









Cisco RF Gateway 1 Configuration Guide

For Your Safety

Explanation of Warning and Caution Icons

Avoid personal injury and product damage! Do not proceed beyond any symbol until you fully understand the indicated conditions.

The following warning and caution icons alert you to important information about the safe operation of this product:

-  You may find this symbol in the document that accompanies this product. This symbol indicates important operating or maintenance instructions.
-  You may find this symbol affixed to the product. This symbol indicates a live terminal where a dangerous voltage may be present; the tip of the flash points to the terminal device.
-  You may find this symbol affixed to the product. This symbol indicates a protective ground terminal.
-  You may find this symbol affixed to the product. This symbol indicates a chassis terminal (normally used for equipotential bonding).
-  You may find this symbol affixed to the product. This symbol warns of a potentially hot surface.
-  You may find this symbol affixed to the product and in this document. This symbol indicates an infrared laser that transmits intensity-modulated light and emits invisible laser radiation or an LED that transmits intensity-modulated light.

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco RF Gateway 1 contains, in part, certain free/open source software ("Free Software") under licenses which generally make the source code available for free copy, modification, and redistribution. Examples of such licenses include all the licenses sponsored by the Free Software Foundation (e.g. GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Berkeley Software Distribution (BSD), the MIT licenses and different versions of the Mozilla and Apache licenses). To find additional information regarding the Free Software, including a copy of the applicable license and related information, please go to http://www.cisco.com/en/US/products/ps8360/products_licensing_information_list.html. If you have any questions or problems accessing any of the links, please contact: spvtg-external-opensource-requests@cisco.com.

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

© 2008-2014 Cisco and/or its affiliates. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

Important Safety Instructions	ix
Laser Safety	xix
Chapter 1 Introduction	1
Chapter 2 RF Gateway 1 Configuration Quick Start	3
Configuring the IP Address Through the Front Panel	4
Connecting the RF Gateway 1 Using a Web Browser.....	5
Changing Device Settings	6
Configuring the Device Name	6
Configuring the Annex	7
Configuring the Clock.....	8
Configuring IP Network Settings	10
Configuring Management Port (10/100) IP Address, Subnet Mask and Default Gateway	10
Network Connectivity Testing.....	14
Configuring Static Routes.....	14
Configuring QAM Output.....	15
Card Presence.....	16
Enabling QAM Port.....	16
Carrier Parameters.....	17
Channel Application Mode	20
Configuring VOD Parameters.....	21
Ingress All VoD.....	21
Video Session Timeout.....	22
Chapter 3 General Configuration and Monitoring	25
QAM Annex and Frequency Plan Configuration	26
QAM Card Configuration.....	28
Global RF Port Configuration	28
QAM Card View	29
QAM RF Port Configuration.....	30
Global QAM Channel Configuration.....	31
QAM Channel Level Configuration.....	33
GbE Interface Configuration	35
GbE Interface Operation Modes	35

Contents

Configuring GbE Interface Settings	42
Configuring GbE Port Operational Mode	42
Configuring the Video/Data IP Address for GbE Port Pair Mode.....	43
Configuring Redundancy for Port Pair Mode	45
Configuring Reversion of Multicast Streams to Primary Port	46
ARP and Route Configuration	48
Clock Configuration	49
Real -Time Clock Setup	49
Simple Network Time Protocol (SNTP).....	50
Monitoring the RF Gateway 1	53
Summary Tab	53
Monitor Tab	54
Fault Management of the RF Gateway 1	65
System Alarms.....	65
System Events.....	67
User Notification of Alarms and Events.....	68
Configuration Management	74
Configuration Save	74
Configuration Backup	74
Configuration Restore	75
Release Management.....	77
Downloading System Release Images	78
Configuring, Monitoring, and Fault Management via SNMP	80
Monitoring Capability.....	81

Chapter 4 Table-Based Video Specific Operation 83

Provisioning.....	84
Channel Application Mode	84
Video Stream Map Configuration	84
Automated Video Stream Map Configuration	87
Advanced Settings.....	89
Advanced Rules for Advanced Settings	93
MPTS Pass-Through Mode of Operation	95
Enabling UDTA.....	96
Status Monitoring	97
Introduction.....	97
Monitoring	97

Chapter 5 Switched Digital Video Specific Operation 99

Provisioning.....	100
Prerequisite Configurations:	100
Channel Application Mode	100
SRM Configuration.....	100
Legacy Mode	101

QAM Channel Configuration	101
Status Monitoring	103
Chapter 6 Wideband Data Specific Operation	105
Provisioning.....	106
Channel Application Mode	106
Data Map Configuration.....	106
Status Monitoring	109
Introduction.....	109
Monitoring.....	109
Chapter 7 Basic M-CMTS Data Specific Operation	113
Provisioning.....	114
Channel Application Mode	114
Data Map Configuration.....	114
Connecting to DTI Server	116
Status Monitoring	119
Introduction.....	119
Monitoring.....	119
Chapter 8 M-CMTS Data DEPI-CP Operation	127
Provisioning.....	128
Channel Application Mode	129
Depi-Remote.....	129
DEPI-Learn	129
Status Monitoring	131
Monitoring.....	131
DEPI Feature Highlights.....	138
Chapter 9 Remapping Unreferenced PIDS	139
Enabling the Feature.....	140
Feature Page	141
Adding Entries to the Remap Table	142
Blocked Unreferenced PIDS	143
Enabling Insert External PAT.....	144
Operator Responsibilities.....	145
PID Remapping.....	145
Inserting External PAT.....	145
Chapter 10 Alarm Configuration	147
Configuring Alarm Settings	148
Alarm Details.....	148

Chapter 11 Variable Fan Speed	151
GUI Feature Option	152
Feature Design Details	153
Chapter 12 Licensing	155
Applications Requiring a Software License	156
Obtaining a License File	157
Installing and Activating a License	161
To Install a License.....	161
To Activate a License.....	162
Secure License Transfer.....	163
Start License Transfer	163
Complete License Transfer	166
Chapter 13 Encryption and Scrambling	169
Introduction	170
Scrambling, Control Word, and Cryptoperiod.....	171
Access Criteria and Access Rights.....	172
Entitlement Control Messages	173
Event Information Scheduler	174
Scrambling Levels	175
Elementary Stream Level Scrambling.....	175
Service Level Scrambling.....	176
Simulcrypt Scrambling.....	177
Timing Parameters.....	178
Steps To Take.....	180
Configuring Broadcast Scrambling and Dual Encryption Broadcast.....	180
Configuring Scrambling General Settings.....	182
Configuring Scrambling Specific Parameters	183
Chapter 14 Security Features	201
Security Features Overview	202
Authentication.....	203
Authentication Configuration.....	203
Remote Authentication	207
Password Recovery.....	209
Enabling HTTPS on the RF Gateway 1	210
Steps for Enabling HTTPS	210
SFTP Support.....	218
GUI Changes for SFTP	218
System Tab Changes.....	218

Installing SFTP	219
Uninstalling SFTP	221
Firewall Settings.....	223

Chapter 15 96 QAM Channel Software 225

Licensing	226
Release Management.....	227
Upgrades.....	227
Revert.....	228
Configuration Management	229
Backup	229
Restore	229
Operational Considerations	230
QAM Configuration	230
Map Configuration	232
Monitoring.....	234
Network Management	235

Chapter 16 NGOD Specific Operation 237

Provisioning.....	238
Channel Application Mode	238
NGOD Settings.....	238
D6/R6 Communication	239
Status Monitoring	241
Troubleshooting.....	242
Logs.....	243

Chapter 17 Customer Information 247

Appendix A Technical Specifications 249

General Specifications	250
Introduction.....	250
Environmental Specifications.....	250
Chassis Mechanical Specifications.....	250
Physical.....	250
Power Supply Specifications.....	251
Electrical Specifications.....	252
GbE Input Interface	252
Management Interface.....	252
DTI Interface.....	252
RF Outputs.....	252
Signal Specifications	253
Specifications Optical Types SFP Modules	254

Contents

Electrical GbE SFP Transceiver	254
Glossary	255
Index	259

Important Safety Instructions

Read these instructions. Keep these instructions. Heed all warnings. Follow all instructions. Only use attachments/accessories specified by the manufacturer.

Read and Retain Instructions

Carefully read all safety and operating instructions before operating this equipment, and retain them for future reference.

Follow Instructions and Heed Warnings

Follow all operating and use instructions. Pay attention to all warnings and cautions in the operating instructions, as well as those that are affixed to this equipment.

Terminology

The terms defined below are used in this document. The definitions given are based on those found in safety standards.

Service Personnel - The term *service personnel* applies to trained and qualified individuals who are allowed to install, replace, or service electrical equipment. The service personnel are expected to use their experience and technical skills to avoid possible injury to themselves and others due to hazards that exist in service and restricted access areas.

User and Operator - The terms *user* and *operator* apply to persons other than service personnel.

Ground(ing) and Earth(ing) - The terms *ground(ing)* and *earth(ing)* are synonymous. This document uses *ground(ing)* for clarity, but it can be interpreted as having the same meaning as *earth(ing)*.

Electric Shock Hazard

This equipment meets applicable safety standards.



WARNING:

To reduce risk of electric shock, perform only the instructions that are included in the operating instructions. Refer all servicing to qualified service personnel only.

Electric shock can cause personal injury or even death. Avoid direct contact with dangerous voltages at all times. The protective ground connection, where provided, is essential to safe operation and must be verified before connecting the power supply.

Important Safety Instructions

Know the following safety warnings and guidelines:

- Dangerous Voltages
 - Only qualified service personnel are allowed to perform equipment installation or replacement.
 - Only qualified service personnel are allowed to remove chassis covers and access any of the components inside the chassis.
- Grounding
 - Do not violate the protective grounding by using an extension cable, power cable, or autotransformer without a protective ground conductor.
 - Take care to maintain the protective grounding of this equipment during service or repair and to re-establish the protective grounding before putting this equipment back into operation.

Installation Site

When selecting the installation site, comply with the following:

- **Protective Ground** - The protective ground lead of the building's electrical installation should comply with national and local requirements.
- **Environmental Condition** - The installation site should be dry, clean, and ventilated. Do not use this equipment where it could be at risk of contact with water. Ensure that this equipment is operated in an environment that meets the requirements as stated in this equipment's technical specifications, which may be found on this equipment's data sheet.

Installation Requirements



WARNING:

Allow only qualified service personnel to install this equipment. The installation must conform to all local codes and regulations.

Equipment Placement



WARNING:

Avoid personal injury and damage to this equipment. An unstable mounting surface may cause this equipment to fall.

To protect against equipment damage or injury to personnel, comply with the following:

- Install this equipment in a restricted access location.
- Do not install near any heat sources such as radiators, heat registers, stoves, or

other equipment (including amplifiers) that produce heat.

- Place this equipment close enough to a mains AC outlet to accommodate the length of this equipment's power cord.
- Route all power cords so that people cannot walk on, place objects on, or lean objects against them. This may pinch or damage the power cords. Pay particular attention to power cords at plugs, outlets, and the points where the power cords exit this equipment.
- Use only with a cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with this equipment.
- Make sure the mounting surface or rack is stable and can support the size and weight of this equipment.
- The mounting surface or rack should be appropriately anchored according to manufacturer's specifications. Ensure this equipment is securely fastened to the mounting surface or rack where necessary to protect against damage due to any disturbance and subsequent fall.

Ventilation

This equipment has openings for ventilation to protect it from overheating. To ensure equipment reliability and safe operation, do not block or cover any of the ventilation openings. Install the equipment in accordance with the manufacturer's instructions.

Rack Mounting Safety Precautions

Mechanical Loading

Make sure that the rack is placed on a stable surface. If the rack has stabilizing devices, install these stabilizing devices before mounting any equipment in the rack.



WARNING:

Avoid personal injury and damage to this equipment. Mounting this equipment in the rack should be such that a hazardous condition is not caused due to uneven mechanical loading.

Reduced Airflow

When mounting this equipment in the rack, do not obstruct the cooling airflow through the rack. Be sure to mount the blanking plates to cover unused rack space. Additional components such as combiners and net strips should be mounted at the back of the rack, so that the free airflow is not restricted.



CAUTION:

Installation of this equipment in a rack should be such that the amount of airflow required for safe operation of this equipment is not compromised.

Important Safety Instructions

Elevated Operating Ambient Temperature

Only install this equipment in a humidity- and temperature-controlled environment that meets the requirements given in this equipment's technical specifications.



CAUTION:

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, install this equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.

Handling Precautions

When moving a cart that contains this equipment, check for any of the following possible hazards:



WARNING:



Avoid personal injury and damage to this equipment! Move any equipment and cart combination with care. Quick stops, excessive force, and uneven surfaces may cause this equipment and cart to overturn.

- Use caution when moving this equipment/cart combination to avoid injury from tip-over.
- If the cart does not move easily, this condition may indicate obstructions or cables that may need to be disconnected before moving this equipment to another location.
- Avoid quick stops and starts when moving the cart.
- Check for uneven floor surfaces such as cracks or cables and cords.

Grounding

This section provides instructions for verifying that the equipment is properly grounded.

Safety Plugs (USA Only)

This equipment may be equipped with either a 3-terminal (grounding-type) safety plug or a 2-terminal (polarized) safety plug. The wide blade or the third terminal is provided for safety. Do not defeat the safety purpose of the grounding-type or polarized safety plug.

To properly ground this equipment, follow these safety guidelines:

- **Grounding-Type Plug** - For a 3-terminal plug (one terminal on this plug is a protective grounding pin), insert the plug into a grounded mains, 3-terminal outlet.

Note: This plug fits only one way. If this plug cannot be fully inserted into the outlet, contact an electrician to replace the obsolete 3-terminal outlet.

- **Polarized Plug** - For a 2-terminal plug (a polarized plug with one wide blade and one narrow blade), insert the plug into a polarized mains, 2-terminal outlet in which one socket is wider than the other.

Note: If this plug cannot be fully inserted into the outlet, try reversing the plug. If the plug still fails to fit, contact an electrician to replace the obsolete 2-terminal outlet.

Grounding Terminal

If this equipment is equipped with an external grounding terminal, attach one end of an 18-gauge wire (or larger) to the grounding terminal; then, attach the other end of the wire to a ground, such as a grounded equipment rack.

Safety Plugs (European Union)

- **Class I Mains Powered Equipment** – Provided with a 3-terminal AC inlet and requires connection to a 3-terminal mains supply outlet via a 3-terminal power cord for proper connection to the protective ground.

Note: The equipotential bonding terminal provided on some equipment is not designed to function as a protective ground connection.

- **Class II Mains Powered Equipment** – Provided with a 2-terminal AC inlet that may be connected by a 2-terminal power cord to the mains supply outlet. No connection to the protective ground is required as this class of equipment is provided with double or reinforced and/or supplementary insulation in addition to the basic insulation provided in Class I equipment.

Note: Class II equipment, which is subject to EN 50083-1, is provided with a chassis mounted equipotential bonding terminal. See **Equipotential Bonding** for connection instructions.

Equipotential Bonding

If this equipment is equipped with an external chassis terminal marked with the IEC 60417-5020 chassis icon ()

), the installer should see CENELEC standard EN 50083-1 or IEC standard IEC 60728-11 for correct equipotential bonding connection instructions.

AC Power

Important: If this equipment is a Class I equipment, it must be grounded.

- If this equipment plugs into an outlet, the outlet must be near this equipment, and must be easily accessible.
- Connect this equipment only to the power sources that are identified on the

Important Safety Instructions

equipment-rating label normally located close to the power inlet connector(s).

- This equipment may have two power sources. Be sure to disconnect all power sources before working on this equipment.
- If this equipment **does not** have a main power switch, the power cord connector serves as the disconnect device.
- Always pull on the plug or the connector to disconnect a cable. Never pull on the cable itself.
- Unplug this equipment when unused for long periods of time.

Connection to -48 VDC/-60 VDC Power Sources

If this equipment is DC-powered, refer to the specific installation instructions in this manual or in companion manuals in this series for information on connecting this equipment to nominal -48 VDC/-60 VDC power sources.

Circuit Overload

Know the effects of circuit overloading before connecting this equipment to the power supply.



CAUTION:

Consider the connection of this equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Refer to the information on the equipment-rating label when addressing this concern.

General Servicing Precautions



WARNING:

Avoid electric shock! Opening or removing this equipment's cover may expose you to dangerous voltages.



CAUTION:

These servicing precautions are for the guidance of qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so. Refer all servicing to qualified service personnel.

Be aware of the following general precautions and guidelines:

- **Servicing** - Servicing is required when this equipment has been damaged in any way, such as power supply cord or plug is damaged, liquid has been spilled or objects have fallen into this equipment, this equipment has been exposed to rain or moisture, does not operate normally, or has been dropped.
- **Wristwatch and Jewelry** - For personal safety and to avoid damage of this

equipment during service and repair, do not wear electrically conducting objects such as a wristwatch or jewelry.

- **Lightning** - Do not work on this equipment, or connect or disconnect cables, during periods of lightning.
- **Labels** - Do not remove any warning labels. Replace damaged or illegible warning labels with new ones.
- **Covers** - Do not open the cover of this equipment and attempt service unless instructed to do so in the instructions. Refer all servicing to qualified service personnel only.
- **Moisture** - Do not allow moisture to enter this equipment.
- **Cleaning** - Use a damp cloth for cleaning.
- **Safety Checks** - After service, assemble this equipment and perform safety checks to ensure it is safe to use before putting it back into operation.

Electrostatic Discharge

Electrostatic discharge (ESD) results from the static electricity buildup on the human body and other objects. This static discharge can degrade components and cause failures.

Take the following precautions against electrostatic discharge:

- Use an anti-static bench mat and a wrist strap or ankle strap designed to safely ground ESD potentials through a resistive element.
- Keep components in their anti-static packaging until installed.
- Avoid touching electronic components when installing a module.

Fuse Replacement

To replace a fuse, comply with the following:

- Disconnect the power before changing fuses.
- Identify and clear the condition that caused the original fuse failure.
- Always use a fuse of the correct type and rating. The correct type and rating are indicated on this equipment.

Batteries

This product may contain batteries. Special instructions apply regarding the safe use and disposal of batteries:

Safety

Important Safety Instructions

- Insert batteries correctly. There may be a risk of explosion if the batteries are incorrectly inserted.
- Do not attempt to recharge 'disposable' or 'non-reusable' batteries.
- Please follow instructions provided for charging 'rechargeable' batteries.
- Replace batteries with the same or equivalent type recommended by manufacturer.
- Do not expose batteries to temperatures above 100°C (212°F).

Disposal

- The batteries may contain substances that could be harmful to the environment
- Recycle or dispose of batteries in accordance with the battery manufacturer's instructions and local/national disposal and recycling regulations.



廢電池請回收

- The batteries may contain perchlorate, a known hazardous substance, so special handling and disposal of this product might be necessary. For more information about perchlorate and best management practices for perchlorate-containing substance, see www.dtsc.ca.gov/hazardouswaste/perchlorate.

Modifications

This equipment has been designed and tested to comply with applicable safety, laser safety, and EMC regulations, codes, and standards to ensure safe operation in its intended environment. See this equipment's data sheet for details about regulatory compliance approvals.

Do not make modifications to this equipment. Any changes or modifications could void the user's authority to operate this equipment.

Modifications have the potential to degrade the level of protection built into this equipment, putting people and property at risk of injury or damage. Those persons making any modifications expose themselves to the penalties arising from proven non-compliance with regulatory requirements and to civil litigation for compensation in respect of consequential damages or injury.

Accessories

Use only attachments or accessories specified by the manufacturer.

Electromagnetic Compatibility Regulatory Requirements

This equipment meets applicable electromagnetic compatibility (EMC) regulatory requirements. See this equipment's data sheet for details about regulatory compliance approvals. EMC performance is dependent upon the use of correctly shielded cables of good quality for all external connections, except the power source, when installing this equipment.

- Ensure compliance with cable/connector specifications and associated installation instructions where given elsewhere in this manual.

Otherwise, comply with the following good practices:

- Multi-conductor cables should be of single-braided, shielded type and have conductive connector bodies and backshells with cable clamps that are conductively bonded to the backshell and capable of making 360° connection to the cable shielding. Exceptions from this general rule will be clearly stated in the connector description for the excepted connector in question.
- Ethernet cables should be of single-shielded or double-shielded type.
- Coaxial cables should be of the double-braided shielded type.

EMC Compliance Statements

Where this equipment is subject to USA FCC and/or Industry Canada rules, the following statements apply:

FCC Statement for Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users will be required to correct the interference at their own expense.

Industry Canada - Industrie Canadienne Statement

This apparatus complies with Canadian ICES-003.
Cet appareil est conforme à la norme NMB-003 du Canada.

GENELEC/CISPR Statement with Respect to Class A Information Technology Equipment

This is a Class A equipment. In a domestic environment this equipment may cause radio interference in which case the user may be required to take adequate measures.

Important Safety Instructions

Laser Safety

Introduction

This equipment can be provided with an infrared laser that transmits intensity-modulated light and emits invisible laser radiation.

Warning: Radiation



WARNING:

- **Avoid personal injury!** Use of controls, adjustments, or performance of procedures other than those specified herein may result in hazardous radiation exposure.
 - **Avoid personal injury!** The laser light source on the equipment emits invisible laser radiation. Avoid direct exposure to the laser light source.
 - **Avoid personal injury!** Viewing the laser output with optical instruments (such as eye loupes, magnifiers, or microscopes) within a distance of 100 mm may pose an eye hazard.
- Do not apply power to the equipment if the fiber is unmated or unterminated.
 - Do not stare into an unmated fiber or at any mirror-like surface that could reflect light that is emitted from an unterminated fiber.
 - Do not view an activated fiber with optical instruments (e.g., eye loupes, magnifiers, microscopes).
 - Use safety-approved optical fiber cable to maintain compliance with applicable laser safety requirements.

Warning: Fiber Optic Cables



WARNING:

Avoid personal injury! Qualified service personnel may only perform the procedures in this document. Wear safety glasses and use extreme caution when handling fiber optic cables, particularly during splicing or terminating operations. The thin glass fiber core at the center of the cable is fragile when exposed by the removal of cladding and buffer material. It easily fragments into glass splinters. Using tweezers, place splinters immediately in a sealed waste container and dispose of them safely in accordance with local regulations.

Laser Safety

The following laser safety precautions are applicable to the equipment. According to the type of optical transmitter inside the equipment, there are different laser safety precautions. A laser label that clearly indicates the laser aperture is affixed to the equipment's rear panel.

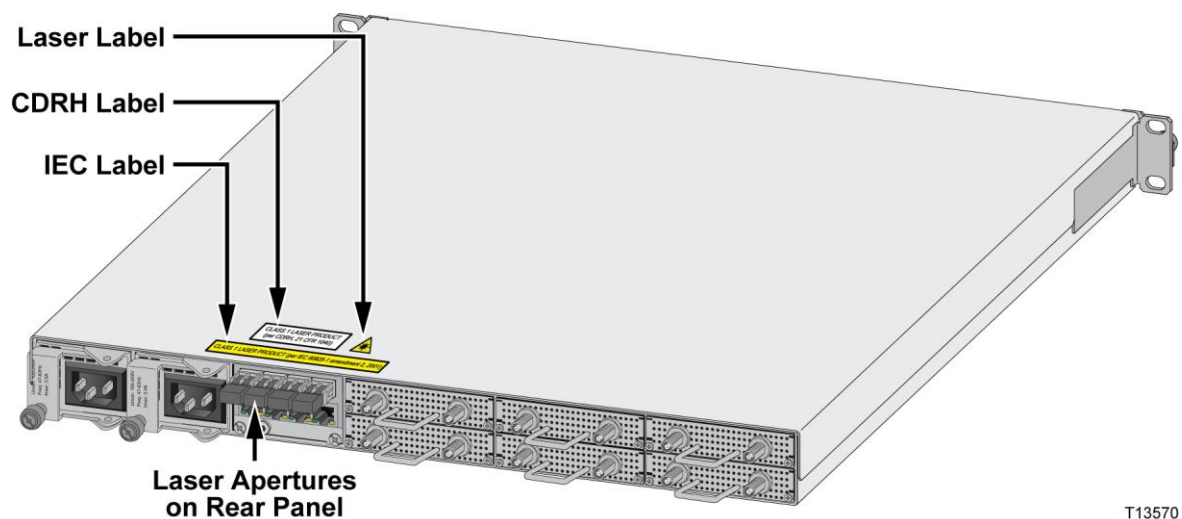


The following illustration displays the location of the laser label.

Depending upon whether you are located in Europe (IEC-standard) or in the U.S. (CDRH-standard), there are different laser safety precautions. For more information about the equipment's laser output, refer to the equipment's data sheet.

Class 1 and Class I Labels

The following illustrations show the class 1 and class I labels attached to the housing, according to the standards.



T13570

In Accordance with the IEC Standard

The Laser type SFP modules used are classified in class 1 laser products according to IEC 60825-1, 1997 amendment 2001.

The label below is attached to the top cover and the package of class 1 laser product.

CLASS 1 LASER PRODUCT (per IEC 60825-1 amendment 2, 2001)

In Accordance with the CDRH Standard

The Laser type SFP modules used are classified in class I laser product per CDRH, 21 CFR 1040 Laser Safety requirements.

For the CDRH standard, a certification label is attached to the top cover of each product classified in class I. See also the product ID label affixed to each product.

CLASS I LASER PRODUCT
(per CDRH, 21 CFR 1040)

1

Introduction

Overview

The Cisco® RF Gateway 1 is a universal edge QAM (U-EQAM) device that offers industry leading performance, and a standards-based solution for video, data, and converged video and data deployments requiring high density and maximum reliability.

Purpose

This configuration guide provides the necessary information to configure the system using the web browser interface.

Who Should Use This Document

This document is intended for authorized service personnel who have experience working with similar equipment. The service personnel should have appropriate background and knowledge to complete the procedures described in this document.

Qualified Personnel

Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product.



WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service this product. Otherwise, personal injury or equipment damage may occur.

Document Version

This is the fifth release of this configuration guide.

2

RF Gateway 1 Configuration Quick Start

This chapter provides the basic information needed to quickly configure the RF Gateway 1 using the web browser user interface.

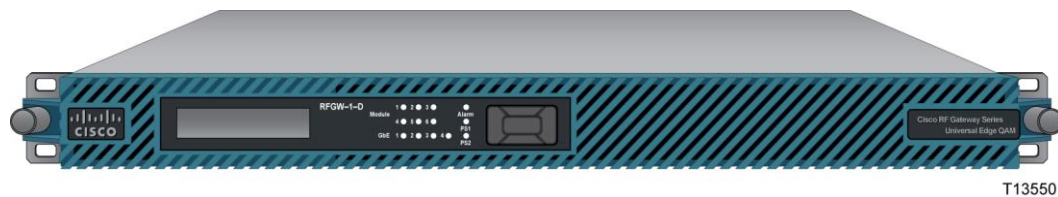
For more information on setting up the RF Gateway 1, see *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01.

