hierarchy of network element domains, the element domain that represents a set of logical elements that are associated with the space segment of an iDirect Velocity™ Network. For example, satellites, beams, and channels.
UDP	User Datagram Protocol. A connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
Upstream Carrier	Synonymous with Inbound Carrier. The carrier transmitted from the remote satellite router to the hub.
Variable Coding and Modulation (VCM)	A method of applying coding to a DVB-S2 data stream in which MODCODs are assigned according to service type. iDirect does not support VCM.
VCM	See Variable Coding and Modulation (VCM).
Virtual Network Operator (VNO)	A member of a VNO User Group. A VNO User Group restricts visibility and access rights of group members based on the permissions granted to the group by the Hub Network Operator (HNO).

Virtual Remote In iDirect Group QoS, an instance of a Group QoS Application running on a remote modem. In Application Based QoS mode, a remote has one Virtual Remote for each Application assigned to the remote. In Remote Based QoS mode, all Applications are combined into a single Virtual Remote.

VLAN Virtual LAN. Any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is an abbreviation of local area network. To subdivide a network into virtual LANs, one configures a network switch or router.

VNO See Virtual Network Operator (VNO).

Appendix A Acronyms & Abbreviations

This list is generic within this document and may contain entries not found in the main body of the document. Some entries may not be defined based on industry standards.

