Disclaimer

Harmonic reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty. The information contained herein is merely descriptive in nature, and does not constitute a binding offer for sale of the product described herein. Harmonic assumes no responsibility or liability arising from the use of the products described herein, except as expressly agreed to in writing by Harmonic. The use and purchase of this product do not convey a license under any patent rights, copyrights, trademark rights, or any intellectual property rights of Harmonic. Nothing hereunder constitutes a representation or warranty that using any products in the manner described herein will not infringe any patents of third parties.

Trademark Acknowledgments

Harmonic and all Harmonic product names are trademarks of Harmonic Inc. All other trademarks are the property of their respective owners.
Documentation Conventions

This manual uses some special symbols and fonts to call your attention to important information. The following symbols appear throughout this manual:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚨</td>
<td>DANGER: The Danger symbol calls your attention to information that, if ignored, can cause physical harm to you.</td>
</tr>
<tr>
<td>⚠️</td>
<td>CAUTION: The Caution symbol calls your attention to information that, if ignored, can adversely affect the performance of your Harmonic product, or that can make a procedure needlessly difficult.</td>
</tr>
<tr>
<td>⚠️</td>
<td>LASER DANGER: The Laser symbol and the Danger alert call your attention to information about the lasers in this product that, if ignored, can cause physical harm to you.</td>
</tr>
<tr>
<td>📝</td>
<td>NOTE: The Note symbol calls your attention to additional information that you will benefit from heeding. It may be used to call attention to an especially important piece of information you need, or it may provide additional information that applies in only some carefully delineated circumstances.</td>
</tr>
<tr>
<td>💡</td>
<td>TIP: The Tip symbol calls your attention to parenthetical information that is not necessary for performing a given procedure, but which, if followed, might make the procedure or its subsequent steps easier, smoother, or more efficient.</td>
</tr>
</tbody>
</table>

In addition to these symbols, this manual uses the following text conventions:

- **Data Entry**: indicates text you enter at the keyboard.
- **User Interface**: indicates a button to click, a menu item to select, or a key or key sequence to press.
- **Screen Output**: shows console output or other text that is displayed to you on a computer screen.
- **Bold**: indicates the definition of a new term.
- **Italics**: used for emphasis, cross-references, and hyperlinked cross-references in online documents.
Table of Contents

Chapter 1  Features and Specifications
1.1 Introduction  ................................................. 8
1.2 Main Firmware Related Features  ........................................ 8
1.3 Management Interfaces  ......................................... 11

Chapter 2  Getting Started
2.1 Initial Configuration of NSG 9000-6G  ......................... 13
  2.1.1 Configuring Ethernet Ports  .................................... 13
2.2 Full Device Configuration  ....................................... 14
  2.2.1 Logging Into the Device via IE  ............................. 15
2.3 Guidelines for Device Configuration  ......................... 17
  2.3.1 Web Client Page  .......................................... 17
  2.3.2 Stages of NSG 9000-6G Configuration  .................... 19

Chapter 3  Configuring Platform Parameters
3.1 Platform Tab Overview  ........................................... 21
  3.1.1 Global Chassis Buttons  ...................................... 22
3.2 Firmware Upgrade  .............................................. 23
  3.2.1 Upgrading the Firmware of a Single NSG 9000-6G Device  .... 24
3.3 Configuring Ethernet Ports  ...................................... 26
3.4 Configuring General Device Parameters  ..................... 27
  3.4.1 Configuring/Viewing Chassis Properties  ................. 27
3.5 Configuring SNMP and Syslog Parameters  .................... 28
  3.5.1 Configuring SNMP  .......................................... 28
  3.5.2 Configuring Syslog Parameters  ............................ 29
3.6 Setting Device Time and Date Parameters  .................... 29
3.7 Configuring Advanced Networking Options  .................. 30
  3.7.1 Configuring Routing Table Parameters  .................. 30
3.8 Configuring Device Security  ................................... 31
  3.8.1 Setting a Password  ......................................... 31
  3.8.2 Controlling Access - Firewall IP Tables  ................ 31
  3.8.3 Controlling Access - Device Access Protocols  .......... 33
3.9 Device Authentication  ......................................... 34
3.10 Input GbE Ports Configuration  ............................... 35
  3.10.1 Configuring Input GbE ports  ............................. 35
  3.10.2 Configuring Input GbE Port Redundancy  ................. 37
3.11 Configuring/Viewing DTI Parameters  ....................... 39
  3.11.1 Configuring DTI Client Parameters  ..................... 39
  3.11.2 Viewing DTI Client and DTI Port Information  .......... 40
3.12 Configuring QAM-RF Modules  ............................... 42
  3.12.1 Configuring Global RF & QAMs Parameters  ............. 43
  3.12.2 Configuring a QAM-RF Module  ........................... 46
  3.12.3 Configuring Module RF Ports  ............................. 47
# Table of Contents

5.3  Defining DVB Scrambling Parameters ............................................. 103  
5.3.1 Defining DVB Session Based Parameters ...................................... 104  
5.3.2 Defining DVB Tier Based Parameters ......................................... 104  
5.3.3 Viewing EIS Information .............................................................. 105  
5.3.4 Defining ECMGs and NSG 9000 Communication Parameters ............. 105  
5.3.5 Viewing CAS Status ................................................................. 106  
5.4  Defining Privacy Mode Scrambling Parameters ................................ 107  

Chapter 6  Monitoring and Troubleshooting  
6.1  Monitoring the NSG 9000-6G Overview ........................................... 108  
6.2  Device Utilization ............................................................................ 108  
6.2.1 Viewing Traffic ............................................................................ 110  
6.2.2 Viewing RF Parameters ............................................................... 112  
6.2.3 Viewing Input Information ............................................................ 112  
6.2.4 Viewing Output Information ......................................................... 112  
6.3  Monitoring NSG 9000-6G Status and Alarms .................................. 114  
6.3.1 Viewing Alarms Via the Web Client .............................................. 114  
6.3.2 Alarm List .................................................................................... 115  
6.3.3 Warning List ................................................................................ 119  
6.3.4 Notification List .......................................................................... 122  
6.3.5 Setting Alarm Parameters ............................................................ 123  
6.4  Diagnosing and Analyzing Traffic ..................................................... 124  
6.4.1 Exporting Device Logs .................................................................. 124  
6.4.2 Capturing the Input and Output Traffic ......................................... 124  
6.5  Generating and Viewing Logs .......................................................... 126  
6.5.1 Alarms Log .................................................................................. 126  
6.5.2 Monitoring the GbE Ports ............................................................. 127  
6.5.3 Monitoring the NGOD ERM Communication ................................ 128  
6.5.4 Monitoring the ISA Communication ............................................ 130  
6.6  Viewing Available Reports ............................................................... 132  
6.7  Device Troubleshooting .................................................................... 132  
6.7.1 Recurrent Upgrade Failures .......................................................... 133  
6.7.2 How to Questions ........................................................................ 133  

Appendix A  Firmware Upgrade Using an External Server  
A.1  Upgrading the Firmware of a Single Device ..................................... 135  
A.2  Upgrading Procedure .................................................................... 135  

Appendix B  Upgrade Server Installation and Configuration  
B.1  Overview ....................................................................................... 140  
B.2  Apache Server .............................................................................. 141  
B.3  IIS Server ..................................................................................... 142  

Appendix C  Standard ES Types and Descriptors  
C.1  Standard Elementary Stream (ES) Types ....................................... 146  
C.2  Standard ES and Program Descriptors (MPEG) ............................. 146  
C.3  Standard ES and Program Descriptors (DVB) ............................... 147
Appendix D Control Panel
D.1 Using the Control Panel .................................................. 148

Appendix E EIA SDT and HRC Standards
E.1 EIA SDT and HRC Standards ........................................... 153
Chapter 1
Features and Specifications

1.1 Introduction

This guide describes the configuration and monitoring instructions for NSG (Network Services Gateway) 9000-6G using its web client.

This universal high density EdgeQAM supports multiple applications and delivers up to 144 QAM-RF output streams. The number of the delivered transport streams is defined according to the device configuration and number of QAM-RF modules mounted in the slots of the device. Each QAM may serve a different application allowing a single device to concurrently support multiple applications. The supported applications are as follows:

- VOD (Video On Demand)
- Broadcast
  - PID Range
  - Service/PID remux
- SDV (Switched Digital Video)
  - ISA
  - NGOD (Next Generation On Demand)
- High Speed Data
  - M-CMTS (Modular CMTS)
  - D2E

1.2 Main Firmware Related Features

The following table describes the main features supported by the narrowcast firmware:

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max input sockets</td>
<td>2000, unicast or multicast</td>
</tr>
</tbody>
</table>
|                          | Max. Input bit rate                    | ■ Up to 6,000 Mbps (6 Gbps) per device  
■ 52 Mbps per socket                                                      |
|                          | Dynamic Extraction of input            | Video only - Dynamic detection of changes in services and PSI tables at the input.                                                            |
|                          | Input Format                           | Video - MPEG2 transport over UDP/IP  
M-CMTS - L2TPv3 streams                                                      |
|                          | VOD - In-band provisioning of IP/UDP unicast sockets | Programs are automatically routed to the required output QAM channel based on their UDP port number. User may select between several different UDP mapping templates. See 4.2.3 Defining Emulation/QAM Mapping Mode on page 77. |
|                          | IP multicast                           | supports IGMP ver 1/2/3                                                                                                                       |
### Table 1-1: Main Firmware Related Features

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiplexing/provisioning</td>
<td>Full multiplexing (any input to any output)</td>
<td></td>
</tr>
<tr>
<td>options</td>
<td>Multicast of any input stream to multiple transport streams.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Socket pass-through: NSG 9000-6G may be configured to pass input sockets in their entirety to a given output QAM channel. However, pass-through sockets may not be multicast to multiple output QAM channels.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spooling of PSI/SI tables</td>
<td></td>
</tr>
<tr>
<td>Processing</td>
<td>Supports SDV:</td>
<td>DVB Scrambling</td>
</tr>
<tr>
<td></td>
<td>NGOD R6 and D6 protocols</td>
<td>Motorola Privacy Mode scrambling</td>
</tr>
<tr>
<td></td>
<td>ISA</td>
<td>Supports services that were encrypted using the Pro:Idiom standard.</td>
</tr>
<tr>
<td>Pre-encrypted Content</td>
<td>Supports pre-encrypted content of various encryption systems/standards:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DVB-CSA</td>
<td>Motorola DigiCypher</td>
</tr>
<tr>
<td></td>
<td>Cisco PowerKey</td>
<td>Pro:Idiom</td>
</tr>
<tr>
<td>Modular CMTS</td>
<td>Serves as an EdgeQAM in WB &amp; NB applications, supports the following DOCSIS 3.0 protocols:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DEPI (MPT)</td>
<td>DRFI</td>
</tr>
<tr>
<td></td>
<td>DTI</td>
<td></td>
</tr>
<tr>
<td>Max output bit rate</td>
<td>See NSG 9000-6G Hardware and Installation User’s Guide</td>
<td></td>
</tr>
<tr>
<td>QAM-RF</td>
<td>See NSG 9000-6G Hardware and Installation User’s Guide</td>
<td></td>
</tr>
<tr>
<td>ASI/GbE Monitoring</td>
<td>The unit duplicates any requested QAM channel to the ASI output port/GbE port for monitoring purposes.</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Control Panel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web client</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCT (Mass Configuration Tool)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CLI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NMX (Harmonic’s Digital Service Manager)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SysLog</td>
<td></td>
</tr>
<tr>
<td>QAM utilization statistics</td>
<td>When NMX is used for alarms and status monitoring, it may also provide statistical reports of QAM utilization.</td>
<td></td>
</tr>
</tbody>
</table>
### Security

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Users authentication and authorization</td>
<td>- Supports two modes of authentication and authorization:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Local - performed by the device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remote - performed by a RADIUS server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Firewall - uses the IP tables of Linux native firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Access Protocols - supports HTTP/HTTPS</td>
</tr>
</tbody>
</table>
1.3 Management Interfaces

Harmonic offers several methods for configuring the NSG 9000-6G devices and monitoring their status. All management interfaces listed below connect to the NSG 9000-6G over LAN, via its ETH1 Ethernet port.

⚠️ Caution: Harmonic strongly recommends using an Ethernet network that is isolated from any other networks or subnets at your site for management of the NSG 9000-6G gateways. It ensures adequate security, and prevents possible disturbances to the normal operation of NSG 9000-6G devices due to uncontrolled network activity.

The table below lists the available management interfaces according to the management purpose for which they are designed:

Table 1-2: Management Interfaces

<table>
<thead>
<tr>
<th>Tool</th>
<th>Purpose</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Panel</td>
<td>Preliminary configuration and monitoring of a single NSG 9000-6G device</td>
<td>The NSG 9000-6G control panel is located on the front panel of the NSG 9000-6G. The control panel is active once the NSG 9000-6G boots up and provides means for preliminary configuration of a single NSG 9000 device. It also allows you to monitor the NSG 9000-6G’s status, view its alarms (if present), and troubleshoot them.</td>
</tr>
<tr>
<td>Web Client</td>
<td>Configuration and monitoring of a single NSG 9000-6G device</td>
<td>The NSG 9000-6G web client is an on-board web-based user interface, that is an integral part of the NSG 9000-6G firmware. The web client is accessible through Microsoft Internet Explorer, and provides means for configuring a single NSG 9000-6G device. It also allows the user to monitor the NSG 9000-6G’s status, view its alarms (if present), and troubleshoot them. For details on Internet Explorer and accessing the web client, see 2.2.1 Logging Into the Device via IE on page 15.</td>
</tr>
</tbody>
</table>
## Table 1-2: Management Interfaces

<table>
<thead>
<tr>
<th>Tool</th>
<th>Purpose</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCT (Mass Configuration Tool)</td>
<td>Configuration of multiple NSG 9000-6G devices</td>
<td>The MCT is a spreadsheet-oriented system designed to configure multiple NSG’s simultaneously. MCT is recommended for large-scale NSG deployments. Besides simultaneous configuration of large number of NSG devices, it also allows users to perform firmware upgrade for multiple devices. MCT is sold separately - contact Harmonic Customer Support for more details. Note: MCT is not automatically updated when an NSG is configured through the web client. Using the web client for configuring individual NSG in an MCT-based site is not recommended. If the web client is used, care should be taken to update MCT with the changed configuration. For details on synchronizing MCT with NSG devices, refer to the MCT online help.</td>
</tr>
<tr>
<td>Command Line Interface (CLI)</td>
<td>Configuration and monitoring of a single NSG 9000-6G device</td>
<td>The CLI comprises commands that are organized in a hierarchical structure of submenus branching down from the root directory. You can use the CLI on any computer that communicates with NSG 9000-6G and that has a free SSH client installed on it.</td>
</tr>
<tr>
<td>NMX - Harmonic’s Digital Service Manager</td>
<td>Status and Alarm Monitoring of multiple NSG 9000-6G devices</td>
<td>NMX may be used for monitoring general status and alarms of multiple NSG 9000-6G devices. A single NMX manager may be used to monitor several hundreds NSG 9000-6G devices, located in several different sites.</td>
</tr>
<tr>
<td>3rd party SNMP monitoring</td>
<td>Status and Alarm Monitoring of multiple NSG 9000-6G devices</td>
<td>The integrated SNMP supports an extended set of SNMP MIBs. In addition, NSG 9000 may generate SNMP traps in the following SNMP versions: v1, v2c, v3.</td>
</tr>
<tr>
<td>Syslog</td>
<td>Monitoring of a single NSG 9000-6G device</td>
<td>This is a standard network protocol for logging device messages. A Syslog server that is registered with the NSG 9000-6G device will receive messages from the device whenever an alarm or warning is asserted or remitted.</td>
</tr>
</tbody>
</table>
Chapter 2
Getting Started

2.1 Initial Configuration of NSG 9000-6G

The NSG 9000-6G device is configured and controlled by a remote management system. Once you have finished cabling the device (see, NSG 9K-6G Hardware and Installation User's Guide), set NSG IP address, that is, the IP addresses of the Ethernet ports located on the back panel of the NSG 9000-6G. To set the NSG IP address, use the control panel located on the front panel of the NSG 9000-6G.

**NOTE:** The NSG 9000-6G requires a user name and password to log in to all management interfaces including the serial communications console, web client and SSH. See 2.2.1 Logging Into the Device via IE on page 15.

2.1.1 Configuring Ethernet Ports

NSG 9000-6G is monitored and configured by a remote management system, via the Ethernet ports located on the back panel of the NSG 9000-6G.

The Ethernet ports labeled ETH1 and ETH2 provide access to two independent networks. The NSG 9000-6G uses the Ethernet port labeled ETH1 to communicate with the management network. You may set the ETH1 IP address, subnet mask and default gateway.

NSG 9000-6G uses the Ethernet port labeled ETH2 to communicate with the CAS network. For ETH 2 you may configure only its IP address and subnet mask.

To configure the Ethernet ports of an individual device, use the Control Panel of the device.

The following sections describe how to configure individual NSG 9000-6G devices using the control panel of the unit.

When you configure the network parameters of ETH ports via the control panel, the application checks the validity of the IP address and network group parameters.

To configure ETH1 port:

Once you are in Config mode (see page 110), do the following:

1. Navigate to the Network Config screen and click <Enter>. The Ethernet Port 1 screen appears.
2. Click <Enter>. The ETH1 IP Address screen appears.
3. Click <Enter>. The Edit IP Address screen appears.
4. Edit the IP address and click <Enter>. The program checks whether you entered a valid IP address and only then applies changes. The Edit Ethernet Subnet Mask screen appears.
5. Edit the subnet mask and click <Enter>. The Edit Default GW screen appears.
6. Edit the ETH gateway and click <Enter>. The program checks whether you entered valid network parameters and only then applies changes. The ETH1 IP Address screen appears.

If invalid network parameters are entered an error message appears.
To configure ETH2 port

**NOTE:** If you are using the ETH2 port, you must configure its IP address on a different subnet than that of the Ethernet 1 port.

Once you are in Config mode, do the following:
1. Navigate to the Network Configuration screen and click <Enter>.
2. Click <Down or Up> to open the Ethernet Port 2 screen.
3. Click <Enter>. The ETH2 IP Address screen appears.
4. Click <Enter>. The Edit IP Address screen appears.
5. Enter the required IP address and click <Enter>. The program checks whether you entered a valid IP address and only then applies changes. The Edit Subnet Mask screen appears.
6. Enter the required subnet mask and click <Enter>. The program checks whether the network group parameters are valid and only then applies the changes. The ETH2 IP Address screen appears.

If invalid network parameters are entered, an error message appears.

**NOTE:** You can re-configure the Ethernet ports using MCT or the Web client. MCT allows the configuration of a number of NSG devices and the Web client allows a remote individual configuration.

For further information about the Control Panel, see **B.1 Using the Control Panel** on page 108.

## 2.2 Full Device Configuration

The NSG 9000-6G web client allows a full configuration of the NSG 9000-6G device. It also allows the user to monitor the NSG 9000-6G’s status, view its alarms (if present), and troubleshoot them. This manual describes and instructs you on how to configure and monitor the device via the web client.

The web client is accessible through a web browser. The following web browsers are supported:

**Table 2-1: Supported Web Browsers**

<table>
<thead>
<tr>
<th>Microsoft Internet Explorer Supported Versions</th>
<th>Mozilla FireFox Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0</td>
<td>3.6 and up</td>
</tr>
<tr>
<td>8.0 Compatibility view</td>
<td></td>
</tr>
</tbody>
</table>

**Using IE 8.0**

To access the web client using IE8, you should use Compatibility View. This view allows to observe browser pages in a mode that is compatible with IE8.

To set compatibility view
1. Open IE8.
2. Select Tools > Compatibility View Settings.

3. Check Display all websites in Compatibility View, or specify the IP address for specific sites.

4. Click Close.

2.2.1 Logging Into the Device via IE

To log into the device via IE, open a browser and login by using the required user name and password. Each user is eligible to a different mode of work with the device. The following table lists the various users and their working mode:

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Working Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest</td>
<td>nsgguest</td>
<td>Allows only to monitor the operation of the device.</td>
</tr>
<tr>
<td>config</td>
<td>nsgconfig</td>
<td>Allows to configure the device and to define the Config and Guest access level password.</td>
</tr>
<tr>
<td>admin</td>
<td>nsgadmin</td>
<td>Allows to configure the device, to define a password to all users and to export and import firewall tables. See page 35.</td>
</tr>
</tbody>
</table>

The current access level appears in the title bar of the web client.

See also, 3.9 Device Authentication on page 34.

To login the device

1. Open an IE browser.
2. Type in the address of the required device.
3. Click Go or press <Enter>.

4. In the Connect To dialog type in the required username and password.

5. To save the password for the future, select Remember my password.

6. Click Ok.

The web client page appears and you may start working with the device according to the restrictions of your access level.

NOTE: To change the password, see 3.8.1 Setting a Password on page 31.
2.3 Guidelines for Device Configuration

Once the NSG 9000-6G is properly cabled and setup in your network, you may access it via the web client in order to configure and monitor it. The web client reads data from the NSG 9000-6G and presents it in an easy to use User Interface (UI).

2.3.1 Web Client Page

Once you have logged into the device, the web client page appears. It includes the following sections:

- **Title bar** - displays the following:
  - Device model, for example: NSG 9000-6G
  - Device name - by default it is the IP address of the device. You can select it and type any name for easy identification and click Apply. For example: Rack 5-NSG 3.
  - Logged-in user
  - Alarm indicator - the alarm indicator is actually a link to the Alarm page and the
indicator provides the following information:

Table 2-3: Alarm Indication

<table>
<thead>
<tr>
<th>Alarm Indication</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green Alarm button</td>
<td>No active alarms.</td>
</tr>
<tr>
<td>Red Alarm button</td>
<td>There is at least one active alarm. Once the mouse pointer hovers on it, a hint appears displaying the alarm description. Once you click it, the Alarm page opens.</td>
</tr>
<tr>
<td>Orange Alarm button</td>
<td>There is at least one active warning. Once the mouse pointer hovers on it, a hint appears displaying the alarm description. Once you click it, the Alarm page opens.</td>
</tr>
</tbody>
</table>

| N Active Alarms      | 'N' stands for the amount of registered alarms/warnings. Click the link to open the Alarm page. |
| N Active Warnings    |                                                                                              |

- Help button - allows you to access information about the various options provided by the web client. The provided help is a context sensitive help. Upon clicking the help button, the help page relevant to the open web client page appears.

- Tabs bar - Links you to parameters required for NSG 9000-6G configuration. The Tabs bar is comprised of two sections:
  - Main tabs - includes the tabs listed in the following table and the Apply button
  - Sub tabs - includes tabs related to the Main tab as the following table describes.

Table 2-4: Available Tabs

<table>
<thead>
<tr>
<th>Main Tab</th>
<th>Sub Tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>■ General - allows to configure chassis parameters, input and output ports and QAM-RF module parameters.</td>
</tr>
<tr>
<td></td>
<td>■ Licensing - allows to manage the licenses</td>
</tr>
<tr>
<td></td>
<td>■ NGOD - allows to set general NGOD ERM parameters to enable communication with the NSG 9000-6G device</td>
</tr>
<tr>
<td></td>
<td>■ ISA - allows to set general ISA parameters to enable communication with the NSG 9000-6G device</td>
</tr>
<tr>
<td>Application</td>
<td>■ VOD - allows to define the VOD parameters. See page 74.</td>
</tr>
<tr>
<td></td>
<td>■ Broadcast - allows to define broadcast session along with service and PID remux. See page 80.</td>
</tr>
<tr>
<td></td>
<td>■ SDV - allows to define SDV sessions. See page 90.</td>
</tr>
<tr>
<td></td>
<td>■ M-CMTS - allows to define M-CMTS sessions. See page 98.</td>
</tr>
<tr>
<td></td>
<td>■ D2E - for future use only</td>
</tr>
<tr>
<td></td>
<td>■ CAS - allows to define the CAS parameters. See page 79.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>■ Traffic - shows the traffic that flows out of the device. See page 110.</td>
</tr>
<tr>
<td></td>
<td>■ Alarms - shows the currently raised alarms. See page 114.</td>
</tr>
<tr>
<td></td>
<td>■ Diagnostics - allows ASI and IP forwarding for monitoring and analysis purposes.</td>
</tr>
<tr>
<td></td>
<td>■ Logs - allows to view the GbE counters, alarm logs, NGOD RTSP messages and RPC communication messages. See page 127 - page 130.</td>
</tr>
</tbody>
</table>
Chapter 2 Getting Started Guidelines for Device Configuration

© 2012 Harmonic Inc. 19 NSG 9000-6G Version 2.7, Rev B

2.3.2 Stages of NSG 9000-6G Configuration

Configuring the NSG 9000-6G model includes the following stages:

- Defining/viewing Platform Parameters, a one time configuration. During this stage, define Ethernet 1&2 ports, GbE input ports and view platform parameters such as status of slots, software version, chassis serial number, and more. You can also set general device parameters such as:
  - Device security parameters (device password)
  - SNMP traps
  - NTP
  - Advanced network options - routing table and Access Control list

- Defining QAM-RF module parameters - during this stage define the following:
  - Global RF and QAMs parameters
  - RF port parameters
  - QAMs parameters
  - View a summary of general attributes

- Licensing - during this stage, view the licenses installed on the NSG device, install new licenses if needed, and assign licenses to QAM channels.

- Applications - during this stage, define the parameters of the required application. The available applications are as follows:
  - VOD
  - Broadcast
  - M-CMTS
  - D2E

- CAS - in case CAS is required, define whether DVB scrambling or Privacy Mode scrambling is required and set the attributes as required.

2.3.2.1 Before you Begin

Before you start configuring and provisioning the device, pay attention to the following:

- Fields that are for viewing only, are greyed out.

- To change parameter values, click in the field and type the required values. Once you click away from the field, the web client interface is updated and displays the new parameters. However, the parameters are not sent to the device.

- To apply changes to fields marked with this icon 
  , you should reset the device.

- To send to the device the newly configured parameters, click Apply. Only when you click Apply, you actually submit the new parameters to the device.
- To delete rows in a table, check the Select box and then click Delete Selected.
- A web page dialog includes a Done button. When clicking this button, you save the new configuration without applying it to the device and you close the web page dialog. To close a web page dialog without saving the configuration, click the button at the upper right corner of each page. For example, see Add License web page dialog on page 60.
Chapter 3
Configuring Platform Parameters

3.1 Platform Tab Overview

The Platform tab is the default tab. As soon as you link to the device it opens with the General tab selected. The Platform tab enables you to configure device parameters which are usually a one time configuration and it is recommended to configure as soon as you start working with the device. The Platform parameters are organized in the following tabs:

- Platform > General Tab - The Platform > General tab includes a graphical view of the device back panel. Focusing on each component, allows to view or configure the parameters of the component in focus. By default, Chassis is selected and the General tab is in focus. The following table lists the available components and the tabs related to each component.

Table 3–1: Platform Page – Components and Available Tabs

<table>
<thead>
<tr>
<th>Selected Component</th>
<th>Available Tabs</th>
</tr>
</thead>
</table>
| Chassis            | - General - view general chassis parameters, define device name, IGMP V2 only and device EdgeCluster (redundancy) parameters. See 3.4 Configuring General Device Parameters on page 27.  
|                    | - Global RF & QAMs - set global QAM-RF module parameters. See page 43.  
|                    | - SNMP & Syslog - set SNMP and Syslog parameters. See page 28.  
|                    | - Time - set device time and time zone parameters. See page 29.  
|                    | - Routing Table - set ETH and GbE ports routing table. See page 30.  
|                    | - Security - set access to the unit. See page 31.  
|                    | - Authentication - set authentication to the unit. See page 34.  
|                    | - Port Redundancy - set GbE port redundancy. See page 37.  
|                    | - EdgeCluster - set the edgeCluster parameters. See page 68.  
| Eth1, 2             | General. See page 26.  
| GbE                 | General. See page 35.  
| DTI card            | General. See page 39.  
| Slot                | - General - view a general summary of the QAM configuration. See page 52.  
|                    | - Module - set ITU-T Annex, constellation, symbol rate and more. See page 46.  
|                    | - Ports - (default view) enable an QAM-RF port, set the number of channels and the power level of the port. See page 47.  
|                    | - QAMs - view and set QAM parameters such as QAM manager. See page 49.  

- Platform > Licensing Tab - The Platform > Licensing tab allows to manage your licenses as explained in 3.14.1 Working with Licenses on page 57.