In This Chapter

- Configuring the IP Address Through the Front Panel 4
- Connecting the RF Gateway 1 Using a Web Browser..... 5
- Changing Device Settings..... 6
- Configuring IP Network Settings 10
- Network Connectivity Testing..... 14
- Configuring QAM Output..... 15
- Configuring VOD Parameters..... 21

Configuring the IP Address Through the Front Panel

The RF Gateway 1 management port IP address can be configured using the LCD and keypad located on the chassis front panel.



To Configure the Management Port IP Address

- 1 After the system fully initializes, use the keypad to page down until you see the mgmt port IP address.
Note: Use the up/down, left/right buttons for navigation and changes. Use the center button for saving changes.
- 2 Page down to position the cursor in the *IP address* field. Use the left/right keys to navigate the cursor below the numbers you want to change. Use the up/down keys to make changes. Continue until all numbers are configured as desired.
- 3 Use the center key to accept changes and exit the *mgmt port IP address* field.
- 4 Page right to find and configure the management port subnet mask and default gateway. Configure each as desired.
- 5 Once finished, use the center key to enter and save information.
- 6 Reboot the RF Gateway 1. The management port IP address is not dynamically configurable, thus reboot/power-cycle is required after changes.
- 7 The management port IP address can be validated by checking the configuration settings on the LCD after reboot.
Note: Alternatively, the operator can attempt to connect to the web GUI at the new IP address via HTTP after reboot.

Connecting the RF Gateway 1 Using a Web Browser

The RF Gateway 1 can be connected to a web browser. The following browsers/display settings are recommended:

Client Platform	Web Browser	Display Settings
Windows XP	Mozilla Firefox 2.0.0.14 Internet Explorer 6.0	1024x768

Note: Java platform version 1.6.0_x is supported under the recommended browsers.

To Connect the RF Gateway 1

- 1 Connect a network cable to the management port located on the rear panel of the RF Gateway 1 chassis.
- 2 Open a web browser and enter the management port IP address.

Result: The RF Gateway 1 *Summary* page is displayed.



Changing Device Settings

The general configuration settings of the RF Gateway 1 are categorized on the Device Information page. This section provides information on changing the device settings.

Note: Once a setting is entered and you click **Apply**, they become active. The settings must be **saved** in order to preserve them in nonvolatile memory. Software version 1.3.11 has an automatic save feature which allows applied database changes to be automatically saved to preserve them in nonvolatile memory. Saved settings will be retained after a reboot or power cycle. This rule applies across all RF Gateway 1 settings.

Configuring the Device Name

To identify the RF Gateway 1, it is recommended that a unique device name be assigned to the unit.

To Configure the Device Name

- 1 Navigate to the *System/System Configuration* page.

Result: The *Device Information* page is displayed.

The screenshot shows the configuration interface for a device named 'rfgw-1d'. The top navigation bar includes buttons for Login, Reboot, Save, Refresh, and Help, along with a Cisco logo and a timestamp of 14:45:15. Below the navigation bar are tabs for Summary, Monitor, Alarms, QAMS, Maps, and System (which is selected). A left-hand menu titled 'System Configuration' lists various settings categories like About, ARP & Routes, Authentication, Backup Configuration, Clock, DTI Config, IP Network, License Management, Logs, Release Management, Restore Configuration, Scrambler, and SNMP & Traps. The main content area is divided into two sections: 'Device Information' and 'SRM Configuration'. The 'Device Information' section contains fields for Device Description (Cisco RFGW-1-D Universal Edge QAM), Device Up Time (0 Days, 00 Hours, 21 Minutes, 58 Seconds), Device Name (rfgw-1d), Device Contact (Cisco Support), Device Location (RFGW-1 Rack1), QAM Encoding Type (ITU-B), Frequency Plan (Standard), Gratuitous ARP State (Enabled), Gratuitous ARP Time (60 seconds), Dejitter Buffer Depth (150 milliseconds), Network PID (8188), Insert Network PID reference in PAT (Enabled), Gbe Port CRC Alarm Set Threshold (10), Gbe Port CRC Alarm Clear Threshold (0), Begin Scrambler Alarm Debounce (0 seconds), and End Scrambler Alarm Debounce (0 seconds). The 'SRM Configuration' section includes SRM IP Address #1, #2, and #3 (all set to 0.0.0.0) and a Reset Indication Rate (5 seconds). At the bottom of the form are 'Apply' and 'Reset' buttons.

- 2 In the *Device Name* field, enter the device name (up to 16 characters supported).
- 3 Click **Apply**.
- 4 Click **Save**.

Configuring the Annex

The annex setting applies to all carriers in the RF Gateway 1, including ITU-A (DVB), ITU-B (open cable), or ITU-C (Japan applications). Mixed annex settings are not supported.

To Configure the Annex

- 1 Navigate to the *System/System Configuration* page.

Result: The *Device Information* page is displayed.

The screenshot shows the configuration page for device 'rfgw-1d'. The 'System' tab is active. The 'Device Information' section contains the following fields:

Device Information	
Device Description	Cisco RFGW-1-D Universal Edge QAM
Device Up Time	0 Days, 00 Hours, 21 Minutes, 58 Seconds
Device Name	rfgw-1d
Device Contact	Cisco Support
Device Location	RFGW-1 Rack1
QAM Encoding Type	ITU-B
Frequency Plan	Standard
Gratuitous ARP State	Enabled
Gratuitous ARP Time	60 seconds
Dejitter Buffer Depth	150 milliseconds
Network PID	8188
Insert Network PID reference in PAT	Enabled
Gbe Port CRC Alarm Set Threshold	10
Gbe Port CRC Alarm Clear Threshold	0
Begin Scrambler Alarm Debounce	0 seconds
End Scrambler Alarm Debounce	0 seconds

The 'SRM Configuration' section contains the following fields:

SRM Configuration	
SRM IP Address #1	0.0.0.0
SRM IP Address #2	0.0.0.0
SRM IP Address #3	0.0.0.0
Reset Indication Rate	5 seconds

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

Note: Changing annex settings will clear the database to defaults.

- 2 In the *QAM Encoding Type* field, enter annex setting.
- 3 Click **Apply**.
- 4 Click **Save**.
- 5 Reboot the device. Reboot/power-cycle is required after changes to the annex setting.

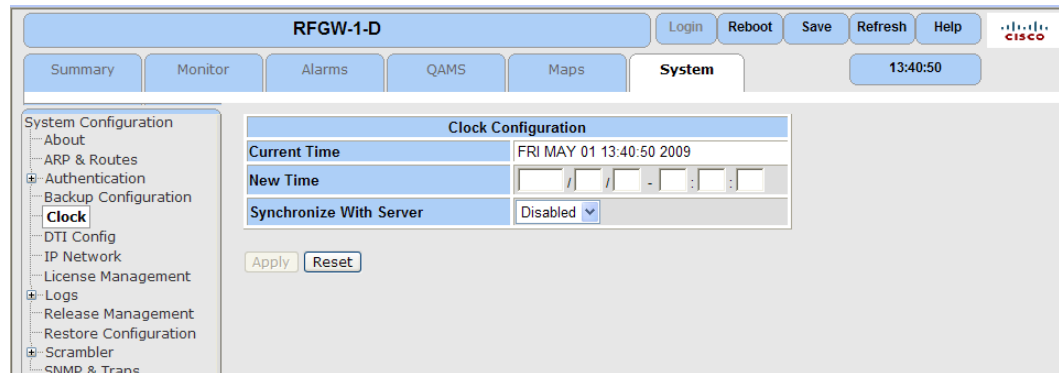
Configuring the Clock

The internal clock of the RF Gateway 1 can be set manually or can be synchronized with a Simple Network Time Protocol (SNTP) time server.

To Change the Internal Clock

- 1 Navigate to the *System/Clock* page.

Result: The *Clock Configuration* page is displayed.



- 2 In the *New Time* field, enter the current time.
- 3 Click **Apply**.
- 4 Click **Save**.

To configure the clock for SNTP, see *Simple Network Time Protocol (SNTP)* (on page 50).

Configuring IP Network Settings

This section provides information for configuring IP Network settings for the RF Gateway 1. Using the System/IP Network page, the user can configure the following.

- Management port IP address, subnet mask, and default gateway
- Conditional Access (CA) port, subnet mask, default gateway
- GbE input port settings, including IP addresses and subnet mask
- Redundancy mode and configuration

Configuring Management Port (10/100) IP Address, Subnet Mask and Default Gateway

To Configure the Management Port (10/100) IP Address, Subnet Mask, and Default Gateway

- 1 Navigate to the *System/IP Network* page.

Result: The *IP Network* page is displayed.

The screenshot displays the configuration interface for 'rfgw-1d'. The left sidebar shows a navigation menu with 'IP Network' selected. The main content area is divided into two sections: '10/100 Ports' and 'GbE Input Ports'.

10/100 Ports Configuration:

	Management	Conditional Access
Port Control		Off
Address Selection Mode	Static	Static
MAC Address	00:50:4b:11:33:2a	00:50:4b:11:33:2b
IP Address	10.90.146.131	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.146.01	150.158.235.254

GbE Input Ports Configuration:

	Port 1	Port 2	Port 3	Port 4
GbE Data Port Mode	Four Port Independent			
MAC Address	00:50:4b:11:33:2c	00:50:4b:11:33:2d	00:50:4b:11:33:2e	00:50:4b:11:33:2f
IP Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On

Port Pair Configuration:

	Port Pair 1	Port Pair 2
Video/Data IP	11.1.1.2	13.1.1.2
Redundancy Mode	Manual	Manual
Primary Port	1	3
Current Active Port	1	3
Detection Mode	Ethernet Link	Ethernet Link
LOS Timeout (s)	1	1
Revert To Primary	Enabled	Enabled
Revert Check Time (s)	2	2

Buttons: Apply, Reset

- 2 In the appropriate field, change the *IP Address*, *Subnet Mask*, and *Default Gateway* settings.
- 3 Click **Apply**.
- 4 Click **Save**.
- 5 Reboot the device.

Note: The management port IP address is not dynamically configurable, thus reboot/power-cycle is required after changes.

To Configure the Conditional Access (CA) Port IP Address, Subnet Mask, and Default Gateway

- 1 Navigate to the System/IP Network page.

Result: The IP Network page is displayed.

The screenshot shows the configuration page for 'rfgw-1d'. The 'System' tab is active, and the 'IP Network' section is expanded in the left sidebar. The main content area is divided into two sections: '10/100 Ports' and 'GbE Input Ports'.

10/100 Ports Configuration:

	Management	Conditional Access
Port Control		Off
Address Selection Mode	Static	Static
MAC Address	00:50:4b:11:33:2a	00:50:4b:11:33:2b
IP Address	10.90.146.131	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.146.01	150.158.235.254

GbE Input Ports Configuration:

Port Configuration	Port 1	Port 2	Port 3	Port 4
MAC Address	00:50:4b:11:33:2c	00:50:4b:11:33:2d	00:50:4b:11:33:2e	00:50:4b:11:33:2f
IP Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On

Port Pair Configuration:

	Port Pair 1	Port Pair 2
Video/Data IP	11.1.1.2	13.1.1.2
Redundancy Mode	Manual	Manual
Primary Port	1	3
Current Active Port	1	3
Detection Mode	Ethernet Link	Ethernet Link
LOS Timeout (s)	1	1
Revert To Primary	Enabled	Enabled
Revert Check Time (s)	2	2

Note: The CA port is only used for scrambling when the EIS and or ECMG equipment is on a separate network.

- 2 Set the Port Control to **On**. The default setting is **Off**.
- 3 In the appropriate field, change the IP Address, Subnet Mask, and Default Gateway settings.
- 4 Click **Apply**.
- 5 Click **Save**.
- 6 Reboot the device.

Note: The CA port IP address is not dynamically configurable, thus reboot/power-cycle is required after changes.

To Configure the Virtual IP Address for each GbE Port Pair for Port Pair Mode

- 1 Navigate to the System/IP Network page.

Result: The IP Network page is displayed.

The screenshot shows the configuration page for 'rfgw-1d'. The left sidebar lists various configuration options, with 'IP Network' selected. The main content area is divided into two sections:

10/100 Ports

	Management	Conditional Access
Port Control		Off
Address Selection Mode	Stabic	Stabic
MAC Address	00:50:4b:11:33:2a	00:50:4b:11:33:2b
IP Address	10.90.146.131	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.146.01	150.158.235.254

GbE Input Ports

GbE Data Port Mode	Four Port Independent			
Port Configuration	Port 1	Port 2	Port 3	Port 4
MAC Address	00:50:4b:11:33:2c	00:50:4b:11:33:2d	00:50:4b:11:33:2e	00:50:4b:11:33:2f
IP Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On
Port Pair Configuration	Port Pair 1		Port Pair 2	
Video/Data IP	11.1.1.2		13.1.1.2	
Redundancy Mode	Manual		Manual	
Primary Port	1		3	
Current Active Port	1		3	
Detection Mode	Ethernet Link		Ethernet Link	
LOS Timeout (s)	1		1	
Revert To Primary	Enabled		Enabled	
Revert Check Time (s)	2		2	

Buttons: Apply, Reset

- 2 In the *GbE Data Port Mode* field, select **Dual Port Pairs**.
- 3 In the *Video/Data IP* address field, change the address.
- 4 In the *Redundancy Mode* field, use the drop-down box to select **Redundancy** for each port pair.
- 5 Click **Apply**.
- 6 Click **Save**.
- 7 Proceed to configure the four physical GbE Ports IP addresses.

To Configure the Physical GbE Ports IP Address and Subnet Mask

- 1 Navigate to the System/IP Network page.

Result: The *IP Network* page is displayed.

The screenshot displays the configuration page for 'rfgw-1d'. The left sidebar shows a navigation menu with 'IP Network' selected. The main content area is divided into two sections: '10/100 Ports' and 'GbE Input Ports'.

10/100 Ports Configuration:

	Management	Conditional Access
Port Control		Off
Address Selection Mode	Static	Static
MAC Address	00:50:4b:11:33:2a	00:50:4b:11:33:2b
IP Address	10.90.146.131	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.146.01	150.158.235.254

GbE Input Ports Configuration:

	Port 1	Port 2	Port 3	Port 4
GbE Data Port Mode	Four Port Independent			
Port Configuration				
MAC Address	00:50:4b:11:33:2c	00:50:4b:11:33:2d	00:50:4b:11:33:2e	00:50:4b:11:33:2f
IP Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On
Port Pair Configuration	Port Pair 1		Port Pair 2	
Video/Data IP	11.1.1.2		13.1.1.2	
Redundancy Mode	Manual		Manual	
Primary Port	1		3	
Current Active Port	1		3	
Redundancy Configuration				
Detection Mode	Ethernet Link		Ethernet Link	
LOS Timeout (s)	1		1	
Revert To Primary	Enabled		Enabled	
Revert Check Time (s)	2		2	

- 2 In the appropriate field, change the IP Address and Subnet Mask.
- 3 In the *Negotiation Mode* field, use the drop-down box to select mode (On or Off).
Note: "On" is recommended for most applications and required for electrical SFPs.
- 4 Click **Apply**.
- 5 Click **Save**.

Network Connectivity Testing

Each of the four physical GbE input ports will respond to PING. Since the GbE input ports are not configurable for default gateway, a static route to the source network of the PING must be added to the GbE port to facilitate PING responses over layer 3 networks. Static routes can be added via the GUI, using the System/ARP & Routes page.

Configuring Static Routes

To Configure Static Routes

- 1 Navigate to the *System/ARP & Routes* page.

Result: The *ARP & Routes* window is displayed.

The screenshot shows the Cisco configuration interface for 'rfgw-1d'. The 'System' tab is selected, and the 'ARP & Routes' section is active. The 'Route Table' is displayed with a 'Management Port' dropdown set to 'Management Port'. Below it, the 'ARP Table' is shown. The 'Static Route Entry' and 'Static ARP Entry' forms are also visible.

Destination IP	Gateway	Flags*	Use	Interface	Hop Count
0.0.0.0/0	10.90.149.1	UGS	73	emac0	0
10.0.0.0/8	link#2	UC	4	emac0	0
10.90.149.87	link#1	UH	0	lo0	0
127.0.0.0/8	127.0.0.1	UR	0	lo0	0
127.0.0.1	127.0.0.1	UH	16	lo0	0

Destination IP	Ethernet Address	Flags*	Use	Interface	Hop Count
10.90.149.1	00:00:0c:07:ac:23	UHL	2544	emac0	1
10.90.149.112	00:13:72:71:23:87	UHL	1700	emac0	1
10.90.149.123	00:19:b9:73:c3:eb	UHL	1949	emac0	1
10.90.152.51	00:00:0c:07:ac:23	UHL	6	emac0	1

- 2 In the *Route Table* window, use the drop-down box to select desired GbE input.
- 3 In the *Static Route Entry* window, enter the IP Address and Subnet Mask for the network or host.
- 4 Click **Add** to add the static route.
- 5 Click **Save**.

Configuring QAM Output

This section provides information for configuring the Quad Channel QAM Card. Using the QAM web page and its sub-menus, the operator can verify and configure:

- QAM card presence
- QAM output control (i.e., mute vs. unmute)
- Carrier parameters (i.e., frequency, spacing, and modulation)
- Channel Application Mode (i.e., video vs. data)

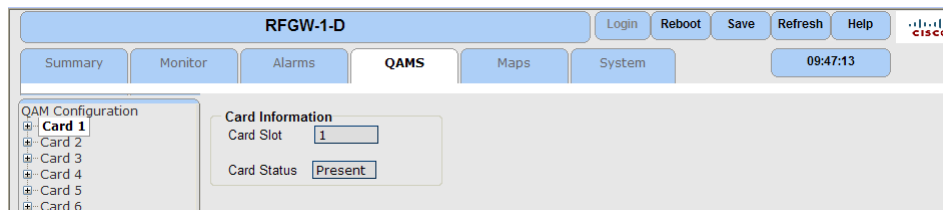
Card Presence

The RF Gateway 1 chassis can be populated with up to six QAM line cards.

To Verify QAM Card

- 1 Navigate to the *QAMS* page.
- 2 In the tree menu, select the desired QAM card.

Result: The web view indicates the status of the QAM card.



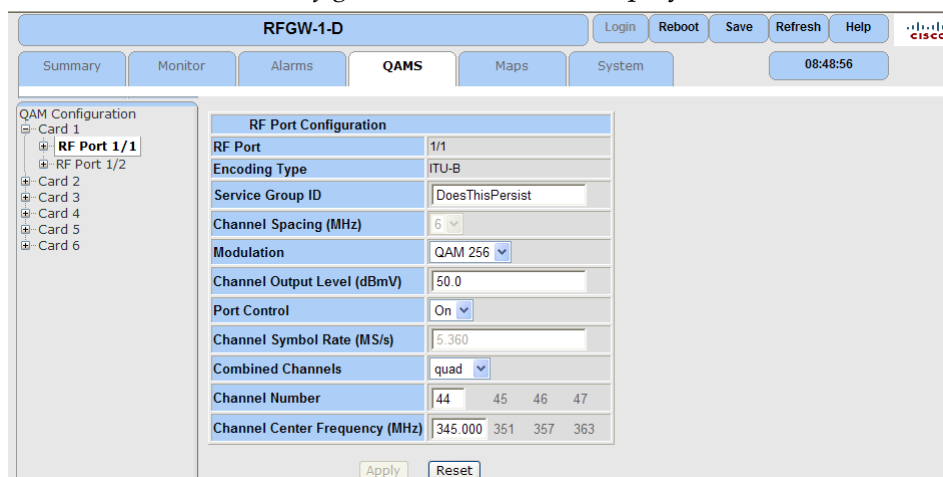
Enabling QAM Port

The RF Gateway 1 QAM line cards have two ports, with four RF output carriers per port. Outputs are enabled/disabled from the port level as well as from the individual carrier level. A global setting for a port must first be enabled, then individual carriers within the port can be independently muted or unmuted as desired.

To Enable QAM Port

- 1 Navigate to the *QAMS* page.
- 2 In the tree menu, select the desired Card/RF Port.

Result: The *RF Port Configuration* window is displayed.



- 3 In the *Port Control* field, set the parameter to On.
- 4 Click **Apply**.
- 5 Click **Save**.

To Enable Individual Carriers

- 1 Navigate to the *QAMS* page.
- 2 Expand the tree menu to select the Card/RF Port/QAM Channel.

Result: The *QAM Channel Configuration* window is displayed.

QAM Channel Configuration	
Card Index	1
Port Index	1
Channel Index	1
Encoding Type	ITU-B
Original Network ID	1
Transport Stream ID	1
Channel Mode	Normal
Channel Spectrum Inversion	Normal
Channel PRBS Stuffing	On
Channel Application Mode	SDV
Channel Interleave Depth	I=128,J=1
Channel PMT Rate	2 tables / second
Channel PAT Rate	2 tables / second

- 3 In the *Channel Mode* field, set the parameter to Normal.
- 4 Click **Apply**.
- 5 Click **Save**.

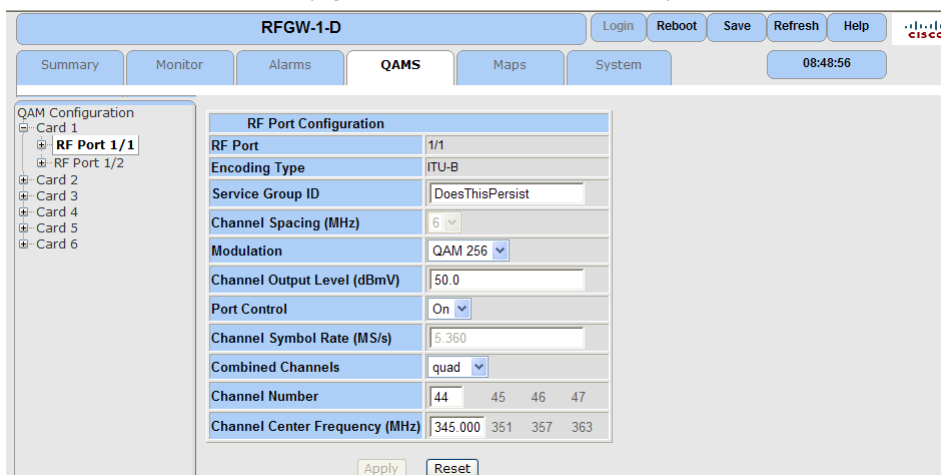
Carrier Parameters

Various settings are configurable for the RF Gateway 1 output carriers. Some settings are configurable on an individual carrier basis, other settings are limited to a particular RF port (group of four carriers).

To Configure Port Output Parameters

- 1 Navigate to the *QAMS* page.
- 2 Expand the tree menu and select desired RF Port.

Result: The *RF Port Configuration* window is displayed.

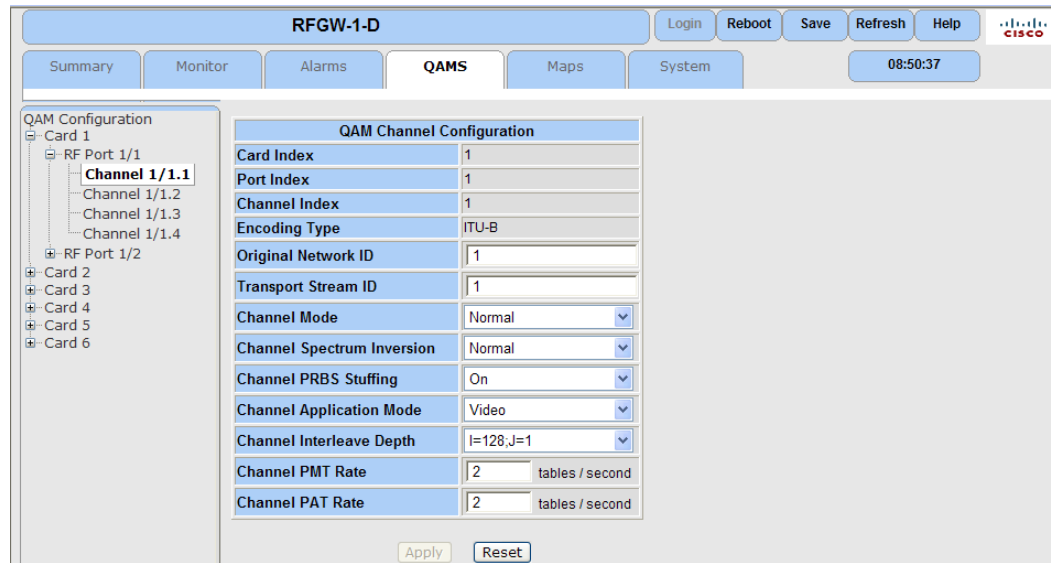


- 3 In the *Port Modulation* field, select desired modulation (64 vs. 256 QAM).
- 4 In the *Port Output Level* field, enter output level.
- 5 In the *Combined Channels* field, select the number of active carriers per port (i.e., for four carriers per port, set Combined Channels to quad).
- 6 In the *Channel Number* field, select channel frequencies.
Note: Combined Channels are limited to be spaced contiguously (separated by the chosen channel spacing) from the frequency of the lowest carrier. Therefore, only the frequency of the first carrier of a port may be configured.
- 7 Click **Apply**.
- 8 Click **Save**.

To Configure Individual Carrier Output Parameters

- 1 Navigate to the *QAMS* page.
- 2 Expand the tree menu, and select the desired QAM Channel.

Result: The *QAM Channel Configuration* window is displayed.



- 3 In the *Transport Stream ID* field, enter stream ID.
- 4 In the *Channel Spectrum Inversion* field, set the parameter to Normal (for most applications).

Note: The following table compares the RF Gateway 1 to an xDQA-24 with respect to Channel Spectrum Inversion and its interpretation.

ITU Annex Setting	xDQA-24 ITU Setting	RF Gateway 1 ITU Setting
ITU-A	Normal	Inverted
ITU-A	Inverted	Normal
ITU-B	Normal	Normal
ITU-B	Inverted	Inverted
ITU-C	Normal	Inverted
ITU-C	Inverted	Normal

- 5 In the *Channel PRBS Stuffing* field, set the parameter to On (for most applications.)
- 6 In the *Channel Interleave Depth* field, select the interleave type.
- 7 In the *Channel PMT Rate* and *Channel PAT Rate* fields, enter desired playout rates.
- 8 Click **Apply**.
- 9 Click **Save**.

Channel Application Mode

The RF Gateway 1 operates in various network scenarios including table video, VOD, SDV, and data modes (pre-DOCSIS 3.0 wideband as well as full M-CMTS (DTI) scenarios). These various scenarios are configurable on a per carrier basis, using the Channel Application Mode setting.

To Configure Channel Application Mode

- 1 Navigate to the *Maps* page.

Result: The following window is displayed.

Location	Channel#	Available	Channel Application Mode
1/1.1	01	Yes	Video
1/1.2	02	Yes	Video
1/1.3	03	Yes	Video
1/1.4	04	Yes	Video
1/2.1	05	Yes	Video
1/2.2	06	Yes	Video
1/2.3	07	Yes	Video
1/2.4	08	Yes	Video
2/1.1	09	Yes	Video
2/1.2	10	Yes	Video
2/1.3	11	Yes	Video
2/1.4	12	Yes	Video
2/2.1	13	Yes	Video

- 2 Select desired Channel Application Mode.