0...9

16APSK Sixteen Amplitude and Phase Shift Keying

8PSK Eight Phase Shift Keying

-A-

A-TDMA Adaptive Time Division Multiple Access

ABS Automatic Beam Switching

AC Alternating Current

ACM Adaptive Coding and Modulation

ACS Antenna Control System

ADC Analog-to-Digital Converter

AES Advanced Encryption Standard

API Application Program Interface

APSK Amplitude and Phase-Shift Keying

ASC Acquisition Signaling Carrier

AZ Azimuth

-B-

BB BaseBand

BGP Border Gateway Protocol

BIM Broadband Interface Module

BIST Built-In Self-Test

BITE Built-In Test Equipment

BPN BUC Part Number

BPSK Binary Phase Shift Keying

BSN BUC Serial Number

BSS Broadcasting Satellite Service

BTP Burst Time Plan

BUC Block Up Converter

BW Bandwidth

-C-

C/N Carrier to Noise ratio

CA Certificate Authority

CBIT Continuous Built In Test

CCM Constant Coding and Modulation

CDR Critical Design Review

CIR Committed Information Rate

CNO Customer Network Observer

COTM Comms-On-The-Move

CPE Customer Premise Equipment

CPU Central Processing Unit

CRC Cyclic Redundancy Check

CSA Canadian Space Agency

-D-

DAC Digital-to-Analog Converter

dB deciBel

dBi deciBel isotropic

dBm deciBel milli-Watt

dBW deciBel Watt

DC Direct Current

DDR Double Data Rate

DHCP Dynamic Host Configuration Protocol

DID Derived ID

DNS Domain Name Service

DSCP Differentiated Services Code Point

DTDMA Deterministic TDMA

DVB-S2 Digital Video Broadcasting over Satellite, Second Generation

-E-

EAP External Access Portal

EIRP Effective Isotropic Radiated Power

Eb/N0 Bit Energy to Noise Power Spectral Density Ratio

EEPROM Electrically Erasable Programmable Read-Only Memory

EIR Enhanced Information Rate

EIRP Effective Isotropic Radiated Power

EL Elevation

EMC ElectroMagnetic Compatibility

EMI ElectroMagnetic Interference

ER Embedded Router

ESR Embedded Service Router

ETSI European Telecommunications Standards Institute

-F-

FAP Fair Access Policy

FCC Federal Communication Commission

FEC Forward Error Correction

FID Functional ID

FMECA Failure Mode Effects Criticality Analysis

FOM Figure of Merit

FPGA Field Programmable Gate Array

FS Functional Specification

-G-

G/T Gain over Temperature

GBWM Global Bandwidth Manager or Management

GHz GigaHertz

GPIO General-Purpose Input/Output

GPS Global Positioning System

GQoS Group (QoS) Quality of Service

GSP Group Service Plan

GUI Graphical User Interface

GW Gateway

-H-

HCP High-Capacity Payload

HLC Hub Line Card

HNO Host Network Operator

HTTP Hypertext Transfer Protocol

-I-

IBIT Initiated Built In Test

ICD Interface Control Document

iDX Evolution Software System

IEC International Electrotechnical Commission

IFL Inter-Facility Link

IF Intermediate-Frequency

IGC Inroute Group Composition

IGMP Internet Group Management Protocol

IP Ingress Protection

IP Internet Protocol

IR Infrared

-K-

kbps kilobits per second

kHz kilohertz

KRFU Ku/Ka-band Radio Frequency Unit

ksps kilo symbols per second

-L-

LAN Local Area Network

LDP Low-Density Parity Coding

LED Light Emitting Diode

LHCP Left Hand Circular Polarization

LNB Low Noise Block Converter

LO Local Oscillator

LOS Loss of Signal

LRU Line-Replaceable Unit

LSHF Low Smoke and Halogen Free

-M-

Mbps Megabits per second

Mcps Megachips per second

MES Mobile Earth Station

MF-TDMA Multi-Frequency TDMA

MGSP Multicast Group Service Plan

MHz Megahertz

MID Manufacturer ID

MIL-STD US Military Standard

MIR Maximum Information Rate

MODCOD MODulation and CODing

MP-BGP Multi-Protocol - Border Gateway Protocol

MPLS Multi-Protocol Label Switching

MPLS-TE Multi-Protocol Label Switching-Traffic Engineering

Msps Mega Symbols per Second

MSSPP Multicast SSPP

MTBF Mean Time Between Failures

MTBUR Mean Time Between Unscheduled Removals

-N-

NAND Negated AND

NF Noise Figure

NOR Negated OR

NMS Network Management System

NSP Network Service Provider

NTP Network Time Protocol

-O-

OAE Outside Antenna Equipment

ODU Outdoor Unit

OEM Original Equipment Manufacturer

OMT Orthogonal-Mode Transducer

OpenAMIP Open Antenna-Modem Interface Protocol

OSD Operational Start Date

OSPF Open Shortest Path First

OTA Over The Air

OTP One Time Programmable

-P-

PA Power Amplifier

PAST Person-Activated Self-Test

PCB Printed Circuit Board

PDR Preliminary Design Review

PEP Performance Enhancing Proxy

PLL Phased Locked Loop

PP Protocol Processor

PPS Packets Per Second

PPS Pulses Per Second

PSK Phase Shift Keying

PSU Power Supply Unit

-Q-

QAM Quadrature Amplitude Modulation