- Platform > NGOD Tab - The Platform > NGOD tab allows to set the parameters required for the NSG NGOD ERM communication. See 3.15.1 Configuring NGOD General Parameters on page 62 and 3.15.2 Configuring ERM Parameters on page 62.
### 3.1.1 Global Chassis Buttons

#### Table 3-2: Global Chassis Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Button Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Identify unit" /></td>
<td>Identify unit</td>
<td>See page 22.</td>
</tr>
<tr>
<td><img src="image" alt="Export Configuration to File" /></td>
<td>Export Configuration to File</td>
<td>See page 22.</td>
</tr>
<tr>
<td><img src="image" alt="Import Configuration to Device" /></td>
<td>Import Configuration to Device</td>
<td>See page 23.</td>
</tr>
<tr>
<td><img src="image" alt="Firmware upgrade" /></td>
<td>Firmware upgrade</td>
<td>See page 23.</td>
</tr>
<tr>
<td><img src="image" alt="Factory default" /></td>
<td>Factory default</td>
<td>See page 26.</td>
</tr>
<tr>
<td><img src="image" alt="If Chassis is selected Reset Device" /></td>
<td>If Chassis is selected Reset Device</td>
<td>See page 23.</td>
</tr>
<tr>
<td><img src="image" alt="If Slot is selected, Reset Module" /></td>
<td>If Slot is selected, Reset Module</td>
<td>See page 23.</td>
</tr>
<tr>
<td><img src="image" alt="Validate" /></td>
<td>Validate</td>
<td>Validates the QAM-RF module configuration only. See page 46.</td>
</tr>
</tbody>
</table>

#### 3.1.1.1 Identifying an NSG9000 Device

To identify unit
1. Select the Platform tab.
   By default Chassis is selected.
2. Click Identify Unit.
   The LEDs of Output ports 4, 5 and 6 are blinking and the button toggles to Stop Blinking.

#### 3.1.1.2 Exporting and Importing Configuration

To Export the configuration to a File
1. Select the Platform tab.
   By default chassis is selected.
2. Click Export Configuration to File.
   The Export File From Device dialog appears.
3. Click either of the following:
   - Open - to open the XML file and to view the configuration of the device.
   - Save - to save the XML file with the device configuration at the required location.
To import configuration
1. Select the Platform tab.
   By default chassis is selected.
2. Click Import Configuration to Device.
   The Import File To Device dialog appears.
3. To locate the required XML file previously exported, click Browse.
4. To import, click Import.
   Wait until a message notifying you of a successful import appears.
5. For the device to run with the newly imported configuration, reset the device.

3.1.1.3 Clearing Configuration

To clear configuration and Revert to Factory Defaults
1. Select the Platform tab.
   By default chassis is selected.
2. Click Factory Default.
   The following message appears:
   This action will clear configuration and reset the device. Are you sure?
3. To confirm the action, click OK.
   The device configuration is removed and device boots up with factory defaults.

3.1.1.4 Resetting an NSG9000 Device

To reset the device
1. Select the Platform tab.
   By default chassis is selected.
2. Click Reset Unit.
3. Click Ok to confirm the action.
   The reset process takes place.

3.1.1.5 Resetting a QAM-RF Module

To reset a QAM-RF module
1. Select the Platform tab.
2. Select the required slot/QAM-RF module.
3. Click Reset Module.
4. Click Ok to confirm the action.
   The reset process takes place.

3.2 Firmware Upgrade

NSG 9000-6G ships with firmware and the web client installed. However, Harmonic periodically releases firmware updates. To find out if the provided firmware meets your needs or must be updated, contact Harmonic Technical Support.
To upgrade the firmware of more than one NSG 9000-6G device, use MCT. See MCT 9.6 and higher SW User Guide, or MCT Online Help.

### 3.2.1 Upgrading the Firmware of a Single NSG 9000-6G Device

The NSG 9000-6G firmware is packaged and delivered within the installer application. The installer turns firmware upgrade into an easy and straightforward procedure. To upgrade using the NSG installer refer to the following instructions. You can still upgrade the firmware using Apache or the IIS HTTP server. For these instructions, refer to Firmware Upgrade Using an External Server on page 135.

Before upgrading, prepare the following:

- **NSG installer** - Obtain the installer from Harmonic's FTP site. The NSG installer includes the new firmware package. The name of the NSG installer indicates the device type and the firmware version. For example: NSG9K6G-2.6.4.3-1-Installer-v1.1.5.exe, where

<table>
<thead>
<tr>
<th>NSG9K6G</th>
<th>device type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6.4.3-1</td>
<td>firmware version</td>
</tr>
<tr>
<td>Installer</td>
<td>application name</td>
</tr>
<tr>
<td>v1.1.5</td>
<td>installer version</td>
</tr>
</tbody>
</table>

- **PC** - Download the NSG installer to a computer that meets the following requirements:
  - Access to the device. Port 22 of the computer should be open to allow communication via the SSH protocol.
  - Around 200MB of free space
  - Any kind of Windows operation system

**NOTE:** Firmware upgrade is service affecting.

⇒ To upgrade using the NSG installer

1. Once you downloaded the NSG installer to your PC, launch the NSG installer.

The NSG installer is extracting files. This may take around 30 seconds. The following dialog appears:

The dialog indicates the firmware version packaged within the Installer you have started.
Chapter 3 Configuring Platform Parameters

Firmware Upgrade

2. In **IP Address**, enter the IP address of the device you wish to upgrade.

3. In **UserName**, enter the username for logging into the device. This username should be eligible to upgrade the firmware. See 2.2.1 **Logging Into the Device via IE on page 15**.

4. In **Password**, enter the required password.

5. By default, **Auto-Reboot** is selected. It allows to reboot the device once the installation of the new firmware is completed.

6. Click **Install**.

   The progress bar indicates that upgrade is taking place while denoting the current stage of the upgrade.

7. **View Log** - during the upgrade, you can click **View Log**.

   A text file appears with detailed information regarding the upgrade. This log allows you to troubleshoot the upgrade process.
8. Wait until a message that the upgrade is complete appears.
9. Click OK and wait until device reboots.
10. In the web client of the device, (Platform > Chassis > General tab) you can verify that the device reports the same version number as the required firmware.

NOTE: The following sections are organized according to the recommended sequence of steps for device configuration.

### 3.3 Configuring Ethernet Ports

The IP address of the ETH ports or NSG 9000-6G primary IP address is configured as part of the NSG 9000-6G installation (see 2.1.1 Configuring Ethernet Ports on page 13). However, when required, you may change the IP address settings via the Platform screen, Ethernet table:

**NOTE:** Configure the IP address of ETH1 on a different subnet than that of ETH2. Configuring both ports to be on the same subnet may result in serious network communication problems. NSG 9000-6G uses the ETH1 port to communicate with the network for management purposes and ETH2 for Conditional Access Systems (CAS) purposes.

To change configuration of ETH1 and ETH2

1. Select the Platform tab.
2. Select the required Ethernet port.
   - The ETH1 or the ETH2 Properties General tab appears.
3. For Eth1, select the General tab.
4. To enable the port, check Enable Port.
5. In MAC Address, view the MAC Address. The MAC address is the physical address of the unit. The address is retrieved and presented in the Platform page for viewing purposes only.
6. Type the required IP address, subnet mask and default gateway of ETH1 and/or ETH2.
7. Click Apply to apply changes.

3.4 Configuring General Device Parameters

3.4.1 Configuring/Viewing Chassis Properties

The General tab allows you to configure and view the following:
- View general device parameters like software version
- Define device name
- Define to work in IGMP V2 protocol only
- Define EdgeCluster parameters. See 3.17 EdgeCluster on page 68.

To view/set chassis properties
1. Select the Platform tab.
2. In Back Panel View, select Chassis > General tab.
The Chassis Properties & Main Board Properties section appears.

3. View the following Chassis information:
   - SW Version - The device's firmware version and revision.
Main Board Part Number - The part number of the main board.
Main Board Serial Number - The serial number of the main board.
Main Board Storage Format - indicates whether a single or dual partition.
Chassis Serial Number - The serial number of the chassis.

4. To define device name, in Device Name (SysName), enter a name. The device name should allow easy identification of the device. Once you click Apply, the newly entered device name appears in the title bar. If you type in the title bar another name, once you click Apply it overrides the device name entered in Device Name box.

NOTE: The Device Name is also required for the SNMP manager for defining the attributes of the SYSTEM MIB. See 3.5 Configuring SNMP and Syslog Parameters on page 28.

5. In System Uptime, view the time the device is up and running since the last reboot.
6. To set the GbE ports to support the IGMPv2 protocol only, select Force IGMP V2. NSG 9000-6G ignores any IGMPv3 messages and does not generate any IGMPv3 messages.

3.5 Configuring SNMP and Syslog Parameters

3.5.1 Configuring SNMP

NSG 9000-6G is capable of reporting its status via SNMP (Simple Network Management Protocol) to a third-party SNMP-based network management systems.

NSG 9000-6G status is reported to the SNMP manager in the following ways:
- SNMP Traps - notifications that the NSG device initiates and sends to the SNMP manager to indicate the assertion or remittance of an alarm or warning. SNMP Traps are sent only to SNMP managers that are registered with the NSG 9000-6G.
- Alarms status queries - the SNMP manager may query the NSG for its current alarms status. The NSG reports this information using standard and custom SNMP MIBs.
- Configuration and Traffic queries - the SNMP manager may query the NSG for various configuration parameters, as well as various traffic counters that indicate the rate of traffic that is flowing through the NSG’s interfaces.

In addition, NSG 9000-6G supports Syslog - a standard-based method for centralized logging of device messages. A Syslog server that is registered with the NSG 9000-6G device will receive messages from the device whenever an alarm or warning is asserted or remitted.

To set SNMP parameters
1. Select the Platform tab.
2. Select Chassis > SNMP & Syslog tab.
3. By default SNMP is enabled. Verify that it is enabled. 
    To disable SNMP, de-select Enable SNMP.

4. In SNMP Community String, enter the required string value for the Get community:
   - Get Community - The name of the community having Read access to the network
     elements. The elements will respond to this community Get commands. The default
     string is public.

5. In SNMP Trap Destination table, enable the required table-row by selecting the Enable box.

6. Enter the IP Address of the computer to which you wish to forward all SNMP traps from
   the NSG.

7. Open the Version list and select the required SNMP version.

8. In System MIB, enter the following information:
   - Contact (SysContact) - enter contact information
   - Location (SysLocation) - enter the location of the device. In other words, the location
     of the host on which the SNMP agent, or server runs.

3.5.2 Configuring Syslog Parameters

To log NSG related events, enable this option and enter the Syslog server IP address as
instructed below:
1. Select the Platform tab.
2. Select Chassis > SNMP tab and focus on the Syslog section.
3. If you wish to log events on the server, enable the Syslog server. To enable, select Enable
   Syslog.
4. In Syslog Server IP address, enter the IP address of the Syslog server.

3.6 Setting Device Time and Date Parameters

Set the device time according to either of the following options:
- Automatically - Synchronize the NSG 9000-6G time with the Universal Time Coordination
  (UTC) by connecting to an NTP (Network Time Protocol) server. If you enable this option,
  you cannot set the time of the unit manually.
- Manually - Use this option when NTP server is not available.

⇒ To set the time of the device according to the NTP server
1. Select the Platform tab.
2. Select Chassis > Time tab.
3. To allow to establish communication with the NTP server, select Enable NTP.
4. Enter the IP address of the NTP server in NTP Server IP Address.

⇒ To set the device time zone
1. Do either of the following:
   - Open the Time Offset list and select the required local time offset to match between the time of the device, that is UTC time, and the Greenwich Mean Time (GMT).
   - Select Enable Daylight Saving.
     The Time Offset is disabled and Location and City/Province are enabled.

2. Select the required location.
3. Select the required city/province.
   The daylight saving time is automatically defined according to the selected location and city/province.

To set the time of the device manually
1. Verify that Enable NTP is not selected.
2. In Date, enter, in the required format, the current date.
3. In Time, enter, in the required format, the current time.
4. Open the Time Zone list and select the required local time offset to match between the time of the device and the Greenwich Mean Time (GMT).

**NOTE:** When you manually set the date and time of the device, this event is logged in the unit alarm log.

### 3.7 Configuring Advanced Networking Options

#### 3.7.1 Configuring Routing Table Parameters

The routing table allows you to define Ethernet routes to specific networks. This option is required in special network topologies that require more than the capabilities of a default gateway.

To set the Routing table parameters, do the following:
1. Select Platform > General tab.
2. In Back Panel View, select Chassis.
3. In Chassis and Main Board Properties, select Routing Table.

4. Click Add Route to add a blank row to the table.
5. Enter the required values as explained below:
   - Destination - Enter the IP address of the destination device or network.
   - Mask - Specify the subnet mask. The combination of mask and destination IP will determine the exact range of IP destinations that may be accessed through this routing entry.
   - Gateway - Enter the IP address of the gateway through which the NSG will attempt to make a connection to a destination. For ETH1 or ETH2, the gateway must be in the same NSG subnet for either ETH1 or ETH2 ports. For GbE 1, 2 and 3 ports, the
gateway must be in the same NSG subnet for each GbE port.

- Interface - Open the list and select the physical port to outflow this routing.
- Delete - Check this box to remove this route. The route is removed once you click Delete Route.

3.8 Configuring Device Security

Configure the following as explained below:

- Passwords, see 3.8.1 Setting a Password on page 31
- Firewall IP tables, see 3.8.2 Controlling Access - Firewall IP Tables on page 31
- Access protocols, see 3.8.3 Controlling Access - Device Access Protocols on page 33

3.8.1 Setting a Password

1. Select the Platform tab.
2. Select Chassis > Security tab.
3. Focus on the Change Password section.
4. In User Name, verify that the required user name appears.
   - If you logged as admin, you are authorized to change your password and the password of all other users.
   - If you logged as Configure, you are authorized to change your password or the password of Monitor.
5. In New Password, enter the new password.
6. In Verify Password, re-enter the new password.
7. To apply the password change, click Change Password.
   - When logging in, use the newly set password.

**NOTE:** After three unsuccessful login trials, or if you forgot the password/user name, reset your password. To reset the password, call Harmonic Customer Support.

3.8.2 Controlling Access - Firewall IP Tables

To control the access to the NSG 9000-6G device, use the firewall IP tables of Linux native firewall known as Uncomplicated Firewall. An experienced user only, should update the firewall using the NSG 9000-6G Command Line Interface (CLI). Once the firewall is updated, you can distribute the file to other NSG 9000-6G devices.
Via the Security tab you can do the following:

- Export or import firewall IP tables:
  - Export - allows to save the IP tables file.
  - Import - allows to control the access to the device. As soon as the import process is complete, the new configuration is active.

**NOTE:** Only user *admin* is allowed to export and import firewall IP tables.

- Define the allowed protocols for accessing the device

⇒ To export firewall IP tables

1. Select the Platform tab.
2. Select Chassis > Security tab.
4. To save the IP tables as a zipped file, click Export Firewall IP Tables.
5. Click Export.
6. In the File Download dialog, click Save.
7. Navigate to the required location and click Save.

⇒ To import firewall IP tables

1. Select the Platform tab.
2. Select Chassis > Security tab.
3. To import the IP tables file, click Import Firewall IP Tables.

4. Browse to the required file and click Import.
5. In the dialog that appears, click Yes.
6. Wait until the following message appears:

   ![IP Tables configuration was loaded successfully to the device]

7. Click Ok to close the message.

### 3.8.3 Controlling Access – Device Access Protocols

By default both HTTP and HTTPS protocols are enabled and you can access the web client using these protocols. However, you can disable the HTTP protocol to allow accessing the NSG 9000-6G device via HTTPS secure-mode only.

HTTPS TCP port is 443 and HTTP TCP port is 80.

**NOTE:** Only user admin can disable the HTTP protocol.

To change the default configuration of access protocols, do the following:
1. Select the Platform tab.
2. Select Chassis > Security tab.
4. To enable/disable the HTTP protocol, select/de-select Enable HTTP.

**NOTE:** When disabling a protocol, the device disconnects for an instant to refresh its connection.
3.9 Device Authentication

NSG 9000 may use a Remote Authentication Dial In User Service (RADIUS) server to authenticate and authorize users who are trying to log into the NSG 9000.

To enable the RADIUS authentication, the following should apply:
- Connection to a RADIUS server - NSG is defined as a client of the RADIUS server
- NSG 9000 is configured to work in Remote mode
- The RADIUS server database should include three types of authorized NSG users. Any user defined in the RADIUS server must belong to one of these groups:
  - Admin
  - Config
  - Guest

The following table lists the permissions of each group of users:

<table>
<thead>
<tr>
<th>User</th>
<th>Device Configuration</th>
<th>Change IP Tables</th>
<th>Password of Local Users</th>
<th>Upgrade</th>
<th>Authentication Mode</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>config</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>guest</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Once a user is trying to log into the NSG 9000 either via HTTP/HTTPS or SSH, NSG 9000 challenges the RADIUS server. Once the user is authenticated and authorized, the user can log into the device.

Upon a communication problem with the RADIUS server, while performing authentication, the NSG automatically switches to a local authentication method. However, once the problem is fixed, remote authentication is performed as long as Remote is the configured authentication mode.

When working in Remote mode, local users cannot login.

To configure RADIUS Mode
1. Open the web client of the device.
2. Select Platform > Chassis > Authentication > tab:
3. Open the Authentication Type list and select either of the following:
   - Local - authentication and authorization is performed locally, against the database of the NSG 9000-6G
   - Remote-RADIUS - authentication and authorization is performed by the RADIUS server. When selected, move to the following step to configure the required parameters.
4. When Remote is selected, configure the following parameters:
   - Server IP - enter the IP address of the RADIUS server
   - Port - the port number over which the RADIUS server communicates with the NSG 9000.
   - Secret - enter a confidential string that is shared between the device and the RADIUS server.
   - Timeout - enter in seconds, the time allowed to elapse between an NSG 9000 request and a response from the RADIUS server.

   **NOTE:** Once you change to Remote and click Apply, any attempt to login, or after refresh, requires the remote authentication.

### 3.10 Input GbE Ports Configuration

The GbE ports are operate as eight independent ports receiving eight different feeds. The port status is reflected in the Platform > General tab as follows:

#### Table 3-4: Input GbE Port

<table>
<thead>
<tr>
<th>Port Status</th>
<th>Display</th>
<th>Display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Grey</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>White</td>
<td></td>
</tr>
<tr>
<td>Part of a port-redundancy pair</td>
<td>Yellow - tool tip indicates whether primary or backup</td>
<td></td>
</tr>
</tbody>
</table>

#### 3.10.1 Configuring Input GbE ports

- To configure GbE port properties:
  1. Select the Platform tab.
  2. In Back Panel View, select the GbE ports.
3. To configure the GbE port parameters, do the following:

- **Enable Port** - select to enable the port.
- **SFP Vendor** - (Read only) view the vendor of the SFP module mounted in the GbE port.
- **SFP mode** - (Read only) view the mode of the SFP module mounted in the GbE. It can be multi mode, single mode or copper.
- **SFP Type** - (Read only) view the type of SFP mounted.
  - Copper - when copper SFP is mounted
  - When fiber SFP is mounted either of the following is indicated:
    - SX - indicates multi-mode SFP, typically used for short distances (up to 200 m)
    - LX - indicates single-mode SFP, typically used for long distances (10km and up).

**NOTE:** If the SFP is not mounted, Not Mounted appears in the SFP Vendor, SFP Mode and SFP Type parameters.

- **Auto Negotiation** - The Auto Negotiation is a handshake protocol used in GbE links. Select this check box to activate the Auto Negotiation protocol only if the other end of the GbE link also uses auto negotiation.
- **MAC Address** - view the physical address of the GbE as retrieved from the device. This is a read only parameter.
- **Status** - reflects the current status of the relevant GbE channel. Displays OK, Link Down, SFP Not Mounted, or Disable Mode.
- **FPGA Version** - view the FPGA version as retrieved from the device. This is a read only parameter.
- **NGOD Input Group Name** - Enter the name of the input group that the NSG relates to when reporting on this interface in its NGOD-D6 messages.
- **NGOD Assigned Bandwidth (Mbps)** - Enter the bandwidth of the GbE port assigned for the NGOD ERM. The default is 1000MB, that is the full capacity of the port is assigned for the NGOD ERM. You can enter a value between 0-1000 in increments of 100. If you enter 0, the GbE port is not available for the NGOD ERM.
- **Route Refresh** - When enabled, the NSG routinely sends "Ping" requests to the gateway of the GbE port. Requests are sent approximately once per 5 seconds, thus preventing expiration of the route.
- **Refresh Interval (Msec)** - Define, in Msec, how often to send a Ping request.
4. In the IP Addresses table, enter the following parameters:
   - **IP Address1** - type in the required IP address
   - **Subnet** - type in the required subnet mask.

### 3.10.2 Configuring Input GbE Port Redundancy

#### 3.10.2.1 Overview

NSG 9000-6G supports 1:1 and N:1 redundancy modes for its GbE input ports. Typical port redundancy configuration depends on the application in which the NSG is deployed as the following scenarios describe:

- **VOD application** - to allow redundancy for IP unicast VOD streams, you should use 1:1 port redundancy. Select a distinct backup port for each primary port, with the **Same IP Address** option checked.
- **Broadcast application** - to allow redundancy for IP multicast streams, you should use 1:1 port redundancy.
- **SDV application** - to allow redundancy for IP multicast SDV streams, use either 1:1 or N:1 redundancy modes depending on the desired level of protection:
  - 1:1 port redundancy - define for each primary port a backup port. De-select the **Same IP Address** option, and set a distinct IP address for the designated backup port. This mode ensures the highest level of protection against various network failures.
  - N:1 port redundancy - allows an efficient use of the eight available input GbE ports, by utilizing a single backup port for protecting several primary ports. The typical and recommended configuration for this mode is to define two groups of 3 primary ports and one backup port. For example, port 4 backs up ports 1-3 and port 8 backs up ports 5-7. In case of a redundancy switch, the backup port starts transmitting also the streams of the failed primary port(s).

In general, the following guidelines apply for the port redundancy feature:

- To configure port redundancy, port should be enabled. (Select GbE Port > General tab)
- A primary port cannot serve as a backup port.
- If the **Same IP Address** option is selected, the backup port is disabled and the IP address of the port changes to the IP address of the primary port. When the primary port fails, the backup port is enabled, using the same IP address of the failed port.
- Configuring port redundancy, blocks the port configuration except for IP address in case **Same IP Address** is selected.
- **Alarm configuration:**
  - By default both Link Down and No Input Traffic alarms trigger port redundancy.
  - The alarm configuration of the primary port and backup port is the same.
  - You can configure the alarms of a primary port only.
  - When selecting a backup Port, the alarm configuration of the primary port also applies to the backup port.
  - In N:1 port redundancy, the alarm configuration applies to the backup port and to all of the primary ports it backs up. Once you configure the backup port to backup an additional primary port, the alarm configuration automatically applies to the primary port.
    Any changes to the alarm configuration immediately applies to the backup port and to all primary ports it backs up.
Chapter 3 Configuring Platform Parameters

Input GbE Ports Configuration

- Upon redundancy switch, automatically the configured backup port is activated. If the backup port fails, a redundancy switch is performed to return to the Primary. If the primary port is still faulty, the redundancy mechanism, re-checks the last active port for a momentary failure. If it is still faulty, the redundancy switch reverts to the primary and keeps checking in increased intervals the configured backup port, until detecting an active port.

- Redundancy switches are written in the alarm log. To view the history of the port redundancy switches, select Monitoring > Logs > Alarm Log and click View Log.

3.10.2.2 Port Redundancy Related Alarms

- Triggering redundancy - Link Down and No Input Traffic
- After the redundancy switch, the following alarm is raised: Backup Port is Active

To configure GbE port redundancy
1. Open the web client of the device.
2. Select Platform > Chassis > Port Redundancy.
3. To view the current status of the ports, click Refresh Port State. The Active Port column is updated to display the currently active port.
4. Open the Backup Port list and select the required backup port for any of the required ports. Active Port, Same IP Address, Trigger alarm columns and the Switch button are enabled. By default, both triggering alarms are selected.
5. In VOD application, to allow redundancy for the IP unicast VOD streams, select a distinct backup port for each primary port with the Same IP Address option checked. In this case, only the primary port is active. Once you select Same IP Address the following takes place:
   - The IP address of the backup port changes to the IP address of the primary port
   - The backup port is disabled
6. By default both triggering alarms are selected. Configure the triggering alarms as required.
7. To manually switch between the ports, click Switch.
3.11 Configuring/Viewing DTI Parameters

To configure and view DTI parameters, select the DTI component and do the following:

- Configure DTI parameters:
  - Enslave NSG 9000-6G clock to the DTI clock by selecting Use DTI Clock
  - Define the DTI port redundancy mode, and select the preferred DTI port (if applicable, depending on the redundancy mode)
  - Configure the SNMP traps

- View the following:
  - DTI client properties and status - via the Client Information section
  - Port Information - via Per Port Information section

3.11.1 Configuring DTI Client Parameters

1. Select the Platform > General tab.
2. In the Back Panel View, select the DTI component. The General tab appears.
3. When working in M-CMTS mode, enslave the NSG clock to the DTI clock. To enslave, select Use DTI Clock.
4. To set the DTI port redundancy mode, open the Redundancy Mode list and select one of the following:
   - Manual - you need to select the DTI port. No automatic switching/activation of ports is done, regardless of the status of the DTI ports.
   - Automatic (no Auto Revert) - selecting the active port is completely automatic, without any intervention and without any preference of a specific port. If the active
port fails, the standby port is activated and assumes the role of "active" as long as it is in normal state. If the latter fails, ports will be switched again. This switching can continue any number of times, without any preference of a specific port.

- **Automatic (Auto Revert)** - in this mode, the selected port (as defined in Selected Port) is always preferred over the other port. In case that the selected port fails, the standby port is automatically activated. Once the selected port is fixed, the NSG automatically switches back to the selected port.

5. To select the active DTI port, open the Selected Port list and select either port 1 or 2.

**NOTE:** The Selected Port list is disabled if Automatic (no Auto Revert) is selected.

6. In Notification, define which notification to send once the status of the DTI client changes:

- **Log Status Change Events** - send a notification to the alarm log upon a change in the status of the DTI client
- **Send Trap on Status Change** - send an SNMP trap upon a change in the status of the DTI client

### 3.11.2 Viewing DTI Client and DTI Port Information

1. Select the Platform > General tab.
2. In the In Back Panel View, select the DTI component.

**NOTE:** The DTI section is enabled only when a DTI client is installed in the device.

The General tab appears.

3. To view DTI client information, focus on Client Information section.

- **In Overall Status**, verify that the DTI status is NORMAL. The following table lists the available Status options:

<table>
<thead>
<tr>
<th>Status</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warmup</td>
<td>Local oscillator has not yet stabilized</td>
</tr>
<tr>
<td>Freerun</td>
<td>DTI client is not locked to the signal of the DTI server, and is running freely using its own internal real-time clock. Freerun indicates that since its last initialization, the client was not locked to the server.</td>
</tr>
<tr>
<td>Normal</td>
<td>DTI client is locked to the DTI server, working normally</td>
</tr>
<tr>
<td>Bridging</td>
<td>This is a transient state, which may last up to 2 seconds. It indicates that the DTI client has experienced a momentary interruption in its timing signal, but is still able to maintain acceptable timing. NSG 9000 is still locked to the DTI server clock.</td>
</tr>
<tr>
<td>Holdover</td>
<td>DTI client lost its sync to the DTI server clock. Working in &quot;best effort mode&quot;, with the last known valid time correction</td>
</tr>
<tr>
<td>Fast</td>
<td>The DTI client has just acquired a valid signal, and is in the process of locking to it. If this status is displayed for a prolonged time, this indicates a problem with the received DTI signal or with the DTI client.</td>
</tr>
</tbody>
</table>

- **In 10Mhz Ref.,** indicates whether the 10Mhz Reference signal is present.
- **In Timestamp,** view the last DTI timestamp
- In Active Port, view the currently active DTI port.
- In FPGA Version, view the installed FPGA version of the DTI client.

4. To view DTI client port information, focus on the Per Port Information section. For each port view the following information:
   - DTI Signal Detected - indicates whether a valid DTI signal is detected.
   - Server Status - indicates the status of the server as it is communicated to the client. Available status indications are as follows: Warmup, Freerun, Fast, Normal, or Holdover.
   - CRC Error Count - indicates the number of CRC error occurrences on the DTI link.
   - Cable Advanced Valid - indicates whether cable advance is valid. A valid, i.e. Stable, Cable Advance value is essential in order for the client to lock to the server.
   - Frame Error Rate - indicates the Frame Error Rate as follows: Below 2%, 2% to 5%, or Over 5%.

3.11.2.1 DTI Client State Diagram
3.12 Configuring QAM-RF Modules

The NSG 9000-6G device has nine slots. Each slot accommodates a single QAM-RF module.

The Back Panel View section, displays the slots while indicating the following QAM-RF module related information:

- Slot number - a number between 1 - 9

**NOTE:** To view the actual mounted module, select the Module tab. See 3.12 Configuring QAM-RF Modules on page 42.

- Slot Status - either of the following appears:
  - Module OK - indicates that the slot is occupied with the configured module and the latter is working.
  - Module Out - indicates that the slot is vacant.
  - Module Fail - indicates that the mounted module is faulty or that the applied configuration does not match the currently mounted module.

**NOTE:** To view licensing granted for this module, select Platform > Licensing > Assign Licenses.

In addition, when selecting a slot, you may access the properties of the mounted module. The Module Properties are arranged in the following tabs:

- Module - See 3.12.2 Configuring a QAM-RF Module on page 46.
- Port - the default tab. See 3.12.3 Configuring Module RF Ports on page 47.
- QAMs - See 3.12.4 Configuring/Viewing QAM Channels on page 49.
- General - See 3.12.5 Viewing QAM-RF Module Information on page 52.
- Redundancy - See 3.13 RF Module Redundancy Overview on page 52.

You can also reset each module by clicking the Reset Module button. See page 23.