- Video
- Data
- SDV
- NGOD
- DEPI Learn
- DEPI Remote

- 3 Click **Apply**.
- 4 Click **Save**.

Configuring VOD Parameters

Ingress All VoD

When this option is enabled the session is able to look for backup streams in other GBE ports when the primary stream goes for input loss.

Navigate to the *System/System Configuration* page.

Result: The following window is displayed

The screenshot shows the Cisco configuration interface for a device named 'rfgw - 1d'. The 'System Configuration' page is active, displaying various configuration parameters. The 'Ingress All Option for VOD' is set to 'Enabled'. Other visible parameters include Device Description, Device Up Time, Device Name, Device Contact, Device Location, QAM Encoding Type, Frequency Plan, Gratuitous ARP State, Gratuitous ARP Time, Dejitter Buffer Depth, Network PID, Insert Network PID reference in PAT, Gbe Port CRC Alarm Set Threshold, Gbe Port CRC Alarm Clear Threshold, Begin Scrambler Alarm Debounce, and End Scrambler Alarm Debounce.

Device Information	
Device Description	Cisco RFGW-1-D Universal Edge QAM
Device Up Time	0 Days, 0 Hours, 5 Minutes, 3 Seconds
Device Name	rfgw - 1d
Device Contact	Cisco Support
Device Location	-
QAM Encoding Type	ITU-B
Frequency Plan	Standard
Gratuitous ARP State	Enabled
Gratuitous ARP Time	60 seconds
Dejitter Buffer Depth	150 milliseconds
Network PID	8188
Insert Network PID reference in PAT	Enabled
Ingress All Option for VOD	Enabled
Gbe Port CRC Alarm Set Threshold	10
Gbe Port CRC Alarm Clear Threshold	0
Begin Scrambler Alarm Debounce	10 seconds
End Scrambler Alarm Debounce	10 seconds

Click **Apply**.

Click **Save**.

Chapter 2 RF Gateway 1 Configuration Quick Start

Note: Once this option is enabled, the user will not be allowed to edit the Allowed Ingress ports setting in the MAPs Page as highlighted below.

The screenshot shows the Cisco configuration interface for 'rfgw - 1d'. The 'Maps' tab is selected, and the 'Stream Map Table' is displayed. The table has columns for Row #, Output QAM Channel, Destination IP Address, UDP Port, Active, Allowed Ingress Ports, Stream Type, Program Number (Input and Output), PMV, and Data Rate (kbps). A red circle highlights the 'Allowed Ingress Ports' column, which contains values like 'Port-1' and 'Port-4'. The 'Active' column has a dropdown menu set to 'True' for row 7. The 'Stream Type' column has a dropdown menu set to 'SPTS' for row 7. The 'Program Number' column has input fields for 'Input' and 'Output' values. The 'Data Rate' column shows values like '0' and '38000'. The interface also includes a 'Video Stream Map' sidebar on the left and buttons for 'Add Row', 'Apply', 'Reset', and 'Mark all rows for Delete' at the bottom.

Row #	Output QAM Channel	Destination IP Address	UDP Port	Active	Allowed Ingress Ports	Stream Type	Program Number		PMV	Data Rate (kbps)
							Input	Output		
0	1/1.1	0.0.0.0	4000	True	Port-1	SPTS	0	4	3	0
1	1/1.1	233.22.22.2	5566	True	Port-1	MPTS	0	1	0	0
2	3/1.1	0.0.0.0	1234	False	Port-4	MPTS	0	1	0	0
3	4/1.1	0.0.0.0	6000	False	Port-1	MPTS	0	1	0	0
4	4/2.1	0.0.0.0	1006	False	Port-1	MPTS	0	1	0	0
5	4/2.1	233.10.21.97	7000	True	Port-1	SPTS	0	1	0	38000
6	3/1.1	0.0.0.0	4000	False	Port-1	SPTS	0	1	0	0
7	5/1.2	0.0.0.0	5555	True	Port-1	SPTS	0	1	0	0
8	5/2.2	0.0.0.0	5000	True	Port-4	SPTS	0	1	0	0
9	5/2.2	233.10.21.97	7000	False	Port-1	SPTS	0	2	1	0

Video Session Timeout

Setting this option will hold the PMT in the output for the time set, to keep the sessions alive in the STB.

- 1 Navigate to the *System/System Configuration* page.

Result: The following window is displayed.

The screenshot shows the Cisco configuration interface for a device named 'rfgw - 1d'. The 'System Configuration' page is active, displaying various system parameters. The 'VOD Session Timeout' parameter is highlighted with a red circle, showing a value of 20 seconds. Other parameters include Device Description, Device Up Time, Device Name, Device Contact, Device Location, QAM Encoding Type, Frequency Plan, Gratuitous ARP State, Gratuitous ARP Time, Dejitter Buffer Depth, Network PID, Ingress All Option for VOD, Gbe Port CRC Alarm Set/Clear Threshold, Begin/End Scrambler Alarm Debounce, Automatic Configuration Save, Pre Encrypted Type, MPTS Defaults, Smart Fan Control, and SRM Configuration.

System Configuration		Device Information	
Device Description	Cisco RFGW-1-D Universal Edge QAM	Device Name	rfgw - 1d
Device Up Time	3 Days, 1 Hours, 46 Minutes, 55 Seconds	Device Contact	Cisco Support
Device Location	Sample	Device Location	Sample
QAM Encoding Type	ITU-B	Gratuitous ARP State	Enabled
Frequency Plan	Standard	Gratuitous ARP Time	00 seconds
Dejitter Buffer Depth	150 milliseconds	Network PID	8188
Insert Network PID reference in PAT	Enabled	Ingress All Option for VOD	Disabled
Gbe Port CRC Alarm Set Threshold	10	Gbe Port CRC Alarm Clear Threshold	0
Begin Scrambler Alarm Debounce	10 seconds	End Scrambler Alarm Debounce	10 seconds
Automatic Configuration Save	Enabled	Pre Encrypted Type	PowerKey
MPTS Defaults	Block and Regenerate PAT	Smart Fan Control	Disabled
VOD Session Timeout	20 seconds	SRM Configuration	Legacy Mode
SRM IP Address #1	0.0.0.0		

- 2 Click Apply.
- 3 Click Save.

3

General Configuration and Monitoring

This chapter provides configuration management as well as general information needed to configure components of the RF Gateway 1.

In This Chapter

■ QAM Annex and Frequency Plan Configuration	26
■ QAM Card Configuration	28
■ GbE Interface Configuration	35
■ ARP and Route Configuration	48
■ Clock Configuration	49
■ Monitoring the RF Gateway 1	53
■ Fault Management of the RF Gateway 1	65
■ Configuration Management	74
■ Release Management	77
■ Configuring, Monitoring, and Fault Management via SNMP	80

QAM Annex and Frequency Plan Configuration

The annex setting applies to all carriers in the RFGW-1, including ITU-A (DVB), ITU-B (open cable), or ITU-C (Japan applications). Mixed annex settings are not supported.

Configuring the Annex

Follow the instructions below to configure the annex.

- 1 Navigate to the *System/System Configuration* page.

Result: The *Device Information* page is displayed.

The screenshot displays the configuration page for a Cisco RFGW-1-D Universal Edge QAM device. The page is titled 'rfgw-1d' and includes navigation tabs for Summary, Monitor, Alarms, QAMS, Maps, and System. The System tab is active, showing the 'Device Information' section. The configuration fields are as follows:

Device Information	
Device Description	Cisco RFGW-1-D Universal Edge QAM
Device Up Time	0 Days, 16 Hours, 31 Minutes, 06 Seconds
Device Name	rfgw-1d
Device Contact	Cisco Support
Device Location	here
QAM Encoding Type	ITU-B
Frequency Plan	Standard
Gratuitous ARP State	Enabled
Gratuitous ARP Time	60 seconds
Dejitter Buffer Depth	150 milliseconds
Network PID	8188
Insert Network PID reference in PAT	Enabled
Gbe Port CRC Alarm Set Threshold	10
Gbe Port CRC Alarm Clear Threshold	0
Begin Scrambler Alarm Debounce	10 seconds
End Scrambler Alarm Debounce	10 seconds
Automatic Configuration Save	Enabled
Pre Encrypted Type	PowerKey
MPTS Defaults	Block and Regenerate PAT
SRM Configuration	
SRM IP Address #1	0.0.0.0 <input type="checkbox"/>
SRM IP Address #2	0.0.0.0 <input type="checkbox"/>
SRM IP Address #3	0.0.0.0 <input type="checkbox"/>
Reset Indication Rate	5 seconds

At the bottom of the page, there are 'Apply' and 'Reset' buttons.

Note: Changing annex settings resets the database to default settings.

- 2 In the *QAM Encoding Type* field, enter the annex setting.

QAM Annex and Frequency Plan Configuration

- 3 In the *Frequency Plan* field, select the desired frequency plan. The standard plan has channels mapped to pre-set frequencies used in North America. The custom plan lets you choose frequencies. ITU-A and ITU-C have custom plans only.
- 4 Click **Apply**.
- 5 Click **Save**.
- 6 Reboot the device. Reboot/power-cycle is required after changes to the annex setting.

QAM Card Configuration

The RFGW-1 has six QAM cards. Each card has two ports. Each port has four channels. The following sections describe how to configure the QAM card.

Global RF Port Configuration

Global RF Port Configuration allows you to configure RF for every port. See the following screen.

RF Port	Spacing (MHz)	Modulation	Output Level (dBmV)	Symbol Rate (MS/s)	Port Control	Combined Carrier	ITU Carrier Number	Carrier Center Frequency (MHz)			
								Ch1 Ch5	Ch2 Ch6	Ch3 Ch7	Ch4 Ch8
1/1	6	QAM 256	50	5.361	On	Quad	50 51 52 53	381.000	387.000	393.000	399.000
1/2	6	QAM 256	50	5.361	On	Quad	54 55 56 57	405.000	411.000	417.000	423.000
2/1	6	QAM 256	50	5.361	Off	None					
2/2	6	QAM 256	50	5.361	Off	None					
3/1	6	QAM 256	50	5.361	Off	None					
3/2	6	QAM 256	50	5.361	Off	None					
4/1	6	QAM 256	50	5.361	Off	None					
4/2	6	QAM 256	50	5.361	Off	None					
5/1	6	QAM 256	50	5.361	Off	None					
5/2	6	QAM 256	50	5.361	Off	None					

Parameters

The following table describes Global RF Port Configuration parameters.

Parameter	Description
RF Port	Refers to the RF port on a particular card. Example: 1/2 indicates card 1, port 2.
Spacing	The spacing between the channel center frequencies of different channels.
Modulation	Refers to the QAM output selected (256 or 64).
Output Level	Refers to the QAM output. The range depends on other parameters.
Symbol Rate	Based on the QAM modulation and ITU standards.
Combined Carrier	Allows you to configure the port for single/dual/quad channel.

Parameter	Description
ITU Carrier Number	<p>This field is only seen if your annex is ITU-B and you have a standard frequency plan selected.</p> <p>Example: In North America, channel 50 is determined to have a center frequency of 381 MHz. Selecting the first channel number picks up the corresponding frequency for channel 1 on that port. The remaining frequencies are populated automatically by channel spacing. Based on those frequencies, the remaining channel numbers are populated.</p> <p>Note: There are certain restrictions on the channel number.</p>
Carrier Center Frequency	<p>Allows you to choose the center frequency of channel 1 and the remaining channels are populated automatically.</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ There are certain restrictions on the channel number. ■ When changing the center frequency of a carrier, all carriers on the associated port are muted for several seconds to prevent spurious emission.

QAM Card View

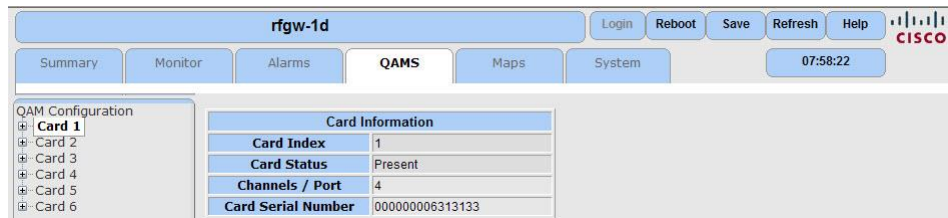
The RFGW-1 chassis can be populated with up to six QAM line cards.

Verifying the QAM Card

Follow the instructions below to verify the QAM card.

- 1 Navigate to the *QAMS* page.
- 2 In the tree menu, select the desired QAM card.

Result: The web view indicates the status of the QAM card.



QAM RF Port Configuration

The QAM RF Port Configuration view shows RF Port Configuration parameters from the Global QAM Configuration page. See the following screen.

RF Port Configuration	
Card Index	1
Port Index	1
Encoding Type	ITU-B
Service Group ID	0
Channel Spacing (MHz)	6
Modulation	QAM 256
Channel Output Level (dBmV)	50.0
Channel Symbol Rate (MS/s)	5.361
Port Control	On
Combined Channels	Quad None
ITU Carrier Number	50 51 52 53
Carrier Center Frequency (MHz)	381.000 387.000 393.000 399.000

Parameters

The following table describes the RF Port Configuration parameters.

Parameter	Description
Card Index	RF port card index on a particular card. Example: 1/2 indicates card 1, port 2.
Port Index	RF port index on a particular card.
Encoding Type	ITU standard.
Service Group ID	Alphanumeric service group identifier.
Channel Spacing	The spacing between the channel center frequencies of different channels.
Modulation	QAM output selected (256 or 64).
Channel Output Level	QAM output. The range depends on other parameters.
Channel Symbol Rate	Symbol Rate based on the QAM modulation and ITU standards.
Port Control	Allows you to turn the port on or off.
Combined Channels	Allows you to configure the port for single/dual/quad channels.

Parameter	Description
ITU Carrier Number	This field is only seen if your annex is ITU-B and you have a standard frequency plan selected. Example: In North America, channel 50 is determined to have a center frequency of 381 MHz. Selecting the first channel number picks up the corresponding frequency for channel 1 on that port. The remaining frequencies are populated automatically by channel spacing. Based on those frequencies, the remaining channel numbers are populated. Note: There are certain restrictions on the channel number.
Carrier Center Frequency	Allows you to choose the center frequency of channel 1 and the remaining channels are populated automatically. Note: There are certain restrictions on the channel number.

Global QAM Channel Configuration

Global QAM Channel Configuration allows you to configure QAM channels on a global level. See the following screen.

RFGW QAM Channel	SRM QAM Channel	ON ID	TS ID	Mode	Spectrum Inversion	PRBS Stuffing	App Mode	Interleave Depth	PMT Rate (tables/sec)	PAT Rate (tables/sec)	DTI Offset (ticks/64)
1/1.1	1	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
1/1.2	2	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
1/1.3	3	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
1/1.4	4	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
1/2.1	5	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
1/2.2	6	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
1/2.3	7	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
1/2.4	8	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
2/1.1	9	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
2/1.2	10	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
2/1.3	11	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
2/1.4	12	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
2/2.1	13	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
2/2.2	14	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
2/2.3	15	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
2/2.4	16	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
3/1.1	17	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0
3/1.2	18	1	0	Normal	Normal	On	SDV	I=128;J=1	10	10	0

Update All Rows Apply Reset

Parameters

The following table describes the Global QAM Channel Configuration parameters.

Parameter	Description
RFGW QAM Channel	RFGW QAM channels are shown in the following format. Example: 1/2.3 = card 1, port 2, channel 3.
SRM QAM Channel	SRM QAM channels are shown in the following format. Example: 1 = SRM Channel 1
ON ID	Original Network Identifier (range 0-65535).
TS ID	Transport Stream Identifier (range 0-65535).
Mode	The channel mode can be normal, continuous, or mute. The default setting is always mute.

Chapter 3 General Configuration and Monitoring

Parameter	Description
Spectrum Inversion	The spectrum can be configured as normal or swap.
PRBS Stuffing	"On" setting is recommended.
Application Mode	Allows the user to configure various network scenarios, including video, data, SDV, and NGOD.
Interleave Depth	Allows you to pick the interleaving depth.
PMT Rate	Default setting recommended.
PAT Rate	Default setting recommended.
DTI Offset	Timing offsets when channel is set to data mode.

Notes:

- 1 You can change values for one row and then update them all by clicking **Update All Rows**.
- 2 Application mode SDV corresponds to GQI mode of operation.
- 3 A chassis can be configured either to operate in GQI VOD system or GQI Broadcast.
- 4 In GQI PowerKey Broadcast mode of operation, only 4 channels per port are supported.

Additional Configuration

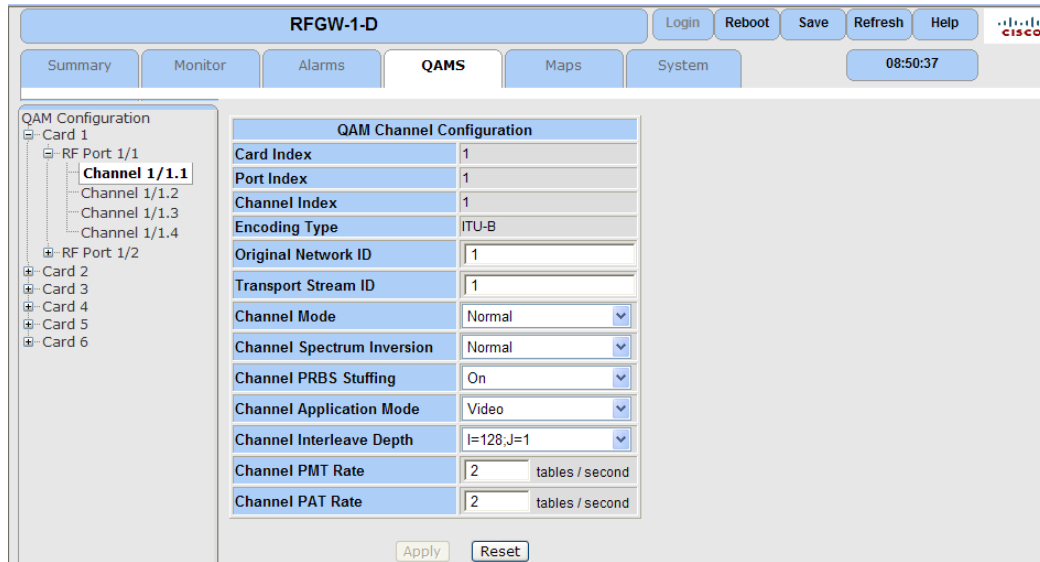
The RFGW-1 provides several additional configuration parameters that apply as needed.

The following parameters are added in System Release 5.1.x.

Parameter	Description
Automatic Configuration Save	When enabled, configuration changes applied to the RFGW-1 are automatically saved to the database.
Pre Encrypted Type	When pre-encrypted streams are routed, the correct CA system must be selected to ensure SI tables are routed correctly.
MPTS Defaults	When creating sessions from MPTS sources (in the Stream Map), the default behavior can be set to regenerate the output PAT, or pass the entire MPTS intact.

QAM Channel Level Configuration

The QAM Configuration channel level view shows you QAM Channel Configuration parameters from the Global QAM Configuration page. The following illustration shows the QAM Channel Configuration screen.



Parameters

The following table explains the QAM Channel Configuration parameters.

Parameter	Description
Card Index	Identifies the QAM card.
Port Index	Identifies the RF port selected for the QAM card.
Channel Index	Identifies the channel number for the port on the QAM card.
Encoding Type	Refers to the ITU standard.
Original Network ID	Original Network Identifier.
Transport Stream ID	Allows you to change the Transport Stream ID.
Channel Mode	The Channel Mode can be normal, continuous or mute. The default setting is always mute.
Channel Spectrum Inversion	The spectrum can be configured as normal or swap.
Channel PRBS Stuffing	Fills up stuffing packets with a Pseudo Random Binary Sequence. This setting is recommended to enhance locking on a receiving device.
Channel Application Mode	Allows you to choose the channel mode.
Channel Interleave Depth	Allows you to choose the interleaving depth.
Channel PMT Rate	Default setting recommended.

Chapter 3 General Configuration and Monitoring

Parameter	Description
Channel PAT Rate	Default setting recommended.

GbE Interface Configuration

GbE Interface Operation Modes

The RF Gateway 1 has four physical GbE input ports that receive video and data streams from the upstream network. These ports may be used independently (four-port independent mode) or configured to implement input redundancy (Dual port-pair mode).

In software releases 02.02.11 or later, the RF Gateway 1 may be configured for the four physical ports to operate independently. In this mode, no redundancy options are available. Each port will retain its hard-coded MAC address in this mode.

Four-Port Independent Mode

In four-port independent mode, the RF Gateway 1 may be configured for the four physical ports to operate independently. In this mode, no redundancy options are available. Each port will retain its hard-coded MAC address in this mode. All the four ports can belong to the same/different IP subnets.

The four-port independent mode supports redundancy for unicast streams if the 'Ingress-All' setting is enabled on the RFGW-1. If the Ingress-All is disabled then all the configured sessions can receive traffic only on the designated input port.

The four-port independent mode does not support redundancy for multicast streams. Multicast sessions can be configured to receive traffic on only one input port.

Ingress-All operation for Unicast Streams in Four-Port Independent Mode

For unicast stream sessions, the input stream can be received on any of the four input ports. The session will latch on to the input port on which the stream is detected first. If a loss of input occurs on the port that is currently receiving the stream, the session will automatically try to detect and switch to other ports where the stream may be available. If none of the input ports are receiving the traffic, then the stream will shut down until any of the ports start receiving traffic.

Source Specific Multicast Operation in Four-Port Independent Mode

When a multicast session is configured on the RFGW-1 with multiple source IP addresses for the input stream, then the RFGW-1 will repeatedly try the sources in the order they are specified (primary, secondary, tertiary and quaternary) until it receives the input stream.

Dual Port-Pair Mode

In port-pair mode, the RF Gateway 1 is preconfigured to implement redundancy as follows. The four input ports are configured to operate as two redundant port-pairs.

Chapter 3 General Configuration and Monitoring

- GbE port-pair 1 is composed of physical ports 1 and 2 (either one can be configured as primary and the other as backup).
- GbE port-pair 2 is composed of physical ports 3 and 4 (either one can be configured as primary and the other as backup).

When operating in the Dual port-pair mode, only one of the physical GbE ports in a pair can be used to receive input traffic (except for the Stream Redundancy detection mode, explained later, where both ports of a pair can be used to receive multicast stream). This port is termed as the Active port of the port pair. If a fault occurs on the current Active port, the RF Gateway 1 will failover to the next physical port.

To facilitate network operation of GbE port redundancy, the RF Gateway 1 implements a single, user-configurable Video/Data IP address for each port-pair. The Video/Data IP address is assumed by the active port of the port-pair. If a failover occurs from an active port to a backup port, the backup port assumes the Video/Data IP address once it becomes active. For all modes of operation, any unicast streams destined for the RF Gateway 1 must be sent to the Video/Data IP address for a given port-pair. The RF Gateway 1 does not implement a layer 2 address. Each physical GbE port is assigned a static, non-configurable MAC address. In this manner, the active physical port of a given port-pair assumes the Video/Data IP address of the port-pair, but retains its own unique hard-coded MAC address.

Several user-configurable options are available to the operator regarding redundancy, including:

- auto vs. manual operation
- revertive vs. non-revertive
- detection mode

Manual Redundancy Mode

The Active port of the pair is set by the user and remains fixed until changed by the user again. It does not depend on the Port or Network status. The active port can be either port 1 or 2 for the first pair and port 3 or 4 for the second pair.

Auto Redundancy Mode

This is the default redundancy mode of the input ports. When operating in the Auto Redundancy mode, the RFGW-1 will dynamically select the Active port for a pair based on the Port and/or the network condition. The user can configure the condition that will trigger the change in the current Active port of the pair. The triggers are referred to as Detection modes. Three different detection modes are available,

- Ethernet Link
- Ethernet Link + UDP/L2TPv3 packets
- Ethernet Link + UDP/L2TPv3 packets + TS Socket

Ethernet Link

The current active port will continue to remain as active until there is a loss of link (cable disconnection or port shutdown on the other end) on that port. If a link loss is detected, the RFGW-1 will try to make the other available port as Active. If the link is not present on both ports, then the last Active port will continue to remain as active (of course without being able to receive any input) until a link is detected on any of the port.

Primary Port and Backup Port

The primary port of a Port-pair is the port which the RFGW-1 will try to make as Active during initialization (e.g. bootup, or when changing the redundancy from manual to auto, or when changing the detection mode of the port-pair). The user can choose either of the port as the primary port for the pair. The other port which is not the primary is termed as Backup port.

Consider the following scenario for example,

Primary port for port-pair 1 is configured as port 2 with detection mode set to Ethernet Link. Then, if during boot up,

Link status of the ports of pair 1	Active Port
Link for both Port 1 and Port 2 is up.	Port 2
Link for Port 1 is up. Link for Port 2 is down.	Port 1
Link for Port 1 is down. Link for Port 2 is up.	Port 2
Link for both Port 1 and Port 2 is down.	Port 2

Revert to Primary Port

The 'Revert to Primary' is a functionality that is available when the RFGW-1 is operating in Ethernet Link detection mode. If this is enabled and if the current active port is the backup port, the RFGW-1 will periodically check the link status on the primary port. If it finds the link has come back, then it will change the Active port as primary port (even though link continues to exist in the backup). The inspection period can be set anywhere from 1 second to 5 minutes.

Ethernet Link & UDP/L2TPv3

The current active port will continue to remain as active until there is a loss of link (cable disconnection or port shutdown on the other end) or loss of traffic (no UDP/L2TPv3 packets – zero input bitrate) on that port. If a link loss is detected or UDP/L2TPv3 loss is detected, the RFGW-1 will try to make the other available port as Active.

If the link is not present on both ports, the last active port will continue to remain as active. If both the ports has connectivity but none of them is receiving any traffic, then the RFGW-1 continuously changes the Active port to monitor for any traffic and will lock to the port which receive the traffic first.

Revert to primary is not supported when the input ports are operating in this detection mode.

Source Specific Multicast Operation in "Ethernet Link" and "Ethernet Link & UDP/L2TPv3" Modes

The SSM operation is similar to the "4-port independent mode" except that the sources will be tried on the current active port of the pair. The SSM operation also works the same way in the manual redundancy mode.

Ethernet Link & UDP/L2TPv3 & TS Socket

This detection mode is also known as "Stream Redundancy" mode of operation. It behaves the same way as the 'Ethernet Link & UDP/L2TPv3' mode except for multicast input streams.

The unicast streams will continue to work the same way as in the 'Ethernet Link & UDP/L2TPv3' mode. The virtual IP address of the port pair will continue to receive unicast traffic only through the Current Active Port.

For Multicast streams, both the ports behave as active. i.e. input can be received either from the backup port or the primary port irrespective of whether that port is the Current Active port or not. The Virtual IP address will not be applicable for multicast input streams. Both the ports in the port pair will receive multicast traffic on their physical IP addresses

Since both the ports can be used to receive traffic at the same time, any multicast input stream can be active on any of the port based on its availability. Different sessions can be set up on different ports (of the port-pair) based on which port the stream is available.