QEF Quasi Error Free

QoS Quality of Service

QPSK Quadrature Phase Shift Keying

-R-

RA Regulatory Area

RCM Reference Clock Module

RF Radio Frequency

RFS Reference System

RGMII Reduced Gigabit Media Independent Interface

RHCP Right Hand Circular Polarization

RMS Root Mean Square

RoHS Restriction of Hazardous Substances

ROM Read-Only Memory

RSSI Receive Signal Strength Indication

RTP Real-Time Protocol

Rx or RX Receive

-S-

SA Service Area

SAS Satellite Access Station

SCPC Single Channel Per Carrier

SGMII Serial Gigabit Media Independent Interface

SIM Subscriber Identity Module

SLA Service Level Agreement

SNR Signal-to-Noise Ratio

SOAP Simple Object Access Protocol

SP Service Provider

SRS Systems Requirement Specification

SRU Shop Replaceable Unit

SSB Single Side Band

SSPC Subscriber Service Plan Component

SSPP Subscriber Service Plan Profile

STP Spanning Tree Protocol

SVN Satellite Virtual Network

-T-

TAC Technical Assistance Center

TBD To Be Determined

TBS To Be Supplied

TDM Time Division Multiplexing

TDMA Time Division Multiple Access

TFI Terminal Functional ID

TMI Terminal Manufacturer ID

TOS Type Of Service

TPCFEC Turbo Product Code FEC

TPN Terminal Part Number

TSN Terminal Serial Number

TSP Terminal Service Plan

TTC Terminal Transmit Control

Tx or TX Transmit

-U-

UDP User Datagram Protocol

UI User Interface

UL Underwriters Laboratories

UMD Update Manager Daemon

UTC Universal Time, Coordinated

-V-

VAC Volts Alternating Current

VCM Variable Coding and Modulation

VDC Volts Direct Current

VNO Virtual Network Operator

VSAT Very Small Aperture Terminal

-W-

WAN Wide Area Network

WFQ Weighted Fair Queuing

WGS Wideband Global SATCOM

Appendix B Re-Configuring an ASC

Re-configuring an ASC, is the subject of this appendix. This task requires a strict set of procedures that must be performed in the sequence they are presented.

Acquisition signaling carrier (ASC) properties may require changing from time-to-time, due to a number of reasons. If ASC properties, such as frequency, symbol rate or polarization, must be changed, the procedure must ensure that all terminals contain valid signaling channels in their CONSTELLATION_OPT file at all times — otherwise the terminals may become stranded.

B.1 Re-Configuring an Acquisition Signaling Carrier

Changes to the ASC downlink properties directly affect the ability of a terminal to obtain a new beam map and ultimately to acquire the network. If the ASC configuration changes, and this change is not reflected in the CONSTELLATION_OPT file, of any terminal, then that terminal will not be able to reacquire into the network.

The sequence of changing the ASC, used by the PP and Terminals, is given in the in the detailed step-by-step instructions of following procedures (Procedure 1 through Procedure 7):

Procedure 1. Add Alternate Outbound Frequency to ASC

The first step in reconfiguring an existing acquisition signaling carrier (ASC), is to configure an alternate frequency, based on the information for the new signaling carrier. This alternate or secondary frequency, which will be added to the CONSTELLATION_OPT options file, will be rolled-out to the terminals before the ASC uplink is modified.

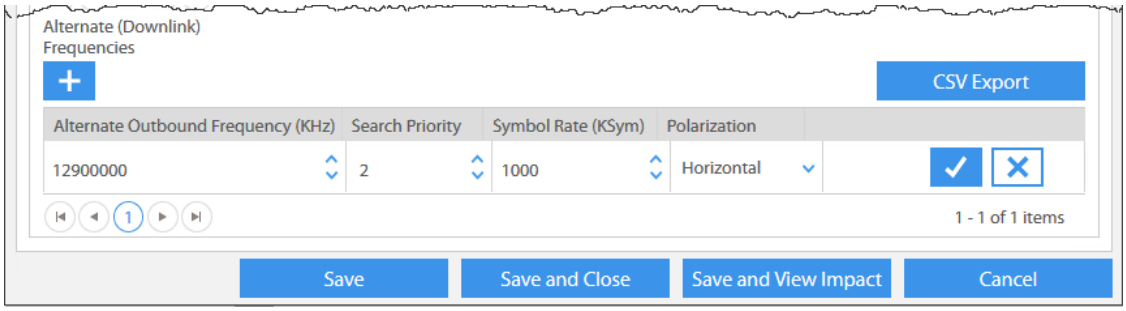

Figure B-1. Add Alternate Downlink Frequency Records Dialog

To add new ASC alternate downlink frequencies:

1. On the NMS **Configuration** tab, click **Browse Transport Domain**.
2. Under **Element Type** filter select **Acquisition Signaling Channel** to list the ASCs.
3. Click **Actions** on the desired ASC and select **Modify Acquisition Signaling Carrier**.
4. From the **Add Acquisition Signaling Carrier** dialog, click the **Add Record** icon under Alternate (Downlink) Frequencies, as shown in Figure B-1. The fields are enabled.
5. Using the information for the new signaling carrier, enter the new **Alternate Outbound Frequency**, in kHz.
6. Enter a **Search Priority**. This value of 1-5, where 1 is the highest and 5 is the lowest, determines the search order when multiple alternate frequency records are configured.
7. Enter the **Symbol Rate**, for the new alternate frequency record, in Ksps.
8. Specify the **Polarization** as **Vertical** or **Horizontal;** or as **LHCP** or **RHCP**.
9. Click the **Update** icon to accept the new Alternate Outbound Frequency record.
10. Click **Save and Close**. Auto-navigate to **Browse Acquisition Signaling Carrier** window.
11. On the newly modified ASC, click **Actions** and then select **Apply Configuration**.