The following sections guide you on how to configure the QAM-RF modules. The QAM-RF module configuration includes the following stages:
Configuring global parameters - the same definitions are sent to all of the QAM-RF modules/QAM channels. The Global configuration is available via the Platform > General > Chassis > Global RF & QAMs tab.

Configuring parameters for each QAM-RF module - To allow the NSG 9000-6G device to support multiple applications, during this configuration you may override the configuration of global parameters such as module encoding mode and QAM manager. The configuration of each QAM-RF module is available via the Platform > General > Slot Module > Module/Ports/QAMs tabs.

3.12.1 Configuring Global RF & QAMs Parameters

**TIP:** Defining the global parameters of the RF ports & QAM channels is the first stage of the QAM-RF module configuration.

When configuring the QAM-RF module parameters, you may send definition to all of the QAM-RF modules/QAM channels as the following table shows.

<table>
<thead>
<tr>
<th>Table 3-6: Setting Global RF &amp; QAM Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required Action</strong></td>
</tr>
</tbody>
</table>
| To send definitions to all of the QAM-RF modules, click Set All Modules and then Apply. | 1. [Set All Modules]  
2. Apply |
| To send definitions to all of the RF ports, click Set All Ports and then Apply. | 1. [Set All Ports]  
2. Apply |
| To send definitions to all of the QAMs, click Set All QAMs and then Apply. | 1. [Set All QAMs]  
2. Apply |

You can globally configure the following:

3.12.1.1 Defining Global RF and QAMs Settings on page 43
3.12.1.2 Defining Number of QAMs and Enabling RF Ports on page 45
3.12.1.3 Closing/Opening all RF Ports on page 45
3.12.1.4 Configuring a Global QAM Manager on page 46
3.12.1.5 Locking Symbol Rate on page 46

3.12.1.1 Defining Global RF and QAMs Settings

To define RF Scheme and Template

1. Select Platform > General tab.
2. In Back Panel View, select Chassis.
3. Select the Global RF & QAMs tab.
4. Focus on the RF Scheme and RF Template sections.

![RF Scheme and RF Template sections]

5. To define the encoding mode, open the ITU-T Annex list and select one of the following:

Table 3-7: Encoding Mode

<table>
<thead>
<tr>
<th>Encoding Mode</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex-A (DVB)</td>
<td>This mode is used mainly in European and Asian countries. Utilizes bandwidth of 8 MHz per QAM-RF channel.</td>
</tr>
<tr>
<td>Annex-B</td>
<td>This is the mode used in North-American countries. Utilizes bandwidth of 6 MHz per QAM-RF channel.</td>
</tr>
<tr>
<td>Annex-C (Japan)</td>
<td>As implied by its name, used mainly in Japan. Similar to Annex-A in the most part, but utilizes bandwidth of 6 MHz per QAM-RF channel.</td>
</tr>
</tbody>
</table>

6. To define the required constellation, open the Constellation list. The Constellation is the type of Quadrature Amplitude Modulation (QAM) used. QAM constellation affects Data Rate and Symbol Rate, and must be set according to HFC network properties. Valid values are:

<table>
<thead>
<tr>
<th>Encoding Mode</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex-A or Annex-C</td>
<td>16, 32, 64, 128, 256</td>
</tr>
<tr>
<td>Annex-B</td>
<td>64 and 256</td>
</tr>
</tbody>
</table>

7. In Symbol Rate (Mps), view/configure the rate of QAM symbols that are encoded and transmitted per second as follows:
   - Annex-B - (Read-only), symbol rate is fixed per constellation
   - Annex-A - configure in the following allowed range: 5.0000 - 6.9565
   - Annex-C - configure in the following allowed range: 5.0000 - 5.3131
8. In Data Rate, (Read-only), view the bit rate of the transport stream in Bps.
9. To apply the configuration to all of the QAM-RF modules, click Set All Modules.

**NOTE:** The configuration will take effect once you click Apply.

10. To set the QAM-RFs frequency, open the RF Template list and select one of the following:
   - Frequency - frequency is entered explicitly as numeric frequency values
   - EIS-STD - frequency is defined using channel numbers based on the EIA-STD channel table. See *EIA SDT and HRC Standards on page 153.*
   - EIA-HRC - RF settings are entered using channel numbers based on the EIA-HRC channel table. See *EIA SDT and HRC Standards on page 153.*

11. To apply the configuration to all of the QAM-RF modules, click Set All Modules.

### 3.12.1.2 Defining Number of QAMs and Enabling RF Ports

- To define the settings of the RF Ports
  1. Select Platform > General tab.
  2. In Back Panel View, select Chassis.
  3. Select the Global RF & QAMs tab.
  4. Focus on the #QAMs per Port and Enable RF Port sections:

![Image of #QAMs per Port](image)

5. To select the number of QAM channels, open the #QAMs per Port list and select the required number of channels.

6. To apply the configuration to all of the QAM-RF ports, click Set All Ports.

7. To enable/disable the QAM-RF ports, select/de-select Enable Port.

8. To enable/disable all RF ports of the device, click Set All Ports.

### 3.12.1.3 Closing/Opening all RF Ports

- To mute all RFs
  1. Select Platform > General tab.
  2. In Back Panel View, select Chassis.
  3. Select the Global RF & QAMs tab.
  4. Focus on the Emergency Shutdown section:

![Image of Emergency Shutdown](image)

5. To mute all RF ports, click Mute All RFs. The button toggles to Unmute All RFs.

6. To open all RF ports, click Unmute All RFs. The button toggles to Mute All RFs.
### 3.12.1.4 Configuring a Global QAM Manager

To configure a QAM Manager

1. Select **Platform > General tab.**
2. In **Back Panel View**, select **Chassis.**
3. Select the **Global RF & QAMs** tab.
4. Focus on the **QAM Manager** section:

   ![QAM Manager](image)

   - To select a QAM manager for all of the QAM-RF modules, open the QAM Manager list and select the required QAM Manager. See, Table 3-10: QAM Manager on page 50.
   - To send configuration to all of the QAMs, click **Set All QAMs**.

   **NOTE:** The configuration will take effect once you click **Apply.**

Once you are done with this configuration, move on to configure each module by selecting the required module and the **Module tab.**

### 3.12.1.5 Locking Symbol Rate

For future use only.

### 3.12.2 Configuring a QAM-RF Module

1. Select the **Platform** tab.
2. In **Back Panel View**, select the required slot.
3. Select the **Module** tab.

<table>
<thead>
<tr>
<th>Module 1 Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Expected Module Type</strong></td>
</tr>
<tr>
<td><strong>Actual Module Type</strong></td>
</tr>
<tr>
<td><strong>ITU-T ANNEX</strong></td>
</tr>
<tr>
<td><strong>Constellation</strong></td>
</tr>
<tr>
<td><strong>Symbol Rate (Mbps)</strong></td>
</tr>
<tr>
<td><strong>Data Rate (bps)</strong></td>
</tr>
</tbody>
</table>

4. Define/View the following module information:

   - **Expected Module Type** - Read only. The module type is NSG-8R1G, OCTAL, up to eight QAM-RF channels per RF port.
   - **Actual Module Type** - Read only. Currently not applicable.
   - **ITU-T ANNEX** - open the list to select the required encoding mode. Changes to the encoding mode override the encoding mode configured during global module configuration. See Table 3-7: Encoding Mode on page 44.
   - **Constellation** - select the required constellation. The Constellation is the type of Quadrature Amplitude Modulation (QAM) used. QAM constellation affects Data Rate and Symbol Rate, and must be set according to HFC network properties. Valid values are: Annex-A or Annex-C: 16, 32, 64, 128, 256. Annex-B: 64 and 256. Changes override the constellation configured during global module configuration.
NOTE: You can configure the Sym Rate 1 & 2 for ANNEX A and ANNEX C only.

- Symbol Rate - define/view the rate of QAM symbols that are encoded and transmitted per second. You can define the symbol rate in Annex A and C. In Annex B, you can only view its value. Changes override the symbol rate configured during global module configuration.
- Data Rate - view the defined data rate.
- Interleaver 1 - view the interleaver values as defined in the QAM tab. NSG 9000-6G has two optional Interleaver values, set the required value for this interleaver.
- Interleaver 2 - See Interleaver 1.
- QAM Placement - Read only. Block is the standard placement of adjacent QAM-RFs along the 48Mhz block, depending on the selected ITU-T Annex.
- RF Template - define/view the RF Template. Define the RF template for Annex B only. View for Annex A and C. The RF template is defined during the global RFs & QAMs configuration. See 3.12.1 Configuring Global RF & QAMs Parameters on page 43. Changes override the RF template configured during global module configuration.

3.12.3 Configuring Module RF Ports

1. Select the Platform tab.
2. In Back Panel View, select the required slot.
3. Select the Port tab.

For each RF port, define the following:
- RF Enable - select to enable the RF port. Enable the port only after completing the output configuration.
- #QAMs per Port - select the number of active QAM channels, from 1-8 active channels (Annex B & C) and 1-6 Annex A. The number of active channels is license dependent and by default two channels are active.

NOTE: The frequency of the QAM channels is consecutive and each channel utilizes six MHz in Annex B & C or eight MHz in Annex A.
- Power Level (dBmV) - The power level of the RF port. Once you define the RF power level, the power level of all QAM channels in the port changes accordingly. All QAM channels have the same power level in relation to the defined power level of the RF port. Once you configure the power level in dBmV, you can view the power level also in dBuV.

- Power Level Per QAM - Define the QAM power level for all QAM channels within the port. This value appears in the QAM tab as a read-only value. Once you configure the power level per port in dBmV, you can view the power level per port also in dBuV.

**NOTE:** Any changes to the RF power level affect the QAMs power level and vice versa.

5. Review the port and its QAM channels configuration via the provided bar graphs as explained in the following section.

### 3.12.3.1 Understanding the RF Port Graph

A bar graph, for each RF port displays the current configuration of the RF port as the following table explains:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF Enable</td>
<td>Blue grid - RF port is enabled</td>
</tr>
<tr>
<td></td>
<td>Red grid - RF port is disabled</td>
</tr>
<tr>
<td># QAMs per Port</td>
<td>Number of bars in graph. Each QAM-RF channel is represented by a bar.</td>
</tr>
<tr>
<td>Power Level (dBmV)</td>
<td>Height of bar. Each bar represents a QAM, however the power level of each QAM depends on the RF port power level.</td>
</tr>
</tbody>
</table>
Once you hover the mouse pointer over a bars you can read QAM channel related information as the following table explains:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Indicates the center frequency of the QAM-RF channel</td>
</tr>
<tr>
<td>Power level</td>
<td>Indicates the power level of the QAM-RF channel</td>
</tr>
<tr>
<td>Mute</td>
<td>Indicates whether mute or not</td>
</tr>
<tr>
<td>Spectral Inversion</td>
<td>Indicates whether spectral inversion is applied</td>
</tr>
<tr>
<td>CW Signal</td>
<td>Indicates whether CW is applied or not</td>
</tr>
<tr>
<td>QAM License</td>
<td>Indicates whether QAM license is granted</td>
</tr>
</tbody>
</table>

### 3.12.4 Configuring/Viewing QAM Channels

1. Select the **Platform** tab.
2. In **Back Panel View**, select the required slot.
3. Select the QAMs tab.

4. Define RF attributes according to the following explanation:
   - **RF Enable** - Read only parameter. To enable the port, see 3.12.3 Configuring Module RF Ports on page 47. Select to enable the port.
   - **RF Output** - Read only. It indicates the QAM-RF output channel in the following pattern x.y.z where:
     - x - Module number
     - y - RF port number
     - z - RF channel number
     For example, 1.2.2 refers to output traffic of module 1, transmitted via RF port 2, QAM channel 2.
   - **QAM Index** - (Read Only). An index number to identify each QAM channel within the 144 available QAM-RF channels of the device.
   - **TS ID** - sets the ID of the transport stream carried over this QAM-RF channel.
   - **QAM Manager** - The QAM manager determines the functionality of the QAM. The default QAM manager is NGOD ERM. You can select one of the following QAM managers:

<table>
<thead>
<tr>
<th>Table 3–10: QAM Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>QAM-RF Manager</strong></td>
</tr>
<tr>
<td>VOD SRM</td>
</tr>
<tr>
<td>NGOD ERM (default)</td>
</tr>
<tr>
<td>ISA SRM</td>
</tr>
<tr>
<td>Broadcast</td>
</tr>
</tbody>
</table>
Table 3–10: QAM Manager

<table>
<thead>
<tr>
<th>QAM-RF Manager</th>
<th>Application</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-CMTS</td>
<td>M-CMTS</td>
<td>The QAM-RFs deliver M-CMTS data and are controlled by the CMTS.</td>
</tr>
<tr>
<td>M-CMTS Dynamic</td>
<td>M-CMTS with DEPI control</td>
<td>The device is controlled by the CMTS device using the Downstream External PHY Interface (DEPI). This interface enables the CMTS device to control the NSG device, and provides the CMTS with a control path for setting up, maintaining, and tearing down sessions. Note: This QAM manager should be applied to all QAM_RF channels of the RF port.</td>
</tr>
<tr>
<td>D2E</td>
<td>D2E</td>
<td>The D2E server controls the QAMs. Future use only.</td>
</tr>
</tbody>
</table>

**NOTE:** To change a QAM Manager, verify that no session, service or PID are provisioned/remuxed to this QAM-RF.

- **Serving Area** - Enter the ID of the area that this QAM channel serves. When working with SAT, the Serving Area value should contain up to 16 bits (range of 1-65535). See 4.2.2.4 Creating and Setting SAT on page 77.
- **NGOD Group Name** - enter the QAM group name that the NSG reports on via its NGOD-D6 messages.
- **EIA Channel** - Appears when in RF Template you select EIS-STD. It indicates the channel number based on the EIA-STD channel table.
- **Frequency** - The RF frequency (Hz) of this transport stream. The following table lists the allowed ranges indicating the center frequencies:

**NOTE:** Frequencies below 50MHz are for special Broadcast deployments that require IF output.

- **Power Level** (dBmV) - Indicates the power level as defined in the RF Port tab. See 3.12.3 Configuring Module RF Ports on page 47.
- **Spectral Inversion** - The spectral inversion is an advanced QAM configuration parameter. If checked, spectral inversion is enabled.
- **Mute** - Allows to mute a single QAM channel without affecting the other channels that flow through the port.
- **CW** - Select for testing purposes only.
- **PSIP Enabled** - select to enable PSIP generation. QAM manager should be: VOD SRM, ISA SRM, or, NGOD ERM. See 4.3.4 Provisioning PSIP Tables on page 89.

### Table 3–11: QAM Channels Frequency

<table>
<thead>
<tr>
<th>ANNEX B &amp; ANNEX C</th>
<th>ANNEX A (DVB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>35,000,000-999,000,000 Hz</td>
<td>36,000,000-998,000,000 Hz</td>
</tr>
</tbody>
</table>

**NOTE:** Frequencies below 50MHz are for special Broadcast deployments that require IF output.
3.12.5 Viewing QAM-RF Module Information

1. Select the Platform tab.
2. In Back Panel View, select the required slot.
3. Select the General tab.

4. View the following information:
   - Serial Number - The serial number of the mounted module.
   - FPGA Version - The version of the interface FPGA card.
   - HUC SW Version - The version of the Harmonic Up Converter firmware. A version of 06.00 and higher indicates an up converter of 1G.
   - Status - Indicates the status of the module:
     - Module OK - the module is mounted and works properly
     - Module is Out - the module is not mounted in the slot
     - Module Failed - the mounted module is faulty or there is a mismatch between the module and the configuration.
   - License Status - shows the QAM channel number, its frequency, and granted QAM/PM licenses. See, 3.14 Managing Your Licenses on page 56.

3.13 RF Module Redundancy Overview

The RF module redundancy protects the network from a faulty QAM-RF module. The RF module redundancy allows an intra-chassis redundancy switch that does not require an additional backup device. You may define the RF module in slot nine as the redundancy module for any faulty RF module. As a result, the redundancy switch takes place among the QAM-RF modules and not between a primary and backup devices.

For the RF module redundancy to take place, the following should apply:
- Up to 8 of the NSG 9000-6G QAM-RF modules in slots one to eight, are configured and provisioned with TSs. The QAM manager of all QAMs of these QAM-RF modules should be Broadcast.

NOTE: RF module redundancy applies to QAM-RF module with Broadcast QAM manager only.
Chapter 3 Configuring Platform Parameters

3.13.1 RF Module Related Alarms

Triggering Alarm

A triggering alarm is any alarm that is critical and is issued by the QAM-RF module, or the upconverter as the following table lists:

Table 3-12: NSG9000-6G Triggering Alarms

<table>
<thead>
<tr>
<th>Object</th>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QAM-RF Module</td>
<td>Critical Error</td>
<td>Internal fatal error in the QAM-RF modules</td>
</tr>
<tr>
<td></td>
<td>Processing Error</td>
<td>QAM-RF global error</td>
</tr>
<tr>
<td></td>
<td>Temperature Out of Range</td>
<td>The upconverter’s temperature is out of the allowed temperature range: (0°C to 70°C)</td>
</tr>
<tr>
<td></td>
<td>Communication Failure</td>
<td>The device cannot communicate with the QAM-RF module</td>
</tr>
<tr>
<td></td>
<td>Initialization Failure</td>
<td>Module initialization failed</td>
</tr>
<tr>
<td>RF Port</td>
<td>Communication Failure</td>
<td>The device cannot communicate with the upconverter.</td>
</tr>
<tr>
<td></td>
<td>RF Level Out of Range</td>
<td>The power level of the RF signal going into the upconverter is out of the allowed range</td>
</tr>
<tr>
<td></td>
<td>PLL1 Failure</td>
<td>Indicates a HW failure</td>
</tr>
<tr>
<td></td>
<td>PLL2 Failure</td>
<td>Indicates a HW failure</td>
</tr>
<tr>
<td></td>
<td>Power Supply Failure</td>
<td>Power level to the upconverter momentarily exceeded its limit</td>
</tr>
<tr>
<td></td>
<td>Software Failure</td>
<td>Indicates a HW failure</td>
</tr>
</tbody>
</table>
Indicative Alarm

Once the intra-chassis redundancy has occurred, the NSG issues the *Backup RF Module activated* warning. The warnings is registered in the Alarm log as the following picture shows:

**NOTE:** Reverting is manual only.

### 3.13.2 Enabling the RF Module Redundancy

By default, QAM-RF module redundancy is disabled. To start RF module redundancy, do the following:

1. Configure all modules beside the module in slot nine.
2. Define the QAM manager of the QAM-RF modules including QAM-RF module nine to Broadcast.
3. In Platform, select the required module.
4. Select the Redundancy tab.
5. Select **Enable Module Redundancy**. A message notifies you that the configuration of the QAM-RF module in slot nine will be removed. However the module is assigned.
6. Click **Ok**. Slot nine is updated with an indication that the module is a backup module.
7. Click **Apply**.

**NOTE:** If a QAM-RF module is not mounted in slot nine, you cannot apply the Module configuration.
The following takes place:

- The Manual Failover button is enabled. At any time, you can manually switch to the backup module.
- The Status box indicates that the Primary module is active.
- You cannot change the configuration of the backup module.
- The QAM-RF module-redundancy is activated. Once any of the QAM-RF modules is faulty, an automatic switch takes place and the QAM-RF module in slot nine operates according to the configuration of the faulty module. The Manual Failover button is disabled and the Revert to Primary button is enabled. The following picture shows the Platform tab upon a redundancy switch:

You cannot change the configuration of the faulty primary module as long as the backup module is active.

### 3.13.3 Reverting Redundancy Module

Reverting back to the primary QAM-RF module once the fault is fixed is manual only.

1. Select Platform > QAM-RF Module > Redundancy.
2. Click Revert to Primary. The Revert to Primary button is enabled once a redundancy switch occurred.
3.13.4 Switch Redundancy Module

Once you enabled the RF redundancy, you can select any assigned module and initiate a manual redundancy switch by clicking Manual Failover. This button is disabled once a redundancy switch takes place.

1. Select Platform > RF Module Redundancy.
2. Enable RF redundancy as explained in 3.13.2 Enabling the RF Module Redundancy on page 54.
3. Select the required RF module.

A manual redundancy switch takes place.

NOTE: If the backup module is active, you cannot perform manual failover.

3.14 Managing Your Licenses

The output QAM-RF channels of the NSG 9000-6G device are license dependent. All licenses are per QAM port and the available licenses are as follows:

- Temporary All License - all of the QAM-RF channels are operating. This license is time limited. It can be limited as follows:
  - 14 days - default license. Once you purchase the device and as soon as the device starts working it works for 14 days with all of its capabilities. This grace period of 14 days allows you to activate your licenses to guarantee device operation according to its licensed functions.
  - 90 day - usually for trial or demo purposes
  - 30 day - usually for trial or demo purposes
- Narrowcast QAM License - (Default Module License for 4 QAM). When you purchase a QAM-RF module, you also receive a license for two QAM channels per QAM-RF port. To operate additional QAM channels of the module, you need to purchase additional QAM licenses.
- PM Scrambling License - allows you to output TSs scrambled in the Privacy Mode encryption technology of Motorola.
- DVB Scrambling License - allows to output TSs via the licensed QAM using DVB scrambling.
- DOCSIS QAM - allows to output DOCSIS data via the licensed QAM.
- DOCSIS QAM + DTI Synch - allows to output DOCSIS data with DTI synchronization via the licensed QAM.
3.14.1 Working with Licenses

To work with licenses, you need to install the purchased licenses on the device. It is recommended to install and to remove licenses using the License Manager tool. Obtain this tool free of charge from Harmonic customer support.

For instructions on how to install, remove, or move licenses across the NSG devices, see License Manager documentation.

For the device to operate according to the purchased license you need to do the following:

Table 3-13: Claiming a License

<table>
<thead>
<tr>
<th>Action</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install a license on the device</td>
<td>Licenses are received from Harmonic as numbered License Packs, and need to be installed onto the NSG device. To install, use the License Manager. In rare cases, install the license via the web client. See page 60.</td>
</tr>
<tr>
<td>Assign a license</td>
<td>Activate a license per each QAM-RF channel. If the requested licenses are installed on the NSG device, after the configuration is applied, the relevant license is enabled on this QAM-RF channel.</td>
</tr>
<tr>
<td>Viewing license status</td>
<td>View license status:</td>
</tr>
<tr>
<td></td>
<td>• At the top section of the Assign Licenses tab</td>
</tr>
<tr>
<td></td>
<td>• Licenses Summary tab</td>
</tr>
<tr>
<td>Remove a license from the device</td>
<td>To remove installed licenses, see License Manager. To view deleted licenses, see page 61.</td>
</tr>
</tbody>
</table>

Licenses are limited by time and an alarm is issued 24 and 72 hours before the license expires. Once a license is expired, NSG 9000-6G disables the channels from the first channel in the first port of the first slot regardless of the channel that has expired.

3.14.1.1 Assigning a License

When assigning a license, you activate a license per each QAM-RF channel. If the requested licenses are installed on the NSG device, after the configuration is applied, the relevant license is assigned/enabled on this QAM-RF channel.

1. Select Platform > Licensing > Assign Licenses.
The **Assign License to QAMs** page opens:

Once the page opens, you can view the current status of each license:

- **Activated licenses** - all checked licenses
- **Unassigned licenses** - all checked licenses with a red background

2. Scroll down to the required module.
3. To request a license, check the required QAM channel(s).
4. To claim a license, click **Apply**.

   The licenses are activated and the QAM channels operate according to the granted license.

If you try to assign more licenses than you purchased and installed, a message appears notifying you of the QAM channel its license is deferred. The channel appears in the table with a red background.
5. To view the total number of the licenses according to their current status, scroll to the top of the page:

<table>
<thead>
<tr>
<th>Assign Licenses To QAMs</th>
<th>QAM License</th>
<th>PM License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Available Licenses</td>
<td>144</td>
<td>144</td>
</tr>
<tr>
<td>Total Requested Licenses</td>
<td>144</td>
<td>1</td>
</tr>
<tr>
<td>Total Claimed Licenses</td>
<td>128</td>
<td>1</td>
</tr>
<tr>
<td>Total Granted Licenses</td>
<td>120</td>
<td>1</td>
</tr>
</tbody>
</table>

Total Available Licenses - the total number of purchased licenses that were added by entering the license key.

Total Requested Licenses - the total number of licenses you checked to allow granting them.

Total Claimed Licenses - the total number of licenses you requested (checked them) and send to the device (click Apply) to claim them. A license is claimed but not granted in the following cases:

- The module is not mounted in the slot
- The module’s state is Failed
- QAM channel is not active due to the selected RF mode
- Total Granted Licenses - the total number of licenses that you requested and are granted, that is that the QAM is operating according to the license.

3.14.1.2 Re-assigning a License

Once you purchased, additional licenses, and you wish to assign them, use the Reconcile Licenses button. Once you click the Reconcile Licenses button, automatically all licenses are reassigned from the first module, module 1, to the last module, module 9. If you try to assign more licenses than you purchased and installed, the QAMs of the last modules are unassigned and appear in red.

To re-assign

1. Select Platform > Licensing > Assign Licenses.
2. The Assign License to QAMs page opens:
   - Click Reconcile License.
   - All licenses are reassigned from the first module, module 1, to the last module, module 9.
### 3.14.1.3 License Summary


<table>
<thead>
<tr>
<th>License Type</th>
<th>Qty</th>
<th>In Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary All Features</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Narrowcast QAM</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>PM Scrambling</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

2. View the following information:

- **License Type** - lists all the available types of licenses:
  - Temporary All License - allows the NSG 9000-6G device to operate with all of its capabilities. Usually this license type is time limited.
  - Narrowcast QAM License - allows to operate the QAM port channels. Usually a module is purchased with a license for two QAM channels per RF port.
  - PM Scrambling License - allows to output TSs via the PM license QAM using Motorola Privacy Mode scrambling technology.
  - DOCSIS QAM - allows to operate the QAM port channels as part of an M-CMTS system.
  - DOCSIS QAM + DTI Sync - allows to operate the QAM port channels as part of an M-CMTS system with DTI sync messages.

- **Qty** - indicates the total number of purchased licenses of that type.
- **In Use** - indicates the number of licenses that were successfully granted.

### 3.14.1.4 Adding a License

1. Select Platform > Licensing > Manage Licenses. The following page appears.
2. To add a license, click Add License. The Add License dialog appears.

3. Enter the license key you received from Harmonic Customer Support.

4. Click Done.

The license is added to the list, the serial and part numbers are generated according to the license key and the license is available. The following details appear in the table:

- **License Description**: provides details about the license.
- **License Part Number**: indicates the part number as generated according to the license key.
- **License Serial Number**: indicates the serial number as generated according to the license key.
- **Qty**: indicates the number of QAM channels included in this license.
- **Expiration Date**: indicates when the license expires.

### 3.14.1.5 Viewing deleted Licenses

**NOTE:** You can delete licenses via the License Manager only.

- To view the deleted licenses, select the Deleted Licenses tab. The table that appears lists the deleted licenses and their details:

<table>
<thead>
<tr>
<th>License Description</th>
<th>Part Number</th>
<th>License SN</th>
<th>Key SN</th>
<th>Qty</th>
<th>Expiration Date</th>
<th>Deletion Receipt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal 14 day</td>
<td>MI6123456</td>
<td>MI6123456</td>
<td>1</td>
<td>2008-08-10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **License Description**: provides details about the license
- **Part Number**: indicates the part number as generated according to the license key.
- **License SN**: indicates the Serial Number of the license
- **Key SN**: indicates the Serial Number of the key
- **Qty**: indicates the number of QAM channels included in this license
- **Expiration Date**: indicates when the license expires
Deletion Receipt - a string you need to record and use when approaching Harmonic Customer Support.

To organize the Available Licenses table
- By default, the first row of the table lists the license entered the latest. To arrange the records in a sequential order, click on any of the column names. An arrow appears to indicate the list order.

### 3.15 Configuring NGOD

When the EdgeQAM is part of an NGOD system architecture, you need to configure the following to allow the QAM-RFs of the EdgeQAM to outflow SDV/VOD sessions:
- Configure and enable an NGOD ER M server as explained below.
- Define the NGOD ERM as the QAM-RF manager of the required QAM-RFs. See 3.12.4 Configuring/Viewing QAM Channels on page 49.

Setting NGOD ERM parameters requires to set general and the ERM parameters.

#### 3.15.1 Configuring NGOD General Parameters

To allow communication with the ERM, the NSG 9000-6G device supports the D6 and R6 NGOD protocols. When communicating using the R6 protocol, NSG is always listening on port 554(RTSP).

1. Select **Platform > NGOD** tab.
2. Focus on the **General** section.
3. In **NGOD Component Name**, enter the component name as defined in the D6 protocol.
4. In **Bandwidth Update Threshold (kbps)**, define the allowed deviation from the current output bit rate of the device (60 to 2000). Whenever the bit rate deviation reaches the value defined in this field, the NSG sends the ERM the updated output bit rate.
5. In **Routing Cost**, enter a value as defined in the D6 protocol (0 to 255).
6. In **R6 RTSP Port**, enter 554 as the port number. When communicating using the R6 protocol NSG is always listening on port 554(RTSP).