When a stream is configured, it will initially get setup on the primary port if it is available. If it is not available on the primary port, it will get set on the backup port if it is available. If the stream is lost on the currently bound port, then the RFGW-1 will automatically switchover the stream to the other port. If a stream is not available on both the ports (of the port pair), then it will be kept toggling between the two ports until it becomes available on any of the port.

The IGMP Joins for multicast streams can be sent on one port or both the ports and is configurable using the 'Multicast Join port',

- Single port
- Dual ports

Multicast Join on Single Port

In this mode, the IGMP join will be sent only on the port where the stream is active. If the stream is not available on both the ports then the IGMP will be sent on the port which is currently being tried (as the stream will be toggled between both the ports). This mode is useful when the user wants to restrict the unnecessary traffic being received.

Multicast Join on Both Ports

In this mode, the IGMP join is sent on both the ports of the pair irrespective of on which port the stream is active. The switching time for stream, in case of loss, will be improved when operating in dual join mode. Also the user can ascertain, from the GUI pages, if the traffic is being received on the alternate port and is ready for switchover in case of input loss.

Reversion of Multicast Stream to Primary Port

The 'Stream Redundancy,' as with the Ethernet Link + UDP/L2TPv3 traffic mode of operation, does not support the reversion of Active port to Primary port.

But it supports the reversion of the multicast input streams to primary port, manually. When this option is selected, all the multicast input streams that are active on the backup port will be forced to become active on the primary port. If the stream is not available on the primary port, it will again switch and become active on the backup port. The user can also use the 'Periodic revert to primary for multicast streams' option to schedule this operation hourly or weekly.

Source Specific Multicast operation in "Stream Redundancy" mode of operation

The SSM operation works slightly different from the 4-port independent mode and the other Dual port pair modes.

Under this mode, since the traffic can be received on both ports of the pair, any given source IP will be tried on both the ports before the other sources are tried.

For example, if a session is created on pair-1 with four sources configured, then the RFGW-1 will try to bind the stream to the primary source on the primary port of pair-1. If the source is available it will lock to it. But if it is not available, then it will try to bind to the same primary source on the backup port. If the primary source is not available on both the ports, the secondary source will first be tried on the primary port and if it is not available then on the backup port. In this way, both ports of the pair will be attempted before switching to the next source IP. The port switching takes priority over the source switching when the RFGW-1 is operating in the stream redundancy mode.

Chapter 3 General Configuration and Monitoring

Ingress-All operation for unicast streams in Dual Port Pair mode

When the 'Ingress-All' setting is enabled on the RFGW-1, the unicast streams can be received on either the Current Active port (virtual IP) of Pair-1 or Pair-2. If the unicast stream is lost on Active port of pair-1, it will get setup on Active port of pair-2 and vice-versa. In effect, the unicast stream will have two input ports.

For network debugging and connectivity testing, each of the four physical GbE input ports are also user-configurable for the IP address, and will respond to PING. Since the GbE input ports are not configurable for default gateway, a static route to the source network of the PING must be added to the GbE port to facilitate PING responses over layer-3 networks. Static routes can be added via the GUI, using the *System/ARP & Routes* page.

Gratuitous ARPs can be enabled for the active GbE ports of the Port-Pairs. Using gratuitous ARP, the RF Gateway 1 makes only the virtual IP address known to the network. At layer 2, the RF Gateway 1 advertises the unique MAC address of the physical active port. The gratuitous ARP function generates ARP's for both the virtual interface as well as the physical interface.

Socket Redundancy Enhancements

- 1 Treat PCR Zero Bitrate as Content Loss
- 2 Manual Stream Switching

Enabling the features

- 1 By default, both the features are disabled.
- 2 Navigate to System Page and Input Redundancy Reversion page in the left pane.
- 3 Enable "Treat PCR Zero Bitrate as Content Loss" feature.
- 4 Enable "Manual Stream Switching" feature.
- 5 Click **Apply**.
- 6 Click **Save** at the top so this setting will be remembered between reboots.

Note: The feature can also be enabled through SNMP.

The screenshot displays the configuration interface for RFGW1. The top navigation bar includes 'Login', 'Reboot', 'Save', 'Refresh', and 'Help' buttons, along with the Cisco logo and the time '04:52:10'. The left sidebar lists various configuration categories, with 'Input Redundancy Reversion' selected. The main content area is titled 'Revert To Primary Gbe Port' and contains the following settings:

- Schedule Revert To Primary Gbe Port:** A checkbox that is currently unchecked.
- Periodic Revert to Primary:** A section with radio buttons for 'Revert On These Days' and a list of days (Sun, Mon, Tue, Wed, Thu, Fri, Sat) with checkboxes. Below this, there are input fields for 'Time of Day to Revert' (0 HH: 0 MM) and a 'Repeat Every' dropdown set to '1' hours.
- Treat PCR Zero Bitrate as Content Loss:** A toggle button currently set to 'Enabled'.
- Manual Stream Switching:** A toggle button currently set to 'Enabled'.

At the bottom of the configuration area, there are 'Apply', 'Reset', and 'Revert to Primary Now' buttons.

Treat PCR Zero Bitrate as Content Loss

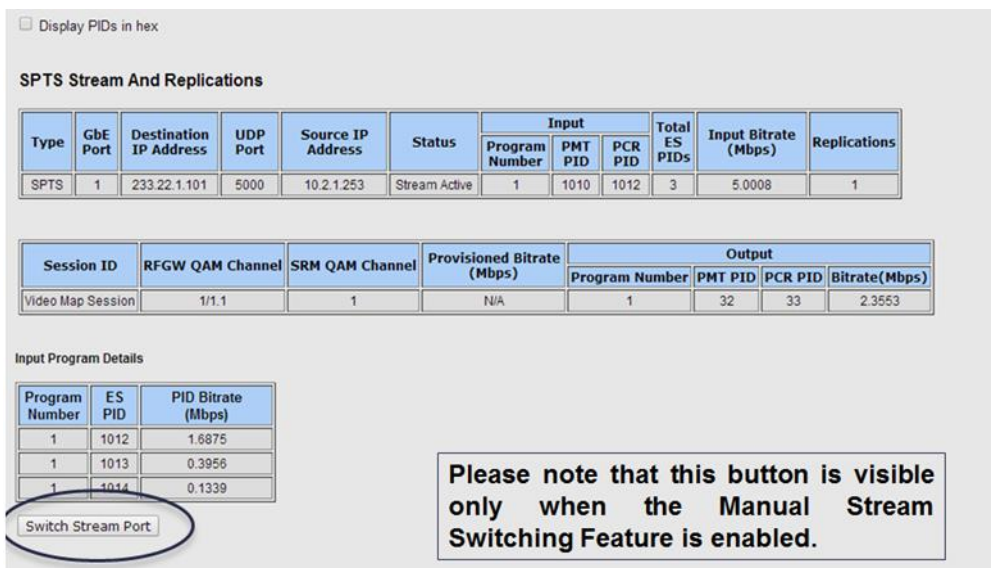
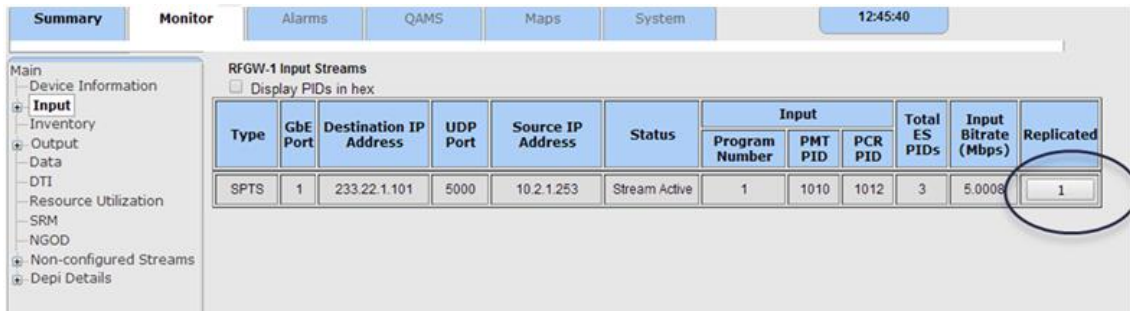
When a stream's PCR PID is not available, we would treat the scenario as similar to content loss and initiate the input stream switch to the backup stream. The switch to the backup stream is initiated without checking for presence of stream on the backup port. The switch rules would be same as Socket Redundancy (port switching has higher priority over source switching)

- The stream should have a valid PCR reference.
- This feature is applicable only for SPTS streams.

Manual Stream Switching

On a per stream basis, there will be a setting that will trigger the failover of the stream to the other port. This setting would be used to toggle a stream across ports. This setting is only for multicast streams available on ports configured for socket redundancy.

This button is available on the Monitor->Input->Stream Replications pop up window. Once the stream is toggled, the stream would switch based on the socket redundancy priorities (port switching has higher priority over source switching).



Configuring GbE Interface Settings

To Change GbE Input Port Settings

- 1 Navigate to the *System/IP Network* page.

Result: The *IP Network* page is displayed.

The screenshot shows the configuration page for 'rfgw-1d'. The left sidebar lists navigation options, with 'IP Network' selected. The main content area is divided into two sections:

10/100 Ports

	Management	Conditional Access
Port Control		Off
Address Selection Mode	Static	Static
MAC Address	00:50:4b:11:33:2a	00:50:4b:11:33:2b
IP Address	10.90.146.131	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.146.01	150.158.235.254

GbE Input Ports

GbE Data Port Mode	Four Port Independent			
Port Configuration	Port 1	Port 2	Port 3	Port 4
MAC Address	00:50:4b:11:33:2c	00:50:4b:11:33:2d	00:50:4b:11:33:2e	00:50:4b:11:33:2f
IP Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On
Port Pair Configuration	Port Pair 1		Port Pair 2	
Video/Data IP	11.1.1.2		13.1.1.2	
Redundancy Mode	Manual		Manual	
Primary Port	1		3	
Current Active Port	1		3	
Redundancy Configuration				
Detection Mode	Ethernet Link		Ethernet Link	
LOS Timeout (s)	1		1	
Revert To Primary	Enabled		Enabled	
Revert Check Time (s)	2		2	

- 2 In the appropriate field, enter the *IP Address* and *Subnet Mask* settings.
- 3 In the *Negotiation Mode* field, use the drop-down box to select mode (**On** or **Off**).
Note: "On" is recommended for most applications and required for electrical SFPs.
- 4 Click **Apply**.
- 5 Click **Save**.

Configuring GbE Port Operational Mode

- 1 Navigate to the *System/IP Network* page.

Result: The *IP Network* page is displayed.

The screenshot shows the configuration page for 'rfgw-1d'. The left sidebar lists various configuration options, with 'IP Network' selected. The main content area is divided into two sections: '10/100 Ports' and 'GbE Input Ports'.

10/100 Ports Configuration:

	Management	Conditional Access
Port Control		Off
Address Selection Mode	Static	Static
MAC Address	00:50:4b:11:33:2a	00:50:4b:11:33:2b
IP Address	10.90.146.131	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.146.01	150.158.235.254

GbE Input Ports Configuration:

GbE Data Port Mode	Four Port Independent			
Port Configuration	Port 1	Port 2	Port 3	Port 4
MAC Address	00:50:4b:11:33:2c	00:50:4b:11:33:2d	00:50:4b:11:33:2e	00:50:4b:11:33:2f
IP Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On
Port Pair Configuration	Port Pair 1		Port Pair 2	
Video/Data IP	11.1.1.2		13.1.1.2	
Redundancy Mode	Manual		Manual	
Primary Port	1		3	
Current Active Port	1		3	
Redundancy Configuration				
Detection Mode	Ethernet Link		Ethernet Link	
LOS Timeout (s)	1		1	
Revert To Primary	Enabled		Enabled	
Revert Check Time (s)	2		2	

- 2 In the *GbE Data Port Mode* field, select **Four Port Independent** or **Dual Port Pairs**.
- 3 Click **Apply**.
- 4 Click **Save**.

Configuring the Video/Data IP Address for GbE Port Pair Mode

- 1 Navigate to the *System/IP Network* page.

Result: The *IP Network* page is displayed.

The screenshot shows the configuration page for 'rfgw-1d'. The left sidebar lists various configuration options, with 'IP Network' selected. The main content area is divided into two sections: '10/100 Ports' and 'GbE Input Ports'.

10/100 Ports Configuration:

	Management	Conditional Access
Port Control		Off
Address Selection Mode	Static	Static
MAC Address	00:50:4b:11:33:2a	00:50:4b:11:33:2b
IP Address	10.90.146.131	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.146.01	150.158.235.254

GbE Input Ports Configuration:

	Port 1	Port 2	Port 3	Port 4
GbE Data Port Mode	Four Port Independent			
Port Configuration	00:50:4b:11:33:2c	00:50:4b:11:33:2d	00:50:4b:11:33:2e	00:50:4b:11:33:2f
MAC Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
IP Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On
Port Pair Configuration	Port Pair 1		Port Pair 2	
Video/Data IP	11.1.1.2		13.1.1.2	
Redundancy Mode	Manual		Manual	
Primary Port	1		3	
Current Active Port	1		3	
Redundancy Configuration				
Detection Mode	Ethernet Link		Ethernet Link	
LOS Timeout (s)	1		1	
Revert To Primary	Enabled		Enabled	
Revert Check Time (s)	2		2	

- 2 In the *Video/Data IP* field, enter the IP Address. This is the GbE Port Pair "virtual" IP address used for streaming Video/Data.
- 3 Click **Apply**.
- 4 Click **Save**.

Configuring Redundancy for Port Pair Mode

- 1 Navigate to the *System/IP Network* page.

Result: The *IP Network* page is displayed.

The screenshot shows the configuration page for 'rfgw-1d' with the 'System' tab selected. The 'IP Network' section is active in the left sidebar. The main content area is divided into two sections: '10/100 Ports' and 'GbE Input Ports'.

10/100 Ports Configuration:

	Management	Conditional Access
Port Control		Off
Address Selection Mode	Static	Static
MAC Address	00:50:4b:11:33:2a	00:50:4b:11:33:2b
IP Address	10.90.146.131	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.146.01	150.158.235.254

GbE Input Ports Configuration:

GbE Data Port Mode	Four Port Independent			
Port Configuration	Port 1	Port 2	Port 3	Port 4
MAC Address	00:50:4b:11:33:2c	00:50:4b:11:33:2d	00:50:4b:11:33:2e	00:50:4b:11:33:2f
IP Address	15.1.1.3	15.1.1.4	25.1.1.3	25.1.1.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On
Port Pair Configuration	Port Pair 1		Port Pair 2	
Video/Data IP	11.1.1.2		13.1.1.2	
Redundancy Mode	Manual		Manual	
Primary Port	1		3	
Current Active Port	1		3	
Redundancy Configuration				
Detection Mode	Ethernet Link		Ethernet Link	
LOS Timeout (s)	1		1	
Revert To Primary	Enabled		Enabled	
Revert Check Time (s)	2		2	

Buttons: Apply, Reset

- 2 In the *Redundancy Mode* field, select desired mode.
 - a Auto mode enables automatic failover to backup ports
 - b Manual mode forces an active port
- 3 In the *Primary Port* field, designate which GbE inputs per port-pair will be assigned the primary port.
- 4 In the *Detection Mode* field, select the desired configuration for the failover condition.
 - Ethernet Link (will use loss of link for the detection mode)
 - Ethernet Link and UDP or L2TPv3 Packets (adds to the detection mode the loss of UDP video or L2TPv3 data packets)
 - Ethernet Link and UDP or L2TPv3 Packets and TS Socket (improves the redundancy of multicast inputs to stream level)

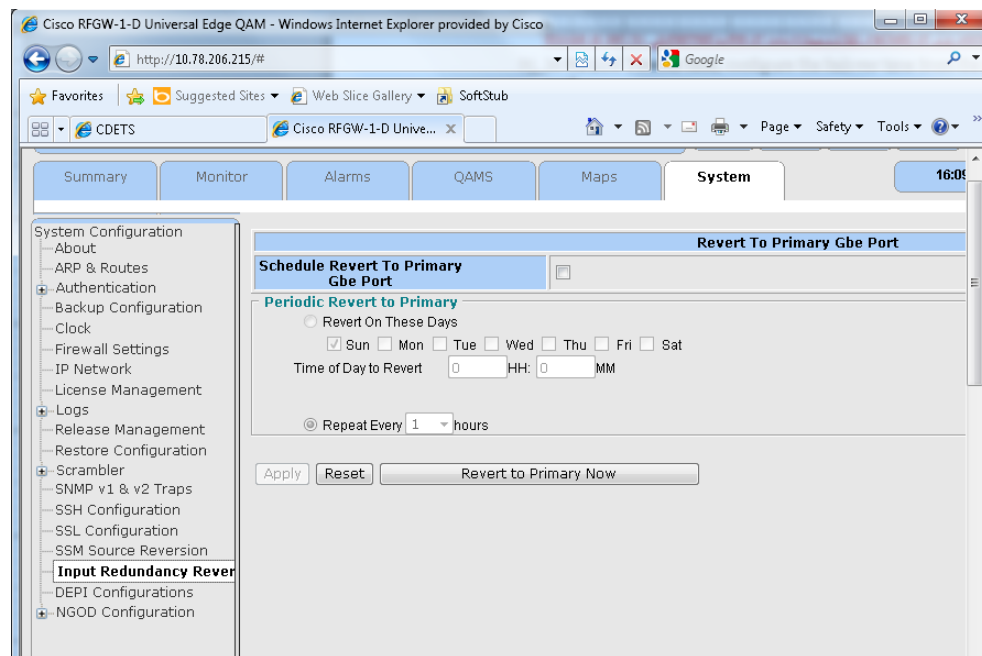
Chapter 3 General Configuration and Monitoring

- 5 In the Multicast Join ports field, configure if the IGMP Joins for multicast streams is to be sent on Single/Both ports. This field is applicable only when the detection mode is set to "Ethernet Link & UDP/L2TPv3 Packets & TS Socket".
- 6 In the *LOS Timeout* field, configure the failover time from the active to inactive port.
- 7 In the *Revert to Primary* field, if automatic revert is desired, set the parameter to "Enabled". This field will not be applicable when the detection mode is set to "Ethernet Link & UDP/L2TPv3 Packets & TS Socket" and will be set to Disabled.
- 8 In the *Revert Check Time* field, enter an uptime range for the primary port before a reversion occurs.
Note: Valid range is 0-300 seconds.
- 9 Click **Apply**.
- 10 Click **Save**.

Configuring Reversion of Multicast Streams to Primary Port

- 1 Navigate to the System/Input Redundancy Revert page.

Result: The Input Redundancy Revert page is displayed.



- 2 Check or Uncheck the Schedule Revert To Primary Gbe Port to Enable/Disable the automatic reversion.
- 3 Select the Reversion type as either one of the below.
 - Revert on These Days
 - Revert Every "X"hours.
- 4 If Selecting the "Revert on These Days", configure the days and time of the day when the reversion is to occur.

- 5 Or if selecting the "Periodic Revert", select the reversion period.
Note: Valid periods are 1, 2, 3, 4, 6, 12 or 24 hours.
 - 6 Click Apply.
 - 7 Click Save.
- Note: The user can also perform an instantaneous Reversion to Primary by clicking on the "Revert to Primary Now" button.

ARP and Route Configuration

To facilitate network connectivity on the management and GbE interfaces, the RF Gateway 1 can create static Route and ARP entries. Static routes provide network connectivity to devices that are not on the network. For example, a static route could be required to support multicast sessions on the GbE interface from a device on another network. Static ARPs are provided to allow connectivity to devices that are not responding to ARP requests. Depending on network configuration and requirements, static ARPs or routes may be required on any of the management or GbE interfaces.

To Configure ARP And Route Entries

- 1 Navigate to the *System/ARP & Routes* page.

Result: The *ARP & Routes* window is displayed.

The screenshot shows the web interface for 'rfgw-1d'. The left sidebar contains a navigation menu with 'ARP & Routes' selected. The main content area is divided into two sections: 'Route Table' and 'ARP Table'. Below these are forms for 'Static Route Entry' and 'Static ARP Entry'.

Route Table

Destination IP	Gateway	Flags*	Use	Interface	Hop Count
0.0.0.0/0	10.90.149.1	UGS	73	emac0	0
10.0.0.0/8	link#2	UC	4	emac0	0
10.90.149.87	link#1	UH	0	lo0	0
127.0.0.0/8	127.0.0.1	UR	0	lo0	0
127.0.0.1	127.0.0.1	UH	16	lo0	0

ARP Table

Destination IP	Ethernet Address	Flags*	Use	Interface	Hop Count
10.90.149.1	00:00:0c:07:ac:23	UHL	2544	emac0	1
10.90.149.112	00:13:72:71:23:87	UHL	1700	emac0	1
10.90.149.123	00:19:b9:73:c3:eb	UHL	1949	emac0	1
10.90.152.51	00:00:0c:07:ac:23	UHL	6	emac0	1

Static Route Entry

Destination IP Address:

Gateway IP Address:

Subnet Mask:

Static ARP Entry

Destination IP Address:

Ethernet Address:

Flags: Permanent ARP Entry
 Publish ARP Entry
 Proxy ARP Entry

- 2 Enter the appropriate parameters on the web interface.
- 3 Click **Add**.

Clock Configuration

The RF Gateway 1 provides several different configuration options for obtaining and maintaining accurate time on the system. These options include time synchronization from a network time server and obtaining time from an on-board real-time clock (RTC).

Real -Time Clock Setup

The RF Gateway 1 has an on-board, real-time clock (RTC) with battery back-up which can be used to provide system time. The RTC can be set manually via the web interface or configured to be updated with network time obtained from an SNTP server. The *Synchronize With Server* parameter is used to control the RTC synchronization behavior. When set to *Disabled*, the RF Gateway 1 obtains system time from the RTC at startup. Once set, the internal system clock runs independently until the RTC is changed. The *Clock Configuration* page provides the following user-configurable options.

- Current Time
- New Time
- Synchronize with Server

To Set the Real Time Clock:

- 1 Navigate to the *System/Clock* page.

Result: The *Clock Configuration* page is displayed.

Clock Configuration	
Current Time	FRI MAY 01 13:40:50 2009
New Time	<input type="text"/>
Synchronize With Server	Disabled

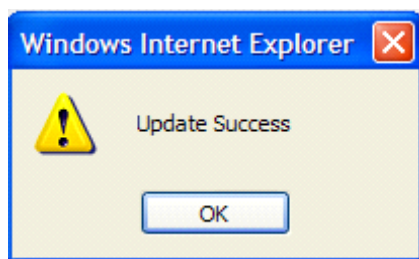
Apply Reset

- 2 In the *New Time* field, enter year, date and current time.

Example: 2008/06/17/0052:26

- 3 Click **Apply**.

Result: The *Update Success* window is displayed.



TP582

- 4 Click **OK**.

Result: The time is displayed in the *Current Time* window.

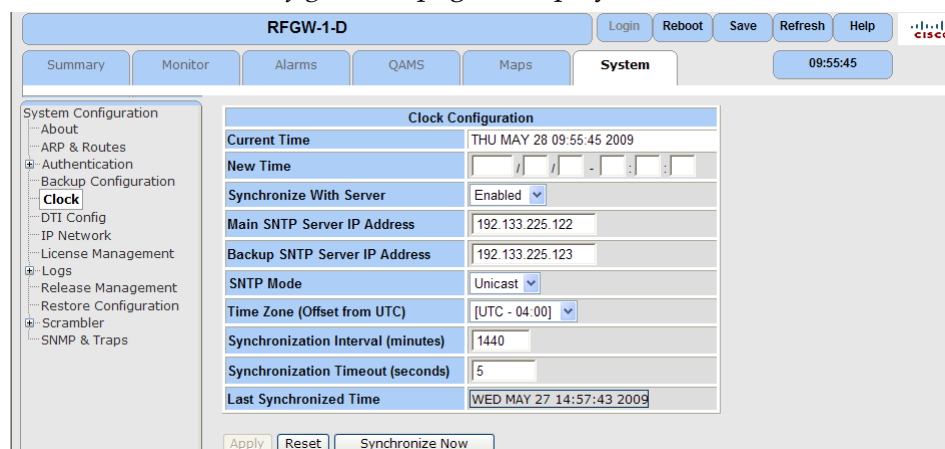
Simple Network Time Protocol (SNTP)

When *Synchronize With Server* is set to *Enabled*, the RF Gateway 1 periodically attempts to obtain network time from one of the SNTP servers specified by the IP address on the Clock Configuration page. If communication with the SNTP server is successful, the RTC and internal system clock are updated. If communication with both SNTP servers fails the internal system clock updates with a value obtained from the RTC. For the remainder of the synchronization interval, the system runs on its own time independent of the RTC and network server. At the start of the next synchronization interval, the system attempts to resynchronize with the network time server and set its clocks accordingly.

To Set the SNTP server for RTC

- 1 Navigate to the *System/Clock* page.

Result: The *Clock Configuration* page is displayed.



- 2 Set *Synchronize with Server* to *Enabled*.
- 3 In the *Main SNTP Server IP Address* field, enter the IP address in xx.xx.xx.xx format.

- 4 In the *Backup SNTP Server IP Address* field, enter the IP address in xx.xx.xx.xx format.
- 5 In the *SNTP Mode* field, select "Unicast" (Multicast is not supported).
- 6 In the *Time Zone* field, select the correct time zone depending on current location.
- 7 The *Synchronization Interval* parameter specifies the interval at which the RF Gateway 1 resynchronizes the system clock and RTC to the network time. Set the SNTP Synchronization rate in minutes. The default is 1440 minutes or 24 hours.
- 8 The *Synchronization Timeout* parameter specifies how long the RF Gateway waits for the network time server to respond. Set the timeout in seconds.
- 9 Click **Apply**.
- 10 Click **Synchronize Now** to force a network synchronization. This sets the system's time and RTC.
- 11 Click **Save**.

Result: On the next system reboot, the system time is displayed in periodic intervals based on the Synchronization Interval setting.

Parameters

The following table explains the Clock Configuration parameters.

Parameter	Description
Current Time	System's current time.
New Time	System's new time.
Synchronize with Server	Specifies the source of time synchronization, network time server or on-board real-time clock.
Main SNTP Server IP Address	IP address of the Main SNTP server.
Backup SNTP Server IP Address	IP address of the Backup SNTP server.
SNTP Mode	Always set to Unicast.
Time Zone (Offset from UTC)	Used to configure an offset from UTC time.
Synchronization Interval	Specifies the interval at which the system resynchronizes the system clock and RTC to the network time.
Synchronization Timeout	Specifies how long the RF Gateway waits for the network time server to respond.
Last Synchronized Time	Indicates when the last successful network synchronization occurred.

Additional Configuration

The RF Gateway 1 provides several additional configuration parameters applicable as needed.