Procedure 2. Confirm Global Network Option Changes

This second procedure is to confirm that the newly added carrier is accurately included in the CONSTELLATION_OPT file. Since this options file is global to the network, it resides at the **Network System** level, and is accessed from the Pulse **NMS Management** tab. Once the changes are validated, they can be safely applied to the network. This action enables all network terminals to receive this option and activate the new constellation options file.

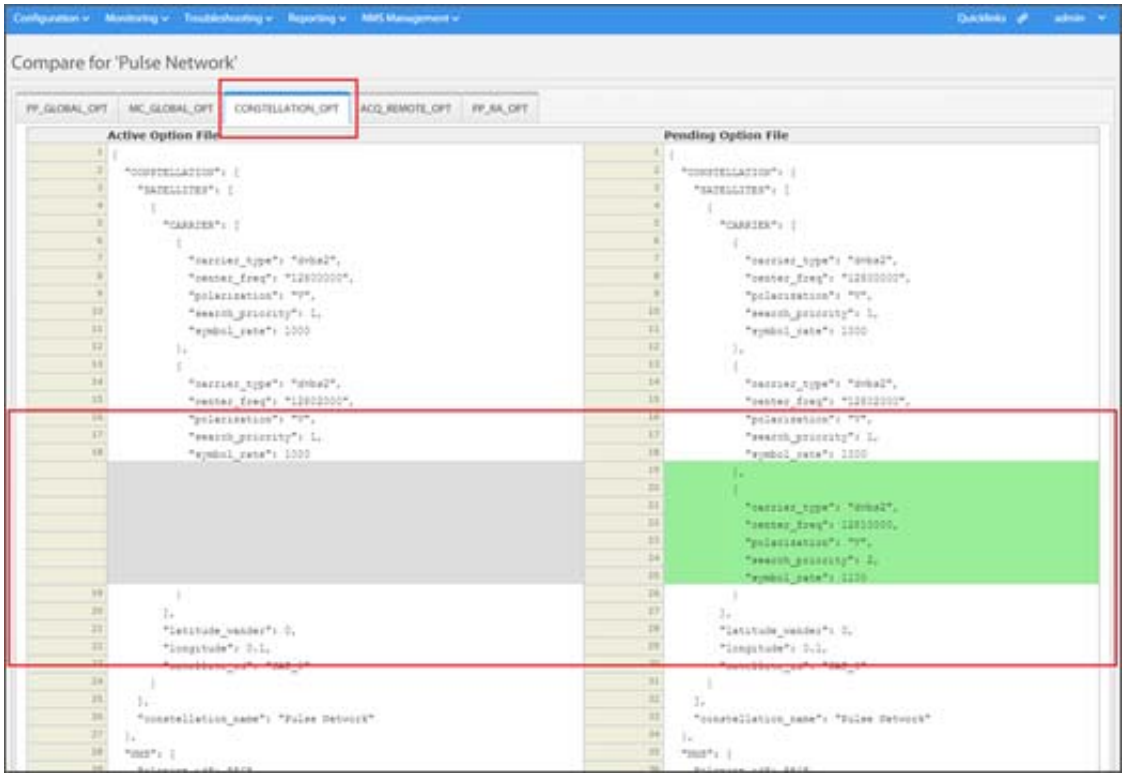

Figure B-2. Compare Pending/Active Constellation Option file

To confirm that updates to the global network options are made:

1. From the **NMS Management** tab under the **NMS Services** menu, under **Browse**, click **Network Systems.**
2. From the **Browse Networks** results, find the correct **Network System** — for example **Pulse Network**; click **Actions** and select **Compare Configuration**. The **Compare for 'Pulse Network'** page opens, as shown in Figure B-2.
3. Click on the **CONSTELLATION_OPT** tab to view a side-by-side comparison of the newly modified "**Pending Option File**," and the currently in-use "**Active Option File**."
4. Verify that the changes are applied. See the highlighted section of the **Pending Options File**, which reflects the alternate frequencies updates that were added to the ASC.
5. After the updates are verified, click **Apply Configuration** to activate the new Constellation Options File on all terminals in the network.

Procedure 3. Verify CONSTELLATION_OPT Received in Terminals

In the previous procedure, applying the modified ASC configuration caused the NMS to push the CONSTELLATION_OPT file to the terminals. Terminals must be in network to receive and locally store the new options file. A verification of whether the CONSTELLATION_OPT file was successfully received by all terminals in the network can be performed by generating a Pulse report of the "Terminal Constellation Configuration Install Success" event as detailed below.

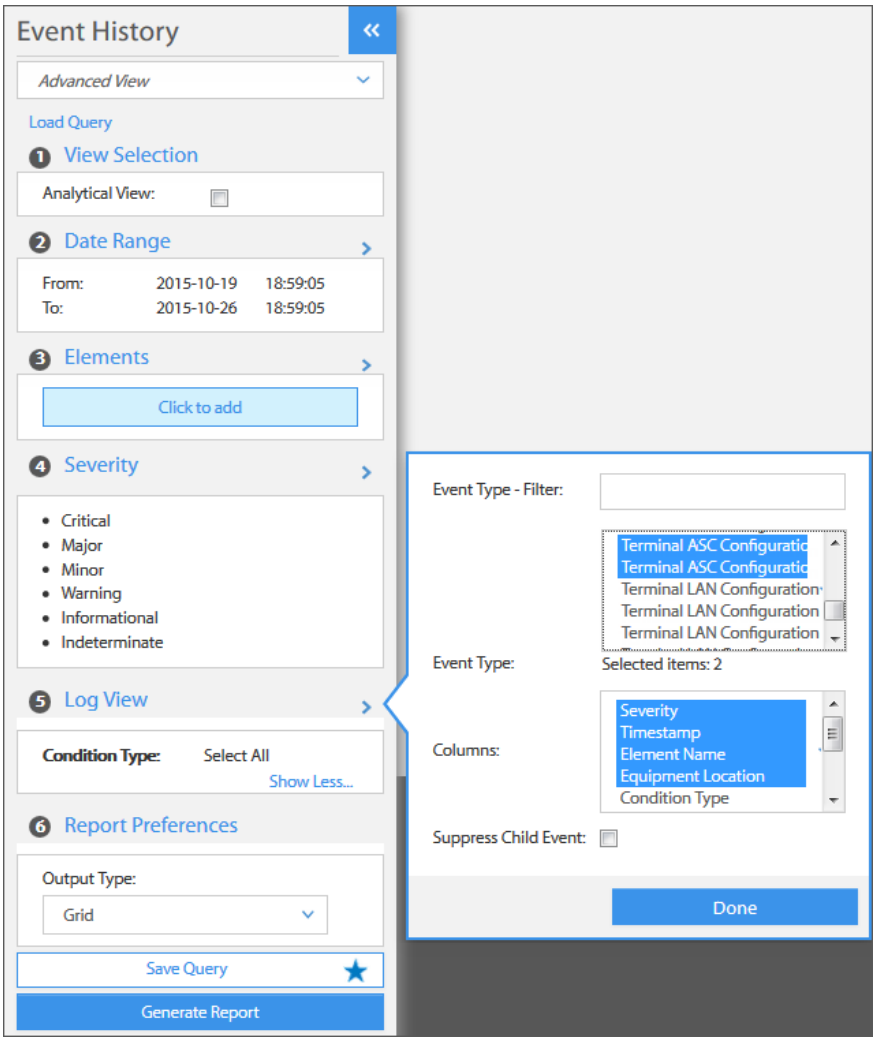

Figure B-3. Filtering Terminal ASC Configuration Install Success Event

To confirm that the constellation option file is on the terminals:

1. Click the Pulse NMS **Reporting** tab and under the **Report Builder** menu select **Events**.
2. Select **Advanced View**.
3. Select the **Date Range**, ensuring that the **From Date** is the date on which the CONSTELLATION_OPT change was pushed from the Pulse to be applied on the Terminals.