#### 3.15.2 Configuring ERM Parameters

1. Select Platform > NGOD tab.
2. Click Add, to add an ERM.
3. In **IP Address**, enter the ERM IP address.
4. In **Port**, enter the ERM TCP port number.
5. In **Version**, select the supported version of the protocol. Version 2 is the default version.
6. In Streaming Zone, enter the streaming zone as defined in the D6 protocol.
7. To enable the NSG-ERM communication, select the Enable ERM box.
8. In Status, view the connection status.
   - Connect indicates that the connection is ok.
   - Idle indicates that there is no connection with the ERM.
9. Check Delete to remove the line when clicking Delete.
10. In ERM Keep Alive view the period of time, in seconds, to indicate the duration between the keepalive messages transmitted by the NSG to the ERM. The default is 30 seconds.
11. In Connection Retry Threshold (sec), enter a period of time in seconds to indicate the duration between retrials to connect to the ERM to send D6 messages.
12. In Hold Time (sec), enter a period of time in seconds to indicate the duration between responses to successive Keep Alive and or UPDATE messages received by the NSG. If the duration time elapses and a response is not received, NSG tries to re-establish the connection with the ERM.

### 3.16 Configuring ISA

The ISA configuration includes the following:
- Defining general parameters
- Defining virtual ISA devices

#### 3.16.1 Defining ISA General Parameters

When the EdgeQAM is part of an ISA SRM system architecture, you need to configure the following parameters to allow the QAM-RFs of the EdgeQAM to outflow SDV/VOD sessions:

1. Select Platform > ISA tab.

2. Define the following parameters:
   - SRM IP Address - enter the IP address of the SRM server
   - Timeout Period (Sec) - enter a period of time in seconds to indicate the duration between the NSG trials to connect to the ISA server.
   - Enable Reset Indication - if selected, an indication is sent to the ISA server (either ERM or SRM). An indication is sent to the ERM/SRM after device reset or once management communication is back in case of communication problems. By default this parameter is off.
   - Enable Announce Message Indication - check to enable the announce message
indication required by the ISA and the RCAS protocols. This message is sent to the SRM due to the following:

- Provisioning a service
- Alarm is raised on the session
- A redundancy switch over the session source
- Session is missing from the output

- Report PMT Section (QuerySessionInfo) - when selected, in QuerySessionInfo, the PMT packet data is sent to the ISA server.
- Out Of Band Mini Carousel - applies to ISA-SDV. Select, in case, the mini carousel is transmitted to the set-top-box out-of-band and not through the video network. When you enable this parameter, the device does not raise the alarm Service Missing for mini carousel sessions.

**NOTE:** The following parameter applies to SDV sessions that are either shell/bind sessions or create sessions with port 0 or a port higher than 8 only.

- SDV Load-Sharing Ports - applies to ISA-SDV sessions. The input port in the provisioning message is not indicated. The edgeQAM attempts to receive the input stream via the input ports indicated in the SDV Load-Sharing Ports box. The default port is GbE port 1. You can configure up to four GbE input ports to handle up to four Gigabytes of SDV traffic. The NSG manages the traffic between the selected input ports. The NSG sends the sessions to the input port for SDV session with less traffic. If SDV ports are equally loaded with traffic, the device sends the traffic to the ports according to the sequential order of the port numbers.

**NOTE:** GbE input port that is selected as an SDV-load sharing port, cannot be a backup port.

**NOTE:** To view the actual input port, select Applications > SDV > ISA Active Sessions.

### 3.16.2 Defining Virtual ISA Units

To enable the ISA server to handle the full capacity of QAM-RFs of the edgQAM, use the virtual IPs for ISA feature. This feature creates virtual IPs only for the use of the ISA server. To create virtual ISA IPs, do the following:

- Create virtual IPs for ISA - requires to define:
  - Eth1 Virtual IPs - You can add virtual IPs to ET1 only. You can add up to 10 Eth1 virtual IPs. Eth1 virtual IPs should be on a subnet other than Eth2 subnet.
  - GbE Virtual IPs - You can add GbE virtual IPs to any of the active GbE ports. You can add up to 10 GbE virtual IPs. The physical GbE port is automatically added as one of the available virtual port IPs and you cannot remove it.

- Associate virtual devices with ISA

#### 3.16.2.1 Creating Virtual IPs for ISA

- To create Eth1 virtual IP
  1. Open the web client of the device.
  2. Select the Platform tab.
4. In Eth1 Properties, select the Virtual IPs (ISA) tab.

5. Click Add Virtual IP.

6. In the table enter the following:
   - Eth1 Virtual IP - enter the required Eth1 virtual IP. Virtual IP should be different than the physical Eth1 IP address and on a subnet other than Eth2.
   - IP Mask - enter a subnet mask.

7. In Status, view the status of the Eth1 virtual IP:
   - In Use - the virtual IP is currently in use
   - No in Use - the virtual IP is currently not in use

To create virtual GbE IP

1. Open the web client of the device.
2. Select the Platform tab.
3. In Back Panel View, select the required GbE port.
4. In GbE Properties, select the ISA Virtual IPs tab.

5. Click Add Virtual IP.

6. In the table, enter the following:
   - GbE Virtual IP - enter the GbE virtual IP.
   - Mask - enter the required IP mask.
   - Management IP - to associate between the GbE virtual IP and an Eth1 virtual IP, view the Eth1 virtual IP.
   - Delete - select to delete the virtual IP once you click Delete Selected.

**NOTE:** The GbE virtual IP following the primary virtual GbE IP supports autodetection.

### 3.16.3 Associating a Virtual Device with ISA

Once you defined the virtual ISA IPs, you may associate them with the QAM-RFs as explained below:

- To associate a virtual device with ISA
  1. Open the web client of the device.
  2. Select the Platform > ISA tab.
3. Click Add Virtual Device.

4. Once you click in the Eth1 Virtual IP field, it is propagated with the Eth1 virtual IPs you defined in 3.16.2.1 Creating Virtual IPs for ISA on page 64.

5. Select the required management IP.

6. Once you click in the GbE Port: Virtual IP field, it is propagated with the available GbE virtual IPs (see 3.16.2.1 Creating Virtual IPs for ISA on page 64). The GBE interface appears in the following format:
   
   \(<x>:<virtual GbE IP>\), where x is the physical GbE port of the edgeQAM, an integer between 1-8. Select the required GbE interface.

7. In Virtual Input Port enter the required port according to the ISA provisioning.

8. To view the QAM channel to output the content, click the ... in QAM Mapping. The following dialog appears:

9. To delete an ISA related virtual device, click Select and then Delete Selected.
3.17 EdgeCluster

3.17.1 EdgeCluster Overview

NSG 9000-6G version 2.7 and up supports an improved EdgeCluster technology. This technology offers high availability obtained by 1:1 device redundancy for broadcast and M-CMTS deployments. The following description and instructions refer to version 2.7 and up only. Customers with edgeCluster below version 2.7, should call customer support for instructions.

The edgeCluster system is organized as follows:

The edgeCluster is comprised of two devices defined as primary and backup. Typically the primary device is active and the backup device is in standby mode. Both devices are configured the same except for the management ports. Both devices are provisioned with sessions that are transmitted by the primary/active device. The backup device stands by ready to become active upon primary failure. Both devices, the primary and the backup communicate with each other via their Eth1 and Eth2 ports:

- Eth1 - management port connection. See NSG 9000-6G Hardware and Installation User Guide. Each device is configured with a unique management port, IP address of Eth1.
- Eth2 - Each device is configured with a unique IP address of Eth2. The subnet of Eth2 ports should be different than the subnet of Eth1 ports. Eth2 ports are connected with an Ethernet crossover cable.

The edgeCluster system described above applies to both M-CMTS and Broadcast deployments with the following differences:

<table>
<thead>
<tr>
<th>Item</th>
<th>Deployment</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>M-CMTS</td>
<td>No use of GbE switch. The downstream GbE port of the GbE source is directly connected to the NSG GbE input ports.</td>
</tr>
</tbody>
</table>
3.17.1.1 Triggering Event for Redundancy Switch

The trigger for a redundancy switch can be one of the following:

- A triggering alarm is raised on the active device. To view the list of the default triggering alarms and to define triggering alarms, see 6.3.5 Setting Alarm Parameters on page 123.

  **NOTE:** Only Advanced users may re-define the triggering alarms.

- A manual redundancy switch, when Redundancy mode is Manual. See 3.17.2 Configuring EdgeCluster on page 69.

- The standby device does not receive heartbeat messages for a pre-defined period of time due to a re-boot failure of the active device.

3.17.1.2 Redundancy Switch Scenario

Both devices constantly send and listen for heartbeat messages. Once a triggering event takes place on the primary/active device, the following takes place:

- The primary/active device closes its QAM-RF ports and reflects its new status to its peer device via a heartbeat message.

- The standby/backup device becomes active, opens its QAM-RF ports and starts transmitting the content.

  **NOTE:** In case of a reboot failure of the active device, once it is back and running, it runs in Standalone mode.

3.17.2 Configuring EdgeCluster

**NOTE:** MCT is the main tool for configuring and controlling devices working in edgeCluster mode. The following descriptions and instructions refer to the web client of the device. To work with MCT, see MCT 11.1 Software Guide.

---

### Table 3-14: EdgeCluster M-CMTS Versus Broadcast

<table>
<thead>
<tr>
<th>Item</th>
<th>Deployment</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>GbE Input Ports</td>
<td>Broadcast</td>
<td>The GbE input ports of both NSG devices must be configured the same. However, each device should have a unique IP address of the input port.</td>
</tr>
<tr>
<td></td>
<td>M-CMTS</td>
<td>The GbE input ports of both NSG devices must be configured the same including the IP addresses of the GbE input ports. Note: For proper edgeCluster operation, GbE ports of the primary and backup devices should have fiber SFPs.</td>
</tr>
<tr>
<td>Redundancy Switch</td>
<td>M-CMTS</td>
<td>Upon redundancy switch, the active device momentarily shuts up its GbE ports to signal the source device that the device is faulty.</td>
</tr>
</tbody>
</table>
Configuring and monitoring the EdgeCluster feature is done via the Platform > Chassis > EdgeCluster tab.

**Chassis & Main Board Properties**

<table>
<thead>
<tr>
<th>General</th>
<th>Global IP &amp; QAMs</th>
<th>SNMP &amp; Syslog</th>
<th>Time</th>
<th>Routing Table</th>
<th>Security</th>
<th>Authentication</th>
<th>Port Redundancy</th>
<th>EdgeCluster</th>
</tr>
</thead>
</table>

**Configuring Platform Parameters**

![Diagram showing EdgeCluster settings](image)

The EdgeCluster tab includes the following options:

**Redundancy Mode** - Allows to select the required redundancy mode:
- Disabled - The device operates in a standalone mode
- Automatic - A redundancy switch automatically takes place upon a triggering event. See 3.17.1.1 Triggering Event for Redundancy Switch on page 69.
- Manual - A redundancy switch is initiated by the user

**Application** - allows to select the required edgeCluster deployment:
- Broadcast
- M-CMTS

**ETH1 Peer IP** - Allows to configure the IP address of Eth1 of the peer device.

**ETH2 Peer IP** - Allows to configure the IP address of Eth2 of the peer device.

**Device Role** - Allows to configure whether primary or backup.

**Device State** - Read only. View the current state of the device, whether active or standby.

**Peer State** - Read only. View the current state of the peer device, whether active of standby.

**Set to Active** - Enabled when device is part of an edgeCluster and the state of the device is standby or failed.

**Set to Standby** - enabled when device is part of an edgeCluster configuration and the device is currently active
To configure EdgeCluster

To configure EdgeCluster, perform the following instructions in their sequential order. Failing to perform the instructions according to their order may adversely affect the EdgeCluster capability.

**NOTE:** The provided instructions assume that you have two devices working with firmware version 2.7 and higher and you would like to work in edgeCluster mode.

**NOTE:** The provided instructions assume that a primary is in Active state and backup is in Standby device.

### Table 3-15: Applying and Configuring EdgeCluster

<table>
<thead>
<tr>
<th>Primary</th>
<th>Backup</th>
</tr>
</thead>
</table>
| 1. Configure the device to be fully operational. Configure the following: QAM-RF ports, input GbE ports, services and edgeCluster parameters. | |}

2. Export the configuration. See [3.1.1.2 Exporting and Importing Configuration on page 22.](#)

3. Open the web client of the device. See [2.2.1 Logging Into the Device via IE on page 15.](#)

4. Select Platform tab > Chassis component > EdgeCluster tab.

5. Configure the EdgeCluster parameters. See [3.1.2 Configuring EdgeCluster on page 69.](#)

6. Click Apply.

7. Verify that Primary Active appears in the title bar of the device.

8. Open the web client of the device. See [2.2.1 Logging Into the Device via IE on page 15.](#)

9. Import the configuration you have exported from the designated peer device. See [3.1.1.2 Exporting and Importing Configuration on page 22.](#)

10. Select Platform tab > Chassis component > EdgeCluster tab.

11. Configure the EdgeCluster parameters. See [3.1.2 Configuring EdgeCluster on page 69.](#)

12. Click Apply.
Once you set the EdgeCluster configuration, various indications appear at the title bar of the web client (for an example, see the following picture) and on the front panel LCD display. The indications reflect the status of the device in the EdgeCluster topology as the following table shows:

### Table 3–16:

<table>
<thead>
<tr>
<th>Device Status</th>
<th>Title Bar</th>
<th>Front Panel LCD</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>■ Primary Active</td>
<td>■ PA</td>
<td>■ Primary is active</td>
</tr>
<tr>
<td></td>
<td>■ Primary Failed</td>
<td>■ PF</td>
<td>■ Upon redundancy switch.</td>
</tr>
<tr>
<td>Backup</td>
<td>■ Backup Active</td>
<td>■ BA</td>
<td>■ Upon a redundancy switch</td>
</tr>
<tr>
<td></td>
<td>■ Backup Failed</td>
<td>■ BF</td>
<td>■ Upon manual revert or failure</td>
</tr>
<tr>
<td></td>
<td>■ Backup Standby</td>
<td>■ BS</td>
<td>■ Backup is in standby mode</td>
</tr>
<tr>
<td>Primary/Backup</td>
<td>RF Disabled</td>
<td>D</td>
<td>The QAM RF ports are disabled. See 3.12.1.3 Closing/Opening all RF Ports on page 45.</td>
</tr>
</tbody>
</table>

#### 3.17.3 EdgeCluster Maintenance

##### 3.17.3.1 EdgeCluster and Firmware Upgrade

When you wish to upgrade the firmware of NSG 9000-6G devices working in EdgeCluster mode, perform the following steps in their provided order:

The provided instructions refer to upgrade from firmware version 2.7.0.0 and above. For upgrade of older versions while devices are in edgeCluster mode, call customer support.

⇒ To upgrade the firmware of the MSG 9000 device in EdgeCluster Mode

**NOTE:** During this procedure you are instructed to upgrade the firmware of the Backup device first.
### 3.17.3.2 Replacing a Faulty Module in EdgeCluster Mode

The following instructions refer to devices that work in edgeCluster mode and you need to replace a faulty QAM-RF module or power supply.

1. Verify that the device with the faulty module is in Standby state.
2. Replace faulty module. See *NSG9000-6G Hardware and Installation Guide*.
3. Verify that the device is working properly.
4. Apply EdgeCluster mode.

---

**Table 3-17: EdgeCluster Firmware Upgrade**

<table>
<thead>
<tr>
<th>Primary Device</th>
<th>Backup Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Verify that both devices are working properly.</td>
<td>2. Upgrade the firmware as instructed on page 24.</td>
</tr>
<tr>
<td></td>
<td>3. Verify that the device is running properly with the newly installed firmware and apply the required configuration to the device. Note: The backup device is currently working with the new firmware.</td>
</tr>
<tr>
<td></td>
<td>4. In the web client of the backup device only, select <strong>Platform &gt; Chassis &gt; EdgeCluster</strong> tab.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Set to Active</strong>. Services are flowing through the backup device.</td>
</tr>
<tr>
<td></td>
<td>6. Upgrade the firmware as instructed on page 24.</td>
</tr>
<tr>
<td></td>
<td>7. Verify that the device is running properly with the newly installed firmware</td>
</tr>
<tr>
<td></td>
<td>8. In the web client of the primary device, select <strong>Platform &gt; Chassis &gt; EdgeCluster</strong> tab.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Set to Active</strong>. Note: Services are flowing through the primary device.</td>
</tr>
</tbody>
</table>
Chapter 4
Configuring Applications

4.1 Applications Overview

NSG 9000-6G operates in the following applications:

VOD Application - The system serves as a highly integrated digital video gateway, capable of multiplexing on-demand content streamed over an IP network.

Broadcast Applications - The system serves as a digital video gateway that passes through streams. In addition it can broadcast remuxed services and PIDs.

SDV Application - The device streams out SDV sessions provisioned by the NGOD ERM or ISA.

M-CMTS Application - NSG 9000-6G supports wideband M-CMTS data PIDs. As part of the M-CMTS system, NSG 9000-6G processes down streams and improves downstream data rates by significantly reducing costs.

D2E Application - NSG 9000-6G supports Multicast IP down streams encapsulated as DOCSIS 3.0 with DBC requests (when required) on dedicated frequencies (D2E server frequencies).

CAS - This version supports Privacy Mode scrambling only.

NOTE: When provisioning static sessions through the web client or MCT, NSG 9000-6G may carry up to 500 sessions only. When dynamic sessions are provisioned through NGOD ERM, ISA SRM or VOD SRM, NSG 9000-6G may carry up to 3,000 dynamic SDV/VOD sessions.

4.2 VOD Application

The VOD application includes two tabs:

- Settings - allows you to set the following:
  - General parameters - session inactivity time
  - MPEG related parameters
  - Emulation mode

- QAMs - a read only page to view QAMs settings

4.2.1 Defining Session Inactivity Time

Define the allowed duration for session inactivity before the session is removed from the output.
1. Select Applications > VOD > Settings tab.

2. In Session Inactivity Teardown Threshold (Sec), enter the allowed period of time in seconds for session inactivity. In case the interval is longer than the indicated time, the session is removed from the output port.

3. By default Allow Auto Detection is selected. Verify that this option is selected to allow auto detection, in the input, of the output QAM according to the indicated UDP port.

### 4.2.2 Defining MPEG Parameters

#### 4.2.2.1 PID Remapping

The PID Remapping option allows you to remap according to a specific paradigm or randomly. In either case, the NSG prevents the assignment of conflicting PIDs.

- **Paradigm** - The elementary stream PIDs are determined according to the ATSC A/53 standard, which defines the PID remapping rules that are listed in the table below:

<table>
<thead>
<tr>
<th>Formula</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ID = 0xN</td>
<td>Service ID = 0x34</td>
</tr>
<tr>
<td>PMT PID = LeftShift (N) = 0xN0</td>
<td>PMT PID = 0x340</td>
</tr>
<tr>
<td>PCR=Video=PMT+1= 0xN1</td>
<td>Video = 0x341</td>
</tr>
<tr>
<td>Audio 1&amp;2 = PMT+ 4/5 = 0xN 4,0xN5</td>
<td>Audio 1&amp;2= 0x344, 0x345</td>
</tr>
<tr>
<td>ECM=PMT+9= 0xN9</td>
<td>ECM PID= 0x349</td>
</tr>
</tbody>
</table>

**NOTE:** The Paradigm mode is not suitable for processing services with service IDs greater than 510. If you are using service ID that are greater than 510 you must use the Random mode.

- **Random** - The NSG remaps incoming PIDs to PID numbers that are randomly selected from a predefined range. Define the range in the PID Range field. The PID range is written in hex-decimal format. Range of acceptable values is 0x21 to 0x1FF0.

Changing the PID remapping mode may interrupt the streams currently flowing through the device. It is recommended to change the remapping mode only when no active streams are flowing through the device.

In addition, changing the PID remapping may affect the operation of some STB (Set-up Boxes.) Various STBs operate better with a specific mode. If you suspect such a case, call the STB vendor before changing the PID remapping.
NOTE: Do not change the default settings unless it is necessary. Changing the parameters may cause serious problems with elementary stream transmission.

NOTE: Changing the PID Remapping mode is global. It applies to the platform and to both VOD and SDV sessions.

To change PID remapping
1. Select Applications > VOD > Settings:

2. By default the remapping method is Paradigm. To change the remapping method, select Random. The PID Range (Per TS) option is enabled.

3. In PID Range (Per TS), define the PID range (in hex-decimal format) that the NSG will use for random PID assignment. The range of acceptable values is 0x21 to 0x1FF0.

NOTE: Changes take affect after device reset only.

4.2.2.2 Pro:Idiom PID Remapping

Pro:Idiom is an encryption system used in various cases, typically for hospitality video broadcast systems. The NSG is capable of processing and streaming Pro:Idiom pre-encrypted content. This entails:

- Passing the Pro:Idiom ECM PID, and remapping it to an appropriate PID number
- Passing a special Pro:Idion descriptor, with descriptor tag 0xAD (173 decimal)

When streaming Pro:Idiom content, the NSG remaps Pro:Idiom PIDs to a user-configurable range of PIDs. To set the range of Pro:Idiom PID numbers, do the following:

- In Pro:Idiom Base PID - enter the base PID to start the range for Pro:Idiom PIDs. The default base PID is 0x1050.

4.2.2.3 Setting PAT/PMT Intervals

1. In PMT Interval, define the interval in milliseconds at which PMT packets are sent over the NSG's output transport streams.

2. In PAT Interval, define the interval in milliseconds at which PAT packets are sent over the NSG's output transport streams.
3. Select Update PMT Version to update the PMT version. This version is incremented every time the PMT’s data is changed (e.g. the Video PID changes).

4.2.2.4 Creating and Setting SAT

Service Area Table (SAT) is a none standard table created to meet special needs of customers. SAT is like the SDT (Service Description Table) defined by the DVB standard. SAT uses the Serving Area parameter. To create SAT, the Serving Area value should contain up to 16 bits (range of 1-65535). For serving area configuration, see Configuring/Viewing QAM Channels on page 49.

1. Select Create SAT (Service Area Table), to create SAT at the output. Once Create SAT is selected, the following parameters are enabled:
   - Original Network ID
   - Serving Area Location in SAT

2. If Create SAT is selected, define the original network ID.

3. If Create SAT is selected, open the Serving Area Location in SAT list and select one of the following:
   - TS ID - the serving area is written to the TS ID.
   - First Service Name - the serving area is written to the first service name
   - Both - the serving area is written to both the TS ID and the first service name.

4.2.3 Defining Emulation/QAM Mapping Mode

By default the QAM Mapping Mode is set to Normal. However, the NSG 9000-6G device may emulate the operation of other NSG 9000-3G devices which require a different mapping of the QAMs. When emulating an NSG 9000-3G, NSG 9000-6G routes the UDP range to a QAM. For example UDP 0x501 is routed to QAM=1.2.1, Service ID=1

Each Emulation Mode is defined by an XML file. Once you select an emulation mode, NSG 9000 loads the required emulation mode XML file.

You can customize up to four QAM Mapping modes and export them to an XML file and when required you can import them to the device.

⇒ To define the QAM mapping mode
1. Select Applications > VOD > Settings tab.

2. Open the Emulation Template list to select the required emulation Template.

   **NOTE:** Changing the emulation template, requires an immediate device reset.

3. To export one of the defined custom QAM Mapping modes, see Exporting Customized QAM Mapping Mode File on page 78.

4. To import a customized QAM Mapping mode, see Importing Customized QAM Mapping Mode File on page 78.

### 4.2.3.1 Exporting Customized QAM Mapping Mode File

1. Select Applications > VOD > Settings.
2. Click Export Custom File.
3. Click either Open or Save the file of the selected QAM Mapping mode.
   - If you select Open, the file opens and you can view it.
   - If you select Save, a Save As dialog opens and you may browse to the required location of the file.

### 4.2.3.2 Importing Customized QAM Mapping Mode File

1. Select Applications > VOD > Settings.
2. Click Import Custom File.
   - The following dialog appears:

   ![Import Emulation Template File To Device dialog](image)

   3. Click Browse to locate the required QAM Mapping mode template.
   4. Open the Override Template list and select which template to override.
5. Click Import.

### 4.2.4 Viewing VOD QAMs

The QAMs tab allows you to view the settings of all the QAMs configured to stream out VOD sessions. These QAMs are managed by the following QAM managers:

- VOD SRM
- NGOD ERM
- ISA SRM

To view VOD QAMs

1. Select Applications > VOD > QAMs.

#### QAM Manager - lists the defined QAM manager for this application. In VOD application, the defined QAM manager can be VOD SRM, NGOD ERM, or ISA SRM. See Configuring/Viewing QAM Channels on page 49.

#### GbE Port - the GbE port routed to this QAM-RF port. The value of this attribute depends on the defined QAM mapping mode. See Defining Emulation/QAM Mapping Mode on page 77.

#### GbE IP Address - the GbE IP address port that is routed to the QAM-RF port.

#### UDP Port Range - the UDP port range that is routed to the QAM-RF.

#### RF Output - see Configuring/Viewing QAM Channels on page 49.

#### QAM Index - An index number to identify each QAM channel within the 144 available QAM-RF channels of the device. This tab displays the available QAM channels as per the number of QAMs Per Port value.

#### QAM Reference No. - (Read Only). This parameter indicates the QAM number of the emulated device. This field appears when the device QAM Mapping mode is NSG 8108 bitmap or encoded and NSG 9116 bitmap or encoded.

#### TS ID - see Configuring/Viewing QAM Channels on page 49.

#### NGOD Group Name - see Configuring/Viewing QAM Channels on page 49.
Chapter 4 Configuring Applications

Broadcast Application

4.3 Broadcast Application

In Broadcast application mode, NSG 9000-6G allows to manually route various content elements to any output QAM channel. NSG 9000-6G allows to create the following types of sessions:

- PID Range - to pass a specific range of PIDs from an input stream to the output while remapping the PIDs. To route a complete input MPTSs, route the maximum MPEG range 0x0 - 0x1FFE, which is the default option.
- Service Remux - to route specific MPEG services (programs) using the Service Remux tab
- PID Remux - to route individual PIDs using the PID Remux tab

4.3.1 Provisioning PID Range Sessions

The PID Range option allows to break down the input stream into ranges and to multiplex them via various outputs while remapping the PIDs. To output a socket without any changes, that is without remapping and without generating tables, use the default PID range 0x0 - 0x1FFE. The following table lists the PID range specifications:

Table 4-1: PID Range Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID range per input session</td>
<td>Up to 144</td>
</tr>
<tr>
<td>PID range per output</td>
<td>Up to 15</td>
</tr>
<tr>
<td>Backup of Input source</td>
<td>Up to 2 backup sources for each input source. Each backup shares the same range configuration</td>
</tr>
</tbody>
</table>

Defining a PID Range sessions, includes the following stages:

- Defining PID ranges of the input stream
- Associating the PID ranges with output QAMs

4.3.1.1 Defining PID Ranges Sessions

To configure a PID range session
NOTE: A session is defined as PID Range during QAM configuration. (See Configuring/Viewing QAM Channels on page 49). The following procedure guides you on how to define the PID Range session.

1. Select Applications > Broadcast > PID Range > Input.

   ![PID Range Table]

2. Define the following parameters:
   - Session ID: Read only. A sequential number to indicate the number of the session in the current page.
   - Type: Define whether the session is a Primary or Backup session.
   - Enable Backup: See PID Range Socket Redundancy on page 83.
   - Active: By default, the primary input socket is the active one. Once you enable a backup socket, check this option to activate the required socket. To view the currently active socket, click Refresh.
   - Multicast: Select to enable multicast. If selected, the IP Address box is cleared.
   - GbE Port: Open the list and select the required input port. Once you define the required GbE port, the IP Address field is updated to display the IP address of the selected port.
   - In IP Address, enter the IP address of the NSG input GbE port, or a multicast address.
   - In UDP Port, enter the UDP port of the input GbE port.
   - In Source IP, enter the IP address of the upstream device that streams the content to the defined GbE port and socket.
   - In Source Name, enter the name of the upstream device that streams the content to the defined GbE port and socket. The name should be unique.

3. To define a PID range, in PID Range, click the Add button.
The following dialog appears:

![PID Range List](image)

- Click **Add Range** and define the PID range by entering the required PID range start and end. Once you enter the required PIDs in hexadecimal, you can view their values also in decimal.
- To exclude the NIT, STD and/or EIT PIDs, select the required one. Once the PID is selected, this PID is not included in the selected PID range.
- Click **Done** to close the dialog and to save the configuration.

4. To view the associated output QAMs, click in **Output QAMs**, the [ ].

   The following dialog appears:

![Output QAMs List](image)

- View the list of associated QAMs for the input at stake. The list includes QAM-RFs with Broadcast QAM Manager. (see page 49).
- In **Status view** the status of the input socket:
  - **Active** - the input source is active
  - **Inactive** - input session is not streamed into the device
4.3.1.2 PID Range Socket Redundancy

An input socket may have up to two backup input sockets. By default, the first input socket is the primary socket.

Default primary Input socket

Backup input sockets

If the primary socket fails, either of the following may take place:

- **Primary socket fails and no traffic is detected on the port** - port redundancy switch will take place. If still no traffic is detected on the socket, a socket redundancy takes place, moving to the following backup socket of the active port. (See Configuring Input GbE Port Redundancy on page 37.)

- **Primary socket fails and traffic is detected on the port** - automatically the following configured socket is activated. If the active input socket is the last one in the list and it fails, a redundancy switch is performed to return to the Primary. The cycle stops at the primary, if there is no traffic on any of the sources. The redundancy mechanism, re-checks the last active source for a momentary failure. If it is still faulty, the redundancy switch reverts to the primary and keeps checking in increased intervals the configured sources, until detecting an active source.