Chapter 3 General Configuration and Monitoring

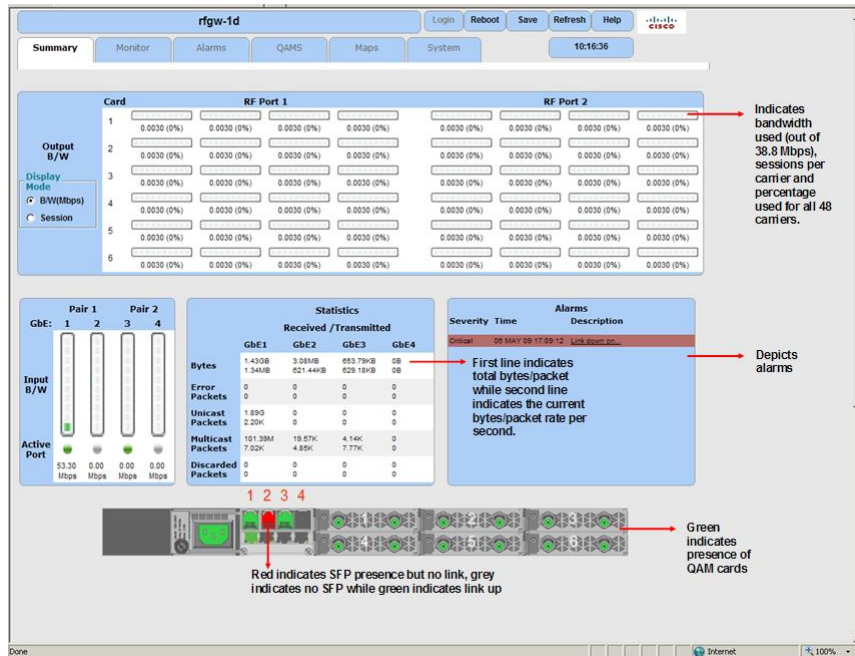
To access the following parameters, navigate to the *System/System Configuration* page.

Parameter	Description
Gratuitous ARP State	Enable/Disable the periodic sending of gratuitous ARP packets.
Gratuitous ARP Time	Amount of time between gratuitous ARP packets.
Dejitter Buffer Depth	Provides the average packet delay through the dejitter buffer. Its default value is 150 milliseconds and it has a range of 5-400 milliseconds. Note, the depth should be greater than PCR interval + network jitter.
Network PID	Network PID range 1-8190 is available
Insert Network PID reference in PAT	Enable/Disable the insertion of network PID in PAT
Gbe Port CRC Alarm Set Threshold	Alarm set threshold range provided within a five second window is 1- 4294967295
Gbe Port CRC Alarm Clear Threshold)	Alarm clear threshold range provided within a five second window is 1- 4294967295
Begin Scrambler Alarm Debounce	Begin Scrambler Alarm debounce range provided is 0-20 seconds
End Scrambler Alarm Debounce	End Scrambler Alarm debounce range provided is 0-120 seconds

Monitoring the RF Gateway 1

Summary Tab

The summary page provides a snapshot of the RF Gateway 1 system. The following illustration shows the summary screen.



Output Bandwidth Panel

The Output B/W panel (top left) shows the bandwidth of each carrier.

- 1 Click **Sessions** in the Display Mode box.

Result: The number of sessions on each carrier will be displayed.

Input Bandwidth Panel

The Input B/W (middle left) panel shows the bandwidth through each of the Gigabit ports. The dot under each port indicates whether port is active (green) or not active (grey).

Statistics Panel

The Statistics panel (middle) gives you details about each input GbE port. The first line indicates cumulative data since the last reboot and the second line indicates current rate.

Chapter 3 General Configuration and Monitoring

Alarms Panel

The Alarms panel (middle right) allows you to quickly tell if something is drastically wrong. Clicking an alarm provides more detailed information.

Back Panel

- Green – Part is inserted and system recognized it.
- Red – The part is there but something's wrong. In this case, no link detected for GbE 2.
- Grey – It is not there. GbE Port 3 not connected in this case.

Monitor Tab

The RF Gateway 1 provides extensive capability for monitoring the current status of the system. The Monitor tab provides utilities for monitoring:

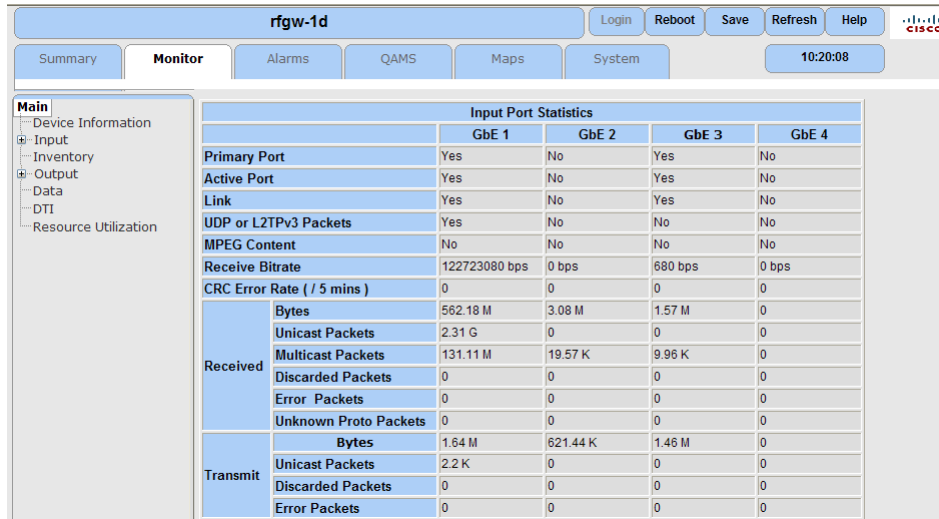
- Input streams (i.e., stream activity, input bitrates)
- Output streams (i.e., per carrier stream mapping, provisioned bitrates)
- Platform related device and inventory information
- Data specific monitoring (i.e., DOCSIS sync presence)
- DTI server connectivity and status
- Resource Utilization (i.e., CPU and memory utilization)

Input Monitoring

The Monitor tab provides utilities for monitoring input ports. Input port statistics are accessible from the Main page of the Monitor tab. The following Status information is provided for each GbE port.

- Primary and active ports
- Link status
- UDP or L2TPv3 packets
- MPEG content presence
- Receive bitrates
- CRC Error Rate (per 5 min)
- Receive and transmit packet counts

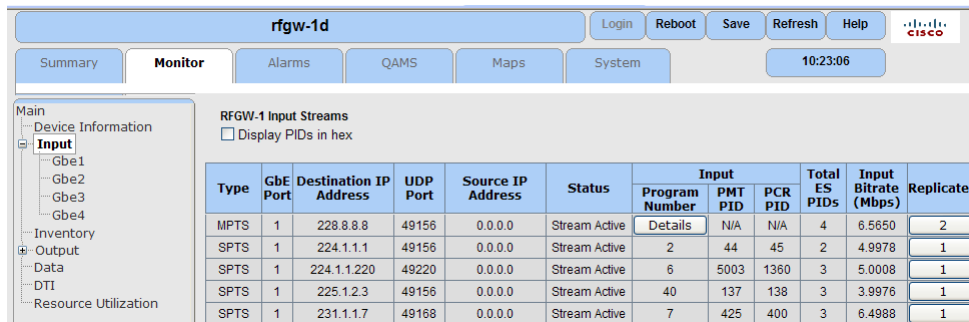
The following illustration shows the *Monitor/Main* page screen.



		GbE 1	GbE 2	GbE 3	GbE 4
Primary Port		Yes	No	Yes	No
Active Port		Yes	No	Yes	No
Link		Yes	No	Yes	No
UDP or L2TPv3 Packets		Yes	No	No	No
MPEG Content		No	No	No	No
Receive Bitrate		122723080 bps	0 bps	680 bps	0 bps
CRC Error Rate (/ 5 mins)		0	0	0	0
Received	Bytes	562.18 M	3.08 M	1.57 M	0
	Unicast Packets	2.31 G	0	0	0
	Multicast Packets	131.11 M	19.57 K	9.96 K	0
	Discarded Packets	0	0	0	0
	Error Packets	0	0	0	0
	Unknown Proto Packets	0	0	0	0
Transmit	Bytes	1.64 M	621.44 K	1.46 M	0
	Unicast Packets	2.2 K	0	0	0
	Discarded Packets	0	0	0	0
	Error Packets	0	0	0	0

The *Monitor/Input* page provides MPEG transport stream specific information, including information for each detected MPEG transport stream on the input. The streams can be filtered and displayed based on the input port.

The following illustration shows the *Monitor/Input* screen.



Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Input			Total ES PIDs	Input Bitrate (Mbps)	Replicated
						Program Number	PMT PID	PCR PID			
MPTS	1	228.8.8.8	49156	0.0.0.0	Stream Active	Details	N/A	N/A	4	6.5650	2
SPTS	1	224.1.1.1	49156	0.0.0.0	Stream Active	2	44	45	2	4.9978	1
SPTS	1	224.1.1.220	49220	0.0.0.0	Stream Active	6	5003	1360	3	5.0008	1
SPTS	1	225.1.2.3	49156	0.0.0.0	Stream Active	40	137	138	3	3.9976	1
SPTS	1	231.1.1.7	49168	0.0.0.0	Stream Active	7	425	400	3	6.4988	1

Parameters

The following table explains the Input Monitoring parameters.

Parameter	Description
Type	Refers to Stream Type (SPTS, MPTS, Plant or Data).
GbE Port	GbE port of the stream.
Destination IP Address	Destination IP address of the stream. For multicast streams, it is the multicast address.
Source IP Address	Source IP address of the stream. For multicast, it is 0.0.0.0

Chapter 3 General Configuration and Monitoring

Status	Describes stream status. <ul style="list-style-type: none">■ Stream active stream is bound to a video source and is active.■ Input Loss: Stream mapped but no video■ Wait for PAT: Stream mapped but waiting for PAT.■ Wait for PMT: Stream mapped but waiting for PMT.■ Content Loss: Stream content loss detected.■ Bad Input: Input stream issues found too many SI changes.■ Wait on Content: Stream content arrival pending.■ Input PID Conflict: Input Stream contains PID conflict.
Input Program Number	Program number of input stream.
Input PMT PID	PID of the stream's PMT.
Input PCR PID	PID of the stream's PCR.
Total Elementary Stream PIDs	Number of input PIDs. Varies with SPTS and MPTS.
Input Bitrate	Bitrate of the input program stream.

For MPTS streams, the Details button (the first button under the *Program Number* parameter) provides additional information on Elementary Streams. The following screen appears.

Device Information

The following platform related device information is available for the RF Gateway 1.

- Temperature
- Power Supply voltage
- Fan tachometer reading
- Resource Utilization (V2.1.9)

The current status of the above components are monitored and if normal thresholds of operation are exceeded, an alarm will generate on the system. Refer to ***Fault Management of the RF Gateway 1*** (on page 65) for additional information.

Inventory

The Inventory page contains status information on the active software and hardware revisions of the system controller board and hot-swappable components in the system. The following illustration shows the Inventory screen.

Inventory				
Device	Slot	Status	Software Version	Hardware Revision
Controller Board	---	Present	02.01.09	01.00.00
GbE SFP	1	Present	---	A
GbE SFP	2	Absent	---	---
GbE SFP	3	Present	---	---
GbE SFP	4	Absent	---	---
QAM Card	1	Present	00.16	01
QAM Card	2	Present	00.16	01
QAM Card	3	Present	00.16	01
QAM Card	4	Present	00.16	01
QAM Card	5	Present	00.16	01
QAM Card	6	Present	00.16	01
Power Supply 1	1	Absent	---	---
Power Supply 2	2	Present	---	---

Parameters

The following table explains the Inventory parameters.

Parameter	Description
Device	System component of an RF Gateway 1.
Slot	Slot number of a device.
Status	Refers to presence or absence of the device.
Software Version	Software version of the device.
Hardware Version	Hardware version of the device.

Output Monitoring

The Output Monitoring page provides information related to how transport streams on the input are bound to QAM resources on the output. The *Details* button under the *Input* parameter provides additional information on the input stream associated with a particular output session. See the following screen.

RFGW-1 Output Sessions
 Display PIDs in hex

Session ID	Type	RFGW QAM Channel	SRM QAM Channel	Output Bitrate (Mbps)	Status	GbE Port	Destination IP Address	UDP Port	Output			Input
									Program Number	PMT PID	PCR PID	
000000000000/1	SPTS	1/1.1	1	3.0636	Bound	1	226.1.1.1	Ignored	2	258	259	Details
000000000000/2	SPTS	1/1.1	1	3.0636	Bound	1	226.1.1.2	Ignored	3	274	275	Details
000000000000/3	SPTS	1/1.1	1	3.0501	Bound	1	226.1.1.3	Ignored	4	290	291	Details
000000000000/4	SPTS	1/1.1	1	3.0531	Bound	1	226.1.1.4	Ignored	5	306	307	Details
000000000000/5	SPTS	1/1.1	1	3.0456	Bound	1	226.1.1.5	Ignored	6	322	323	Details
000000000000/6	SPTS	1/1.1	1	3.0516	Bound	1	226.1.1.6	Ignored	7	338	339	Details
000000000000/7	SPTS	1/1.1	1	3.0531	Bound	1	226.1.1.7	Ignored	8	354	355	Details
000000000000/8	SPTS	1/1.1	1	3.0531	Bound	1	226.1.1.8	Ignored	9	370	371	Details
000000000000/9	SPTS	1/1.1	1	3.0531	Bound	1	226.1.1.9	Ignored	10	386	387	Details
000000000000/16	SPTS	1/1.1	1	3.0546	Bound	1	226.1.1.10	Ignored	11	402	403	Details
000000000000/17	SPTS	1/1.2	2	3.0636	Bound	1	226.1.1.1	Ignored	2	258	259	Details
000000000000/18	SPTS	1/1.2	2	3.0636	Bound	1	226.1.1.2	Ignored	3	274	275	Details
000000000000/19	SPTS	1/1.2	2	3.0501	Bound	1	226.1.1.3	Ignored	4	290	291	Details
000000000000/20	SPTS	1/1.2	2	3.0531	Bound	1	226.1.1.4	Ignored	5	306	307	Details
000000000000/21	SPTS	1/1.2	2	3.0456	Bound	1	226.1.1.5	Ignored	6	322	323	Details
000000000000/22	SPTS	1/1.2	2	3.0516	Bound	1	226.1.1.6	Ignored	7	338	339	Details
000000000000/23	SPTS	1/1.2	2	3.0531	Bound	1	226.1.1.7	Ignored	8	354	355	Details
000000000000/24	SPTS	1/1.2	2	3.0531	Bound	1	226.1.1.8	Ignored	9	370	371	Details

Parameters

The following table describes the Output parameters.

Parameter	Description
Session ID	The ID of the output session.
Type	Refers to Session Type (SPTS, MPTS, Plant or Data).
RFGW QAM Channel	Output QAM channel for a particular session ID.
SRM QAM Channel	The channel identification for the SRM.
Output Bitrate	Output bitrate of a session.
Status	Describes session status. <ul style="list-style-type: none"> ■ Unbound: The session is not active. ■ Bound: The session is active and bound to QAM resources on the output. ■ Bad input: The input stream associated with this stream is invalid.
GbE Port	The GbE port of the input stream associated with an output session.
Destination IP Address	Destination IP address of the stream. For multicast streams, it is the multicast address.
UDP Port	UDP port of the input stream associated with a session.
Output	Refers to output program number, PMT PID, and PCR PID for a session.
Input	Provides details on the input stream associated with an output session.

Session Refresh

The RFGW-1 generates an input pid conflict alarm (Alarms/Events section) if any ES or the PMT pid in an MPTS is the same as a pid already in use in the same MPTS. Recall that it is the user's responsibility to ensure that the pids in an MPTS are unique. To clear the pid conflict alarm it is necessary to not only resolve the input pid conflict at the source e.g. the DCM but also to refresh the associated sessions as seen in the following screen shots. Recall that the pid conflict is to be resolved before refreshing the session.

Once input PID conflict is detected, the services that are involved in the conflict will not be routed to the output.

Session Refresh Procedure

Find out the IP address of the MPTS with the conflict:

Alarms/Events

Active Alarms

11 out of 11 active alarms listed

Date/Time	Type	Severity	Instance	Threshold	Actual	Units	Details
07 MAR 12 12:13:03	IpPIDConflict	Major	1	n/a	n/a	n/a	Input.PID.Conflict: GbePort = 2, Stream IP = 233.12.34.56, UDP = 0. Resolve the PID conflict at the input and perform a session refresh to recover.

Verify that the MPTS displays the input pid conflict by viewing the input monitor page:

RFGW-1 Input Streams

Display PIDs in hex

Type	Gbe Port	Destination IP Address	UDP Port	Source IP Address	Status	Program Number	PMT PID	PCR PID	Total ES PIDs	Input Bitrate (Mbps)	Replicated
MPTS	3	233.12.34.56	Ignored	0.0.0.0	Input PID Conflict	Details	N/A	N/A	68	69.9916	1.0

Hunt for the output session with the pid conflict by searching through the output monitor detail pages:

RFGW-1 Output Sessions

Display PIDs in hex

Session ID	Type	RFGW QAM Channel	SRM QAM Channel	Output Bitrate (Mbps)	Status	Gbe Port	Destination IP Address	UDP Port	Program Number	PMT PID	PCR PID	Input
000000000000000000012018*	SPTS	4/1.1	49	1.8304	Bound	3	233.12.34.56	Ignored	20	1596	1587	Details
000000000000000000013719	SPTS	4/1.2	50	2.4846	Bound	3	233.12.34.56	Ignored	21	1596	1597	Details
000000000000000000014720*	SPTS	4/1.3	51	0.0000	Bound	3	233.12.34.56	Ignored	22	1606	1607	Details

RFGW-1 Input Details - Windows Internet Explorer

Display PIDs in hex

Type	Gbe Port	Destination IP Address	UDP Port	Source IP Address	Status	Program Number	PMT PID	PCR PID	Total ES PIDs	Input Bitrate (Mbps)
MPTS	3	233.12.34.56	Ignored	0.0.0.0	Input PID Conflict	All	N/A	N/A	68	69.9871

Once the PID conflict is resolved at the headend device, then after refreshing the session, the PID conflict alarm will be cleared. The state in the Input Monitor page will also change to Active only after the session refresh is completed. Even if the input PID conflict is resolved, but the session refresh button is not clicked, then state in Input monitor page will remain as "Input PID conflict"

Data Monitoring

The Data Monitoring page provides information related to how data streams on the input are bound to QAM resources on the input. The following illustration shows the Data Monitoring screen.

Output Channel	Type	GbE Input	Output Bitrate (Mbps)	Destination IP	UDP / DEPI	Status	Synch State	Synch Counter
1/1.1	DOCSIS MPT w/o UDP	1	0.8787	12.1.1.2	1	Stream Active	Primary	21571
1/1.2	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	2	Stream Active	Non-Primary	0
1/1.3	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	3	Stream Active	Non-Primary	0
1/1.4	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	4	Stream Active	Non-Primary	0
1/2.1	DOCSIS MPT w/o UDP	1	0.8787	12.1.1.2	5	Stream Active	Primary	22303
1/2.2	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	6	Stream Active	Non-Primary	0
1/2.3	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	7	Stream Active	Non-Primary	0
1/2.4	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	8	Stream Active	Non-Primary	0
2/1.1	DOCSIS MPT w/o UDP	1	0.8769	12.1.1.2	9	Stream Active	Primary	22303
2/1.2	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	10	Stream Active	Non-Primary	0
2/1.3	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	11	Stream Active	Non-Primary	0
2/1.4	DOCSIS MPT w/o UDP	1	0.0006	12.1.1.2	12	Stream Active	Non-Primary	0

Parameters

The following table explains the Data parameters.

Parameter	Description
Output Channel	The output channel for a data stream.
Type	Type of data stream (DOCSIS MPT with UDP, DOCSIS MPT without UDP, DOCSIS PSP with UDP, DOCSIS PSP without UDP, MPEG, DATA).
GbE Input	GbE input associated with the data stream.
Output Bitrate	Bitrate of the data stream.
Destination IP	Destination IP of the data stream.
UDP/DEPI	Destination UDP or DEPI session ID for the data stream.
Status	Status of the data stream (Stream Active, Stream Inactive).

Parameter	Description
Synch State	Describes whether the data flow is a primary flow containing DOCSIS synch messages or a non-primary flow that does not contain sync messages.
Synch Counter	The number of sync messages received in a primary flow.

DTI Monitoring

DTI Monitoring provides monitoring of status and statistical information on the DOCSIS Timing Interface. The following parameters are available.

- Active Port
- Client Status
- DTI Port Status (for each port)
- DTI Statistics

The following screen shows DTI monitoring.

The screenshot displays the DTI monitoring page for device rfgw-1d. The interface includes a navigation menu on the left and a main content area with several data sections:

- Active Port:** Neither
- Client Status:**
 - State: Free run
 - 10.24 MHz Activity-State: Present
 - Time Stamp: 0x1E5114C0
- DTI Port Status:**

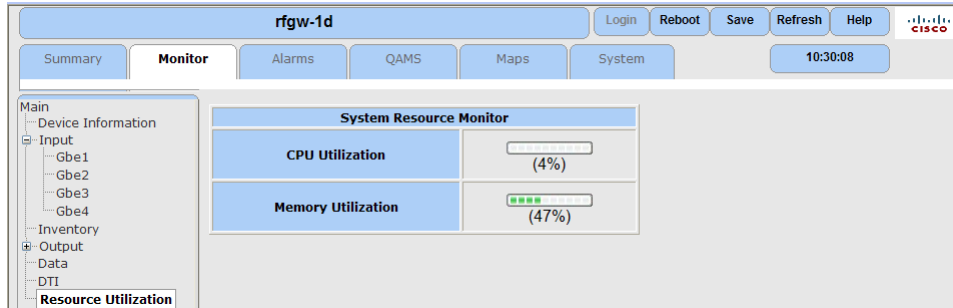
	Port 1	Port 2
DTI Signal Detected	No	No
Server Device Type	0x0	0x0
Server Status	N/A	N/A
CRC Error Count	0x0	0x0
Cable Advance	0x0	0x0
TOD Count	0x0	0x0
Frame Error rate	< 2%	< 2%
- DTI Statistics:**

T3 State Transition Count	0x0
T4 State Transition Count	0x0
T6 State Transition Count	0x0
T7 State Transition Count	0x0
Normal Time Count	0x0
Holdover Time Count	0x0
Phase Error	0x0
Integral Frequency Term	0x73d
EFC Value	0xe04
DTI Client Specification Version	1
Firmware Revision	276
Port Switch Count	0

For more information on DTI statistics, refer to *Basic M-CMTS Data Specific Operation* (on page 113).

Resource Utilization

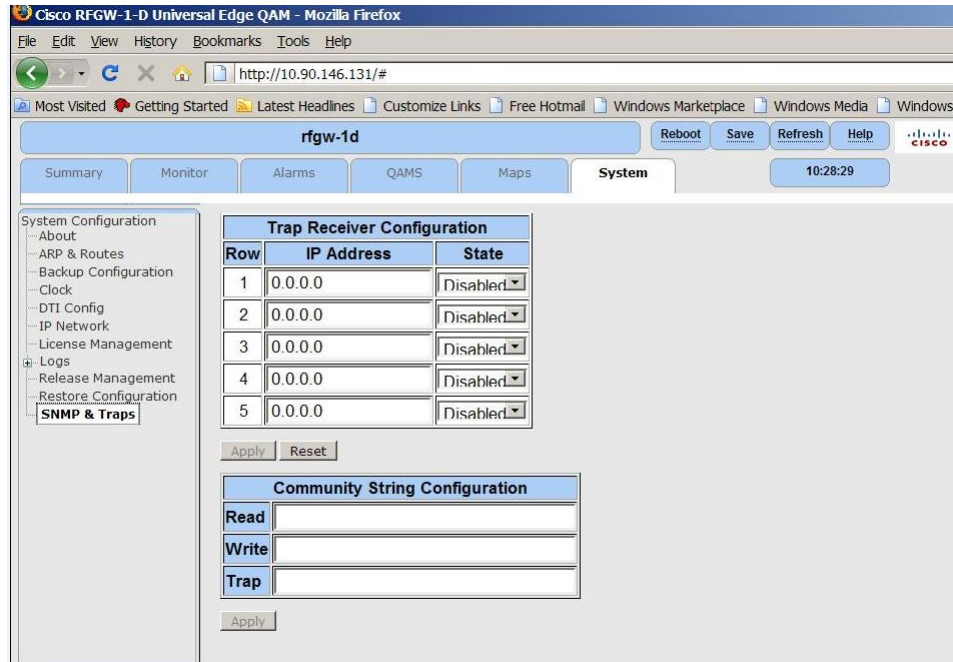
CPU and memory utilization are displayed for the operator in real time for monitoring.



SNMP Configuration

SNMP configuration is done on the GUI using the *System/SNMP & Traps* page. There are two configurations as shown in the examples below.

The first configuration is for software versions prior to 2.01.09. Refer to the screen below.



In this configuration, three community strings can be set. The "Read" string is the get community string. The "Write" string is the set community string and the "Trap" string is the trap community string. In this configuration, all traps are SNMPv1. Up to 5 traps can be enabled/disabled.

Chapter 3 General Configuration and Monitoring

The second configuration is for software versions 2.01.09 and later. Refer to the screen below.

The screenshot displays the configuration interface for a device named 'rfgw-1d'. The interface includes a top navigation bar with buttons for 'Login', 'Reboot', 'Save', 'Refresh', and 'Help', along with a Cisco logo and a timestamp of '09:42:18'. Below this is a secondary navigation bar with tabs for 'Summary', 'Monitor', 'Alarms', 'QAMS', 'Maps', and 'System'. A left-hand sidebar lists various configuration categories, with 'SNMP & Traps' selected. The main content area is titled 'Trap Receiver Configuration' and contains a table with five rows. Each row has columns for 'Row', 'IP Address', 'State', and 'Trap Community string'. All 'State' values are 'Disabled' and all 'Trap Community string' values are represented by six asterisks. Below the table are 'Apply' and 'Reset' buttons. At the bottom of the main area is a 'Community String Configuration' section with 'Read' and 'Write' input fields and an 'Apply' button.

Row	IP Address	State	Trap Community string
1	0.0.0.0	Disabled	*****
2	0.0.0.0	Disabled	*****
3	0.0.0.0	Disabled	*****
4	0.0.0.0	Disabled	*****
5	0.0.0.0	Disabled	*****

In this configuration, the "Read" string is the get community string. The "Write" string is the set community string. Traps can be set to disabled for each receiver. Each trap receiver can have its own trap community string.

Fault Management of the RF Gateway 1

The RF Gateway 1 supports automatic detection and user notification of changes in the system. Changes may be classified as either Events or Alarms. Alarms carry a state while events are important instances that occur in time and are reported. For example, *Link Lost* and *Link OK* are two well-defined states and are associated with an alarm. *Events Startup*, *Configuration Backup*, and *Second Power Supply Inserted* do not have a state but are important events reported by the system.

System Alarms

System Alarms are conditions with state that occur on the system that the user may want to be aware of. The RF Gateway 1 provides user notification of changes in alarm state. These notifications can be via SNMP traps, system log or the front panel fault LED. System alarms can not be masked or filtered and will always be indicated on the system.