4. Click the **Element Selector** to open the Basic Search window, and use the **Element Type** filter and select **Terminal** to display all terminals found in the NMS.
5. Click **select all** and click **Done** to load all of the found Terminals to the Configurator.
6. Click the **Log View** selector and use the **Event Type - Filter** to filter the list based on the event "**Terminal Constellation Configuration Install Success**," and click Done. Only terminals that successfully received the Constellation Options file will be listed in the report.
7. Click **Generate Report** to view a report of the terminals that successfully received the Constellation Options file.

NOTE: The following troubleshooting tips apply to whether a terminal receives the CONSTELLATION_OPT option file pushed from the Pulse NMS:

- **Terminal in Network When Option File Push Occurs —** file should be pushed correctly and stored locally on the terminal. Receipt of the file should be verifiable.
- **Terminal in Network But Options File Push Fails —** the OTA upgrade troubleshooting steps should be performed, to check for any problems with the upgrade.
- **Terminals Out of Network When Option File Push Occurs —** will not receive the option file. Operators must wait until these terminals reacquire and are in sync with the NMS — the terminals should then receive the new CONSTELLATION_OPT file.

NOTE: Network Operators must determine, based on experience, how long to give out-of-network terminals to re-acquire the network and sync up with the NMS — for example, the wait-time will be significantly shorter for 10 terminals as opposed to 100 terminals.

- **Terminals Powered Off When Option File Push Occurs —** If one or more terminals were powered off for an extended period, they may have received the CONSTELLATION_OPT file, prior to being powered off. If, however, a terminal does not have a valid signaling carrier in its constellation file or the file is missing, then it will be unable to join the network and subsequently be stranded. The CONSTELLATION_OPT file will have to be updated locally, by an installer, using the Remote Terminal Web User Interface.

Procedure 4. Update the ASC Up-Link Frequency

The previous procedure was to verify if all of the satellite terminals had received the new alternate frequencies that were contained in the CONSTELLATION_OPT file. With that part of the re-configuration completed, the new ASC Up-link configuration can be implemented. Once the Up-link Frequency is updated, the changes are updated on the PP, and the PP can use the new Up-link frequency — which will already be known by the satellite terminals.

NOTE: This step may be unnecessary if the operator change only affects the satellite itself and the PP-satellite up-link is not modified.

Perform the following steps to configure the new ASC Up-link:

1. On the NMS **Configuration** tab, click **Browse Transport Domain**.
2. Under **Element Type** filter select **Acquisition Signaling Channel** to only list ASCs.
3. Click **Actions** on the appropriate ASC and select **Modify Acquisition Signaling Carrier**.
4. Modify the field entries for **Gateway (Uplink) Frequency**, **Gateway (Uplink) Polarization**, **Power**, **Symbol Rate**, **Primary Outbound Frequency**, and **Polarization**.
5. Based on the new signaling carrier, enter the new **Primary Outbound Frequency**, in kHz.
6. Click **Save and Close** to save and open the **Browse Acquisition Signaling Carrier** window.
7. On the appropriate ASC, click **Actions** and **Apply Configuration**.