To configure a backup socket

1. Click the Expand all link.
2. Click Add Session.
3. Configure the required parameters of the newly added session as explained in To configure a PID range session on page 80.

To select the active input socket

By default, the first input socket in the list is the active socket. However, you can define any of the configured input sockets to be active if it receives traffic.

1. To view the currently active input socket, click the Refresh link.
2. Click the Expand all link  Expand All  .

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Session</td>
<td>Delete Selected</td>
</tr>
<tr>
<td>Refresh</td>
<td>Expand All</td>
</tr>
</tbody>
</table>

Active buttons to set the active input socket

3. To select another input socket as active, click the required Active button.

### 4.3.1.3 Associating Input Sessions With Output QAMs

1. Select Applications > Broadcast > PID Range > Output.

2. View the following parameters:
   - RF Output - Read only. This column is populated with all of the QAM-RFs with Broadcast QAM Manager. (see page 49). The RF port is indicated in the following format: X,Y,Z (T) where:
     - X – module number (1…9)
     - Y – RF port number (1…2)
     - Z – channel number (1…8/6-Annex A)
     - T – QAM index number (1…144)
   - QAM Frequency - Read only. indicates the output frequency

3. To select the input port, in Source Name open the list and select the input GbE port over which the stream flowed into the NSG device.

4. To select ranges, in Ranges open the list and select the required ranges to outflow over this QAM-RF. The list is populated with all of the ranges defined for this input port.

5. To remap, enter in PID Remap Start the required PID. The PID Remap End is updated automatically.

6. To add another range, click . You can add up to 5 PID ranges per output QAM.

### 4.3.1.4 Removing an Output Configuration

You can remove an input PID Range session only when it is not associated with an output. To de-associate an input from an output, do the following:

1. Select Applications > Broadcast > PID Range > Output.
2. In Selected, check the required output.

3. Click Clear Configuration. The selected output is removed from the table.

4.3.2 Provisioning Service Remux Sessions

You can route a service from any input to any output. You can select whether to:

- Output the service with its input ID or to remap it.
- Remap the service PIDs.

When provisioning static sessions through the web client or MCT, session ID starts at 10,000 and you can configure up to 500 sessions only.

**NOTE:** You cannot remux PIDs of remuxed services.

To route a service

1. Select Applications > Broadcast > Service Remux tab:

   ![Diagram of session table with options to add, duplicate, and delete sessions]

   - Click to add a session to route a service
   - Click Duplicate, to add a session with definitions exactly as the selected session
   - Click Duplicate Range, to add sessions according to the defined range

   ![Session table with columns for Session ID, Multicast, GbE Port, IP Address, UDP Port, Source IP, RF Output, Service ID, No PID Remapping, and Select]

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Multicast</th>
<th>GbE Port</th>
<th>IP Address</th>
<th>UDP Port</th>
<th>Source IP</th>
<th>RF Output</th>
<th>Service ID</th>
<th>No PID Remapping</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
<td></td>
<td></td>
<td>192.168.9.4</td>
<td></td>
<td>3.6.8.0</td>
<td>2.1.2(1)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Click Add Session. A row is added to the table with a session ID.

   Session ID- Read only. A sequential number starting at 10000, to indicate the number of the session in the current page.

3. To define the input socket, do the following:

   - Select Multicast, if required. If selected, the IP address is removed from the IP Address box.
   - Select the input GbE Port. Open the GbE Port list to select the required input port.
Once you define the required GbE port, the IP Address field is updated to display the IP address of the selected port, unless Multicast is selected.

- In IP Address, enter the required unicast/multicast IP address of the input port. By default, the IP address of the selected port appears, unless multicast is selected.
- In UDP Port, indicate the UDP port.
- In Source IP, view the IP address of the upstream device that streams the content to the defined GbE port and socket.

4. To define the output QAM, enter in RF Output the required QAM-RF channel in the following format: X.Y.Z (T) where:
   - X – module number (1…9)
   - Y – RF port number (1…2)
   - Z – channel number (1…8/6Annex A)
   - T – QAM index number (1…144)

5. In Service ID enter the required output service ID. You can output the service with the same input ID number or to remap the service.

6. To output a service without remapping its PIDs, select No PID Remap.

**NOTE:** If you disable PID remapping, verify there is no PID conflict in the output.

To route a service using the Duplicate button

Once you defined a service and need to route another service with similar configuration, do the following:

1. In Service Remux page, check the Select box of the required service/session.
2. Click Duplicate.
   - The selected row is duplicated and appears as the last row in the table.
3. Define the required parameters as explained in **To route a service** on page 85.

To route a service to a few output ports

1. In Service Remux page, check the Select box of the required service.
2. Click Duplicate Range.
   - The following page appears:

   ![Duplicate Range -- Webpage Dialog](http://10.40.13.246/Internet)

3. To define the range of the output QAM (logical port number), enter in From QAM and To QAM a number between 1-144 to indicate the beginning and the end of the range, respectively.
4. Click Done.

☞ To delete a remuxed service
1. In Service Remux page, check the Select box of the required service.
2. Click Delete Selected.

4.3.3 Provisioning PID Remux Sessions

You can route a PID from any input to any output. You can route up to 8 PIDs to an output, or configure up to 1152 PID sessions. You can select whether to add a PMT reference to the PID.

You can route an input PID to a few outputs and remap a PID to output it over different outputs. However, you cannot route a PID to the same output with different remapped PIDs.

The PID 0x10 is reserved for the Network Information Table (NIT). If you remux a PID and remap it to PID 0x10, the PAT points to it as a NIT table PID. NSG 9000-6G ignores any of the PID 0x10 configuration such as PMT reference and added descriptor.

☞ To route a PID
1. Select Applications > Broadcast > PID Remux.

2. Click Add Session.
   A row is added to the table with a session ID.

   Session ID- Read only. A sequential number to indicate the number of the session in the current page.

3. To define the input socket, do the following:
   - Select Multicast box if required. If selected the IP Address box is cleared.
   - To select the input GbE Port, open the GbE Port list and select the required port. Once you define the required GbE port, the IP Address field is updated to display the IP address of the selected port, unless Multicast is selected.
   - In IP Address, enter the required unicast/multicast IP address of the input port. By default, the IP address of the selected port appears, unless multicast is selected.
   - In UDP Port, indicate the UDP port.
   - In Source IP, enter the IP address of the upstream device that streams the content to the defined GbE port and socket.

4. To define the required PID, in Input PID, enter in hexadecimal the required input PID number.

5. To define the output to stream out the configured PID, enter, in RF Output, the required output QAM in the following format: X,Y,Z (T) where:
   X – module number (1…9)
Y – RF port number (1…2)
Z – channel number (1…8/6-Annex A)
T – QAM index number (1…144)

6. In Output PID enter the output PID number in hexadecimal. You can output the PID with the same input PID number or to remap the PID.
7. To allow PMT reference, select the PMT Ref box. The ES Type field is enabled.
8. If you selected the PMT Reference box, enter the ES Type to stream out the PID. This is the ES type that the PMT table points to. See, Standard ES Types and Descriptors on page 146.
9. To add a descriptor, click Descriptor...
The Descriptor List page opens.
10. Click Add Descriptor.

11. In Descriptor Type and Descriptor Value, enter the required parameters as defined by the MPEG standard.
12. To close the dialog and save configuration, click Done.

To route a PID using the Duplicate button

Once you defined a PID and need to route another PID with similar configuration, do the following:
1. In PID Remux page, check the Select box of the required PID.
2. Click Duplicate.
The selected row is duplicated and appears as the last row in the table.
3. Define the required parameters as explained in To route a PID on page 87.

To route a PID to a few output ports
1. In PID Remux, check the Select box of the required PID.
2. Click Duplicate Range.
The following dialog appears:

```
3. To define the range of the output QAM (logical port number), enter in From QAM and To QAM a number between 1-144 to indicate the beginning and the end of the range, respectively.
4. To close the dialog and to apply the required range, click Done.
5. Define the required parameters as explained in To route a PID on page 87.
```

4.3.4 Provisioning PSIP Tables

Program and System Information Protocol (PSIP) is used for transmitting service meta-data in ATSC networks. Typically, PSIP applies only to North-American cable systems. This meta-data relates to each channel in the broadcast MPEG transport stream of a TV station. It is also used for publishing information about television programs so that viewers can select what to watch by title and description.

NSG9000-6G supports the generation of the following PSIP tables:

- **MGT - Master Guide Table.** It defines the type, packet identifiers, and versions for all of the other PSIP tables included in this TS except for the System Time Table (STT)
- **CVCT - Cable Virtual Channel Table.** Assigns numbers to each virtual channel and enables EITs to be associated with the channel.

The generated MGT and CVCT tables comply with the ATSC A-65-A specification. Both tables are streamed over PID 0x1FFB. You can configure up to 20 entries for generating a PSIP table for the QAM. Exceeding services routed to the QAM assumes the default values, as explained in Service ID.

**NOTE:** PSIP tables are generated only once you have enabled PSIP generation in the QAM tab. See Configuring/Viewing QAM Channels on page 49.

To provision PSIP per TS
1. Select Applications > Broadcast > PSIP.

2. To select the required QAM/TS, open the Module list, Port list and QAM list and select the required module, port and QAM, respectively. Once you have indicated the required module, port and QAM, a table appears in the PSIP page.

3. To add a blank row to the table, click Add Entry. To delete an entry, click Delete Entry.

4. View/configure the following parameters required for PSIP generation:
   - # - view the sequential number of the table entry.
   - Name - enter the name of the program/service to appear in the PSIP table. The default service name is Ch 1.
   - Major - indicates a major broadcast group. Enter a number in the range of 0-1023.
   - Minor - enter a number in the range of 0-1023.
   - Service ID - enter the ID of the service routed to the QAM. In case PSIP is enabled for the QAM and the routed service is not indicated in the PSIP tables, the following values appear in the table:
     - Name - CHxxxx, where xxxx indicate the service ID.
     - Major - assumes the TS ID
     - Minor - default value is service ID

4.4 SDV Application

The SDV application includes the following tabs:
- Settings - allows you to set the following:
  - SDV redundancy
  - MPEG related parameters
- QAMs - a read only page to view QAMs settings
- NGOD Active Sessions - lists all the provisioned NGOD sessions.
- ISA Active Sessions - lists all the provisioned ISA sessions.
4.4.1 SDV Settings

4.4.1.1 NGOD Redundancy

NSG 9000-6G supports the RTSP protocol with various redundancy modes. Select one of the following redundancy modes:

Hot/Warm - the default option. The service has only one redundant service. NSG 9000-6G JOINs the primary service, and upon failure, JOINs the backup multicast group. As a result, the backup service is streamed from the switch to the input port of the device.

Hot/Hot - the service has one redundant service. NSG 9000-6G JOINs both the primary and backup multicast groups and both groups are steamed to the device. Upon failure, the backup service is provisioned to the device resulting in a short fail-over time.

Hot/Warm/Warm - the service has at least two redundant services. NSG 9000-6G JOINs the primary multicast group. Upon failure NSG 9000-6G JOINs the first backup service and as a result the backup service is streamed into the device. If this trial fails, NSG 9000-6G JOINs the second backup multicast group.

Hot/Hot/Hot - the service has at least two redundant services. NSG 9000-6G JOINs all three multicast groups. All three services are streamed to the input port to allow short fail-over time.

4.4.1.2 ISA Redundancy

Service redundancy - activated once the device does not detect the service at the input port. Service redundancy is supported in one of the methods described in NGOD Redundancy.

The Allow Shared Backup Source option allows a single service/socket to backup more than one primary sockets. Once this option is selected, the redundancy switch may take up to four seconds.

To define SDV socket redundancy mode

1. Select Applications > SDV > Settings.

2. To set the redundancy mode, do either of the following:
   - To set the NGOD redundancy mode, open the NGOD Redundancy Mode list and select one of the modes listed in the Table 4-2: SDV Redundancy Modes table.
   - To set the ISA redundancy mode, open the ISA Redundancy Mode list and select one
of the modes listed in the Table 4-2: SDV Redundancy Modes table.

### Table 4-2: SDV Redundancy Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hot/Warm</td>
<td>The default option. The service has only one redundant service. NSG 9000-6G JOINs the primary service, and upon failure, JOINs the backup multicast group. As a result, the backup service is streamed from the switch to the input port of the device.</td>
</tr>
<tr>
<td>Hot/Hot</td>
<td>The service has one redundant service. NSG 9000-6G JOINs both the primary and backup multicast groups and both groups are steamed to the device. Upon failure, the backup service is provisioned to the device resulting in a short fail-over time.</td>
</tr>
<tr>
<td>Hot/Warm/Warm</td>
<td>The service has at least two redundant services. NSG 9000-6G JOINs the primary multicast group. Upon failure NSG 9000-6G JOINs the first backup service and as a result the backup service is streamed into the device. If this trial fails, NSG 9000-6G JOINs the second backup multicast group.</td>
</tr>
<tr>
<td>Hot/Hot/Hot</td>
<td>The service has at least two redundant services. NSG 9000-6G JOINs all three multicast groups. All three services are streamed to the input port to allow short fail-over time.</td>
</tr>
</tbody>
</table>

3. ISA Redundancy mode - check Allow Shared Backup Source to allow a single service/socket to backup more than one primary sockets. Once this option is selected, the redundancy switch may take up to four seconds.

**NOTE:** To define port redundancy in SDV application, see Configuring Input GbE Port Redundancy on page 37.

### 4.4.1.3 Defining MPEG Parameters

See Defining MPEG Parameters on page 75.

### 4.4.2 Viewing SDV QAM Parameters

The QAMs parameters allows you to view all of the SDV available QAMs.
1. Select Applications > SDV > QAMs.

2. View the following information.
   - QAM Manager - lists the defined QAM manager. In SDV the QAM manager can be NGOD ERM or ISA.
   - Eth1 Virtual IP - displays the Eth1 of the virtual device that the SDV QAM is associated with.
   - RF Output - see Configuring/Viewing QAM Channels on page 49
   - QAM Index - see Configuring/Viewing QAM Channels on page 49
   - TS ID - see Configuring/Viewing QAM Channels on page 49
   - NGOD Group Name - see Configuring/Viewing QAM Channels on page 49
   - QAM Frequency - see Configuring/Viewing QAM Channels on page 49
   - Symbol Rate - see Configuring a QAM-RF Module on page 46.
   - Interleaver - see Configuring/Viewing QAM Channels on page 49
   - Spectral Inversion - see Configuring/Viewing QAM Channels on page 49
   - Status - can be either of the following:
     - Active - the QAM is operating properly
     - Muted - the QAM is muted
     - RF Disabled - the RF port is disabled
     - No License - there is not license for this QAM license
     - Module Out - no QAM-RF module is mounted in the slot

4.4.3 Viewing NGOD Active Sessions

The NGOD Active Sessions tab lists all the NGOD sessions provisioned to the device. NSG 9000-6G supports up to 2,000 NGOD sessions.

⇒ To view NGOD active sessions
1. Select Applications > SDV > NGOD Active Sessions.

2. To view the currently provisioned session, click Refresh Sessions.

3. View the following information:
   - On Demand Session ID - a unique session ID generated by the NGOD system.
   - Session ID - a unique session ID generated by the NSG 9000-6G device.
   - RF Output - the output QAM-RF channel through which the service is streamed out of the device.
   - Service ID - the ID of the output service
   - NGOD Group Name - the QAM group name that the NSG reports on via its NGOD-D6 messages.
   - GbE Port - indicates the GbE input port of the incoming service.
   - Destination IP - the IP address (unicast or multicast) of the input session.
   - UDP Port - the UDP port of the input session.
   - Active Source IP - indicates the IP address of the current source and whether it is the primary or the backup source. For example, 1:123.123.123.100, where: 1 - primary source, 123.123.123.100 - source IP address
   - Bitrate - the required bitrate for this session.

4. To view further information, click Details.
The following dialog appears:

5. View the following session information:
   - On Demand Session ID - a unique session ID generated by the NGOD system.
   - Session ID - a unique session ID generated by the NSG 9000-6G device.
   - Session Group - an optional field. A value given by the ERM for managing the session list length.
   - Bitrate - indicates the required bitrate for this session.
   - No PID Remap - indicates whether No PID Remap is selected for this session. See Provisioning Service Remux Sessions on page 85.

6. View the following Output information:
   - TS ID - the ID of the output TS that carries the output session.
   - Output Service ID - the ID of the output service.

7. View the following Input Redundancy information:
   - # - a sequential number to indicate the number of the listed input redundancy ports.
   - GbE Port - indicates the number of the input GbE port.
   - Input Service ID - indicates the ID of the input service
   - Multicast IP Address - the multicast IP address of the input service
   - UDP Port - the UDP port of the input service
   - Source IP Address - indicates the IP address of the broadcasting device.
   - Active - indicates whether this input port is currently active. The row of the active port is darker.

4.4.3.1 Exporting NGOD Active Sessions

1. Select Applications > SDV > NGOD Active Sessions.
2. Click Export Sessions.

3. Click Export.

4. Select Open or Save.

5. View the .XML file.

4.4.4 Viewing ISA Active Sessions

The ISA Active Sessions tab lists all the ISA sessions provisioned to the device.

To view ISA active sessions

1. Select Applications > SDV > ISA Active Sessions.

2. To view the currently provisioned sessions, click Refresh Sessions.

3. To export the currently ISA active sessions to an XML file, click Export Session.

4. View the following information:
   - Session ID - a unique session ID generated by the NSG 9000-6G device.
   - State - indicates the status of the session:
     - Bind - the session is provisioned
     - Alloc - the session is allocated but not yet provisioned
   - RF Output - the output QAM-RF channel through which the service is streamed out of the device.
   - Service ID - the ID of the output service
   - GbE Port - indicates the GbE input port of the incoming service.
   - Destination IP Address - the IP address (multicast/unicast) that the service is sent to.
   - UDP Port - the input UDP port
   - Active Source IP - the IP address of the source IP
Chapter 4 Configuring Applications

SDV Application

- Bitrate - the bitrate of the provisioned session.

5. To view further information, click Details. The following dialog appears:

![Dialog](https://example.com/dialog.png)

6. View the following session information:
   - Session ID - a unique session ID generated by the NSG 9000-6G device.
   - Bitrate - the bitrate of the session.
   - Time Created - the first time the session was provisioned.
   - State - indicates the status of the session:
     - Bind - the session is provisioned
     - Alloc - the session is allocated but not yet provisioned

7. View the following Output information:
   - TS ID - the ID of the output TS that carries the output session.
   - Service ID - the ID of the output service.
   - No PID Remap - indicates whether PID remapping is applied.

8. View the following Input Redundancy information:
   - # - a sequential number to indicate the number of listed input redundancy ports.
   - GbE Port - indicates the number of the input GbE port.
   - Input Service ID - the ID of the input service
   - IP Address - the IP address of the input service
   - UDP Port - the UDP port of the input service
   - Source IP Address - indicates the IP address of the broadcasting device.
   - Active - indicates whether this input port is currently active. The row of the active port is darker.

To export ISA Active Sessions to an .XML file, see Exporting NGOD Active Sessions on page 95.
4.4.5 Monitoring SDV Connections

The Connections tab lists all SDV managers together with a messages counter. The counter monitors the connection between the SDV managers and the edge QAM.

Each time a message is received by the edge QAM, the counter registers another incidence and updates the number of messages. You may refresh the connection when required.

To monitor SDV connections
1. Select Applications > SDV > Connections.
2. View the Manager IP and the number of messages and whether it increases.
3. To refresh connection, click Refresh Connection.

4.5 M-CMTS Application

When NSG 9000-6G is integrated in an M-CMTS system, do the following:

- Create an M-CMTS session by defining the QAM Manager as M-CMTS
- Configure the session - When you configure an M-CMTS session, you choose to output a socket without any changes, that is without remapping and without generating tables.

To create an M-CMTS session
1. Select Platform > General tab.
2. select the required slot.
3. Select the QAMs tab.
4. For the required RF Output, open the QAM Manager list and select M-CMTS.
   Once you select Applications > M-CMTS tab, the M-CMTS sessions appear and you can define their parameters.

To configure an M-CMTS session

When you configure a session, select the required input port and route it to the required output as instructed below:
1. Select Applications > M-CMTS tab:

Sessions appear in the table according to your QAM configuration in Platform > General > Slot > QAMs. Each session appears with a unique session ID.

Session ID- Read only. A sequential number starting at 10000, to indicate the number of the session in the current page.

**NOTE:** Steps 2&3 are relevant to primary DS channels only. In case of wideband sessions, move to step 4.

2. Relevant to primary DS channels only - To synchronize with the DTI time, select DTI Sync Restamping. The EdgeQAM re-stamps the DTI sync packets.

3. Relevant to primary DS channels only - In DOCSIS Sync Compensation, enter the sync compensation. The CMTS core router automatically inserts DOCSIS sync packets into the primary DS QAM channels. To ensure the accuracy of the DOCSIS sync packets, the EdgeQAM re-stamps them. Depending on RF network topology, it may be required to fine-tune the sync messages that flow over the various QAM channels of the EdgeQAM. The fine-tuning ensures consistent timing of CMs across all cable interfaces of the system. To fine-tune the sync offset across cable interfaces, use the DOCSIS Sync Compensation option. The sync offset units are ticks of the CMTS 10.24 MHz clock, where 1 tick=97.6 nano-sec. The typical allowed offset difference between modems is +/- 6 ticks. To define the sync compensation value, measure the average Cable Modem (CM) timing offset difference (you can view the timing offset values via the CMTS console) and calculate the desired compensation value for the QAMs of the port. Typically, the compensation value of adjacent QAMs in the port is identical for each QAM in the port.

4. To select the input GbE Port, open the GbE Port list and select the required port. Once you defined the required GbE port, the GbE IP Address box is updated to display the IP address of the selected port.

5. In GbE IP Address, enter the IP address of the GbE input port.

6. In L2TP Session ID, enter the required session ID.

7. View the following Read-only information:
   - In RF Output, view the QAM channel to output the session where:
     - X – module number (1…9)
     - Y – RF port number (1…2)
     - Z – channel number (1…144)
   - QAM Index - see Configuring/Viewing QAM Channels on page 49.
   - Interleaver - see Configuring/Viewing QAM Channels on page 49.
4.6 D2E Application

The Direct to Edge (D2E) application is for future use only.

When NSG 9000-6G is operating as part of a D2E system, configure it in the same manner as a regular Wideband M-CMTS application:

- Set the QAM manager for the relevant QAMs to M-CMTS
- Configure the sessions as regular Wideband M-CMTS sessions
Chapter 5  
Conditional Access System (CAS)

5.1 CAS Overview

The Conditional Access System (CAS) prevents unauthorized viewing of programs by scrambling services that later on can be decrypted using the correct decrypting key. NSG devices support the following CAS modes:

- DVB SCR scrambling - an encryption mode for the DVB protocol.
- Privacy Mode - an encryption mode developed by Motorola Inc.

5.1.1 DVB SCR Scrambling Overview

A typical CAS is comprised of a few elements. The NSG 9000 includes the SCS, CWS and scrambling modules. Following is a short description of the CAS elements.

- Event Information Scheduler (EIS) - in charge of all of the headend's schedule information and the CAS configuration to ensure that services are encrypted correctly. It initiates the Scrambler Control Group (SCG) message, the actual request sent by the EIS to the NSG 9000 that encryption is required. The SCG message includes the service ID, time slot and the access criteria.
- SimulCrypt Synchronizer (SCS) - controls and manages the scrambling parameters to allow encryption. It receives requests for encryption and passes them on to the Control Word (CW) generator. Once a CW is initiated the SCS passes it to ECMG.
- Control Word Server (CWG) - generates the encryption key.
- Scrambling Unit - encrypts the services.
- Entitlement Control Message Generator (ECMG) - receives control words and access criteria and generates an Entitlement Control Message (ECM) stream in return.

The EIS sends the NSG 9000 an SCG message, a request to encrypt a service component. In turn, the NSG 9000 sends a message to the ECMG which contains the following:

- Control Word (CW) - the encryption key generated by the NSG 9000.
- Crypto Period (CP) - indicates (in seconds) how often the NSG 9000 generates a new CW.
- Access Criteria (ACC) - a permission to access the service.

The ECMG generates an ECM stream that is sent to the NSG 9000 and is added to the TS.

### 5.1.2 Privacy Mode Scrambling Overview

Privacy Mode is a real-time encryption method which was developed by Motorola and licensed to Harmonic for VOD applications. Privacy Mode requires an MCT machine which serves as the Privacy Mode ERS proxy as the following illustration shows:

![Privacy Mode Scrambling Diagram]

When using Privacy Mode scrambling, the only additional configuration that is required within the NSG web client is to enable CAS and to set the behavior upon ECM expiration. However, Privacy Mode also requires an MCT machine which serves as the Privacy Mode ERS proxy. For information on how to configure Privacy Mode parameters in MCT, refer to the *MCT User’s Guide*.

### 5.2 Defining Global CAS Parameters

- To set global CAS parameters, do the following:

1. Select Applications > CAS. The following tab opens.
2. In CAS Properties, open the Encryption Mode (DVB PM) list and select either of the following:
   - DVB Scrambling - an encryption mode for the DVB protocol.
   - Privacy Mode Scrambling - an encryption mode developed by Motorola Inc.

3. To enable CAS, select the CAS Enable box.
   
The fields of the selected encryption mode are enabled.

5.3 Defining DVB Scrambling Parameters

Once you selected the DVB Scrambling mode, and enabled the CAS, move to the DVB Settings section and do the following:

1. In CP Duration (Sec), enter the required value. By default it is 15 seconds. The Crypto Period defines how often the NSG changes the control word (or "key") for encrypted services. Valid values range between 1-6554.

2. In ECMG Failover Retries, define the number of times the NSG 9000 unit tries to establish communication with the Entitlement Control Message Generator (ECMG) before issuing the alarm ECMG Connection Failure.

3. In CA Descriptor Location, select a location in the PMT for the CA descriptor. The CA descriptor may appear either in a service or elementary level or in both levels.

4. Open the DVB Scrambling Mode box and select either of the following:
   - Session based - the EIS is external and it issues an SCG for each service for which encryption is required. When selected, the DVB Session based features are enabled.
   - Tier based - all services are scrambled with the same control word and ECM and there is no external EIS. Once selected, the DVB Tier Based features are enabled.
5.3.1 Defining DVB Session Based Parameters

Once you selected this option in DVB Scrambling Mode, define the session based parameters as follows:

1. In TS ID Provisioning, select how to generate the TS ID to be provisioned:
   - Direct - The default option. The provisioned TS ID is the same as the output TS ID.
   - By QAM Index - The provisioned TS ID is according to the QAM number that is a number between 1-144.

2. In EIS SCS Port Number, define the TCP port through which NSG communicates with the EIS. Valid values range between 1-65535.

3. In Clear to Scramble (Sec) enter the clear time in seconds before starting to scramble the service, once the SCG is received. Valid values range between 0-9999. The default value is 0 seconds.

5.3.2 Defining DVB Tier Based Parameters

Once you selected this option in DVB Scrambling Mode, define the tier based parameters as follows:

1. Select Block Upon Failure, to allow the device to block the stream to protect the content. When a stream is blocked, no picture appears on the end user screen. This action takes place in case the NSG 9000 could not establish communication with the ECMG.

2. In Failed to Scramble Timeout (Sec), define the period of time between outputting the service and recognizing CAS failure. When CAS failure is recognized the following takes place:
   - Scrambling with the last available ECM
   - Block the stream. Applies in case ECM is not available and Block Upon Failure is selected.
   - Outflow a clear stream. Applies in case ECM is not available and Block Upon Failure is not selected.

3. NSG 9000-6G supports SimulCrypt in DVB Tier Based mode and it allows to encrypt the content with up to 3 different Conditional Access Systems. You can define up to three ECMs each with its own Access Criteria. To configure the ECMs, enter the required values in the ECM Group table as explained below:
   - ECM PID - enter the ECM PID.
   - Super CAS ID - enter the Super CAS ID of the ECMG as provided by the vendor.
Access Criteria - enter an access criteria as provided by the vendor.

5.3.3 Viewing EIS Information

You can work with multiple EIS devices. The EIS tab lists all EIS connected to the device. NSG 9000-6G supports up to six EIS machines:

To view EIS log
1. Select Applications > CAS > EIS tab.
2. To update the listed information, click Refresh.
3. View the following information:
   - Date - indicates the date of connection between the NSG and the EIS.
   - Time - indicates the time of connection.
   - Channel ID - indicates the channel of communication between the NSG and the EIS.
   - Description - shortly describes the connection (setup, closed).
   - State - indicates the current status of the NSG and EIS connection.

5.3.4 Defining ECMGs and NSG 9000 Communication Parameters

This section instructs you on how to define the ECMG & NSG 9000 communication parameters.

To define ECMGs
1. Select Applications > CAS > ECMG. The ECMG page appears. Each row in the page represents an ECMG. You can define up to 10 ECMGs.