The default alarms supported by the system are defined in the alarm configuration area of the database. The default alarm configuration parameters include items such as alarm label, severity, mask, threshold, and enabled notifications. These parameters are defaults and are not configurable through the web interface.

While active, the system maintains additional information on each of the alarms such as alarm originator, state, instance, and other descriptive details including triggering threshold, actual value, and units. Alarms have two possible state values, Alarm and Clear. Each alarm has two possible severity levels, Critical or Major. The supported alarms are described in the following table.

Name	Severity	Description
Power On Self Test	Critical	A failure during power on self test has been detected.
GbE Port Link	Critical	A GbE port has changed state.
UDP Traffic	Major	Complete loss of UDP traffic has been detected.
Fan Failure	Major	One of the four chassis fans RPM is measuring below threshold.
FPGA Temperature	Major	A FPGA board temperature has exceeded the threshold.
Power Supply Shutdown	Critical	A power supply has indicated an imminent shutdown.
DTI Port Link	Critical	A DTI port has changed state.
Power Supply Voltage	Critical	One or more power supply voltages is performing outside of the acceptable threshold.
Continuity Count Error	Critical	MPEG continuity counts have been detected on one or more elementary streams.

Chapter 3 General Configuration and Monitoring

Name	Severity	Description
Stream De jitter	Major	One or more transport streams are present with excessive jitter.
QAM Temperature	Major	A QAM temperature has exceeded an acceptable threshold.
QAM NCO Lock	Major	A QAM has lost NCO Lock.
Release Invalid	Major	Active system release is invalid.
DTI Backup Port	Major	Backup DT Alarm: Port failover or backup port not connected in auto failover mode.
QAM Oversubscribed	Major	Input rate on provisioned QAM BW exceeds QAM capacity.
License	Major	Unlicensed feature in use.
QAM General Failure	Major	Combined temperature and voltage alarm.
QAM Initialization	Major	QAM card failed to initialize.
EIS Channel Closed by Peer		EIS channel connection closed by CA System.
EIS Connection Lost	Major	EIS channel connection to CA System lost.
ECMG No Channel Available	Major	No ECMG channel available.
ECMG Connection Lost	Major	ECMG connection to CA System lost.
CW Stream Clear Extension	Major	Clear extension alarm: Scrambling not started.
CW Stream CP Extension no Comp	Major	CP extension due to mismatch between SCG and components.
CW Stream CP Extension no ECMs	Major	CP extension due to failure to receive ECMs.
ECM Stream PID could not be Allocated	Major	PID cannot be allocated or already in use.
GbE Port CRC	Major	CRC error threshold exceeded on GbE port.
Bind Failed	Major	Bind failed on EIS for socket port.
QAM Voltage	Major	QAM card over temperature threshold.
QAM Summary	Major	QAM card summary alarm, including UPX failure.
Input PID Conflict	Major	PID conflict is detected in the input stream
License Violation	Major	The upper 48 QAM channels require a DATA and/or a POWERKEY, and/or a DVB license.

System Events

System Events are conditions without state that the user may want to be aware of. The RF Gateway 1 provides user notification of these events. These notifications can be via SNMP traps or the system log. System events cannot be masked or filtered and will always be indicated on the system.

The default events supported by the system are defined in the event configuration area of the database. The default event configuration parameters include items such as event label, mask, and enabled notifications. These parameters are defaults and are not configurable through the web interface.

The system reports additional information on actual events such as event originator, instance, and other descriptive details including triggering threshold, actual value, and units. Supported events are described in the following table.

Name	Description
QAM Card Mount	A QAM card has been inserted or removed from the chassis.
QAM Configuration Change	A configuration change has been detected on a QAM card parameter.
Power Supply Mount	A redundant power supply has been inserted or removed from the chassis.
SFP Mount	An SFP has been inserted or removed from the RF Gateway chassis.
Download	A download event has occurred on the chassis.
Log Near full	The log is 80% full.
Log Almost full	The log is 90% full.
Log Full	The log is 100% full and will roll over.
Configuration Backup	The system configuration has been backed up.
Configuration Restore	The system configuration has been restored.
Configuration Save	The system configuration has been saved to the flash file system.
Release Invalid	Invalid inactive release detected on the system.
Startup	The RFGW has entered startup (boot)
DOCSIS	DTI sync changed from/to active. DOCSIS SYNC messages are received/not received from CMTS.
DTI	Operating mode of the DTI port change.
Exception	Exception reported by low level operating system.
Download License	The RFGW-1 has been instructed to download a license via FTP. FTP complete.
OLS	License feature has been added.
EIS Active Proxy Removed	Active EIS proxy has been removed.

Name	Description
ECMG Active Proxy Removed	Active ECMG proxy removed
ECMG Channel Error	Received channel error for SuperCAS ID
GbE Port Switch	Redundant input port failover.
Download SSL	Security documents injected.
Download SSH	Security documents injected.
Stream Source Switch	Multicast SSM source switch.
NCS CAM Change	A new non-configured stream enters the RFGW-1.
Stream Status Change	When a multicast stream becomes Active/when the state changes from Active to Input Loss/when the user forces revert multicast stream to primary port.
CA Blob Length Error	More than 4CA blobs in a create session request. The extra blobs are discarded.
Ingress All	When a unicast stream is Active on a certain input port and the stream is detected on other port(s) duplicate stream detected.

User Notification of Alarms and Events

The system provides notifications of Alarms and Events in a variety of ways. These include Front Panel Alarm Indication, Alarm Table (web interface), SNMP Traps and Log Entries.

Front Panel Alarm Indication

A fault LED on the front panel is provided to allow quick and easy notification of an alarm existing on the system. When one or more alarms are active, the LED is solid red. When no alarms are active, the LED is off. The fault LED blinks during system boot but stabilizes to indicate alarm status after the system has initialized.

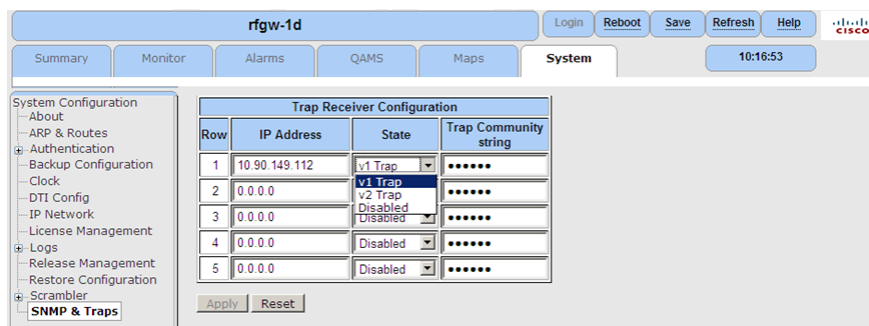
Alarm Table

The alarm table is another indicator of alarm status. The table is accessible through the web interface and provides detailed information regarding alarm status. A condensed version of the alarm status is also available on the Summary page of the web interface. The alarm table is shown below.

rfgw-1d							
Summary	Monitor	Alarms	QAMS	Maps	System	18:57:01	
Active Alarms							
Date/Time	Type	Severity	Instance	Threshold	Actual	Units	Details
14 JAN 70 03:01:28	Power Supply	Critical	1	Power supply 1 is in FAULT state. OT_WARN = 0, DC_GOOD = 1, left/right board temps = 30/27
Active alarm count: 1							

SNMP Traps

SNMP traps may also be used to provide notification of system alarms and events. The SNMP & Traps page of the web interface allows for configuration of trap receivers for this purpose. When configured, SNMP traps will be sent for all system alarms and events. The RF Gateway 1 supports SNMP V1 and V2 traps and a trap community string as shown below.

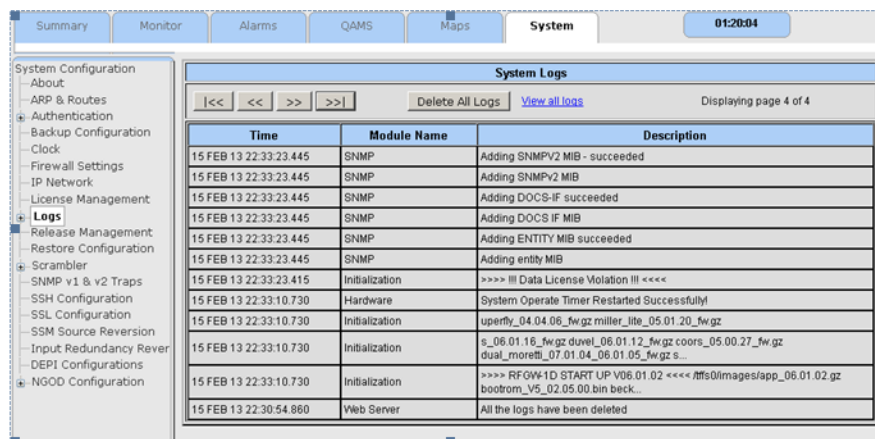


Active Alarms Table

The active alarms table is a dynamic table containing all currently active alarms. This table is accessible using the OID rfgw1ActiveAlarmTable (1.3.6.1.4.1.1429.1.12.1.2.14.1). A detailed description of the table can be found in the SA-RFGW-1-MIB proprietary MIB.

System Log

The system log provides a record of alarms and events that have occurred on the system. Log entries are always provided for each system alarm and event. The system is also capable of lower level logging for more detailed monitoring. In this case, log filtering is provided to control the type and level of information written to the log. The logged information can be categorized as module-related or low-level alarms. An example of a log screen showing various alarms and events on the system is shown below. An intuitive user interface is provided to navigate through the logs, delete logs and save logs to a file.

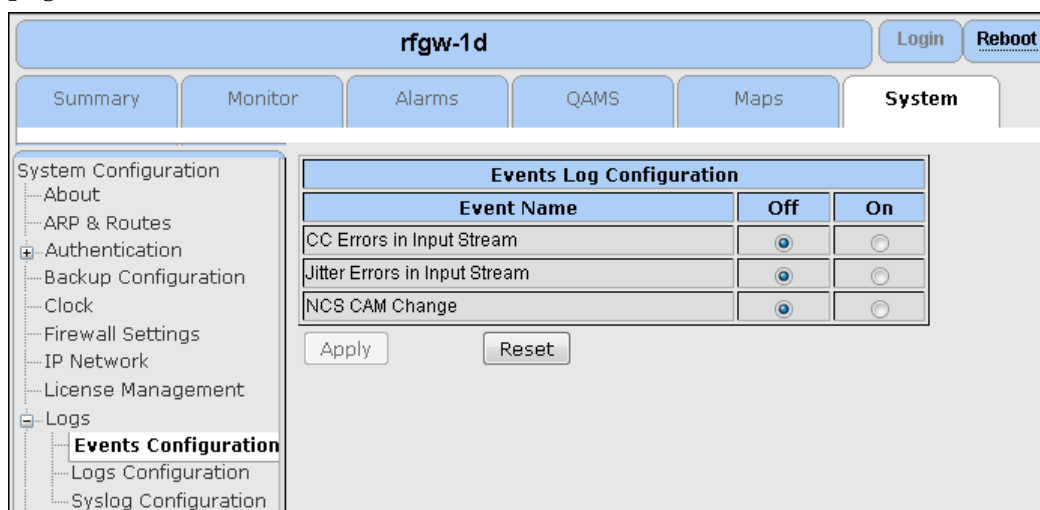


System Log Configuration

The RF Gateway 1 can be configured to filter events and alarms based on module and verbosity level. As an advanced configuration option, the RF Gateway 1 can also be configured for low level alarms. Module and low level alarms may be filtered with terse or verbose log levels or turned off completely by the user. It is recommended that all low level logging be set to **Off** unless actively troubleshooting.

To Configure Events

- 1 Navigate to the System/System Configuration/Logs/Events Configuration page.



- 2 Turn on/off the logging for the events listed in the UI.
- 3 Click **Apply**.

To Configure System Logs

- 1 Navigate to the System/System Configuration/Logs/Logs Configuration page.

The screenshot shows the Cisco configuration interface for a device named 'rfgw-1d'. The top navigation bar includes buttons for 'Login', 'Reboot', 'Save', 'Refresh', and 'Help', along with the Cisco logo and the time '13:25:49'. Below this is a secondary navigation bar with tabs for 'Summary', 'Monitor', 'Alarms', 'QAMS', 'Maps', and 'System'. The 'System' tab is active, and the left-hand navigation menu is expanded to 'Logs Configuration'. The main content area displays a table titled 'System Log Configuration' with columns for 'Module Name', 'Off', 'Terse', and 'Verbose'. Each row represents a different system module with radio buttons to select the logging level. At the bottom of the table are 'Apply', 'Reset', and 'Show Advanced Filters' buttons.

Module Name	Off	Terse	Verbose
Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Download, Backup & Restore	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
DTI	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
FTP License	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Hardware	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
IGMP	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Initialization	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Input Ports	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Logging	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
OLS Licensing	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
QAM Cards	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
PowerKEY	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Scrambler	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SDV Communications	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SNMP	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Stream Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
NGOD Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
DEPI CP Management	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

- 2 Select the desired logging level for each module category.
- 3 Click **Apply**.

Advanced Logging Filters

Logging filters for low-level alarms are configured as follows.

- 1 Click **Show Advanced Filters**.

Result: The advanced filters window is displayed.

Advanced Filters			
Module Name	Off	Terse	Verbose
Calibration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Plane Hardware	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dejitter Buffer	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Factory	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Front Panel	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Input Stream Processing	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Low Level Alarms	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Output Stream Processing	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Packet Processor	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Resource allocator	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Scheduler Modulator	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SFP MAC	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Socket	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web Server	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

- 2 Select the desired filter levels for each category of low-level alarms.

Note: It is recommended that all low level logging be set to **Off** unless actively troubleshooting.

- 3 Click **Apply**.

To Configure Syslog

- 1 Navigate to the *System/System Configuration/Logs/Syslog Configuration* page to configure the details of the remote syslog server.

The screenshot shows the configuration page for the Syslog Server. The interface includes a top navigation bar with 'rfgw-1d' and 'Login/Reboot' buttons. Below this is a secondary navigation bar with tabs for 'Summary', 'Monitor', 'Alarms', 'QAMS', 'Maps', and 'System'. A left-hand navigation tree is expanded to 'Logs/Syslog Configuration'. The main configuration area contains the following fields:

Syslog Server Configuration	
Enable Syslog	Disabled
IP Address	
UDP Port	514

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

- 2 Set Enable Syslog field as Enabled.
- 3 Enter the IP Address and UDP Port of the remote syslog server.
- 4 Click **Apply**.

Configuration Management

Configuration Save

The RF Gateway 1 allows configuration changes to be saved to the files in the flash file system. Configuration information can be classified as platform-generic or platform-specific. Platform-generic information applies to many systems while platform-specific applies to individual systems. For example, IP addresses and system name or location are platform-specific parameters. QAM card configuration is considered generic and common to many systems. This segregation provides the ability to clone and distribute system configuration throughout the network. Platform-generic information is saved by clicking the **Save** button at the top of the web interface page.

This operation performs a global save of the RF Gateway 1 configuration. The configuration information is saved in the file /tffs0/rfgw_xml_db.gz in the flash with a backup copy also kept in /tffs0/rfgw_xml_db_bkup.gz. Once saved in the flash, the system configuration file can then be transferred to a remote FTP server as described in *Configuration Backup* (on page 74).

The platform-specific configuration parameters are saved in a different set of files, /tffs0/rfgw_ot.xml for primary and /tffs0/rfgw_ot_bkup.xml for backup. These files are updated as certain parameters are changed from the web interface. These parameters are unlikely to change after their initial configuration.

Software version 1.3.11 has an automatic save feature which allows applied database changes to be automatically saved to preserve them in nonvolatile memory.

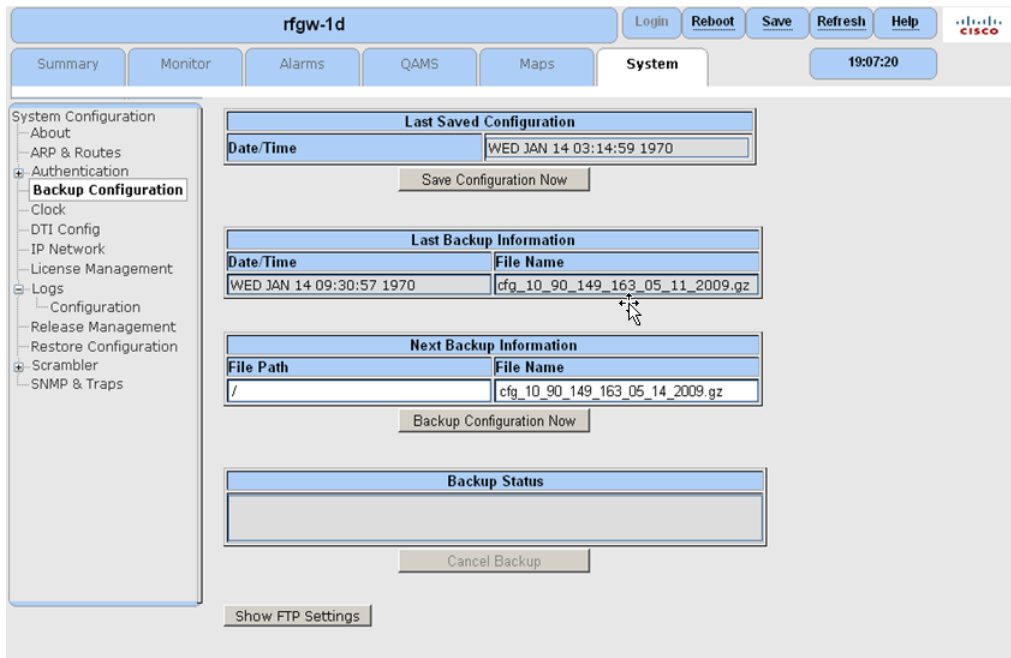
Configuration Backup

The RF Gateway 1 performs configuration backup via FTP to a backup server. The backup databases generally contain QAM parameters, channel application modes and mapping tables. The backup databases generally do not include IP networking settings (including management as well as GbE input port parameters).

To Backup Configuration

- 1 Navigate to the *System/Backup Configuration* window.

Result: The following window is displayed.



- 2 Click **Show FTP Settings** at the bottom of the window.

Result: The Configuration FTP Server window is displayed.

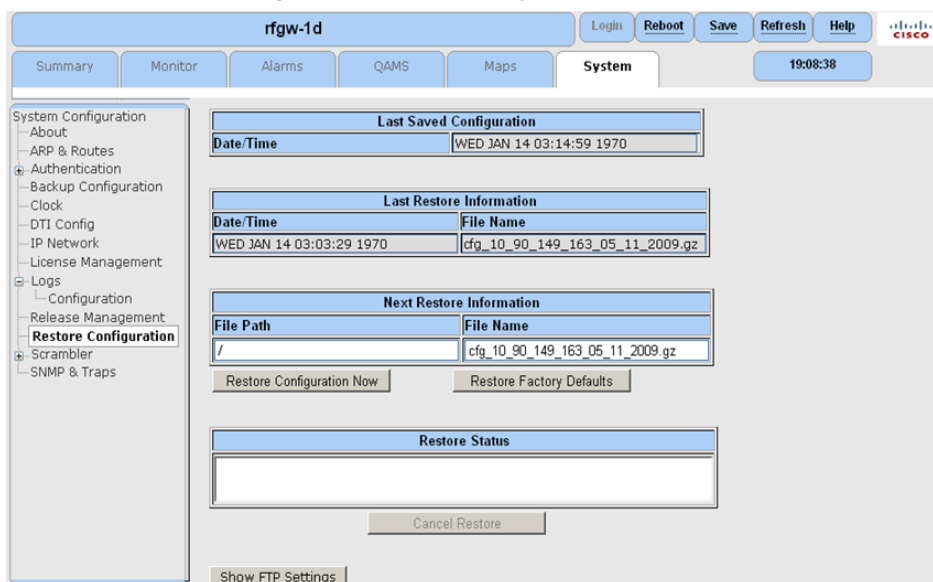
- 3 Enter the backup server's IP address.
- 4 Enter the FTP user name.
- 5 Enter the FTP password.
- 6 Click **Apply**.
- 7 Click **Test FTP Connection**. Verify your connection with the FTP login success popup.
Note: If a failure occurs, recheck the IP address, user name and password.
- 8 Click **Save**.
- 9 In the "Next Backup Information" table, enter the backup file name.
Example: cfg_01.gz
- 10 Click **Backup Configuration Now** to initiate backup.
Note: If backup failure occurs, recheck the path to the backup directory.

Configuration Restore

To Restore Configuration

- 1 Navigate to *System/Restore Configuration* page.

Result: The following window is displayed.



- 2 Click **Show FTP Settings** at the bottom of the window.

Result: The *Configuration FTP Server* window appears.

- 3 Enter the backup server's IP address.
- 4 Enter the FTP user name.
- 5 Enter the FTP password.
- 6 Click **Apply**.
- 7 Click **Test FTP Connection**. Verify your connection with the FTP login success popup.
- Note:** If a failure occurs, recheck the IP address, user name and password.
- 8 Click **Save**.
- 9 In the "Next Restore Information" table, enter the backup file name.
Example: cfg_01.gz
- 10 Select **Restore Configuration Now** to initiate restore.

Notes:

- If restore failure occurs, check the path to the backup directory.
- The device automatically reboots after restoring a saved configuration.
- Close the browser after the device begins rebooting.

Release Management

Software and firmware upgrades to the RF Gateway 1 are controlled via system release. Using the System/Release Management web page, the operator can provision the RF Gateway 1 to perform system release upgrades via FTP from a release directory on an upgrade server.

Each unique system release directory on the upgrade server contains the necessary software and firmware components to upgrade an RF Gateway 1 device from any previous revision.

The components of a system release include:

- application software image
- programmable firmware images
- boot code
- system release file (.xml)

The FTP server should be on a network that is accessible from the management port of the RF Gateway 1. When a software download is initiated, the RF Gateway 1 retrieves the system release file which contains the file names of the software and firmware components of the system release. The RF Gateway 1 then determines which files of the system release differ from those already resident on its flash file system. If file names do not match, they are automatically FTP'ed from the upgrade server.

A system release may include changes to any or all of the software or firmware components. As a result, the software application image may change for a new release and a firmware image may not. Likewise, a firmware image may change and the application image may not. The RF Gateway 1 retrieves the software and firmware images that changed since the last system release upgrade.

Downloading System Release Images

To Download Images

- 1 Navigate to the *System/Release Management* page.

Result: The following screen is displayed.

The screenshot shows the Cisco System Configuration interface for a device named 'rfgw-1d'. The top navigation bar includes 'Login', 'Reboot', 'Save', 'Refresh', and 'Help' buttons, along with a Cisco logo and the time '19:10:04'. The main menu on the left lists various configuration categories, with 'Release Management' highlighted. The central panel is divided into three sections: 'Current Firmware' with input fields for 'Active Release' (02.01.09), 'Inactive Release' (01.03.09), and 'Downloaded Release', accompanied by 'Revert' and 'Activate' buttons; 'Release File Information' with fields for 'Release File Path' and 'Release File Name', and 'Download Release' and 'Cancel' buttons; and 'Release Status' with an empty table. A 'Show FTP Settings' button is located at the bottom of the panel.

- 2 Click **Show FTP Settings** at the bottom of the window.

Result: The FTP window is displayed.

- 3 Enter the upgrade server's IP address.
- 4 Enter the FTP username.
- 5 Enter the FTP password.
- 6 Click **Apply**.

Result: The FTP Settings Applied Successfully pop-up appears.

- 7 Click **OK** to continue.
- 8 Click **Test FTP Connection**. Verify your connection with the FTP Login Success pop-up.

Note: If a failure occurs while verifying FTP connection, recheck your upgrade server IP address, username and password.

- 9 Click **Save**.

Note: Changes will be lost if not saved.

- 10 Locate the Release File Path field and enter the full path to the upgrade directory.

Example: /SW_Releases/RevA/V01.02.00

- 11 Enter the Release File name.

Example: rfgw1_rel_06_01_02.xml

12 Click the **Download Release** button to initiate download process.

Result: The RF Gateway 1 will FTP all necessary files (application & firmware) from the upgrade server as dictated in the system release file.

Note: If download failure occurs, recheck the path and filename of the system release file.

13 After the download process completes successfully, select **Activate**.

Result: The device automatically reboots to the new release.

14 Close the browser after the device begins rebooting.

A single previous system release is retained by the system after an upgrade. Once the system release upgrade is activated from the GUI, the previously active system release is retained as inactive. If the operator wishes to restore the inactive release at a later time, a revert capability is available using the System/Release Management web view.

Configuring, Monitoring, and Fault Management via SNMP

The RFGW-1 supports a set of proprietary and standard MIBs via SNMPv2. Through SNMP, the RFGW-1 can be configured and monitored. In addition, Fault Management is supported through the generation of SNMP traps for all system alarms and events.

The following table shows the MIBs supported.

MIB Name	Description
CISCO-RFGW-1-MIB (proprietary)	This MIB module contains objects necessary for management of the RFGW-1 device. This includes status, statistics, equipment inventory, remote download/upload, table definition, and other configurations as needed for the QAM.
CISCO-RFGW-1-TRAP-MIB.mib (proprietary)	Trap control MIB for the RFGW-1.
DOCS-IF-MIB	This is the MIB Module for DOCSIS 2.0 compliant Radio Frequency (RF) interfaces in Cable Modems (CM) and Cable Modem Termination Systems (CMTS).
ENTITY-MIB	The MIB module for representing multiple logical entities supported by a single SNMP agent.
SNMPv2-MIB	The MIB module for SNMP entities.
IF-MIB	The MIB module to describe generic objects for network interface sub-layers. This MIB is an updated version of MIB-II's ifTable, and incorporates the extensions defined in RFC 1229.

Monitoring Capability

The RFGW-1 can be monitored to evaluate network and other operational statistics by utilizing any MIB browser or other tool (for example, snmpget, snmpwalk) that collects SNMP information. Output bandwidth statistics can be retrieved using the CISCO-RFGW-1-MIB. See the following screen.

The screenshot shows the Reasoning MIB Browser interface. The left pane displays a tree view of MIBs under 'rfgw1QanChannel'. The right pane shows a 'Result Table' with columns for Name/OID, value, and Type. The table lists 48 entries for 'rfgw1QanChannelBandwidth' with values of 3799962. The bottom pane shows the MIB details for 'rfgw1QanChannelBandwidth', including its OID, syntax, access, status, and a description of the amount of bandwidth currently used on the QAM channel.