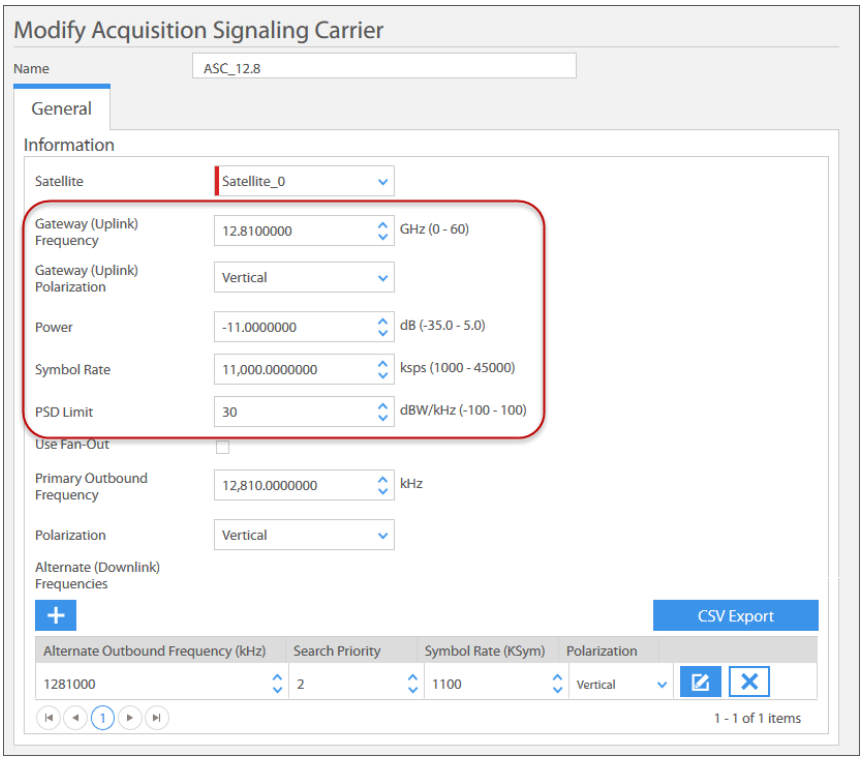

Figure B-4. ASC Uplink Parameters

Procedure 5. Confirm Global Network Option Changes

The steps of **Procedure 4** made the original intended changes to the ASC, by updating the Uplink parameters. This change was only possible after the alternate frequencies were successfully pushed to the satellite terminals. This change, which should be confirmed, should be reflected at the Network System level — indicated in the PP_GLOBAL_OPT file.

Once the changes to the ASC Uplink are validated, they can be safely applied to the network. This PP can then transmit on the new ASC Uplink.

To confirm that updates to the ASC are reflected in the global network options:

1. From the **Configuration** tab, under **NMS Management**, click **Browse Networks.**
2. Find the correct **Network System** — for example **Pulse Network**; click **Actions** and **Compare Configuration**. The **Compare for 'Network'** page opens.
3. Click on the **PP_GLOBAL_OPT** tab to view a side-by-side comparison of the newly modified "**Pending Option File**," and the currently in-use "**Active Option File**." Here in addition to the CONSTELLATION_OPT, there will also be changes in PP_GLOBAL_OPT.
4. Verify that the changes are applied. See the highlighted section of the **Pending Options File**, which reflects the Uplink parameters updates that were added to the ASC.
5. After the updates are verified, click **Apply Configuration** to activate the new Constellation Options File on all terminals in the network.

Procedure 6. Remove Alternate Downlink Signaling Carriers

The steps of **Procedure 5** verified that the configuration updates to the ASC Uplink parameters were reflected at the Network System level, and therefore in the PP_GLOBAL_OPT file. Now that all satellite terminals have received the new satellite configuration and have adjusted to the new signaling carrier, the old signaling carriers — previously configured in **Procedure 1** as an alternate outbound frequency, may now be removed from the list of alternate carriers.