<table>
<thead>
<tr>
<th>Active</th>
<th>Name</th>
<th>Priority</th>
<th>SuperCasID (Mac)</th>
<th>Protocol Revision</th>
<th>IP Address</th>
<th>Port</th>
<th>Channel ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>negre</td>
<td>1</td>
<td>1120136908</td>
<td>REV2</td>
<td>192.168.187.205</td>
<td>5555</td>
<td>1</td>
<td>CONNECTED</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>0</td>
<td>REV2</td>
<td>0.0.0.0</td>
<td>0</td>
<td>10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Define the communication parameters according to the following explanation:
   - Active - Check the box in the left most column to make the current ECMG active.
   - Name - Enter the name of the ECMG brand.
Priority - to allow redundancy, set priority by indicating the primary and secondary ECMG of the same SuperCasID. In case of ECMGs with the same SuperCasID, NSG 9000 always tries to connect first to the ECMG with the highest priority. Assign priority from 1-10 with 1 as the highest priority.

SuperCasID (Hex) - A 32-bit hexadecimal number that consists of the 16-bit CA vendor ID and an additional 16-bit number that distinguishes one ECM generator from another for the same CAS vendor. The super CAS ID determines which access criteria is coupled with each ECMG. The CAS vendor provides this value.

Protocol Revision - Specifies the CAS mode of operation. Select Revision 1, 2 or 3.

IP Address - The IP address of the ECMG. The CAS vendor provides this value.

Port - The number (in decimal format) of the TCP port used to connect the ECMG. The CAS vendor provides this value.

Channel ID - indicates the channel of communication between the NSG and the ECMG.

Status - Indicates the state of the connection:
- Connected - The ECMG and NSG are communicating.
- Disconnected - No communication is taking place at the moment.

5.3.5 Viewing CAS Status

5.3.5.1 Viewing the SCG Parameters

1. Select Applications > CAS > SCGs tab. The SCG page appears.

   The following information is listed:

   Number of SCGs - indicates the number of listed SCGs.

   SCG ID - The ID number of the SCG.

   CP Number - A running counter of the number of Crypto Periods. It indicates the number of times the ECM has been changed for this stream.

   TS ID/QAM Index - The stream that carries the service to be encrypted as sent by the EIS.

   Service ID - The ID of the program/service being scrambled using the specific SCG.

   State - Indicates the status of the service as follows:
   - Scrambling - Indicates that the service is encrypted.
   - Clear - Indicates that scrambling failed.

   Access Criteria - the access criteria as provided by the vendor.

2. Click Refresh to update the information in the SCG table.

5.3.5.2 Viewing ECM Parameters

The Entitlement Control Message (ECM) page provides information about the ECM stream that is sent to the NSG and is added to the TS.
1. Select Applications > CAS > ECMs tab. The ECM page appears and you can view the following information:

<table>
<thead>
<tr>
<th>Stream ID</th>
<th>ECM ID</th>
<th>SuperCasID (Hex)</th>
<th>SCG ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x3a9</td>
<td>180100000</td>
<td>1</td>
</tr>
</tbody>
</table>

Number of ECMs - indicates the number of listed ECMs.
Stream ID - The ID number of the stream.
ECM ID - The ID of the ECM as sent by the EIS.
SuperCasID - Identifies the ECMG that encrypts this program. This number is provided by the CAS vendor.
SCG ID - The ID of the SCG that requested the ECM stream.

2. Click Refresh to update the information.

5.4 Defining Privacy Mode Scrambling Parameters

1. Select Applications > CAS > Privacy Mode Settings section.

2. Open the Stream Processing on ECM Expiration list and select either of the following:
   - Scramble with Last ECM - All NSGs of the VODS should be updated with the new ECM.
   - Don’t Scramble - do not scramble the stream.

**TIP:** Once provisioning/multiplexing is complete, enable the RF ports. See 3.12.3 Configuring Module RF Ports on page 47.
Chapter 6
Monitoring and Troubleshooting

6.1 Monitoring the NSG 9000-6G Overview

Monitoring the NSG 9000-6G comprises the following two aspects:
- Monitoring the device utilization
- Monitoring the device status

6.2 Device Utilization

The Traffic tab displays a read-only information about the output streams of the device. This information is displayed in the following views:
- Service View - default view. It displays the output services running over each QAM-RF channel.
- Bitrate View - displays the actual bit rate of each active QAM-RF channel.
- Output view - displays information on the selected output content. See 6.2.4 Viewing Output Information on page 112.
- Input view - displays the number of incoming services and the current frequency. See 6.2.3 Viewing Input Information on page 112.

The Service and Bit rate view pages are divided into nine sections. Each section represents a QAM-RF module with both output ports and QAM-RF channels. Each section includes the following:
- Module Number - displayed as a link. Once you click it, the Module Traffic page opens. When the module is assigned but no module is mounted in the slot, the module number appears with (Card Missing) indication.
- RF Port Number - displayed as a link. Once you click it, you can view the selected module global configuration and the configuration of the RF parameters. See 6.2.2 Viewing RF Parameters on page 112.
- Bar graph - represents the output TSs of each RF port. Each RF port is represented by a unique color. The available colors are as follows:

<table>
<thead>
<tr>
<th>Color</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orange</td>
<td>Service based traffic - VOD, SDV, NGOD and ISA</td>
</tr>
<tr>
<td>Dark red</td>
<td>Pass Through sessions</td>
</tr>
</tbody>
</table>

Table 6-1: Bar Graph Colors
The number at the top of each bar, indicates the following:

- **Service view** - the amount of services output in that TS.
- **Bitrate view** - the actual bit rate in Mbps.

Each bar is labeled in the following pattern x.y.z where:

- x - module number
- y - RF port number
- z - RF channel number

For example: bar 1.2.2 presents output traffic of module 1, output via RF 2 port, channel 2.

**NOTE:** Hover the mouse pointer over the bar to view the QAM-RF manager. Hover the mouse pointer over the bar label to view the service ID and its frequency.

The following figure shows a section of the Service view:
The following figure shows the same section in Bitrate view:

6.2.1 Viewing Traffic

The Module Traffic page displays all the services outputted via each QAM-RF channel together with detailed information on each service.

To view the traffic streamed out of the device in a bar graph display:
2. Click Module #.
   The following page opens. It shows the traffic flowing via RF port 1 of module 1:

3. To view detailed information about a service, select the required service in the bar graph.
The following page opens. It shows the traffic flowing via RF port 1 of module 1 with detailed information regarding service 5 of QAM-RF 1.1.1:

```
NOTE: Currently, the Module Traffic page shows only eighteen services per channel.

You can view traffic also via the Input view and Output View pages.
2. To view updated information, click Refresh Output/Input Information.
3. View the following service related information:

   NOTE: PIDs appear in Hex. and in decimal in the following pattern: Hex. (Decimal.)

   - Service ID - Read Only. The ID number of the service.
   - Port:IP - The number of the input port and its IP address.
   - UDP Port - The UDP according to the source configuration.
   - PMT Ver - The version of the PMT PID
   - PMT PID - The PID over which the service’s Program Map Table (PMT) is transmitted.
   - PCR PID - The PID of the service’s Program Clock Reference (PCR).
   - ECM PID - The PID of the Entitlement Control Message (ECM).

The following picture shows the Output view tab. It shows the traffic flowing via RF port 1 of module 1 with information regarding service 5 of QAM-RF 1.1.1:
```
See also 6.2.4 Viewing Output Information on page 112.

### 6.2.2 Viewing RF Parameters

2. Click RF #.
The following page opens.

3. In Module # Properties, view module parameters.
4. In RF Parameters, view RF parameters.

### 6.2.3 Viewing Input Information

To view the number of incoming services and the input bitrate, do the following:

1. Select Monitoring > Traffic > Input View tab.
2. View the required information.

### 6.2.4 Viewing Output Information

1. Select Monitoring > Traffic > Output View tab.

2. Open the Output Module list and select the required QAM-RF module.
3. In the tree view, do one of the following:
   - To view TS related information, select the required TS.
   - Drill down to the required service and select it.

4. View the required information. The following information appears:

```
+----------------+----------------+----------------+----------------+----------------+
|TS|Service/service Remux|PID|PID Remux|
+----------------+----------------+----------------+----------------+
|QAM Manager    |Service ID      |Orig PID        |Orig PID        |
|Serving Area   |Port:IP         |Remap PID       |Remap PID       |
|NGOD QAM Group Name |UDP Port    |PID Type        |PID Type        |
|Input Source   |PMT PID         |Language        |PMT Reference   |
|UDP Port Range |PCR PID         |ES Descriptors  |ES Descriptors  |
|ASI Forwarding |ECM PID         |                |                |
|                |                |PMT Ver         |                |
|                |                |Source IP       |                |
|                |                |Service Descriptors|            |
```

5. View the required information.
6.3 Monitoring NSG 9000-6G Status and Alarms

When ever the NSG 9000-6G detects an internal failure or problems related to the input/output streams, it asserts an alarm to indicate the specific failure. The alarms are exhibited as follows:

<table>
<thead>
<tr>
<th>Component</th>
<th>Reaction Upon Malfunction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front Panel</td>
<td>The Alarm LED is illuminated in red when an alarm is issued and in orange when a warning is issued.</td>
</tr>
</tbody>
</table>
| Web client | ■ The alarm indicator turns red  
 ■ The number of active alarms is updated  
 ■ a message appears notifying you of the nature of the problem |
| NMX | Alarm is issued in the NMX alarm manager |

6.3.1 Viewing Alarms Via the Web Client

The Active Alarms tab allows you the following:

- View the alarms/warnings
- Save active alarm log as an XML file
- Configuring the alarms

To view alarms in the web client

1. Select Monitoring > Alarms > Active Alarms.

2. View the alarms. You can also save the alarm log as an XML file. The alarms are listed with the following parameters:
   - # - index number of the alarm.
   - Module - the faulty component.
   - Description - describes the fault that invoked the alarm. Red color entry - indicates an alarm, orange color entry - indicates a warning.
NOTE: You may view the alarms also by moving the mouse pointer to the Alarm indicator located in Title bar. A window opens displaying the current alarms.

To save active alarms log to file
1. Select Monitoring > Alarms > Active Alarms.
2. Click Export.
3. Browse to the required location and click Save.

### 6.3.2 Alarm List

The following table lists the alarms of NSG 9000-6G according to the module that issues the alarm. The alarms are arranged in alphabetical order with a short description and a solution to remit the alarm. Alarms with a star are NOT reflected in NMX.

<table>
<thead>
<tr>
<th>Alarm Message</th>
<th>Trigger Device Redundancy</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan X Failure</td>
<td>No</td>
<td>Fan X (x= 1-4) is malfunctioning.</td>
<td>Replace the fan as instructed in the HW User’s Guide.</td>
</tr>
<tr>
<td>Front Panel Communication Failure</td>
<td>No</td>
<td>Cannot establish communication with the control panel module.</td>
<td>1. Replace the front panel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Replace the Processing module.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Call Customer Support.</td>
</tr>
<tr>
<td>Front Panel Missing</td>
<td>No</td>
<td>Front panel is missing.</td>
<td>Verify that the front panel is fastened securely to its place.</td>
</tr>
<tr>
<td>High Temperature Failure</td>
<td>Yes</td>
<td>The unit is overheating Raised when board FPGA processor temperature &gt;= 80°C, or board CPU temperature &gt;= 75°C.</td>
<td>Check front panel connection and the speed of the fans.</td>
</tr>
<tr>
<td>NGOD R6 Connection Loss</td>
<td>No</td>
<td>NGOD VREP0-R6 client has lost connection and there are live SDV sessions within the NSG.</td>
<td>Check the Ethernet connection to the R6 client.</td>
</tr>
<tr>
<td>No Input Traffic</td>
<td>Yes</td>
<td>All configured and enabled GbE ports receive no input data.</td>
<td>Check source.</td>
</tr>
<tr>
<td>Power Supply X Failure</td>
<td>Yes</td>
<td>Power supply (x= 1-2) is malfunctioning.</td>
<td>Replace power supply unit.</td>
</tr>
<tr>
<td>Service Missing</td>
<td>No</td>
<td>There is at least one defined service without active input</td>
<td>Check source.</td>
</tr>
<tr>
<td>System Voltage Error</td>
<td>Yes</td>
<td>Invalid voltage is detected in the device</td>
<td>1. Reboot the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. If persists, call Customer Support.</td>
</tr>
<tr>
<td>Temp/Voltage Communication Error</td>
<td>No</td>
<td>Cannot read the temperature or voltage.</td>
<td>Call Customer Support.</td>
</tr>
<tr>
<td>Unsupported HW Configuration: Mixed PS Models</td>
<td>No</td>
<td>Different types of power supply units are installed on the device</td>
<td>Replace at least one power supply units so both units are of the same type. See NSG9000-6G Hardware and Installation User Guide.</td>
</tr>
<tr>
<td>Alarm Message</td>
<td>Trigger Device Redundancy</td>
<td>Description</td>
<td>Solution</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Slot</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Card Missing*       | Yes                       | No module is mounted in the slot and the corresponding RF port is enabled. | 1. Disable the RF port.  
2. Mount a module in the slot.  
3. Enable the corresponding RF port. |
| Card Mismatch*      | No                        | Mismatch between the mounted module and the sent configuration.              | Check configuration or mounted module.                                    |
| GbE Port            |                           |                                                                             |                                                                          |
| CRC Error           | No                        | At least one packet has CRC error                                           | Check the switch, fiber, and copper connections. Check source (input or output). |
| ETH Buffer Overflow | No                        | Management traffic on the GbE port exceeds the port’s capacity.            | Check sources for excessive management traffic.                           |
| Invalid Input Packet| No                        | The payload length of an input UDP packet is not divisible by 188 bytes a standard length of an MPEG packet | Check source.                                                            |
| L2TPv3 Sequence Error| No                       | The sequence number of L2TP frames is not sequential, which means that some L2TP frames were dropped in the input. | Check input source.  
Check switch.  
Check fiber and copper connections. |
| Link Down (SFP)     | Yes                       | Problematic link to the SFP.                                               | Verify that the fiber is connected properly to the SFP.                  |
| SFP Missing         | Yes                       | The SFP connector is missing from the GbE port.                            | Check that the SFP connector is fully inserted                            |
| GbE Card            |                           |                                                                             |                                                                          |
| GbE Controller Failure| Yes                      | PHY ID Error; instable communication with GbE module.                      | 1. Reset unit.  
2. If problem persists, call Customer Support.                            |
| MPEG Buffer Overflow | No                       | Buffer is overloaded with too high bit rate                               | Reduce bit rate.                                                        |
| MPEG Sync Loss      | No                        | GbE traffic contains No valid MPEG data                                   | 1. Check source.  
2. Check the input cable and replace if defective.                        |
<p>| General HW Failure  | No                        | GbE module fatal error.                                                    | Call Customer Support                                                   |
| TS Out              |                           |                                                                             |                                                                          |
| TS Out Overflow     | No                        | The actual output bit rate exceeds the configured QAM output bit rate.     | Deprovision several services of the specific output until the alarm clears. |
| VOD Session         |                           |                                                                             |                                                                          |
| PAT Corrupted*      | No                        | Invalid PAT                                                                | Check source.                                                           |
| PAT Missing*        | No                        | PAT is missing in input signal.                                            | Check source.                                                           |</p>
<table>
<thead>
<tr>
<th>Alarm Message</th>
<th>Trigger Device Redundancy</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAT Disappeared</td>
<td>No</td>
<td>PAT was in input signal and disappeared.</td>
<td>Check source</td>
</tr>
<tr>
<td>PMT Corrupted*</td>
<td>No</td>
<td>Invalid PMT</td>
<td>Check source</td>
</tr>
<tr>
<td>PMT Missing*</td>
<td>No</td>
<td>PMT is missing in input signal.</td>
<td>Check source</td>
</tr>
<tr>
<td>PMT Disappeared</td>
<td>No</td>
<td>PMT was in input signal and disappeared.</td>
<td>Check source</td>
</tr>
<tr>
<td>Audio PID Missing*</td>
<td>No</td>
<td>Audio PID is missing in input signal.</td>
<td>Check source</td>
</tr>
<tr>
<td>Video PID Missing*</td>
<td>No</td>
<td>Video PID is missing in input signal.</td>
<td>Check source</td>
</tr>
<tr>
<td>VOD program not scrambled*</td>
<td>No</td>
<td>VOD program is not scrambled while either of the following applies:</td>
<td>Check source</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Configured to DVB-CAS mode and CAS is enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provisioned program is VOD auto detect and service is not scrambled</td>
<td></td>
</tr>
<tr>
<td>VOD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invalid UDP Detected*</td>
<td>No</td>
<td>The UDP is destined to an invalid output port</td>
<td>Check source</td>
</tr>
<tr>
<td>Session</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Missing*</td>
<td>No</td>
<td>Service is missing in input signal.</td>
<td>Check source</td>
</tr>
<tr>
<td>PID Range</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Missing</td>
<td>No</td>
<td>Traffic is not detected on one of the configured input sockets.</td>
<td>Check source</td>
</tr>
<tr>
<td>QAM-RF Module</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initialization Failure</td>
<td>No</td>
<td>Card initialization failed because the actual card is different than the assigned card.</td>
<td>Replace module, or assign proper configuration</td>
</tr>
</tbody>
</table>
| Communication Failure         | No                        | The device cannot communicate with the QAM-RF module                                                  | 1. Check that the module is properly inserted  
|                               |                           |                                                                                                       | 2. Assign the module |
| Critical Error: Repeated CIC  | No                        | The affected QAM-RF module has suffered repeated CIC overflow events. To prevent service interruption | 1. Replace the affected module.  
| Overflow                      |                           | on adjacent QAM channels, both RF ports of the module has been shut-off.                              | 2. Contact Harmonic Customer Support . |
| Critical Error                | No                        | Internal fatal error in the QAM-RF modules                                                              | 1. Re-install the module  
<p>|                               |                           |                                                                                                       | 2. If problem persists, call Customer Support . |
| Processing Error              | No                        | QAM-RF global error                                                                                   | Replace module |</p>
<table>
<thead>
<tr>
<th>Alarm Message</th>
<th>Trigger Device Redundancy</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Temperature Out of Range      | No                        | The temperature is out of the defined range  
Module temperature $\geq 85°C$.                                                                  | Call Customer Support             |
| QAM Channel                   |                           |                                                                                                |                                   |
| QAM License Missing           | Yes                       | The QAM License is either expired or is not granted.                                            | Request a QAM license             |
| PM License Missing            | Yes                       | The Privacy Mode license is either expired or is not granted.                                   | Request a PM license              |
| SCR License Missing           | Yes                       | The DVB scrambling license is either expired or is not granted.                                 | Request a DVB scrambling license  |
| DOCSIS QAM + DTI Sync License Missing | Yes                  | This license is either expired or is not granted.                                               | Request this license              |
| DOCSIS QAM License Missing    | Yes                       | The DOCSIS QAM license is either expired or is not granted.                                     | Request a DOCSIS QAM license      |
| RF port                       |                           |                                                                                                |                                   |
| Communication Failure         | No                        | The device can not communicate with the upconverter.                                             | 1. Reset unit  
2. Replace the module  
3. If problem persists, call Customer Support |
| RF Level Out of Range         | No                        | The power level of the RF signal going into the upconverter is out of the allowed range.        | Call Customer Support             |
| PLL1 Failure                  | No                        | Indicates a HW failure                                                                           | Replace the module                |
| PLL2 Failure                  | No                        | Indicates a HW failure                                                                           | Replace the module                |
| Power Supply Failure          | No                        | Power level to the upconverter momentarily exceeded limits.                                      | Call Customer Support             |
| Software Failure              | No                        | Indicates a failure of the RF software.                                                          | Replace the module                |
| CAS Privacy Mode              |                           |                                                                                                |                                   |
| ECM Expired                   | No                        | ECM Expired                                                                                     | Update PM ECM via MCT.            |
| ECM Missing                   | No                        | ECM is missing                                                                                   | Updated Privacy Mode ECM via MCT. |
| DVB CAS                       |                           |                                                                                                |                                   |
| SCS ECMG Communication Failure| No                        | Connection between SCS and ECMG is not established                                                | ✓ Check link of Ethernet port 2  
✓ Check ECMG definitions in the web client. Make sure all parameters match the properties of the CAS system in use. |
6.3.3 Warning List

The following table lists the warnings of NSG 9000-6G according to the module that issues the warning. The warnings are arranged in alphabetical order with a short description and a solution to remit the warning. Warnings with a star are NOT reflected in NMX.

<table>
<thead>
<tr>
<th>Alarm Message</th>
<th>Trigger Device Redundancy</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECM Stream Error</td>
<td>No</td>
<td>Cannot get ECM from ECMG</td>
<td>• Check connectivity to ECMG</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Check with the ECMG vendor that AC is valid</td>
</tr>
<tr>
<td>DTI Card</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DTI Client Not Locked</td>
<td>Yes</td>
<td>The status of the DTI client is not NORMAL</td>
<td>Check that DTI server status is NORMAL</td>
</tr>
<tr>
<td>Service Remux Session</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAT Corrupted*</td>
<td>No</td>
<td>Invalid PAT</td>
<td>Check source</td>
</tr>
<tr>
<td>PAT Missing*</td>
<td>No</td>
<td>PAT is missing in input signal.</td>
<td>Check source</td>
</tr>
<tr>
<td>PMT Corrupted*</td>
<td>No</td>
<td>Invalid PMT</td>
<td>Check source</td>
</tr>
<tr>
<td>PMT Missing*</td>
<td>No</td>
<td>PMT is missing in input signal.</td>
<td>Check source</td>
</tr>
<tr>
<td>Service Remux Source Failure*</td>
<td>No</td>
<td>When Service Remux is configured and the input socket is not active.</td>
<td>Check source</td>
</tr>
<tr>
<td>CMTS Session</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Socket CMTS Source Failure*</td>
<td>No</td>
<td>When CMTS socket is configured and the input socket is not active.</td>
<td>Check source</td>
</tr>
<tr>
<td>PID Remux Session</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PID Remux Source Failure*</td>
<td>No</td>
<td>When PID Remux is configured and the input socket is not active.</td>
<td>Check source</td>
</tr>
<tr>
<td>License</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| License Expired          | No                        | License expired                                  | Add and request a new license.                

6.3.3 Warning List

The following table lists the warnings of NSG 9000-6G according to the module that issues the warning. The warnings are arranged in alphabetical order with a short description and a solution to remit the warning. Warnings with a star are NOT reflected in NMX.

<table>
<thead>
<tr>
<th>Alarm Message</th>
<th>Triggers Device Redundancy</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nearing High Temperature</td>
<td></td>
<td>The unit is close to overheating.</td>
<td>Check front panel connection and the speed of the fans.</td>
</tr>
<tr>
<td>NGOD D6 Connection Loss</td>
<td></td>
<td>NGOD VREPO-D6 server has lost connection and there are live SDV sessions within the NSG.</td>
<td>Check the Ethernet connection to the D6 server.</td>
</tr>
<tr>
<td>Alarm Message</td>
<td>Triggers Device Redundancy</td>
<td>Description</td>
<td>Solution</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>Running on Temporary License*</td>
<td></td>
<td>The system is running with an active temporary license while using the non-default features granted by the license.</td>
<td>Claim the required license.</td>
</tr>
<tr>
<td>GbE Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Port Active</td>
<td>Redundancy switch has taken place</td>
<td>Check primary port</td>
<td></td>
</tr>
<tr>
<td>Management Packets Reached Rate Limit</td>
<td>Management packets may drop because rate is reaching its limit.</td>
<td>Check non-video traffic on the GbE port</td>
<td></td>
</tr>
<tr>
<td>SFP Communication Error</td>
<td>Instable communication with the SFP module</td>
<td>1. Verify that the SFP module is mounted properly 2. Replace SFP 3. Reset unit 4. If problem persists, call Customer Support</td>
<td></td>
</tr>
<tr>
<td>GbE Card</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exceeding Max Sockets</td>
<td>The number of incoming streams exceeds the allowed limit.</td>
<td>Check the source.</td>
<td></td>
</tr>
<tr>
<td>Extraction Buffer Overflow</td>
<td>Extraction descriptor FIFO overrun.</td>
<td>Check PSI bit rate.</td>
<td></td>
</tr>
<tr>
<td>GbE Management Rx Failure</td>
<td>Management traffic buffer overload resulting in management packets loss.</td>
<td>Check the bit rate of the management packets.</td>
<td></td>
</tr>
<tr>
<td>GbE Management Tx Failure</td>
<td>Detecting problems when trying to transmit management data</td>
<td>1. Reset unit. 2. If problem persists, call Customer Support.</td>
<td></td>
</tr>
<tr>
<td>TS Out</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic on Invalid TS*</td>
<td>The input traffic points to an invalid output.</td>
<td>Check source and QAM mapping.</td>
<td></td>
</tr>
<tr>
<td>Missing PSIP Configuration for TS</td>
<td>PSIP is enabled and there is no PSIP configuration for the services. Services are transmitted with default PSIP configuration.</td>
<td>Check PSIP configuration for correct service ID indication</td>
<td></td>
</tr>
<tr>
<td>RF Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nearing Temperature Out of Range</td>
<td>The upconverter’s temperature is almost out of the allowed temperature range: (0°C to 70°C).</td>
<td>□ Check for proper operation of the cooling fans. □ Make sure that air inlets in the device’s front panel are clean. □ If problem persists, power-off the device and contact Customer Support.</td>
<td></td>
</tr>
<tr>
<td>Alarm Message</td>
<td>Triggers Device Redundancy</td>
<td>Description</td>
<td>Solution</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
</tbody>
</table>
| CIC Overflow           | No                         | The affected QAM-RF module has suffered repeated CIC overflow events. To prevent service interruption on adjacent QAM channels, both RF ports of the module has been shut-off. | 1. Replace the affected module.  
2. Call Customer Support.       |
| DTI port               |                            | DTI port lost connection with the DTI server                                                                                                       | Check DTI cable.                         |
| CAS Privacy Mode       |                            | ECM is about to expire.                                                                                                                               | Update PM ECM via MCT.                  |
| DVB CAS                |                            | Connection to the ECMG has failed and services may not be encrypted properly  
- Check link of Ethernet port 2  
- Check ECMG definitions in the web client. Make sure all parameters match the properties of the CAS system in use. |                                          |
| PID Range              | No                         | One of the backup sockets is activated                                                                                                               | Check source                             |
| License                |                            | License will expire in the next 24 hours.                                                                                                                                                  | Add and request a new license.           |
|                        |                            | License will expire in the next 72 hours.                                                                                                                                                  | Add and request a new license.           |
| Redundancy             |                            | Standby device does not receive Heartbeat messages from Eth1 of Active device.                                                                       | Check Ethernet connection.              |
| No Heartbeat on Eth1¹  |                            | Standby device does not receive Heartbeat messages from Eth2 of Active device.                                                                       | Check Ethernet connection.              |
| No Heartbeat on Eth2²  |                            | Standby device does not receive Heartbeat messages from Eth2 of Active device.                                                                       | Check Ethernet connection.              |
### 6.3.4 Notification List

The following table lists notifications of NSG 9000-6G. A notification is a message sent from the device to the alarm log to denote a status change without raising any alarm. However, depending on the configuration, a notification issue may trigger an SNMP trap.

<table>
<thead>
<tr>
<th>Notification Message</th>
<th>Description</th>
<th>Displayed in Alarm Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active DTI Port Is/Changed to &lt;#&gt;</td>
<td>The active port of the NSG’s DTI client has changed (from 1 to 2 or vice-versa)</td>
<td>No</td>
</tr>
<tr>
<td>DTI Client Status Changed</td>
<td>The status of DTI Client has changed to the value reflected in Platform &gt; General DTI.</td>
<td>No</td>
</tr>
<tr>
<td>Corrupt Firmware File, Booting with Previous Firmware</td>
<td>Could not load new firmware file to flash due to file corruption.</td>
<td></td>
</tr>
<tr>
<td>Cannot Find BOOTP Server, Booting with Previous IP</td>
<td>BOOTP server did not respond within the defined time out, NSG 9000-6G booted with its previous IP settings.</td>
<td></td>
</tr>
<tr>
<td>Reboot System Recovered from Watchdog Reset</td>
<td>System recovered from HW Watchdog reset</td>
<td></td>
</tr>
<tr>
<td>Reboot System Recovered from Power Reset</td>
<td>System recovered from power reset</td>
<td></td>
</tr>
<tr>
<td>Reboot Shutdown at &lt;Date&gt;</td>
<td>Shutdown at &lt;Date&gt; (Reboot)</td>
<td></td>
</tr>
<tr>
<td>Configuration Error &lt;#&gt;</td>
<td>Configuration failed in XML validation</td>
<td></td>
</tr>
<tr>
<td>SLOT &lt;#&gt; QAM-RF Module Reset by user Status=OK/Fail</td>
<td>User initiated QAM-RF reset in slot &lt;#&gt;. The status is either OK or Fail.</td>
<td></td>
</tr>
<tr>
<td>IPlnp &lt;#&gt; Manual Revert from backup port &lt;#&gt;</td>
<td>User manually reverted to the GbE input port &lt;#&gt; from backup port &lt;#&gt;</td>
<td></td>
</tr>
<tr>
<td>IPlnp &lt;#&gt; Manual Switch to backup port &lt;#&gt;</td>
<td>User manually switched from GbE input port &lt;#&gt; to backup port &lt;#&gt;</td>
<td></td>
</tr>
<tr>
<td>IPlnp-X Switch to Backup Port Y</td>
<td>Port redundancy - switched automatically from the Primary port to the Backup port because of no bit rate at the Primary port</td>
<td></td>
</tr>
<tr>
<td>IPlnp-X Cannot Switch to Backup Port Y - Occupied</td>
<td>Port redundancy - tried to automatically switch from a primary port to a backup port but the backup port was occupied.</td>
<td></td>
</tr>
<tr>
<td>IPlnp Backup Port Y switched to Primary X</td>
<td>Port redundancy - switched automatically from the Backup port to the Primary port because of no bit rate at the Backup port</td>
<td></td>
</tr>
<tr>
<td>Firmware File Download Failed</td>
<td>Failed to download new firmware file using the specified path.</td>
<td></td>
</tr>
<tr>
<td>Switched to Alternate Source</td>
<td>The NSG has switched to the alternative IP/UDP source that is configured for this session</td>
<td></td>
</tr>
<tr>
<td>GbE Card - Output Buffer Sync Byte Error</td>
<td>GbE card detected and invalid packet.</td>
<td></td>
</tr>
<tr>
<td>IPTSIN MPEG Sync Loss</td>
<td>IP input traffic contains no valid MPEG data</td>
<td></td>
</tr>
<tr>
<td>TS-Out Near Overflow</td>
<td>The actual output bit rate is nearing the configured QAM output bit rate.</td>
<td></td>
</tr>
<tr>
<td>Clock Update Started</td>
<td>RTC clock is being updated.</td>
<td></td>
</tr>
</tbody>
</table>
### 6.3.5 Setting Alarm Parameters

The Alarms > Settings page lists the alarms according to their class, that is the object that issues the alarm.