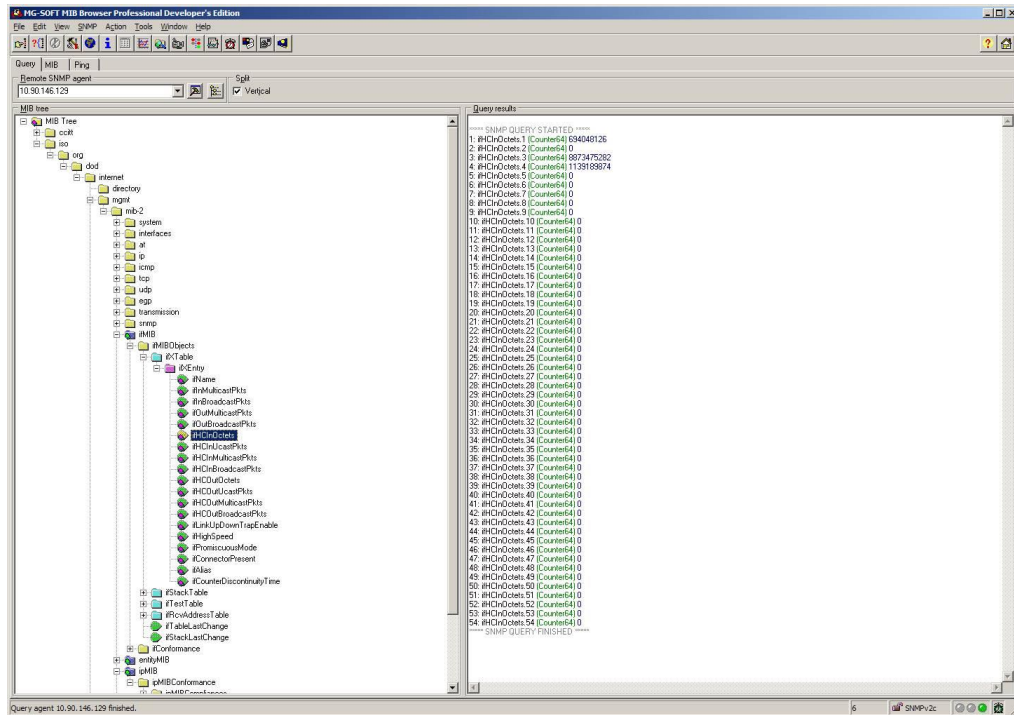
Name/OID	value	Type
rfgw1QanChannelBandwidth.1	3799962	Gauge
rfgw1QanChannelBandwidth.2	3799962	Gauge
rfgw1QanChannelBandwidth.3	3799962	Gauge
rfgw1QanChannelBandwidth.4	3799962	Gauge
rfgw1QanChannelBandwidth.5	3799962	Gauge
rfgw1QanChannelBandwidth.6	3799962	Gauge
rfgw1QanChannelBandwidth.7	3799962	Gauge
rfgw1QanChannelBandwidth.8	3799962	Gauge
rfgw1QanChannelBandwidth.9	3799962	Gauge
rfgw1QanChannelBandwidth.10	3799962	Gauge
rfgw1QanChannelBandwidth.11	3799962	Gauge
rfgw1QanChannelBandwidth.12	3799962	Gauge
rfgw1QanChannelBandwidth.13	37999763	Gauge
rfgw1QanChannelBandwidth.14	37999763	Gauge
rfgw1QanChannelBandwidth.15	3799962	Gauge
rfgw1QanChannelBandwidth.16	37999161	Gauge
rfgw1QanChannelBandwidth.17	37999161	Gauge
rfgw1QanChannelBandwidth.18	37999161	Gauge
rfgw1QanChannelBandwidth.19	37999161	Gauge
rfgw1QanChannelBandwidth.20	37999161	Gauge
rfgw1QanChannelBandwidth.21	3799962	Gauge
rfgw1QanChannelBandwidth.22	3799962	Gauge
rfgw1QanChannelBandwidth.23	3799962	Gauge
rfgw1QanChannelBandwidth.24	3799962	Gauge
rfgw1QanChannelBandwidth.25	3799962	Gauge
rfgw1QanChannelBandwidth.26	3799962	Gauge
rfgw1QanChannelBandwidth.27	3799962	Gauge
rfgw1QanChannelBandwidth.28	3799962	Gauge
rfgw1QanChannelBandwidth.29	3799962	Gauge
rfgw1QanChannelBandwidth.30	3799962	Gauge
rfgw1QanChannelBandwidth.31	3799962	Gauge
rfgw1QanChannelBandwidth.32	3799962	Gauge
rfgw1QanChannelBandwidth.33	3799962	Gauge
rfgw1QanChannelBandwidth.34	3799962	Gauge
rfgw1QanChannelBandwidth.35	3799962	Gauge
rfgw1QanChannelBandwidth.36	3799962	Gauge
rfgw1QanChannelBandwidth.37	3799962	Gauge
rfgw1QanChannelBandwidth.38	3799962	Gauge
rfgw1QanChannelBandwidth.39	3799962	Gauge
rfgw1QanChannelBandwidth.40	3799962	Gauge
rfgw1QanChannelBandwidth.41	3799962	Gauge
rfgw1QanChannelBandwidth.42	3799962	Gauge
rfgw1QanChannelBandwidth.43	3799962	Gauge
rfgw1QanChannelBandwidth.44	3799962	Gauge
rfgw1QanChannelBandwidth.45	37999763	Gauge
rfgw1QanChannelBandwidth.46	37999763	Gauge
rfgw1QanChannelBandwidth.47	37999763	Gauge
rfgw1QanChannelBandwidth.48	37999763	Gauge

MIB Details:

- Name: rfgw1QanChannelBandwidth
- OID: 1.3.6.1.4.1.1429.1.12.1.2.9.1.1.11
- MIB: SA-RFGW-1-MIB
- Syntax: Unsigned32 (0..51607)
- Access: read-only
- Status: current
- DefVal:
- Indexes: rfgw1QanChannelIndex
- Descr: The amount of bandwidth currently used on this QAM channel. Note that the maximum value for the range is for a QAM that is using annex ITU-A, QAM 256 and 7M symbols per second. Here are the ranges for the possible RF port bandwidth based on the possible settings:
ITU-A QAM 64 7 Mps:0-38705
ITU-A QAM 256 7 Mps:0-51607
ITU-B QAM 64 5.057 Mps:0-29970
ITU-B QAM 256 5.361 Mps:0-38814
ITU-C QAM 64 5.5 Mps:0-30411
ITU-C QAM 256 5.5 Mps:0-40549

Chapter 3 General Configuration and Monitoring

Input Statistics can be accessed using the IF-MIB. See the following screen.



4

Table-Based Video Specific Operation

This chapter provides information for provisioning the RF Gateway 1 for table-based video operation.

In This Chapter

- Provisioning..... 84
- Status Monitoring 97

Provisioning

The following sections provide information for provisioning the RF Gateway 1 for table-based video operation.

Prerequisite Configurations:

- GbE input ports, including Video/Data IP address
- QAM outputs
- Channel Application Mode = Video

Once a carrier is in video mode, the video stream map becomes active for that carrier. The video stream map serves as a routing table, which maps incoming video to unique output carriers.

Channel Application Mode

To Verify Channel Application Mode

- 1 Navigate to the *Maps* page.
- 2 In the tree menu, select **Map Configuration**.

Result: Channel Application Mode is revealed for each output carrier.

Note: The correct setting is "Data".

The screenshot shows the configuration page for RFGW-1-D. The 'Maps' tab is selected, and the 'Map Configuration' section is expanded. A table displays the configuration for 13 different locations. Each location has a 'Channel Application Mode' dropdown menu set to 'Video'.

Location	Channel#	Available	Channel Application Mode
1/1.1	01	Yes	Video
1/1.2	02	Yes	Video
1/1.3	03	Yes	Video
1/1.4	04	Yes	Video
1/2.1	05	Yes	Video
1/2.2	06	Yes	Video
1/2.3	07	Yes	Video
1/2.4	08	Yes	Video
2/1.1	09	Yes	Video
2/1.2	10	Yes	Video
2/1.3	11	Yes	Video
2/1.4	12	Yes	Video
2/2.1	13	Yes	Video

Video Stream Map Configuration

For a specific output carrier, using the Maps/Video Stream Map page, the following can be configured:

- Input Stream Destination IP address and UDP port
- Allowable ingress port or port-pair

- Stream Type (i.e., SPTS, MPTS)
- Program Number



WARNING:

The user is responsible for making sure there are no program number or PMVs on a given carrier as well as making sure all replicated transport streams have identical advanced settings. If not, the system may have to be reset to default settings to recover.

To Configure the Video Stream Map

- 1 Navigate to the *Maps* page.
- 2 In the tree menu, select Video Stream Map.

Result: The *Stream Map Table* is displayed.

The screenshot shows the 'rfgw-1d' web interface. The 'Maps' tab is selected. On the left, a tree menu shows 'Video Stream Map' selected. The main area displays the 'Stream Map Table' with the following data:

Row #	Output QAM Channel	Destination IP Address	UDP Port	Active	Allowed Ingress Ports	Stream Type	Program Number	PMV	Data Rate (kbps)
0	1/1.1	0.0.0.0	49158	True	Pair 1	SPTS	0	3	0
1	1/1.1	0.0.0.0	49160	True	Pair 1	SPTS	0	4	0
2	1/1.1	0.0.0.0	49162	True	Pair 1	SPTS	0	5	0
3	1/1.1	0.0.0.0	49164	True	Pair 1	SPTS	0	6	0
4	1/1.1	0.0.0.0	49166	True	Pair 1	SPTS	0	7	0
5	1/1.1	0.0.0.0	49168	True	Pair 1	SPTS	0	8	0
6	1/1.1	0.0.0.0	49170	True	Pair 1	SPTS	0	9	0
7	1/1.1	0.0.0.0	49172	True	Pair 1	SPTS	0	10	0
8	1/1.1	0.0.0.0	49174	True	Pair 1	SPTS	0	11	0
9	1/1.1	0.0.0.0	49176	True	Pair 1	SPTS	0	12	0
10	1/1.1	0.0.0.0	49178	True	Pair 1	SPTS	0	13	0

Below the table are 'Add Row', 'Apply', and 'Reset' buttons. The 'Base Rules' section includes fields for Base Value, Row Increment, Channel Offset, Start QAM Channel (1/1.1), End QAM Channel (1/1.1), Row Start, and Row End, with 'Implement Rules' and 'Reset' buttons. A 'Show Advanced Settings' button is at the bottom.

- 3 Locate the rows corresponding to the desired Output QAM Channel.
Note: The RF Gateway 1 web pages use the notation "Card/Port. Channel" to refer to individual carriers.
- 4 In the *Destination IP Address* field, enter the IP address.

Chapter 4 Table-Based Video Specific Operation

- For unicast streams, entering 0.0.0.0 is equivalent to specifying the GbE Video/Data IP address configured for the port pair (port-pair mode) or the physical address GbE port (independent mode) selected in step 7. Alternatively, the Video/Data IP address (port-pair mode) or GbE port address (independent mode) of the desired GbE port or port-pair may be explicitly entered.
 - For multicast streams, enter the multicast address of the desired stream.
- 5 In the *UDP Port* field, enter the destination UDP port of the desired stream. For unicast streams, the UDP port number uniquely identifies the stream. For multicast streams, this field is ignored.
- 6 In the *Active* field, select the appropriate setting.
- True - forward (route) the stream to the corresponding QAM output channel
 - False - block the stream to the corresponding QAM channel
 - Delete - deletes the entire routing entry (row) from the stream map.
- 7 In the *Allowed Ingress Ports* field, select the allowed ingress port-pair (port pair mode) or allowed ingress GbE port (independent mode).
- Pair 1 (Ports 1 and 2) - available in port pair mode
 - Pair 2 (Ports 3 and 4) - available in port pair mode
 - Port 1 - available in independent mode
 - Port 2 - available in independent mode
 - Port 3 - available in independent mode
 - Port 4 - available in independent mode
- 8 In the *Stream Type* field, select the stream type.
- SPTS - Single program encapsulated in the input flow
 - MPTS - Multiple programs encapsulated in the input flow
 - Data - A data stream does not include a PAT or PSI. A data stream is played out at a constant configured rate.
 - Plant - One or more elementary streams without timing information. A plant stream may include a PAT and is played out at a constant configured rate.
- 9 In the *Program Number* field, enter the "Input or "Output" program number.
- For MPTS streams, no input or output program number may be entered.
 - For SPTS streams, entering a 0 input program number will permit any incoming stream to be routed to the port. Entering a non-zero input program number will require the program number of the corresponding input stream to match before forwarding (routing) the stream to the corresponding QAM channel.
 - For SPTS streams, a unique output program number must be entered for each QAM Output Channel.

- 10 In the Pid Map Value (PMV) field, enter the following guidelines:
- For MPTS and data streams, no PMV value may be entered (PIDs are not remapped).
 - For SPTS and plant streams, the PMT PID value is determined by the following equation:
 - $\text{PMT PID} = (\text{PMV} + 1) * 16$
 - All elementary stream PIDs will be incrementally based off the PMT PID calculation.
- 11 In the Data Rate field, enter values according to the following guidelines.
- SPTS or MPTS Stream Type - No data rate may be entered. Playout rate is determined by timing recovery.
 - Data - A data rate should be selected to play out at a constant configured rate of 1-38812 Kbps and within the limitations of the output bandwidth of the QAM Output Channel.
 - Plant - A data rate should be selected to play out at a constant configured rate to include the SI data and within the limitations of the output bandwidth of the QAM Output Channel.
- 12 Click **Apply**.
- 13 Click **Save**.

Notes:

- When muxing 2 incoming MPTS streams to 1 output carrier (or when muxing 1 MPTS with 1 or more SPTSs), the operator is responsible for preventing PID conflicts and over-subscription of the carrier.
- To prevent PID conflicts, the operator must know what PIDs are being sent down in each of the MPTS streams, and if there are conflicts, they must be fixed at the source device. When muxing an MPTS with SPTSs streams, the operator must carefully choose PMV values for the SPTS streams that do not cause PID conflicts between the remapped SPTS streams and the passed-through MPTS stream. (The PMV value determines the PMT PID of the remapped SPTS and all elementary stream PIDs immediately follow the PMT PID in order. The $\text{PMT PID} = (\text{PMV} + 1) * 16$.)
- To prevent oversubscription of the carrier, the operator must know the maximum bitrates of all the services being mapped to the carrier and make sure the total bitrate can not exceed the capacity of the QAM carrier.

Automated Video Stream Map Configuration

Using advanced stream map generation, the operator can add multiple rows to the stream map simultaneously.

Chapter 4 Table-Based Video Specific Operation

To Configure Video Stream Map Using Base Rules

- 1 Navigate to the *Maps* page.
- 2 In the tree menu, select **Video Stream Map**.

Result: The *Stream Map Table* is displayed.

Stream Map Table

Row #	Output QAM Channel	Destination IP Address	UDP Port	Active	Allowed Ingress Ports	Stream Type	Program Number		PMV	Data Rate (bps)	
							Input	Output			
0	0	1/1.1	0.0.0.0	49158	True	Pair 2	SPTS	1	3	13	0
1	1	1/1.1	0.0.0.0	49160	True	Pair 2	SPTS	1	4	14	0
2	2	1/1.1	0.0.0.0	49162	True	Pair 2	SPTS	1	5	15	0
3	3	1/1.1	0.0.0.0	49164	True	Pair 2	SPTS	1	6	16	0
4	4	1/1.1	0.0.0.0	49166	True	Pair 2	SPTS	1	7	17	0
5	5	1/1.1	0.0.0.0	49168	True	Pair 2	SPTS	1	8	18	0
6	6	1/1.1	0.0.0.0	49170	True	Pair 2	SPTS	1	9	19	0
7	7	1/1.1	0.0.0.0	49172	True	Pair 2	SPTS	1	10	20	0
8	8	1/1.1	0.0.0.0	49174	True	Pair 2	SPTS	1	11	21	0
9	9	1/1.1	0.0.0.0	49216	False	Pair 1	SPTS	0	32	32	0
10	10	1/1.1	0.0.0.0	49218	False	Pair 1	SPTS	0	33	33	0

Add Row Apply Reset

Base Rules

Base Value	0.0.0.0	49158	True	Pair 1	SPTS	1	3	13	0
Row Increment	0	2				0	1	1	
Channel Offset	0	0							
Start QAM Channel	1/1.1	End QAM Channel	1/1.1	Row Start	0	Row End	30		

Implement Rules Reset

TP568

- 3 In the Base rules window, enter the Base Value (base values are the initial values the operator wants as the very first row in the stream map).
- 4 In the *Row Increment* field, enter row increments for the desired parameters. An increment value of 0 will retain a parameter without increment for each row. Typically, increment value of 0 is used for IP address.
- 5 In the *Channel Offset* field, enter desired offset (determines the increment for the channel output).

Example: Entering 10 in the UDP column of the Channel Offset row generates 10 entries in the stream map for each channel.

Note: Base Rules can be used at the full-device, card, port or individual channel level. Channel Offset is "don't care" when implementing Base Rules at the channel level.

- 6 In the *Start QAM Channel* field, enter the start and end QAM Channel.
- 7 Enter Row Start and Row End (defines rows the base values will be applied to).
- 8 Click Implement Rules.

- 9 Click **Apply**.
- 10 Click **Save**.

Advanced Settings

Advanced settings are useful for the following reasons:

- restrict input sources
- block PIDs
- split streams, etc.

Notes:

The RF Gateway 1 default database includes a pre-configured video stream map for the advanced settings. The default settings accept any source IP addresses, do not block the PIDS, break MPTS streams into SPTS for dejittering, and do not ignore UDP port.

The GUI can enable settings such as *PCR PID Select*, *MPTS Dejitter* and *Blocked PID* (only for MPTS streams).

To Configure Advanced Settings

- 1 Navigate to the *Maps* page.
- 2 Expand the tree menu to select the desired QAM Channel.

Result: The *Stream Map Table* is displayed.

The screenshot shows the configuration page for 'rfgw-1d'. The 'Maps' tab is selected, and the 'Video Stream Map' configuration is active. The 'Stream Map Table' is displayed with the following data:

Row #	Output OAM Channel	Destination IP Address	UDP Port	Active	Allowed Ingress Ports	Stream Type	Program Number	PMV	Data Rate (kbps)
0	1/1.1	0.0.0.0	49158	True	Pair 1	SPTS	0	3	0
1	1/1.1	0.0.0.0	49160	True	Pair 1	SPTS	0	4	0
2	1/1.1	0.0.0.0	49162	True	Pair 1	SPTS	0	5	0
3	1/1.1	0.0.0.0	49164	True	Pair 1	SPTS	0	6	0
4	1/1.1	0.0.0.0	49166	True	Pair 1	SPTS	0	7	0
5	1/1.1	0.0.0.0	49168	True	Pair 1	SPTS	0	8	0
6	1/1.1	0.0.0.0	49170	True	Pair 1	SPTS	0	9	0
7	1/1.1	0.0.0.0	49172	True	Pair 1	SPTS	0	10	0
8	1/1.1	0.0.0.0	49174	True	Pair 1	SPTS	0	11	0
9	1/1.1	0.0.0.0	49176	True	Pair 1	SPTS	0	12	0
10	1/1.1	0.0.0.0	49178	True	Pair 1	SPTS	0	13	0

Below the table are 'Add Row', 'Apply', and 'Reset' buttons. The 'Base Rules' section includes fields for Base Value, Row Increment, Channel Offset, Start OAM Channel (1/1.1), End OAM Channel (1/1.1), Row Start, and Row End. 'Implement Rules' and 'Reset' buttons are also present. A 'Show Advanced Settings' button is located at the bottom.

3 Configure the basic settings for a stream map.

Note: As you become an advanced user, basic and combined settings can be configured simultaneously.

4 Click **Show Advanced Settings**.

Result: The Advanced Settings window is displayed.

The screenshot shows the 'Advanced Settings' window. At the top left is a 'Hide Advanced Settings' button. Below it is a table with the following columns: Row #, Source IP Address (sub-columns 1, 2, 3, 4), Ignore UDP Port, PCR PID Select, MPTS Dejitter (sub-columns Mode, Ref), and Blocked PIDs. There are 11 rows, each with a '0' in the Row # column. All Source IP Address fields contain '0.0.0.0'. All Ignore UDP Port fields are set to 'False'. All PCR PID Select fields are set to 'From PMT'. All MPTS Dejitter Mode fields are set to 'One Stream'. All MPTS Dejitter Ref fields are set to '0'. All Blocked PIDs fields contain '0, 5191, -1, -1'. Below the table are 'Apply' and 'Reset' buttons. Below that is the 'Advanced Rules' section with fields for Value, Start QAM Channel (1/1.1), End QAM Channel (1/1.1), Row Start, Row End, and a dropdown set to 'True'. There are also 'Implement Rules' and 'Reset' buttons at the bottom.

- 5 In the *Source IP Address* field, enter the source IP addresses you want your stream to listen to.

- The default '0.0.0.0' implies don't care.
- 1 is primary
- 2 is secondary
- 3 is tertiary
- 4 is quaternary

Note: If the device detects a stream which matches any of these three, it will pass it through.

- 6 In the *Ignore UDP Port* field, select True or False.

Note: The Ignore UDP Port setting can potentially make the configuration of the GbE network easier because only the multicast IP address must be provisioned (i.e., remembered), but it assumes that only one stream on each multicast address will be present. Thus, care must be taken to ensure each MPTS has its own unique IP address. Failure to do this will result in problems such as over-subscription and dejittering issues.

- 7 In the *PCR PID Select* field, the user can choose the following for MPTS streams:

- From PMT
- First detected

Notes:

- We recommend a setting of *From PMT*.
- More than 1 PID in a service may have PCR timestamps. If *From PMT* is selected, the RF Gateway 1 ignores all PCR timestamps except the PID specified in the PMT as the PCR PID. If *First Detected* is selected, the RF Gateway 1 determines the PCR reference PID by whichever PID it first receives a PCR timestamp on.

- 8 In the *MPTS Dejitter* field, the user can choose the following mode for MPTS Dejitter:

- One Stream
- Break Into SPTS
- The Ref is 0

Notes:

- If you have a stat-muxed stream, we recommend a setting of *One Stream*.
 - The *Ref* field specifies the service to use as program clock reference for the MPTS. Normally, this field has a value of 0 which indicates the system will use the PCR reference of the first PID received with a PCR timestamp.
 - An MPTS stream consists of multiple programs with each program having its own embedded PCR reference. For stat-muxed CBR MPTS streams, any of the PCR references may be used to properly dejitter the entire MPTS. However, if the MPTS is not CBR, the PCR in a program should only be used for dejittering that program. Therefore, the RF Gateway 1 supports splitting an MPTS into individual programs and dejittering each individually with its own PCR reference.
 - When creating an MPTS entry in the RF Gateway 1 Stream Map Table, it is very important that the Advanced Setting of MPTS Dejitter is set correctly. If the incoming MPTS stream has been created by a stat-mux device and has a Constant-Bit Rate (CBR) envelope, the dejitter mode setting should be set to "One Stream". This setting keeps the stat-muxing intact and passes the CBR stream to the output. However, if the incoming MPTS is not stat-muxed and is simply rate-limited or rate-clamped, or if it is just a mux of VBR programs, the dejitter mode must be set to "Break Into SPTS". The "Break Into SPTS" setting dejitters each program in the MPTS individually based on their own PCR.
- 9 In the *Blocked PIDs* field, the user can enter PMT PIDs of programs you want to block. The RF Gateway 1 does not support blocking individual audio or video. The stuffing PID is 8191.

Note:

- If an MPTS entry is the only input stream routed to an output carrier, only the Null PID (8191) needs to be specified in the blocked PID list. (All others in the list should be set to -1 or removed.) However, if another MPTS or a SPTS is going to be provisioned to mux out on the same carrier as this MPTS, the PAT PID must be blocked by entering a 0 in the blocked PID list. Blocking the PAT PID causes the PAT to be generated by the RF Gateway 1 and includes all programs routed to that output.
- Up to 32 blocked PIDs can be specified in the blocked PID list including unreferenced PIDs (e.g. PSIP or EMM PIDs) which are not present in the PAT.

10 Click **Apply**.

11 Click **Save**.

Advanced Rules for Advanced Settings

Using advanced stream map generation, the operator can modify multiple rows to the advanced settings on the stream map simultaneously.

Note: We recommend working at the carrier level.

- 1 Navigate to the *Maps* page.
- 2 Expand the tree menu to select the desired QAM Channel.

Result: The *Stream Map Table* is displayed.

The screenshot shows the Cisco configuration interface for 'rfgw-1d'. The 'Maps' tab is selected, and the 'Video Stream Map' is expanded in the left-hand menu. The main area displays the 'Stream Map Table' with 11 rows of configuration data. Below the table are 'Add Row', 'Apply', and 'Reset' buttons. At the bottom, there is a 'Base Rules' section with various input fields and dropdown menus, and 'Implement Rules' and 'Reset' buttons. A 'Show Advanced Settings' button is located at the very bottom.

Row #	Output QAM Channel	Destination IP Address	UDP Port	Active	Allowed Ingress Ports	Stream Type	Program Number		PMV	Data Rate (kbps)
							Input	Output		
0	1/1.1	0.0.0.0	49158	True	Pair 1	SPTS	0	3	3	0
1	1/1.1	0.0.0.0	49160	True	Pair 1	SPTS	0	4	4	0
2	1/1.1	0.0.0.0	49162	True	Pair 1	SPTS	0	5	5	0
3	1/1.1	0.0.0.0	49164	True	Pair 1	SPTS	0	6	6	0
4	1/1.1	0.0.0.0	49166	True	Pair 1	SPTS	0	7	7	0
5	1/1.1	0.0.0.0	49168	True	Pair 1	SPTS	0	8	8	0
6	1/1.1	0.0.0.0	49170	True	Pair 1	SPTS	0	9	9	0
7	1/1.1	0.0.0.0	49172	True	Pair 1	SPTS	0	10	10	0
8	1/1.1	0.0.0.0	49174	True	Pair 1	SPTS	0	11	11	0
9	1/1.1	0.0.0.0	49176	True	Pair 1	SPTS	0	12	12	0
10	1/1.1	0.0.0.0	49178	True	Pair 1	SPTS	0	13	13	0

Chapter 4 Table-Based Video Specific Operation

- 3 Configure the basic settings for a stream map.

Note: As you become an advanced user, basic and combined settings can be configured simultaneously.

- 4 Click **Show Advanced Settings**.

Result: The Advanced Settings window is displayed.

The screenshot shows the 'Advanced Settings' window. At the top, there is a 'Hide Advanced Settings' button. Below it is a table with columns: Row #, Source IP Address (with sub-columns 1, 2, 3, 4), Ignore UDP Port, PCR PID Select, MPTS Dejitter (with sub-columns Mode and Ref), and Blocked PIDs. The table contains 11 rows, each with input fields for IP addresses, dropdowns for 'Ignore UDP Port' (set to 'False'), 'PCR PID Select' (set to 'From PMT'), 'MPTS Dejitter Mode' (set to 'One Stream'), 'Ref' (set to '0'), and 'Blocked PIDs' (set to '0, 5191, -1, -1'). Below the table are 'Apply' and 'Reset' buttons. At the bottom, there is an 'Advanced Rules' section with fields for 'Value', 'Start QAM Channel', 'End QAM Channel', 'Row Start', and 'Row End', along with 'Implement Rules' and 'Reset' buttons.

- 5 In the *Source IP Address* field, enter the source IP addresses you want your stream to listen to.