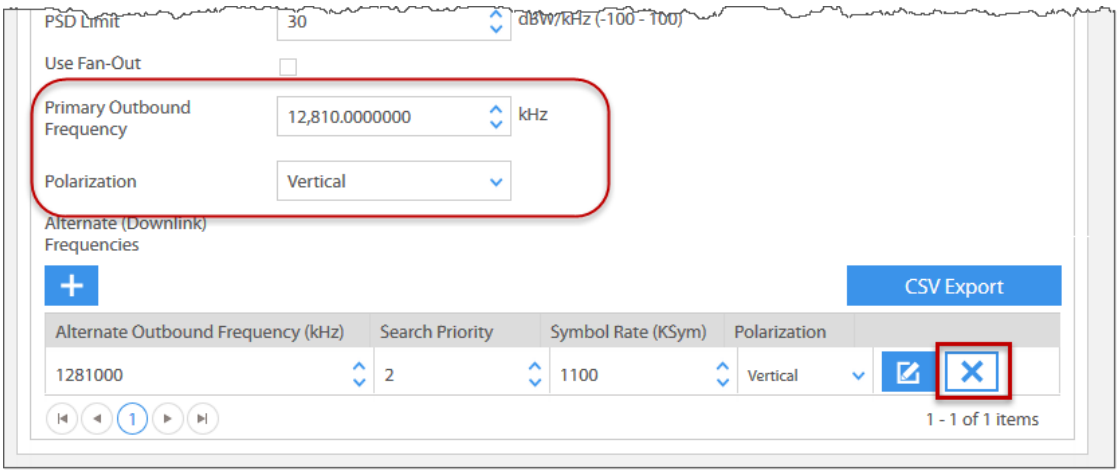

Figure B-5. Alternate Signaling Carrier Records

Steps to configure the ASC Primary Beam and remove the alternate carriers:

1. On the NMS **Configuration** tab, click **Browse Transport Domain**.
2. Under **Element Type** filter select **Acquisition Signaling Channel** to list the ASCs.
3. Click **Actions** on the desired ASC and select **Modify Acquisition Signaling Carrier**.
4. Under the **Alternate (Downlink) Frequencies** section, click the **Delete Record** icon, to remove the previously entered Alternate Downlink Frequency record. See Figure B-5.
5. Click **Save and Close** to save changes and open the **Browse Transport Domain** window.
6. On the newly modified ASC, click **Actions** and then select **Apply Configuration**.

Procedure 7. Confirm Global Network Option Changes

This procedure is to verify the updates to the ASC **Primary Outbound Frequency**, and the removal of the **Alternate (Outbound) Frequencies**. These changes should be reflected at the Network System level — indicated in the CONSTELLATION_OPT file.

To confirm that updates to the global network options are made:

1. From the **Configuration** tab, under **NMS Management**, click **Browse Networks.**
2. Find the correct **Network System** — for example **Pulse Network**; click **Actions** and **Compare Configuration**. The **Compare for "Network"** page opens.

3. Click on the **CONSTELLATION_OPT** tab to view a side-by-side comparison of the newly modified "**Pending Option File**," and the currently in-use "**Active Option File**."
4. Verify that the changes are applied. See the highlighted section of the **Pending Options File**, which reflects the alternate frequencies updates that were removed from the ASC.
5. If the updates can be verified, then click **Apply Configuration** to activate the new Constellation Options File on all terminals in the network.

B.1.1 Terminals Acquire with New Configuration

Although the new signaling carrier is now added to the Terminal, it will not consult the signaling carrier and will be unaware of the changes, as long as it is in network. If, however, the service channel becomes unavailable for any reason, the terminal will drop out of the network. On an attempt to reacquire, if the terminal is unable to join the last known working service channel, it will enter the search mode and perform the following steps:

1. The terminal will try all visible service carriers supported by the modem configuration.
2. If the terminal fails to acquire on any of those carriers, it will then switch to ASC mode and will attempt to lock onto the available ASC carriers — by cycling through the carriers in the constellation file until it successfully locks.
3. Upon receiving a new OTA beam map, the terminal will switch back and restart the service carrier search cycle based on the information from the new OTA beam map.
4. Based upon the terminal capabilities, the new OTA beam map and other configurations, the terminal will identify a service channel and acquire into the network.

iDirect

13861 Sunrise Valley Drive, Suite 300
Herndon, VA 20171-6126
+1 703.648.8000
+1 866.345.0983

www.idirect.net

Advancing a Connected World