<table>
<thead>
<tr>
<th>Notification Message</th>
<th>Description</th>
<th>Displayed in Alarm Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock Update Finished</td>
<td>The update of the RTC clock is completed</td>
<td></td>
</tr>
<tr>
<td>Application Process Restart</td>
<td>Application recovered from SW Watchdog reset</td>
<td></td>
</tr>
<tr>
<td>VOD Session - PAT Missing</td>
<td>The CIC module within the QAM modulator has gone through a momentary overflow, and recovered</td>
<td>No</td>
</tr>
<tr>
<td>CIC Overflow</td>
<td>The CIC module within the QAM modulator has gone through a momentary overflow, and recovered</td>
<td>No</td>
</tr>
</tbody>
</table>

The Alarms > Settings page includes the following information for each alarm:

- **Class**: the module that issues the alarm
- **Alarm Description**: the alarm text
- **Alarm ID**: the ID of the alarm
- **Severity**: defines whether the alert is an alarm or a warning

You can configure alarm parameters and define triggering alarms as explained below:

1. **To define alarms settings**
   1. Select Monitoring > Alarms > Settings tab.
   2. Set the following parameters:

   **NOTE**: Once you have changed any of the default values and sent them to the device (Apply), the Set Defaults button appears next to the alarm its parameters were changed.

   - **Assert Threshold (Msec)** - a latency period indicated in milliseconds for this alarm. When a module discovers a condition that would normally cause it to assert this
alarm, it waits for the time specified in the Assert Threshold (Msec) field before asserting the alarm.

- Remit Threshold (Msec) - a latency period indicated in milliseconds for this alarm. When a module discovers a condition that would normally cause it to remit this alarm, it waits for the time specified in the Remit Threshold (Msec) field before remitting the alarm.

- Scan Interval (Msec) - defines how often the device checks for the conditions that raise the alarm. This field allows you to define a break, in milliseconds, in checking for the conditions that raise the alarm.

- Trigger Redundancy - defines whether the alarm triggers a redundancy switch.

- Add to Log - defines whether to write the alarm to the log of active alarms.

- Send Trap - defines whether to send an SNMP trap when the alarm is raised.

- Disable Alarm - when selected, this alarm is not issued upon correlated failure

- Set Default - click to revert the alarm settings to its default settings. This option appears only once you have changed any of the alarm parameters.

**NOTE:** The Set Default button reverts all alarms to their default settings.

### 6.4 Diagnosing and Analyzing Traffic

#### 6.4.1 Exporting Device Logs

You can export device logs as a zip archive file. The logs include the alarm log and additional files that include comprehensive system and application configuration information.

1. Select Monitoring > Diagnostics.

2. Click Export Logs.

3. In the Export File dialog, browse to the required location for saving the configuration.

4. Click Save.

The device logs are exported to your PC as a Zip.archive file.

#### 6.4.2 Capturing the Input and Output Traffic

##### 6.4.2.1 Capturing IP Input Content

Capture IP input streams to verify the integrity of video MPEG input streams, or to perform an analysis of the MPEG structures of the streams.
The IP Forwarding feature allows to mirror the input of one of GbE input ports on the output of another unused GbE port. Connect the mirroring port to devices that accept GbE input such as an MPEG analyzer. For cabling instructions, see NSG 9000-6G Installation and Hardware guide.

The configuration includes the following:
- Source port - the port that receives the input MPEG over IP traffic of interest.
- Destination port - the port that outputs the mirrored traffic from the Source port.

When configuring IP Forwarding, consider the following issues:
- Verify that the Destination port is enabled. See 3.10.1 Configuring Input GbE ports on page 35. You may also need to connect to a gigabit ethernet switch in order to establish link, and to make sure no packets are dropped from the output port. To verify the link status, see 3.10.1 Configuring Input GbE ports on page 35.
- Use a separate VLAN for the connection to the output port and to the sniffer PC.

**NOTE:** Use socket forwarding for diagnostic purposes only and not during normal operation.

1. Select Monitoring > Diagnostics and focus on the IP Forwarding section.
2. To enable mirroring, select Enable Forwarding.
3. Open the Forwarding Level list and select whether to forward a port or a socket. If you select a socket, define its parameters in the Sockets List table.
4. Open the Source Port list and select the GbE port that inputs the required content.
5. Open the Destination Port list and select the port to mirror the source port.
6. In the Sockets List table, define the following:
   - GbE/MC IP Address - the destination GbE or Multicast IP address of the socket.
   - GbE Port - enter the UDP port
   - Source IP - enter the IP address of the port that streamed the socket into the device.
   - To delete the socket, select Delete.

6.4.2.2 Capturing Output Traffic

NSG 9000-6G incorporates an ASI monitoring port. It can mirror the output MPEG traffic from any QAM-RF channel.

Once you have selected the QAM channel to be probed, the MPEG stream that is output on that QAM-RF channel is mirrored to the ASI monitor port, where you can input it to an MPEG analyzer, any device that has an ASI input connection.

1. Select Monitoring > Diagnostics and focus on the IP Forwarding section.
2. To enable mirroring, select Enable Forwarding.
3. Open the Forwarding Level list and select whether to forward a port or a socket. If you select a socket, define its parameters in the Sockets List table.
4. Open the Source Port list and select the GbE port that inputs the required content.
5. Open the Destination Port list and select the port to mirror the source port.
6. In the Sockets List table, define the following:
   - GbE/MC IP Address - the destination GbE or Multicast IP address of the socket.
   - GbE Port - enter the UDP port
   - Source IP - enter the IP address of the port that streamed the socket into the device.
   - To delete the socket, select Delete.
1. Select Monitoring > Diagnostics.

2. Open the Probe Location list and select either of the following:
   - Before Scrambler - to probe as a clear stream
   - After Scrambler - to probe as a scrambled stream

3. In ASI Forwarding section, open the Probed QAM list to select the QAM-RF channel to be forwarded for diagnosis.

6.5 Generating and Viewing Logs

You can view the following logs:
- Alarms log
- GbE Counters
- NGOD logs
- ISA logs

6.5.1 Alarms Log

The Alarms log displays the recent alarms in a chronological order. The log can display up to 100 alarms.

To view an updated log, refresh the log. You may view, refresh, clear or save the log.

To view the alarms log:
1. Select Monitoring > Logs > Alarms Log.
2. To display the log, click View Log.

**NOTE:** The view Log button toggles to Refresh Log.

<table>
<thead>
<tr>
<th>#</th>
<th>Date</th>
<th>Time</th>
<th>Module</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11/15/2008</td>
<td>14:31:51</td>
<td>Platform</td>
<td>Traffic on Invalid TS (TS ID 2)</td>
<td>On</td>
</tr>
<tr>
<td>2</td>
<td>11/15/2008</td>
<td>14:31:51</td>
<td>Platform</td>
<td>Traffic on Invalid TS (TS ID 3)</td>
<td>On</td>
</tr>
<tr>
<td>5</td>
<td>11/15/2008</td>
<td>14:31:51</td>
<td>Platform</td>
<td>Traffic on Invalid TS (TS ID 3)</td>
<td>On</td>
</tr>
<tr>
<td>7</td>
<td>11/15/2008</td>
<td>14:31:51</td>
<td>Platform</td>
<td>Traffic on Invalid TS (TS ID 3)</td>
<td>On</td>
</tr>
<tr>
<td>8</td>
<td>11/15/2008</td>
<td>14:31:51</td>
<td>Platform</td>
<td>Traffic on Invalid TS (TS ID 3)</td>
<td>On</td>
</tr>
</tbody>
</table>

The log displays the alarms registered up to the time you generated the log and informs you of the following:
- # - a sequential number.
Chapter 6 Monitoring and Troubleshooting

Generating and Viewing Logs

- Date - the date the alarm was issued.
- Time - the time the alarm was issued.
- Module - the module that raised the alarm.
- Description - a brief description of the alarm.
- State - indicates whether the alarm is raised.

To refresh alarms log

Since the Alarms log displays the alarms up to the time you generated the log, refresh it to view an updated log by performing the following:

- In the Alarms Log tab, once the alarms log is displayed, click Refresh Log.
  The log is updated to display the latest alarms.

To clear the log

1. Select Monitoring > Logs > Alarms Log.
2. To clear the log, click Clear Log.
   The currently displayed log disappears. Once you click View Log, a new log is generated.
   It includes alarms registered since the last clear log.

To save log to file

1. Select Monitoring > Logs > Alarms Log.
2. To save the log, click Export.
3. Select a location for saving the file and click Save.
   The log is saved as an XML file in the location of your choice.

6.5.2 Monitoring the GbE Ports

The Counters page monitors the operation of the GbE ports.

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
<th>Value</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>GbE-Port-1</td>
<td>Transmitted management packets</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Received management packets</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP/IP Packet Sequence Errors</td>
<td>150992765</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CRC Errors</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LSPM:C Out of Sequence Errors</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast Data Counter</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Uncast Discard Data Counter</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>GbE-Port-2</td>
<td>Transmitted management packets</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Received management packets</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP/IP Packet Sequence Errors</td>
<td>219465066</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CRC Errors</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LSPM:C Out of Sequence Errors</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast Data Counter</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Uncast Discard Data Counter</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>GbE-Port-3</td>
<td>Transmitted management packets</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Received management packets</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP/IP Packet Sequence Errors</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CRC Errors</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LSPM:C Out of Sequence Errors</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast Data Counter</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

Each GbE port is monitored for the following events:

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmitted Management Packets</td>
<td>The number of legal management packets transmitted by the active GbE port.</td>
</tr>
<tr>
<td>Received Management Packets</td>
<td>The number of legal management packets received by the active GbE port.</td>
</tr>
</tbody>
</table>
To monitor GbE ports

1. Select Monitoring > Logs > Counters tab. View the following information:
   - Module - indicates the GbE port
   - Description - indicates each event
   - Value- shows the number of occurrences

2. To reset a counter, click in the required row.

3. To reset all counters, click Clear All Counters.

### 6.5.3 Monitoring the NGOD ERM Communication

To monitor the communication of the NGOD ERM with NSG 9000-6G, allow tracing. Once you do that, Data Logging indication appears in the title bar of the device:

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP/IP Packet Sequence Errors</td>
<td>At least one UDP/IP packet is missing</td>
</tr>
<tr>
<td>CRC Errors</td>
<td>The number of Ethernet MAC CRC errors detected by the active GbE port.</td>
</tr>
<tr>
<td>L2TPv3 Out of Sequence Errors</td>
<td>Indicates the number of errors in the L2TPv3 Sequence parameter.</td>
</tr>
<tr>
<td>Unicast Byte Counter</td>
<td>Counts bytes of UDP/L2TP valid packets with destination IP equal to one of the input port self IPs. The counter does not count management packets.</td>
</tr>
<tr>
<td>Unicast Discard Byte Counter</td>
<td>Counts bytes of UDP/L2TP valid packets with destination IP equal to one of the input port self IPs, that are discarded due to non configured CAM. Does not count management packets.</td>
</tr>
</tbody>
</table>

Each time an event occurs, the counter of the event registers another incidence and updates the number of incidence. You may reset the counter when required, and upon reboot, all counters are reset.

To monitor GbE ports

1. Select Monitoring > Logs > Counters tab. View the following information:
   - Module - indicates the GbE port
   - Description - indicates each event
   - Value- shows the number of occurrences

2. To reset a counter, click in the required row.

3. To reset all counters, click Clear All Counters.

### NOTE:
Device reset does not cancel tracing. If you reset the device while tracing, when the device boots up, tracing continues and Data Logging appears in red in the title bar of the web page indicating that tracing is taking place.

You can trace the following messages:

- RTSP
- VREP

To monitor the NGOD ERM - NSG 9000-6G by tracing RTSP messages
1. Select Monitoring > Logs > NGOD RTSP.
2. To start tracing the communication, click Start Tracing. Data Logging appears in the device title bar.
3. To stop tracing, click Stop Tracing.
4. To view the communication, click Show Messages.
5. View the messages. The messages are displayed with the following parameters:

- # - a sequential number.
- Time - the time and date of the message
- From/To - indicates the sender and the addressee
- Message Type - indicates message type
- Message Content - displays the message content

6. To clear messages, click Clear Messages.

To monitor the NGOD ERM - NSG 9000-6G by tracing VREP messages
1. Select Monitoring > Logs > NGOD VREP.
2. To start tracing the communication, click Start Tracing. Data Logging appears in the device title bar.
3. To stop tracing, click Stop Tracing.
4. To view the communication, click Show Messages (Parse).
5. View the messages. The messages are displayed with the following parameters:

- # - a sequential number.
- Time - the time and date of the message
- From/To - indicates the sender and the addressee
- Message Type - indicates message type
- Message Content - displays the message content

6. To view message as raw data, click Show Messages (Raw Data).
7. To clear messages, click Clear Messages.
8. To include Keep Alive messages in the log, select Capture Keep Alive Messages.

### 6.5.4 Monitoring the ISA Communication

To monitor the communication of the ISA SRM with NSG 9000-6G, allow tracing. Once you do that, Data Logging indication appears in the title bar of the device:

T

To monitor ISA communication with NSG 9000-6G
1. Select Monitoring > Logs > ISA RPC.
2. To start tracing the communication, click Start Tracing.

**NOTE:** Device reset does not cancel tracing. If you reset the device while tracing, when the device boots up, tracing continues and Data Logging appears in red in the title bar of the web page indicating that tracing is taking place.

3. To stop tracing, click Stop Tracing.

4. To view the communication, click Show Messages.

5. View the messages. The messages appear with the following parameters:
   - # - a sequential number
   - Time - the time and date of the message
   - From/To - indicates the sender and the addressee
   - Type - indicates the communication protocol via which the message was sent
   - Function - indicates the message purpose
   - Message Content - a short description of the message

6. To view Result Codes parameter, click Result Code. A dialog that lists and explains the available result codes opens.

7. To clear messages, click Clear Messages.
### 6.6 Viewing Available Reports

This version of the NSG 9000-6G web client allows you to view a report of the RF settings. To view global RF settings and RF module settings:

1. Select Reports > RF Configuration.
2. To view RF module parameters, view the following:

<table>
<thead>
<tr>
<th>Module No. - Slot 1-9</th>
<th>QAM Index - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module Type See 3.12 Configuring QAM-RF Modules on page 42</td>
<td>QAM Manager - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</td>
</tr>
<tr>
<td>Annex See Table 3-7: Encoding Mode on page 44</td>
<td>Frequency - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</td>
</tr>
<tr>
<td>Symbol Rate - See 3.12.1 Configuring Global RF &amp; QAMs Parameters on page 43.</td>
<td>EIA Channel - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</td>
</tr>
<tr>
<td>Constellation - See 3.12.2 Configuring a QAM-RF Module on page 46.</td>
<td>Power Level - See 3.12.3 Configuring Module RF Ports on page 47.</td>
</tr>
<tr>
<td>QAM Placement - See 3.12.2 Configuring a QAM-RF Module on page 46.</td>
<td>Interleaver - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</td>
</tr>
<tr>
<td>RF Template - See,</td>
<td>Spectral Inversion - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</td>
</tr>
<tr>
<td>RF No. - See 3.12.3 Configuring Module RF Ports on page 47.</td>
<td>Mute - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</td>
</tr>
<tr>
<td>RF Enable - See 3.12.3 Configuring Module RF Ports on page 47.</td>
<td>CW - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</td>
</tr>
<tr>
<td># QAMs per Port - 3.12.3 Configuring Module RF Ports on page 47.</td>
<td></td>
</tr>
<tr>
<td>QAM No. - See 3.12.4 Configuring/Viewing QAM Channels on page 49.</td>
<td></td>
</tr>
</tbody>
</table>

### 6.7 Device Troubleshooting

The troubleshooting section describes and refers you to essential procedures for solving issues related to the general device functionality and to VOD and SDV applications.

*NOTE:* This section assumes that you are an experience user of the NSG9000, or a technical support personnel.
6.7.1 **Recurrent Upgrade Failures**

Recurrent failures to upgrade the NSG9000 device, may stem from improper configuration of the management network. NSG 9000 supports Auto-negotiation and full duplex.

- Verify that the management network is configured as auto-negotiation and full duplex.

6.7.2 **How to Questions**

6.7.2.1 **How to Export Configuration**

See 3.1.1.2 *Exporting and Importing Configuration* on page 22.

6.7.2.2 **How to Export Device Logs**

Device logs are exported as a zip archive file. The file includes the alarm log and other logs related to device performance and activity.

See 6.4.1 *Exporting Device Logs* on page 124.

6.7.2.3 **How to capture IP input**

See 6.4.2.1 *Capturing IP Input Content* on page 124

6.7.2.4 **How to capture output MPEG traffic**

See 6.4.2.2 *Capturing Output Traffic* on page 125

6.7.2.5 **How to check the QAM manager**

This procedure applies to both VOD and SDV sessions. See 3.12.1.4 *Configuring a Global QAM Manager* on page 46.

6.7.2.6 **How to Monitor Current Traffic**


6.7.2.7 **How to monitor VOD sessions?**

1. Check QAM manager, see 3.12.1.4 *Configuring a Global QAM Manager* on page 46
3. To capture IP traffic, see 6.4.2.1 *Capturing IP Input Content* on page 124

6.7.2.8 **How to monitor SDV sessions?**

1. Check QAM manager, see 3.12.1.4 *Configuring a Global QAM Manager* on page 46.
2. Verify active sessions and connections to the SRM
   To check active sessions, see 4.4.4 *Viewing ISA Active Sessions* on page 96.
   To check connection to the ISA SRM, see 4.4.5 *Monitoring SDV Connections* on page 98.
3. You can also verify that session control messages are being received from the SRM. See 6.5.4 *Monitoring the ISA Communication* on page 130.

6.7.2.9 **How to Configure Statically a Failed SDV Session**

If you determine that a specific session request has failed, you may configure that session statically for test purposes.

1. To verify that the SDV session is available, obtain the multicast IP address and UDP port for the service.
2. Add the session as explained in 4.3.2 Provisioning Service Remux Sessions on page 85. Enter a unique service ID to prevent a conflict with an existing service on the QAM channel you are testing.

3. Once the configuration is complete, click Apply.
Appendix A
Firmware Upgrade Using an External Server

A.1 Upgrading the Firmware of a Single Device

**NOTE:** To upgrade from any version older than version 2.4.1 to version 2.4.1 and higher, you should use MCT. MCT allows a smooth and problem-free process. To upgrade, you can use either MCT Pro or MCT Lite which fully supports the NSG firmware upgrade feature. MCT Lite is provided by Harmonic free of charge. To take advantage of other MCT features, purchase MCT Pro.

A.1.1 Before Upgrading

Before upgrading, prepare the following:

- HTTP Server - Firmware upgrade of NSG 9000-6G is based on HTTP download and requires an HTTP server. Installing and configuring an HTTP server is a one time procedure. For instructions on how to install and configure an HTTP server, see *Upgrade Server Installation and Configuration* on page 140.

- Firmware package - Obtain the new firmware zipped files from Harmonic's FTP site. New firmware packages are distributed as self-extracting ZIP archives. Starting from firmware version 2.4.1, the NSG firmware distribution includes two separate self-extracting archives that are separately executed:
  - Main firmware archive - when executed, this file extracts the firmware package to a folder which is named the same as the version number (e.g. 2.4.1.13-1), under the X:\HTTPROOT\Harmonic\NSG9K6G\Y.Z.B-1 where x.y.z.bb-1 represents unique identification of the package, for instance 2.4.1.13-1. x.y.z are identical to the official name of the release.
  - NSG-Upgrade archive - this archive, which is much smaller in size, holds various software components that the NSG utilizes during the upgrade process. It must be extracted separately from the main archive. When executed, this file extracts its content to a folder named HTTPROOT\Harmonic\NSG9K6G\nsg-upgrade x.y.z-1 where x.y.z-1 represents version identification information, for example nsg-upgrade 1.0.6-1.

A.2 Upgrading Procedure

**NOTE:** In case the device is working in an EdgeCluster mode, refer, before you start upgrading, to *3.17.3 EdgeCluster Maintenance* on page 72.

1. Make sure that you have either the Apache or the IIS HTTP server installed and configured on your firmware repository server machine. See *Upgrade Server Installation and Configuration* on page 140.

2. Obtain the new firmware zipped files from Harmonic's FTP site.

3. Browse to the firmware files and double click the main firmware archive: NSG9K-6G_X.Y.Z.BB-1.exe where x.y.z.bb-1 represents version identification number. The following message appears:

   This self-extracting archive mounts the NSG9000-6G Firmware package on your PC.

4. Click OK.
The following dialog appears while WinZip Self-Extractor extracts the files:

5. When extraction is done the following screen appears prompting you to enter the required drive.

You should enter the same drive that you chose when configuring the Apache Web Server or when configuring the IIS.
The following message appears:

Firmware package for NSG9000-6G version x.y.z.bb-1 has been successfully copied to X:\HTTPROOT\Harmonic\NSG9K6G.

NOTE: X stands for the selected drive.

6. To extract the nsg-upgrade file, repeat steps 3-5 for the file nsg-upgrade x.y.z-1.

7. Open the web client of the NSG 900-6G device. See 2.2.1 Logging Into the Device via IE on page 15.

8. Select the Platform tab.
   By default Chassis is selected.

9. Click Firmware Upgrade.
   The following dialog appears:
10. In Repository Server IP Address, enter the IP address of your HTTP server.

11. In Firmware Directory, enter the name of the subdirectory that holds the extracted files. For example, 2.4.1.13-1.

12. Open the Reboot After Install list and select either of the following:
   - Automatic - to automatically reboot after installing the firmware. The device reboots of its own accord during the upgrade procedure. However, this option does not require any intervention once the upgrade procedure is initiated.
   - Manual - to reboot after install following user confirmation only. This option allows background download. While downloading the new firmware, the device is fully operational. You can reboot the device at your convenience and control the time the device is out of service for rebooting with the new firmware file.

13. To install, click Install.
   The following message appears:

14. To proceed, click OK.
The Installation Status page appears:

This page informs you of the installation status. The installation status log is updated every 3 seconds during the installation.

**NOTE:** During the installation of the new firmware, you cannot access the web client of the device. If you close and reopen the web client the Status Installation page appears.

When the installation is finished, either of the following takes place:

- If you selected Automatic reboot, the device reboots automatically. Move to Step 16.
- If you selected Manual reboot, the following message appears:

![Microsoft Internet Explorer]

15. Click OK, to complete the installation and to reboot with the new firmware version.

If you click Cancel, you cancel the firmware installation and you will need to re-start the installation for the device to run with a new upgraded firmware.

16. Select Platform > Chassis > General tab and verify that the device reports the same version number as the required firmware.
A.2.1 Recovering from Upgrade Problems

To allow recovery from incidents such as failed upgrade or corrupt configuration that causes an endless loop of reboot, use the Recovery menu included in the boot sequence.

The Recovery menu is available only via a serial connection to the device. If such connection is established, you can invoke the Recovery menu by pressing <Enter> when prompted at a certain point during the boot sequence: as the following picture shows:

You can choose one of the following menu options:

- Reset Device to factory default - device reboots with factory default parameters.
- Switch to backup partition - device reboots from backup partition
- Temporarily disable application - for Harmonic technical support only
- Continue boot process - resumes the boot process
- Reboot - restarts device reboot
- Enter debug shell - for Harmonic technical support only
Appendix B
Upgrade Server Installation and Configuration

B.1 Overview

Firmware upgrade of NSG 9000-6G is based on HTTP download and requires an HTTP server on the LAN. Use either of the following HTTP servers as the Upgrade server:

- Apache Web server - Harmonic provides a customized installation package

This appendix guides you on how to prepare the Upgrade server as follows. The configuration of the Upgrade server is a one-time procedure.

- Apache Web server - installation instructions
- IIS - configuration instructions. Instructions varies according to the operating system.

NOTE: You can use the HTTP server also for running the MCT or the NSG web client.

B.1.1 Upgrade Server Requirements

The Upgrade server PC should meet the following requirements:

Table 6-4: Upgrade Server Requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Operation System</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optical drive</td>
<td>One of the following:</td>
<td>HTTP server - Either of the following:</td>
</tr>
<tr>
<td></td>
<td>Windows2000</td>
<td>- Apache Web Server</td>
</tr>
<tr>
<td></td>
<td>Windows XP</td>
<td>- Pre-installed IIS</td>
</tr>
<tr>
<td></td>
<td>Windows 2003 server</td>
<td></td>
</tr>
<tr>
<td>USB interface</td>
<td></td>
<td>NSG firmware distribution package</td>
</tr>
<tr>
<td>Pentium 4 or higher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>At least 10gbyte free space on the hard drive</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B.1.2 Upgrade Server Installation Guidelines

Use either the Apache Web Server or the IIS server. Any attempt to install the Apache server on a computer with IIS, will stop the IIS operation.

For Apache installation and configuration instructions, see B.2 Apache Server on page 141.

For IIS configuration instructions, see B.3 IIS Server on page 142.
B.2 Apache Server

This section guides you on how to install and configure the Apache server.

B.2.1 Installing the Apache Web Server

To install the Apache server, use Harmonic’s customized installation package supplied on the Upgrade CD-ROM.

Prior to installing read the following:
- Apache currently does not work under Windows Vista.
- Apache server uses port 80 which is usually used by Skype. If Skype is installed on the Upgrade server computer, a conflict may arise. Re-configure Skype prior to the Apache installation.
- If you are using a firewall, you may need to configure or disable firewall.

The installation batch script performs the following:
- Installs Apache at c:\xampplite\apache.
- Sets X:\HTTPROOT as the WWW root directory. X Represents the drive letter that you select.

The web server is configured with the following:
- Anonymous access enabled
- Directory browsing enabled

To install the Apache web server
1. On the Upgrade CD-ROM, browse to the Apache_setup_x file. (x = version number)
2. Double click the setup file to run the file.
3. In the Apache Setup dialog, click OK.
   Apache self extracts. A batch sequence window appears notifying that it installs Apache in the C:\XAMPPLITE directory and stops IIS if it is running.
4. On your keyboard, press <Y> and then <Enter> to continue.
   Batch steps are executed:
   Batch Step #1 stops and uninstalls the Apache service if installed.
   Batch Step #2 stops IIS.
   Batch Step #3 checks if port 80 is available.
   Batch Step #4 sets up the root directory.
   Batch Step #5 creates Start menu shortcuts under Apache for Harmonic. If your interface is not English then the links are placed in C:\xampplite\Harmonic\Links. You can manually copy them to the desktop.
   Batch Step #6 installs and starts the Apache Web service.

B.2.2 Testing the Operation of the Apache Web Server

Select Start > All Programs > Apache for Harmonic > Test_service.
In your default browser a window appears with the message:
Your server is running correctly!
B.3 IIS Server

This section guides you on how to configure the IIS server. With IIS you must manually create the directories and the alias Harmonic that comprise the Harmonic virtual directory. IIS can run under a few operation systems. Each operation system requires different configuration. The following table lists the OS with the corresponding instructions:

### Table 6-5: IIS – Operation System and Instructions Reference

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Instructions Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>See B.3.2 Configuring IIS Upgrade Server with Windows XP &amp; Windows 2003 on page 144.</td>
</tr>
</tbody>
</table>

#### B.3.1 Configuring IIS Upgrade Server with Windows 2000

The configuration under Windows 2000 includes the following stages:

- Creating the directories: `HTTPROOT\Harmonic\NSG9k6G`
- Creating Harmonic alias

##### B.3.1.1 Creating Directories Under Windows 2000:

1. Right-click My Computer.
2. Select Explore.
3. Select a volume.
5. Type `HTTPROOT` for the new folder name, and press <Enter>.
6. Double-click the new HTTPROOT folder.
7. Select File > New > Folder.
8. Type `Harmonic` for the new folder name, and press <Enter>.
9. Double-click the new Harmonic folder.
10. Select File > New > Folder.
11. Type `NSG9K6G` for the new folder name, and press <Enter>.

The following picture shows the required directory structure:
B.3.1.2 Creating the Harmonic Alias under Windows 2000

1. Select Start > Settings > Control Panel.
2. Double-click Administrative Tools.
3. Double-click Internet Services Manager.
   The Internet Information Services dialog appears.
4. Expand the tree in the left panel.
5. Right-click Default Web Site.
   The Virtual Directory Creation Wizard appears.
5. Click Next.
6. In the Alias box enter Harmonic and click Next.
7. Click Browse.
8. Select the folder named Harmonic under X:\HTTPROOT. (X represents the volume that you chose)
9. Click OK.
10. Click Next.
11. To set the access permissions for the virtual directory, select the Browse box.

Select Browse, to set access permissions

12. Click Next.
13. Click Finish.

Windows creates the Harmonic virtual directory.

B.3.2 Configuring IIS Upgrade Server with Windows XP & Windows 2003

The configuration under Windows XP/Windows 2003 includes:

- Creating the Harmonic virtual directory
- Enabling the Browse feature

To configure the IIS Upgrade Server with Windows XP/Windows 2003

1. Select Start > Control Panel.
2. Double-click Administrative Tools.
3. Double-click Internet Information Services.

The Internet Information Services window displays.
4. Expand the tree in the left panel.
5. Expand Web Site.
6. Right-click Default Web Site.
7. Select New > Virtual Directory.

The Virtual Directory Creation Wizard appears.
8. Click Next.
9. In the Alias box enter Harmonic and click Next.
10. Click Browse.
11. Select a drive.
12. Click Make New Folder.
13. Type HTTPROOT for the new folder name, and press <Enter>.
14. Click Make New Folder.
15. Type Harmonic for the new folder name, and press <Enter>.
16. Click Make New Folder.
17. Type NSG9K6G for the new folder name, and press <Enter>.
18. Select the X:\HTTPROOT\Harmonic folder. (X=the drive selected in step 11)

19. Click OK.
20. Click Next.
21. To set the access permissions for the virtual directory, select the Browse box.

22. Click Next.
23. Click Finish.

Windows creates the Harmonic virtual directory.
Appendix C
Standard ES Types and Descriptors

C.1 Standard Elementary Stream (ES) Types

The following standards are used to define types of elementary stream:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>ITU-T</td>
</tr>
<tr>
<td>0x1</td>
<td>ISO/IEC 11172 Video</td>
</tr>
<tr>
<td>0x2</td>
<td>ITU-T Rec. H.262</td>
</tr>
<tr>
<td>0x3</td>
<td>ISO/IEC 11172 Audio</td>
</tr>
<tr>
<td>0x4</td>
<td>ISO/IEC 13818-3 Audio</td>
</tr>
<tr>
<td>0x5</td>
<td>ITU-T Rec. H.222.0</td>
</tr>
<tr>
<td>0x6</td>
<td>ITU-T Rec. H.222.0</td>
</tr>
<tr>
<td>0x7</td>
<td>ISO/IEC 13522 MHEG</td>
</tr>
<tr>
<td>0x8</td>
<td>ITU-T Rec. H.222.0</td>
</tr>
<tr>
<td>0x9</td>
<td>ITU-T Rec. H.222.1</td>
</tr>
<tr>
<td>0xA</td>
<td>ISO/IEC 13818-6 type A</td>
</tr>
<tr>
<td>0xB</td>
<td>ISO/IEC 13818-6 type B</td>
</tr>
<tr>
<td>0xC</td>
<td>ISO/IEC 13818-6 type C</td>
</tr>
<tr>
<td>0xD</td>
<td>ISO/IEC 13818-6 type D</td>
</tr>
<tr>
<td>0xE</td>
<td>ISO/IEC 13818-1 auxiliary</td>
</tr>
<tr>
<td>0xF-0x7F</td>
<td>ITU-T Rec. H.222.0</td>
</tr>
<tr>
<td>0x80 - 0xFF</td>
<td>User Private</td>
</tr>
</tbody>
</table>

C.2 Standard ES and Program Descriptors (MPEG)

The following MPEG standards are used to extend the definitions of elementary stream and programs:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2</td>
<td>Video stream descriptor</td>
</tr>
<tr>
<td>0x3</td>
<td>audio stream descriptor</td>
</tr>
<tr>
<td>0x4</td>
<td>hierarchy descriptor</td>
</tr>
</tbody>
</table>
Appendix C Standard ES Types and Descriptors

C.3 Standard ES and Program Descriptors (DVB)

The following DVB standards are used to extend the definitions of elementary stream and programs:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x51</td>
<td>Mosaic descriptor</td>
</tr>
<tr>
<td>0x52</td>
<td>Stream identifier descriptor</td>
</tr>
<tr>
<td>0x56</td>
<td>Teletext descriptor</td>
</tr>
<tr>
<td>0x59</td>
<td>Subtitling descriptor</td>
</tr>
<tr>
<td>0x5F</td>
<td>Private data specifier</td>
</tr>
<tr>
<td>0x60</td>
<td>Service move descriptor</td>
</tr>
<tr>
<td>0x65</td>
<td>CA system descriptor</td>
</tr>
<tr>
<td>0x66</td>
<td>Data broadcast ID descriptor</td>
</tr>
</tbody>
</table>
Appendix D
Control Panel

D.1 Using the Control Panel

You can set preliminary configuration and control the NSG 9000-6G unit via its front panel. The front panel includes a control panel comprised of a Liquid Crystal Display (LCD) and six buttons as the following figure shows:

D.1.1 Control Panel Display

The 2-line, 16-character control panel display shows the screens, sub-screens, sub-screen options, error messages, warnings and alarms. The control panel display is comprised of two lines:

Line 1 - displays the name of the current screen/sub-screen or selected option.

Line 2 - displays the parameter value and all editing tasks are performed in this line. In editing mode the cursor is blinking to indicate the selected character.

D.1.2 Control Panel Screen Concept

The control panel screens are organized in a hierarchical fashion to indicate that a main screen contains sub-screens and sub-screen options. You may access a sub-screen only via its main screen. The available main screens are as follows:

Power Up screen - A main screen that appears as soon as the NSG 9000-6G boots up and after a thirty minutes of inactivity. The screen shows the company’s name, NSG 9000-6G type and IP address.

Network Config screen - allows to access sub-screens for ETH configuration.

Setup screen - allows to reset the device.

Alarm screen - displays the last active alarm or warning. You can browse through the alarms to view them.

Product Information screen - via its sub-screens you can view information about the NSG 9000-6G.
The following table lists the main screens, their browsing sequence, sub-screens and their options:

<table>
<thead>
<tr>
<th>Screen</th>
<th>Browsing Sequence</th>
<th>Sub-Sequence</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Config</td>
<td>Down - Alarms</td>
<td>ETH1 IP</td>
<td>Edit ETH1</td>
</tr>
<tr>
<td></td>
<td>Up - Product Info.</td>
<td>ETH2 IP</td>
<td>Edit ETH2</td>
</tr>
<tr>
<td>Alarms</td>
<td>Down - Setup</td>
<td>Active alarms and warnings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Up - Network Config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setup</td>
<td>Down - Product Info.</td>
<td>Up - Alarms</td>
<td>Reset device</td>
</tr>
<tr>
<td>Product Info.</td>
<td>Down - Network Config</td>
<td>Up - Setup</td>
<td>Chassis Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DGboard Info.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GbE Info.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Software Information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Control panel hotkeys help</td>
</tr>
</tbody>
</table>

**D.1.2.1 Moving along the Screens**

To move along the screens and sub-screens of the control panel, use the following buttons of the control panel keypad:

<table>
<thead>
<tr>
<th>Button</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up &amp; Down</td>
<td>● browse through the screens/sub-screens.</td>
</tr>
<tr>
<td></td>
<td>● browse through sub-screen options.</td>
</tr>
<tr>
<td></td>
<td>● while editing, browse through numerical characters.</td>
</tr>
<tr>
<td>Left &amp; Right</td>
<td>while editing, move the cursor along the line.</td>
</tr>
<tr>
<td>Enter</td>
<td>● executes a selection of a screen/sub screen and of its available options.</td>
</tr>
<tr>
<td></td>
<td>● quits an editing session and applies changes.</td>
</tr>
<tr>
<td>Esc</td>
<td>● moves up a menu level.</td>
</tr>
<tr>
<td></td>
<td>● quits an editing session without applying changes.</td>
</tr>
</tbody>
</table>

**D.1.2.2 Hotkeys**

The hotkeys are a combination of up to three keys pressed simultaneously. The following table lists the available hotkeys and describes their functionality:

<table>
<thead>
<tr>
<th>Hotkeys</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Esc&gt; &amp; &lt;Enter&gt;</td>
<td>Moves you to the screen at the top of the sequence.</td>
</tr>
</tbody>
</table>
### D.1.3 Configuring Device Parameters

Configure the NSG 9000-6G unit only after boot up. The control panel allows you to configure the following:

- IP address, subnet mask and gateway of ETH1
- IP address and subnet mask of ETH2

To configure various parameters and to apply the changes, you are required to enter a password. This limitation allows authorized users only to change the NSG 9000-6G settings. The password is the following sequence of buttons: Left-Right Left-Right Up-Down Enter.

To configure device parameters:

1. Navigate to the required parameter and click <Enter> twice.
2. Enter the password.
   The screen name changes to Edit (screen name). A blinking cursor appears on the first character of the second line of the screen.

3. Start editing.

### Hotkeys

<table>
<thead>
<tr>
<th>Hotkeys</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| ![Reset NSG](image) | Reset NSG
| ![Increase contrast](image) | Increases the contrast of the display area. Press the Up key, until the required contrast is achieved. |
| ![Decrease contrast](image) | Decreases the contrast of the display area. Press the Down key, until the required contrast is achieved. |
| ![Clear entry field](image) | While editing, clears the entry field and moves cursor to the bottom left. |

![Hotkeys diagram](image)
4. Do one of the following:
   - To quit the editing session and to apply changes, click <Enter>.
     The screen name appears without the word “Edit”.
     The newly configured parameter appears in the second line of the screen.

   - To quit the editing session without applying the changes, click <Esc>.
     The screen name appears without the word “Edit”.
     Unchanged parameters appear in the second line of the screen.

### D.1.4 Reset the NSG 9000-6G Unit

Via the control panel you may reset the NSG 9000-6G unit when required.

To reset the NSG 9000-6G unit:

- Do either of the following:
  - Navigate to the Reset NSG 9000-6G sub-screen of the Setup main screen and click <enter>,
  - Or,
  - Press <Esc> & Left & Right arrow for at least 3 seconds. Confirm with Right arrow.
  - Once boot up starts, the control panel displays the same messages as during power up.
  - If BOOTP is enabled, an additional message appears indicating that the NSG 9000-6G
  - connects to the BOOTP server.

### D.1.5 Viewing NSG 9000-6G Parameters

The control panel allows to view the following NSG 9000-6G parameters:

- Alarms and Warnings - up to 100 alarms/warnings
- Product Information
- Control panel hotkeys

#### D.1.5.1 Viewing Alarms/Warnings

You may browse through the alarms/warnings to view them. If an alarm/warning is cancelled,
it disappears from the screen and the following alarm/warning is presented. If there are no
alarms/warnings, the message “No alarms/Warn” appears. You can view up to 100 alarms/
warnings.

To monitor alarms/Warnings

1. Navigate to the Alarm screen.
   The screen displays the number of alarms and warnings (from left to right)
2. Click <Enter>.
3. Browse through the alarms/warnings, using the <Down or Up> keys.
When a warning is displayed, the following sign appears at the top right corner of the LCD display: (W).

D.1.5.2 Viewing ETH ports MAC Address

✍ To monitor the ETH1 MAC Address

1. Navigate to the Network Config screen and click <Enter>. The Ethernet Port 1 screen appears.
2. Click <Enter>. The ETH1 IP Address screen appears.
3. Click <Down or Up> until the ETH1 MAC Address screen appears.

✍ To monitor the ETH2 MAC Address

1. Navigate to the Network Config screen and click <Enter>. The Ethernet Port 1 screen appears.
2. Click <Down or Up> to open the Ethernet Port 2 screen.
3. Once the Ethernet Port 2 screen appears, click <Enter>.
4. Click <Down or Up> until the ETH2 MAC Address screen appears.

D.1.5.3 Viewing Product Information

The Product Information screen is related to the following sub-screens:

- Chassis Info - view the serial number of the chassis
- DGBoard Info - view the DGBoard serial number and DGBoard FPGA number
- GbE Info - view GbE FPGA Version
- Software Info - view firmware version
- LCD Hotkeys Help - allows to view the various available hotkeys

✍ To view product information

1. Navigate to the Product Info. screen.
2. Click <Enter>.
3. Browse through the sub-screens and their related options using the <Down or Up> and <Enter> keys.

D.1.5.4 Viewing Hotkeys

1. Navigate to the Product Information screen.
2. Click <Enter>.
3. Click <Down or Up> until the Hotkey screen appears.
4. Click <Enter>.
5. Click <Down or Up> to view the hotkeys.
E.1  EIA SDT and HRC Standards

The EIA (Electronic Industries Association) sets internationally recognized standards for standard frequencies (EIA SDT) and for Harmonic related carriers (EIA HRC).

Table 6-6: EIA SDT and HRC

<table>
<thead>
<tr>
<th>EIA Channel Number</th>
<th>STD (Zero Offset) MHz</th>
<th>HRC MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-------</td>
<td>73.7500</td>
</tr>
<tr>
<td>2</td>
<td>57.0000</td>
<td>55.7500</td>
</tr>
<tr>
<td>3</td>
<td>63.0000</td>
<td>61.7500</td>
</tr>
<tr>
<td>4</td>
<td>69.0000</td>
<td>67.7500</td>
</tr>
<tr>
<td>5</td>
<td>79.0000</td>
<td>79.7500</td>
</tr>
<tr>
<td>6</td>
<td>85.0000</td>
<td>85.7500</td>
</tr>
<tr>
<td>7</td>
<td>177.0000</td>
<td>175.7500</td>
</tr>
<tr>
<td>8</td>
<td>183.0000</td>
<td>181.7500</td>
</tr>
<tr>
<td>9</td>
<td>189.0000</td>
<td>187.7500</td>
</tr>
<tr>
<td>10</td>
<td>195.0000</td>
<td>193.7500</td>
</tr>
<tr>
<td>11</td>
<td>201.0000</td>
<td>199.7500</td>
</tr>
<tr>
<td>12</td>
<td>207.0000</td>
<td>205.7500</td>
</tr>
<tr>
<td>13</td>
<td>213.0000</td>
<td>211.7500</td>
</tr>
<tr>
<td>14</td>
<td>123.0000</td>
<td>121.7500</td>
</tr>
<tr>
<td>15</td>
<td>129.0000</td>
<td>127.7500</td>
</tr>
<tr>
<td>16</td>
<td>135.0000</td>
<td>133.7500</td>
</tr>
<tr>
<td>17</td>
<td>141.0000</td>
<td>139.7500</td>
</tr>
<tr>
<td>18</td>
<td>147.0000</td>
<td>145.7500</td>
</tr>
<tr>
<td>19</td>
<td>153.0000</td>
<td>151.7500</td>
</tr>
<tr>
<td>20</td>
<td>159.0000</td>
<td>157.7500</td>
</tr>
<tr>
<td>21</td>
<td>165.0000</td>
<td>163.7500</td>
</tr>
<tr>
<td>22</td>
<td>171.0000</td>
<td>169.7500</td>
</tr>
<tr>
<td>23</td>
<td>219.0000</td>
<td>217.7500</td>
</tr>
<tr>
<td>24</td>
<td>225.0000</td>
<td>223.7500</td>
</tr>
<tr>
<td>25</td>
<td>231.0000</td>
<td>229.7500</td>
</tr>
<tr>
<td>EIA Channel Number</td>
<td>STD (Zero Offset) MHz</td>
<td>HRC MHz</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>26</td>
<td>237.0000</td>
<td>235.7500</td>
</tr>
<tr>
<td>27</td>
<td>243.0000</td>
<td>241.7500</td>
</tr>
<tr>
<td>28</td>
<td>249.0000</td>
<td>247.7500</td>
</tr>
<tr>
<td>29</td>
<td>255.0000</td>
<td>253.7500</td>
</tr>
<tr>
<td>30</td>
<td>261.0000</td>
<td>259.7500</td>
</tr>
<tr>
<td>31</td>
<td>267.0000</td>
<td>265.7500</td>
</tr>
<tr>
<td>32</td>
<td>273.0000</td>
<td>271.7500</td>
</tr>
<tr>
<td>33</td>
<td>279.0000</td>
<td>277.7500</td>
</tr>
<tr>
<td>34</td>
<td>285.0000</td>
<td>283.7500</td>
</tr>
<tr>
<td>35</td>
<td>291.0000</td>
<td>289.7500</td>
</tr>
<tr>
<td>36</td>
<td>297.0000</td>
<td>295.7500</td>
</tr>
<tr>
<td>37</td>
<td>303.0000</td>
<td>301.7500</td>
</tr>
<tr>
<td>38</td>
<td>309.0000</td>
<td>307.7500</td>
</tr>
<tr>
<td>39</td>
<td>315.0000</td>
<td>313.7500</td>
</tr>
<tr>
<td>40</td>
<td>321.0000</td>
<td>319.7500</td>
</tr>
<tr>
<td>41</td>
<td>327.0000</td>
<td>325.7500</td>
</tr>
<tr>
<td>42</td>
<td>333.0000</td>
<td>331.7500</td>
</tr>
<tr>
<td>43</td>
<td>339.0000</td>
<td>337.7500</td>
</tr>
<tr>
<td>44</td>
<td>345.0000</td>
<td>343.7500</td>
</tr>
<tr>
<td>45</td>
<td>351.0000</td>
<td>349.7500</td>
</tr>
<tr>
<td>46</td>
<td>357.0000</td>
<td>355.7500</td>
</tr>
<tr>
<td>47</td>
<td>363.0000</td>
<td>361.7500</td>
</tr>
<tr>
<td>48</td>
<td>369.0000</td>
<td>367.7500</td>
</tr>
<tr>
<td>49</td>
<td>375.0000</td>
<td>373.7500</td>
</tr>
<tr>
<td>50</td>
<td>381.0000</td>
<td>379.7500</td>
</tr>
<tr>
<td>51</td>
<td>387.0000</td>
<td>385.7500</td>
</tr>
<tr>
<td>52</td>
<td>393.0000</td>
<td>391.7500</td>
</tr>
<tr>
<td>53</td>
<td>399.0000</td>
<td>397.7500</td>
</tr>
<tr>
<td>54</td>
<td>405.0000</td>
<td>403.7500</td>
</tr>
<tr>
<td>55</td>
<td>411.0000</td>
<td>409.7500</td>
</tr>
<tr>
<td>56</td>
<td>417.0000</td>
<td>415.7500</td>
</tr>
<tr>
<td>EIA Channel Number</td>
<td>STD (Zero Offset) MHz</td>
<td>HRC MHz</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>57</td>
<td>423.0000</td>
<td>421.7500</td>
</tr>
<tr>
<td>58</td>
<td>429.0000</td>
<td>427.7500</td>
</tr>
<tr>
<td>59</td>
<td>435.0000</td>
<td>433.7500</td>
</tr>
<tr>
<td>60</td>
<td>441.0000</td>
<td>439.7500</td>
</tr>
<tr>
<td>61</td>
<td>447.0000</td>
<td>445.7500</td>
</tr>
<tr>
<td>62</td>
<td>453.0000</td>
<td>451.7500</td>
</tr>
<tr>
<td>63</td>
<td>459.0000</td>
<td>457.7500</td>
</tr>
<tr>
<td>64</td>
<td>465.0000</td>
<td>463.7500</td>
</tr>
<tr>
<td>65</td>
<td>471.0000</td>
<td>469.7500</td>
</tr>
<tr>
<td>66</td>
<td>477.0000</td>
<td>475.7500</td>
</tr>
<tr>
<td>67</td>
<td>483.0000</td>
<td>481.7500</td>
</tr>
<tr>
<td>68</td>
<td>489.0000</td>
<td>487.7500</td>
</tr>
<tr>
<td>69</td>
<td>495.0000</td>
<td>493.7500</td>
</tr>
<tr>
<td>70</td>
<td>501.0000</td>
<td>499.7500</td>
</tr>
<tr>
<td>71</td>
<td>507.0000</td>
<td>505.7500</td>
</tr>
<tr>
<td>72</td>
<td>513.0000</td>
<td>511.7500</td>
</tr>
<tr>
<td>73</td>
<td>519.0000</td>
<td>517.7500</td>
</tr>
<tr>
<td>74</td>
<td>525.0000</td>
<td>523.7500</td>
</tr>
<tr>
<td>75</td>
<td>531.0000</td>
<td>529.7500</td>
</tr>
<tr>
<td>76</td>
<td>537.0000</td>
<td>535.7500</td>
</tr>
<tr>
<td>77</td>
<td>543.0000</td>
<td>541.7500</td>
</tr>
<tr>
<td>78</td>
<td>549.0000</td>
<td>547.7500</td>
</tr>
<tr>
<td>79</td>
<td>555.0000</td>
<td>553.7500</td>
</tr>
<tr>
<td>80</td>
<td>561.0000</td>
<td>559.7500</td>
</tr>
<tr>
<td>81</td>
<td>567.0000</td>
<td>565.7500</td>
</tr>
<tr>
<td>82</td>
<td>573.0000</td>
<td>571.7500</td>
</tr>
<tr>
<td>83</td>
<td>579.0000</td>
<td>577.7500</td>
</tr>
<tr>
<td>84</td>
<td>585.0000</td>
<td>583.7500</td>
</tr>
<tr>
<td>85</td>
<td>591.0000</td>
<td>589.7500</td>
</tr>
<tr>
<td>86</td>
<td>597.0000</td>
<td>595.7500</td>
</tr>
<tr>
<td>87</td>
<td>603.0000</td>
<td>601.7500</td>
</tr>
</tbody>
</table>
Table 6-6: EIA SDT and HRC

<table>
<thead>
<tr>
<th>EIA Channel Number</th>
<th>STD (Zero Offset) MHz</th>
<th>HRC MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>609.0000</td>
<td>607.7500</td>
</tr>
<tr>
<td>89</td>
<td>615.0000</td>
<td>613.7500</td>
</tr>
<tr>
<td>90</td>
<td>621.0000</td>
<td>619.7500</td>
</tr>
<tr>
<td>91</td>
<td>627.0000</td>
<td>625.7500</td>
</tr>
<tr>
<td>92</td>
<td>633.0000</td>
<td>631.7500</td>
</tr>
<tr>
<td>93</td>
<td>639.0000</td>
<td>637.7500</td>
</tr>
<tr>
<td>94</td>
<td>645.0000</td>
<td>643.7500</td>
</tr>
<tr>
<td>95</td>
<td>93.0000</td>
<td>91.7500</td>
</tr>
<tr>
<td>96</td>
<td>99.0000</td>
<td>97.7500</td>
</tr>
<tr>
<td>97</td>
<td>105.0000</td>
<td>103.7500</td>
</tr>
<tr>
<td>98</td>
<td>111.0000</td>
<td>109.7500</td>
</tr>
<tr>
<td>99</td>
<td>117.0000</td>
<td>115.7500</td>
</tr>
<tr>
<td>100</td>
<td>651.0000</td>
<td>649.7500</td>
</tr>
<tr>
<td>101</td>
<td>657.0000</td>
<td>655.7500</td>
</tr>
<tr>
<td>102</td>
<td>663.0000</td>
<td>661.7500</td>
</tr>
<tr>
<td>103</td>
<td>669.0000</td>
<td>667.7500</td>
</tr>
<tr>
<td>104</td>
<td>675.0000</td>
<td>673.7500</td>
</tr>
<tr>
<td>105</td>
<td>681.0000</td>
<td>679.7500</td>
</tr>
<tr>
<td>106</td>
<td>687.0000</td>
<td>685.7500</td>
</tr>
<tr>
<td>107</td>
<td>693.0000</td>
<td>691.7500</td>
</tr>
<tr>
<td>108</td>
<td>699.0000</td>
<td>697.7500</td>
</tr>
<tr>
<td>109</td>
<td>705.0000</td>
<td>703.7500</td>
</tr>
<tr>
<td>110</td>
<td>711.0000</td>
<td>709.7500</td>
</tr>
<tr>
<td>111</td>
<td>717.0000</td>
<td>715.7500</td>
</tr>
<tr>
<td>112</td>
<td>723.0000</td>
<td>721.7500</td>
</tr>
<tr>
<td>113</td>
<td>729.0000</td>
<td>727.7500</td>
</tr>
<tr>
<td>114</td>
<td>735.0000</td>
<td>733.7500</td>
</tr>
<tr>
<td>115</td>
<td>741.0000</td>
<td>739.7500</td>
</tr>
<tr>
<td>116</td>
<td>747.0000</td>
<td>745.7500</td>
</tr>
<tr>
<td>117</td>
<td>753.0000</td>
<td>751.7500</td>
</tr>
<tr>
<td>118</td>
<td>759.0000</td>
<td>757.7500</td>
</tr>
</tbody>
</table>
Table 6-6: EIA SDT and HRC

<table>
<thead>
<tr>
<th>EIA Channel Number</th>
<th>STD (Zero Offset) MHz</th>
<th>HRC MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>119</td>
<td>765.0000</td>
<td>763.7500</td>
</tr>
<tr>
<td>120</td>
<td>771.0000</td>
<td>769.7500</td>
</tr>
<tr>
<td>121</td>
<td>777.0000</td>
<td>775.7500</td>
</tr>
<tr>
<td>122</td>
<td>783.0000</td>
<td>781.7500</td>
</tr>
<tr>
<td>123</td>
<td>789.0000</td>
<td>787.7500</td>
</tr>
<tr>
<td>124</td>
<td>795.0000</td>
<td>793.7500</td>
</tr>
<tr>
<td>125</td>
<td>801.0000</td>
<td>799.7500</td>
</tr>
<tr>
<td>126</td>
<td>807.0000</td>
<td>805.7500</td>
</tr>
<tr>
<td>127</td>
<td>813.0000</td>
<td>811.7500</td>
</tr>
<tr>
<td>128</td>
<td>819.0000</td>
<td>817.7500</td>
</tr>
<tr>
<td>129</td>
<td>825.0000</td>
<td>823.7500</td>
</tr>
<tr>
<td>130</td>
<td>831.0000</td>
<td>829.7500</td>
</tr>
<tr>
<td>131</td>
<td>837.0000</td>
<td>835.7500</td>
</tr>
<tr>
<td>132</td>
<td>843.0000</td>
<td>841.7500</td>
</tr>
<tr>
<td>133</td>
<td>849.0000</td>
<td>847.7500</td>
</tr>
<tr>
<td>134</td>
<td>855.0000</td>
<td>853.7500</td>
</tr>
<tr>
<td>135</td>
<td>861.0000</td>
<td>859.7500</td>
</tr>
<tr>
<td>136</td>
<td>867.0000</td>
<td>865.7500</td>
</tr>
<tr>
<td>137</td>
<td>873.0000</td>
<td>871.7500</td>
</tr>
<tr>
<td>138</td>
<td>879.0000</td>
<td>877.7500</td>
</tr>
<tr>
<td>139</td>
<td>885.0000</td>
<td>883.7500</td>
</tr>
<tr>
<td>140</td>
<td>891.0000</td>
<td>889.7500</td>
</tr>
<tr>
<td>141</td>
<td>897.0000</td>
<td>895.7500</td>
</tr>
<tr>
<td>142</td>
<td>903.0000</td>
<td>901.7500</td>
</tr>
<tr>
<td>143</td>
<td>909.0000</td>
<td>907.7500</td>
</tr>
<tr>
<td>144</td>
<td>915.0000</td>
<td>913.7500</td>
</tr>
<tr>
<td>145</td>
<td>921.0000</td>
<td>919.7500</td>
</tr>
<tr>
<td>146</td>
<td>927.0000</td>
<td>925.7500</td>
</tr>
<tr>
<td>147</td>
<td>933.0000</td>
<td>931.7500</td>
</tr>
<tr>
<td>148</td>
<td>939.0000</td>
<td>937.7500</td>
</tr>
<tr>
<td>149</td>
<td>945.0000</td>
<td>943.7500</td>
</tr>
<tr>
<td>EIA Channel Number</td>
<td>STD (Zero Offset) MHz</td>
<td>HRC MHz</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>150</td>
<td>951.000</td>
<td>949.7500</td>
</tr>
<tr>
<td>151</td>
<td>957.000</td>
<td>955.7500</td>
</tr>
<tr>
<td>152</td>
<td>963.000</td>
<td>961.7500</td>
</tr>
<tr>
<td>153</td>
<td>969.000</td>
<td>967.7500</td>
</tr>
<tr>
<td>154</td>
<td>975.000</td>
<td>973.7500</td>
</tr>
<tr>
<td>155</td>
<td>981.000</td>
<td>979.7500</td>
</tr>
<tr>
<td>156</td>
<td>987.000</td>
<td>985.7500</td>
</tr>
<tr>
<td>157</td>
<td>993.000</td>
<td>991.7500</td>
</tr>
<tr>
<td>158</td>
<td>999.000</td>
<td>997.7500</td>
</tr>
</tbody>
</table>