- a The default '0.0.0.0' implies don't care.
- b 1 is primary
- c 2 is secondary
- d 3 is tertiary
- e 4 is quaternary

Note: If the device detects a stream which matches any of these three, it will pass it through.

- 6 In the *Ignore UDP Port* field, select True or False.
- 7 In the *PCR PID Select* field, the user can choose the following for MPTS streams,
 - From PMT
 - First detected

Note: We recommend selecting "From PMT".

- 8 In the *MPTS Dejitter* field, the user can choose the following mode for MPTS Dejitter,
 - One Stream
 - Break Into SPTS.
 - The Ref is 0.

Note: If you have a stat-muxed stream, we recommend "One Stream.
- 9 Enter the starting and ending rows where you want your settings to be applied.
- 10 Click **Implement Rules** to apply settings.
- 11 Click **Save**.

MPTS Pass-Through Mode of Operation

Table based Video Operation can be used generically to enable MPTS Pass Through for broadcast applications.

- Individual PIDs can be blocked as required in the Advanced Settings window. The PAT is blocked using default PID 0.
- If TSIDs are provisioned and the PAT is not blocked, the RF Gateway 1 will pass through the incoming source stream as is.

Note: TSIDs are entered individually for all streams if the PAT is blocked.

Enabling UDTA

In software version 6.04.XX, a new field has been added to the stream map which allows PSIP and EAS to merge. To enable UDTA, merging PSIP and EAS is required as the QAM TV tuners rely on PSIP information on the SI BASE PID 0x1FFB and EAS also comes in the same PID 0x1FFB. To enable this feature, a new stream map entry is added to specify a stream as PSIP or EAS. See screen below.

Row #	Output QAM Channel	Destination IP Address	UDP Port	Active	Allowed Ingress Ports	Stream Type	Program Number		PMV	Data Rate (kbps)	PSIP/EAS present	
							Input	Output				
0	0	1/1.2	0.0.0.0	5000	True	Port-2	MPTS	0	1	0	0	None PSIP EAS
1	1	1/1.2	232.1.1.173	5052	False	Port-2	Data	0	1	0	100	EAS
2	0	1/1.3	0.0.0.0	5000	False	Port-2	MPTS	0	1	0	0	PSIP
3	1	1/1.3	232.1.1.173	5052	False	Port-1	Data	0	1	0	1000	EAS

This new field supports 3 possible values:

- None
- PSIP
- EAS

The default value for this field is "None".

Below are the constraints that need to be considered when configuring the RFGW to work in the UDTA environment.

- For streams that do not need PSIP and EAS, merge must be set as "None."
- The PSIP setting is supported only for stream map entries configured as "MPTS."
- The EAS setting is supported only for stream map entries configured as "DATA."
- In case of replication of streams marked as PSIP or EAS, the streams should be marked as PSIP or EAS across all the channels where they are configured.
- Only one PSIP and one EAS is allowed per QAM channel.
- For entries configured as SPTS and Plant, this option will be disabled.

Status Monitoring

Introduction

This section provides information for status monitoring for video streams using the RF Gateway 1 web page.

The RF Gateway 1 provides utilities for monitoring:

- Input streams (i.e., stream type, status, IP, UDP, input bitrate)
- Output streams (i.e., session ID, destination QAM channel)

Monitoring

To View Input Monitoring

- 1 Navigate to the *Monitor* page.
- 2 In the tree menu, select the **Input/GbE** port.

Result: Input monitoring is shown for each GbE port.

The screenshot shows the 'Monitor' page for 'rfgw-1d'. The left sidebar contains a tree menu with 'Input' expanded to show 'Gbe1', 'Gbe2', 'Gbe3', and 'Gbe4'. The main content area displays 'RFGW-1 Input Streams' with a checkbox for 'Display PIDs in hex'. Below this is a table with the following data:

Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Input			Total ES PIDs	Input Bitrate (Mbps)	Replicated
						Program Number	PMT PID	PCR PID			
MPTS	1	228.8.8.8	49156	0.0.0.0	Stream Active	Details	N/A	N/A	4	6.5620	8
SPTS	1	239.255.100.100	49160	0.0.0.0	Stream Active	4	38	34	2	18.9985	8

To View Output Monitoring

- 1 Navigate to the *Monitor* page.
- 2 In the tree menu, select the Output/Card/RF Port.

Result: Output monitoring is shown for each QAM Card.

Session ID	Type	Output QAM Channel	Output Bitrate (Mbps)	Status	GbE Port	Destination IP Address	UDP Port	Program Number	PMT PID	PCR PID	Input
Video Map Session	MPTS	1/1.1	6.5650	Bound	1	228.8.8.8	49156	All	N/A	N/A	Details
Video Map Session	SPTS	1/1.1	18.7925	Bound	1	239.255.100.100	49160	33	544	545	Details
Video Map Session	SPTS	1/1.2	18.7925	Bound	1	239.255.100.100	49160	33	544	545	Details
Video Map Session	SPTS	1/1.2	2.2545	Bound	1	228.8.8.8	49156	32	528	529	Details
Video Map Session	SPTS	1/1.3	2.2545	Bound	1	228.8.8.8	49156	2	48	49	Details
Video Map Session	SPTS	1/1.3	18.7925	Bound	1	239.255.100.100	49160	3	64	65	Details
Video Map Session	SPTS	1/1.4	18.7925	Bound	1	239.255.100.100	49160	2	48	49	Details
Video Map Session	SPTS	1/1.4	2.2545	Bound	1	228.8.8.8	49156	3	64	65	Details
Video Map Session	SPTS	1/2.1	2.2545	Bound	1	228.8.8.8	49156	2	48	49	Details
Video Map Session	SPTS	1/2.1	18.7925	Bound	1	239.255.100.100	49160	3	64	65	Details
Video Map Session	SPTS	1/2.2	2.2545	Bound	1	228.8.8.8	49156	2	48	49	Details
Video Map Session	SPTS	1/2.2	18.7925	Bound	1	239.255.100.100	49160	3	64	65	Details
Video Map Session	SPTS	1/2.3	2.2545	Bound	1	228.8.8.8	49156	2	48	49	Details
Video Map Session	SPTS	1/2.3	18.7925	Bound	1	239.255.100.100	49160	3	64	65	Details
Video Map Session	SPTS	1/2.4	2.2545	Bound	1	228.8.8.8	49156	2	48	49	Details
Video Map Session	SPTS	1/2.4	18.7925	Bound	1	239.255.100.100	49160	3	64	65	Details

To View Input Details

Additional input information (for the output stream) can be retrieved by clicking the Input/Details button on the output monitoring screen.

Result: The following screen is displayed.

Display PIDs in hex

Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Input			Total ES PIDs	Input Bitrate (Mbps)	Replications
						Program Number	PMT PID	PCR PID			
MPTS	1	228.8.8.8	49156	0.0.0.0	Stream Active	N/A	N/A	N/A	4	6.5665	1

Input program details

Program Number	ES PID	PID Bitrate (Mbps)
1	45	2.0575
1	46	0.1970
2	42	4.0999
2	43	0.1970

Type	Status	Input			ES PIDs	Input Bitrate (Mbps)	Replications
		Program Number	PMT PID	PCR PID			
SPTS	Stream Active	1	44	45	2	2.2650	7
SPTS	Stream Active	2	41	42	2	4.3014	0

5

Switched Digital Video Specific Operation

This chapter provides information for provisioning the RF Gateway 1 for Switched Digital Video (SDV) operation.

In This Chapter

- Provisioning..... 100
- Status Monitoring 103

Provisioning

This section provides information for provisioning the RF Gateway 1 for SDV operation.

Prerequisite Configurations:

- GbE input ports, including Video/Data IP address
- QAM outputs
- Channel Application Mode = SDV

Once a carrier is in SVD mode, it should be used with an SRM (e.g., USRM, DNCS) and SDV Server configured with all the required video sessions.

Channel Application Mode

To Verify Channel Application Mode

- 1 Navigate to the *Maps* page.
- 2 In the tree menu, select **Map Configuration**.

Result: Channel Application Mode is displayed for each output carrier.

Location	Channel#	Available	Channel Application Mode
1/1.1	01	Yes	SDV
1/1.2	02	No	Video
1/1.3	03	No	Video
1/1.4	04	No	Video
1/2.1	05	Yes	Video
1/2.2	06	Yes	Video
1/2.3	07	Yes	Video
1/2.4	08	Yes	Video
2/1.1	09	Yes	Video
2/1.2	10	Yes	Video
2/1.3	11	Yes	Video
2/1.4	12	Yes	Video

SRM Configuration

To Provide SRM IP Address

Depending on the RF Gateway 1 network configuration, it may not be necessary to enter SRM IP address information in the "SRM Configuration window, for example USRM based SDV. Conversely, DNCS acting as SRM will require the SRM IP address to be populated with the DNCS IP address.

- 1 Navigate to the *System/System Configuration* page.

Result: SRM Configuration page is shown.

SRM Configuration	
SRM IP Address #1	0.0.0.0
SRM IP Address #2	0.0.0.0
SRM IP Address #3	0.0.0.0
Reset Indication Rate	5 seconds
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

SRM Configuration	Legacy Mode
SRM IP Address #1	0.0.0.0 <input type="checkbox"/>
SRM IP Address #2	0.0.0.0 <input type="checkbox"/>
SRM IP Address #3	0.0.0.0 <input type="checkbox"/>
Reset Indication Rate	5 seconds
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

- 2 Enter a valid SRM IP Address.
- 3 Set the 'GQI Announce Mode' to Enabled, if the RFGW-1 must send the GQI Announce Messages to the SRM to indicate the events on the Video Plane.

Legacy Mode

Legacy mode is intended to make older DNCS software versions (greater than 4.5) to support the RFGW-1 by spoofing the DNCS into thinking the RFGW-1 is a GQAM. A DNCS crash is likely if the Legacy Mode is selected with new DNCS software versions earlier than 4.5.

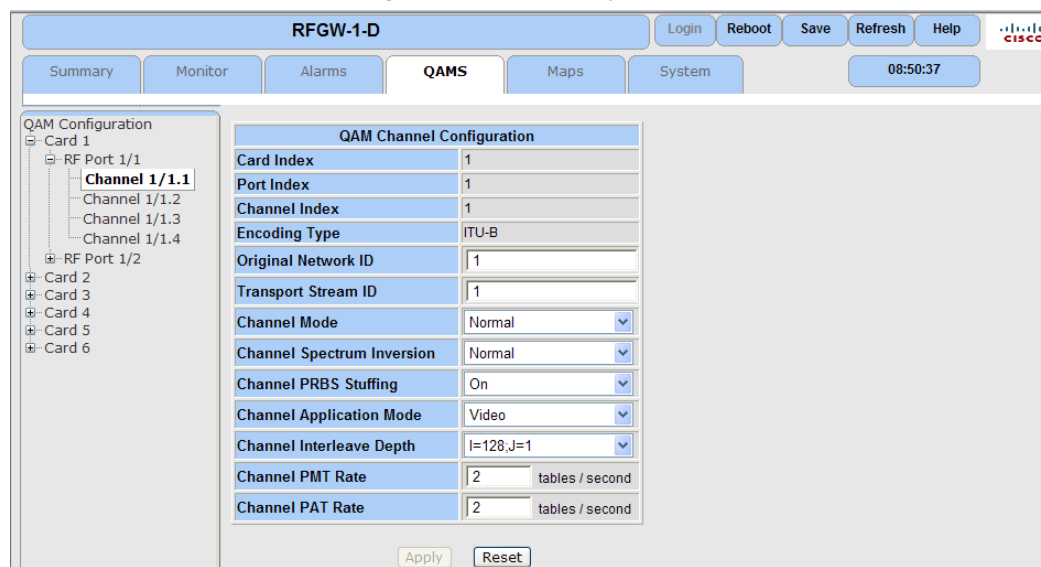
DO NOT SELECT LEGACY MODE IF THE DNCS IS RUNNING A SOFTWARE VERSION earlier than 4.5.

QAM Channel Configuration

To Provide Transport Stream ID and Verify Channel Application Mode

- 1 Navigate to the *QAMS/QAM Configuration* page.
- 2 Select the QAM Card/RF Port/Channel page.

Result: QAM Channel Configuration is displayed.



- 3 Select SDV for Channel Application Mode.
- 4 Enter a unique integer as the Transport Stream ID.
- 5 Click **Apply**.
- 6 Click **Save**.

Status Monitoring

For information on Status Monitoring, refer to *Status Monitoring* (on page 97).

6

Wideband Data Specific Operation

This section provides information for provisioning the RF Gateway 1 for Cisco Wideband operation.

In This Chapter

- Provisioning..... 106
- Status Monitoring 109

Provisioning

This section provides information for provisioning the RF Gateway 1 for Cisco Wideband operation.

Prerequisite Configurations:

- GbE input ports, including Video/Data IP address
- QAM outputs
- Channel Application Mode

Channel Application Mode

To Verify Channel Application Mode

- 1 Navigate to the *Maps* page.
- 2 In the tree menu, select **Map Configuration**.

Result: Channel Application Mode is revealed for each output carrier.

Note: The correct setting is "Data".

The screenshot shows the configuration page for RFGW-1-D. The 'Maps' tab is selected, and the 'Map Configuration' section is expanded to show a table of output carriers. The table has four columns: Location, Channel#, Available, and Channel Application Mode. All 'Available' values are 'Yes', and all 'Channel Application Mode' values are 'Video'. The table is as follows:

Location	Channel#	Available	Channel Application Mode
1/1.1	01	Yes	Video
1/1.2	02	Yes	Video
1/1.3	03	Yes	Video
1/1.4	04	Yes	Video
1/2.1	05	Yes	Video
1/2.2	06	Yes	Video
1/2.3	07	Yes	Video
1/2.4	08	Yes	Video
2/1.1	09	Yes	Video
2/1.2	10	Yes	Video
2/1.3	11	Yes	Video
2/1.4	12	Yes	Video
2/2.1	13	Yes	Video

At the bottom of the table, there are 'Apply' and 'Reset' buttons.

Data Map Configuration

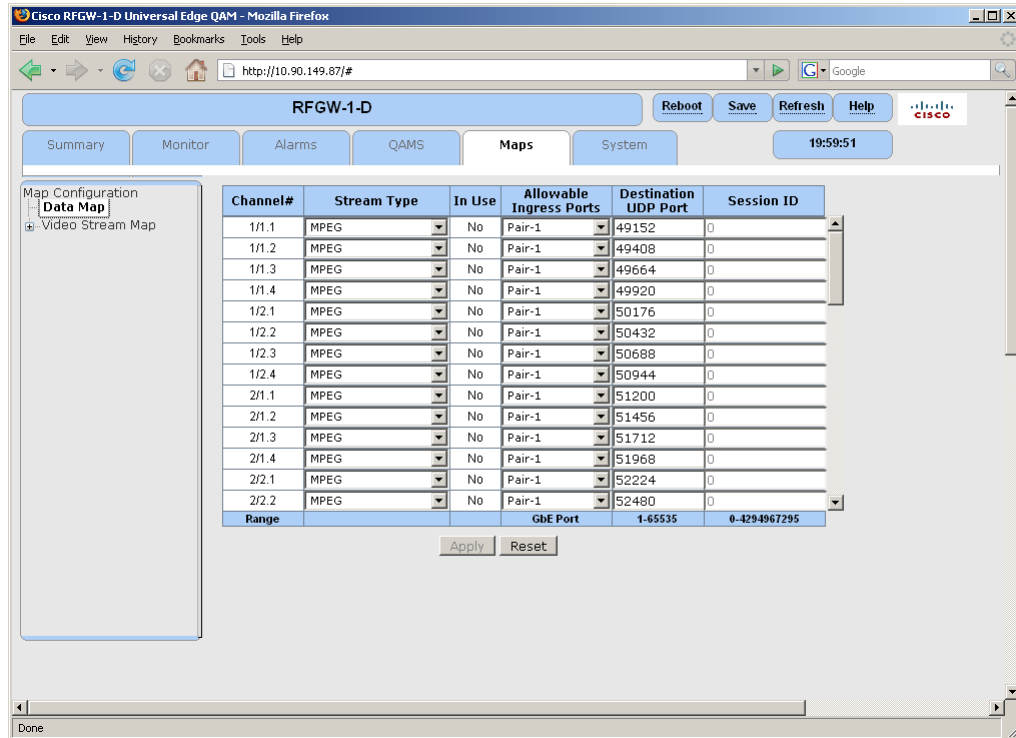
For a specific output carrier, using the Maps/Data Map web page, the operator can configure:

- Input Stream Type
- Allowable ingress port or port-pair
- Input stream Destination UDP port

Note: Once a carrier is in data mode, Data Map becomes active for that carrier. The Data Map serves as a routing table which maps incoming data to unique output carriers.

To Configure the Data Map

- 1 Navigate to the *Maps* page.
- 2 In the tree menu, select **Data Map**.



- 3 Configure the Stream Type to be MPEG for the desired carrier.

Note: The Stream Type setting of the RFGW-1-D is dependent upon the rf-channel configuration for the relevant controller modular-Cable in the CMTS. The following table lists the valid Stream Type settings for each of the rf-channel options in the uBR10K.

rf-channel (CMTS)	Stream Type (RFGW-1-D)
udp-port	MPEG
depi-remote-id	DOCSIS MPT w/o UDP

In DOCSIS 2.0 Cisco Wideband operation, the eQAM device carries only wideband channels (non-primary DOCSIS). For non-primary flows in DOCSIS 2.0 Cisco Wideband operation, rf-channels are typically configured as udp-ports in the CMTS, and the valid Stream Type is MPEG. For DOCSIS 3.0 Cisco Wideband operation, most operators are migrating to using depi-remote-id for all rf-channels. This is done primarily to provide flexibility in defining primary and non-primary channels. For flows defined as depi-remote-id in the CMTS, the valid Stream Type is DOCSIS MPT w/o UDP.

Chapter 6 Wideband Data Specific Operation

- 4 Select the **Allowable Ingress Ports** which receives the flows from the CMTS. The correct GbE port (independent mode) or port-pair (port-pair mode) will have its GbE port physical address (independent mode) or Video/Data IP address (port-pair mode) under the System/IP Network web view configured to match the eQAM IP address in the CMTS.
- 5 Enter the **Destination UDP Port** for the input stream to be mapped out to the relevant RF Gateway 1 carrier. The Destination UDP Port must match the udp-port of the corresponding rf-channel in the CMTS.

Notes:

- Session ID will automatically set to "N/A" when Stream Type is MPEG.
 - For a given ingress port pair, the UDP port or session ID must be unique.
- 6 Click **Apply**.
 - 7 Click **Save**.

Status Monitoring

Introduction

This section provides information for status monitoring for video streams using the RF Gateway 1 web page.

The RF Gateway 1 provides utilities for monitoring:

- Input streams (i.e., stream type, status, IP, UDP, input bitrate)
- Output streams (i.e., session ID, destination QAM channel)

Monitoring

To View Input Monitoring

- 1 Navigate to the *Monitor* page.
- 2 In the tree menu, select the Input/GbE port.

Result: Input monitoring is shown for each GbE port.

The screenshot shows the Cisco RFGW-1-D Universal Edge QAM web interface. The browser title is "Cisco RFGW-1-D Universal Edge QAM - Mozilla Firefox". The address bar shows "http://10.90.146.127/#". The page has a top navigation bar with "Reboot", "Save", "Refresh", and "Help" buttons. Below this is a secondary navigation bar with "Summary", "Monitor", "Alarms", "QAMS", "Maps", and "System" tabs. The "Monitor" tab is active, and the time "05:26:18" is displayed. On the left, a tree menu shows "Main" > "Device Information" > "Input" > "Gbe2" selected. The main content area is titled "RFGW-1 Input Streams" and includes a checkbox for "Display PIDs in hex". Below this is a table with the following columns: Type, GbE Port, Destination IP Address, UDP Port, Source IP Address, Status, Program Number, PMT PID, PCR PID, Total ES PIDs, Input Bitrate (Mbps), and Replicated. The table contains 20 rows of data, all showing "Stream Active" status and an input bitrate of approximately 0.9 Mbps.

Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Program Number	PMT PID	PCR PID	Total ES PIDs	Input Bitrate (Mbps)	Replicated
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9114	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9126	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9111	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9099	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9084	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9090	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9084	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9102	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9099	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9078	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9078	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9093	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9096	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9096	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9093	1

Chapter 6 Wideband Data Specific Operation

To View Output Monitoring

- 1 Navigate to the *Monitor* page.
- 2 In the tree menu, select the Output/Card/RF Port.

Result: Output monitoring is shown for each QAM Card.

howdieoodoo Reboot Save Refresh Help Cisco

Summary Monitor Alarms QAMS Maps System 05:26:53

Main
- Device Information
- Input
- Inventory
- Output
 + Card 1
 + Card 2
 + Card 3
 + Card 4
 + Card 5
 + Card 6
- Data
- DTI

RFGW-1 Output Sessions
 Display PIDs in hex

Session ID	Type	Output QAM Channel	Output Bitrate (Mbps)	Status	CbE Port	Destination IP Address	UDP Port	Output			Input
								Program Number	PMT PID	PCR PID	
N/A	DMPT	1/1.1	0.9111	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.2	0.9126	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.3	0.9111	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.4	0.9105	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.1	0.9096	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.2	0.9093	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.3	0.9099	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.4	0.9099	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details

Done

To View Data Monitoring

- 1 Navigate to the *Monitor* page.
- 2 In the tree menu, select **Data**.

Result: Data monitoring is revealed for each GbE port.

The screenshot shows the Cisco RFGW-1-D Universal Edge QAM web interface in Mozilla Firefox. The browser address bar shows 'http://10.90.146.127/#'. The page title is 'howdiedoodie'. The interface includes a navigation menu with 'Summary', 'Monitor', 'Alarms', 'QAMS', 'Maps', and 'System'. The 'Monitor' tab is active. On the left, a tree menu shows 'Main' > 'Device Information' > 'Input' > 'Gbe1', 'Gbe2', 'Gbe3', 'Gbe4', 'Inventory' > 'Output' > 'Card 1' through 'Card 6', and 'Data' (highlighted). The main content area displays a table with the following data:

Output Channel	Type	GbE Input	Output Bitrate (Mbps)	Destination IP	UDP / DEPI	Status	Synch State	Synch Counter
1/1.1	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	1	Stream Active	Primary	6143575
1/1.2	DOCSIS MPT w/o UDP	2	0.8543	172.18.10.1	2	Stream Active	Primary	6143576
1/1.3	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	3	Stream Active	Primary	6143577
1/1.4	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	4	Stream Active	Primary	6143580
1/2.1	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	5	Stream Active	Primary	6143624
1/2.2	DOCSIS MPT w/o UDP	2	0.8523	172.18.10.1	6	Stream Active	Primary	6143621
1/2.3	DOCSIS MPT w/o UDP	2	0.8520	172.18.10.1	7	Stream Active	Primary	6143564
1/2.4	DOCSIS MPT w/o UDP	2	0.8528	172.18.10.1	8	Stream Active	Primary	6143564
2/1.1	DOCSIS MPT w/o UDP	2	0.8526	172.18.10.1	9	Stream Active	Primary	6142531
2/1.2	DOCSIS MPT w/o UDP	2	0.8520	172.18.10.1	10	Stream Active	Primary	6142531
2/1.3	DOCSIS MPT w/o UDP	2	0.8517	172.18.10.1	11	Stream Active	Primary	6142532
2/1.4	DOCSIS MPT w/o UDP	2	0.8511	172.18.10.1	12	Stream Active	Primary	6142532

To View Input Details

Additional input information (for the output stream) can be retrieved by pressing the Input/Details button on the output monitoring screen.

Result: The following screen is displayed.

The screenshot shows a web browser window titled "http://10.90.146.127 - RFGW-1 Input Details - Mozilla Firefox". The page content includes a checkbox for "Display PIDs in hex" which is unchecked. Below this is a table with input details, followed by "Input Program Details" with a sub-table, and finally an "Output" table.

Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Input			Total ES PIDs	Input Bitrate (Mbps)
						Program Number	PMT PID	PCR PID		
Data	2	172.18.10.1	1	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.8949

Input Program Details

Program Number	ES PID	PID Bitrate(bps)

Session ID	Output QAM Channel	Provisioned Bitrate(Mbps)	Output			
			Program Number	PMT PID	PCR PID	Output Bitrate (Mbps)
00000000000100000000	1/1.1	51253876	0	0	0	0.8940

Done

7

Basic M-CMTS Data Specific Operation

Introduction

This section provides information for provisioning the RF Gateway 1 for DOCSIS compliant M-CMTS operation.

In This Chapter

- Provisioning..... 114
- Status Monitoring 119

Provisioning

This section provides information for provisioning the RF Gateway 1 for M-CMTS operation.

Prerequisite configurations:

- GbE input ports, including Video/Data IP address
- QAM outputs
- Channel Application Mode

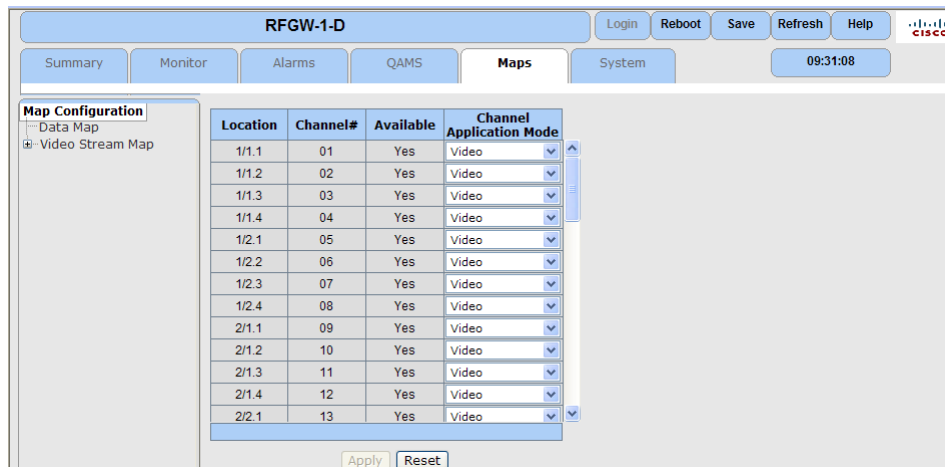
Channel Application Mode

To Verify Channel Application Mode

- 1 Navigate to the *Maps* page.
- 2 In the tree menu, select **Map Configuration**.

Result: Channel Application Mode is revealed for each output carrier.

Note: The correct setting is "Data".



Location	Channel#	Available	Channel Application Mode
1/1.1	01	Yes	Video
1/1.2	02	Yes	Video
1/1.3	03	Yes	Video
1/1.4	04	Yes	Video
1/2.1	05	Yes	Video
1/2.2	06	Yes	Video
1/2.3	07	Yes	Video
1/2.4	08	Yes	Video
2/1.1	09	Yes	Video
2/1.2	10	Yes	Video
2/1.3	11	Yes	Video
2/1.4	12	Yes	Video
2/2.1	13	Yes	Video

Data Map Configuration

For a specific output carrier, using the Maps/Data Map web page, the operator can configure:

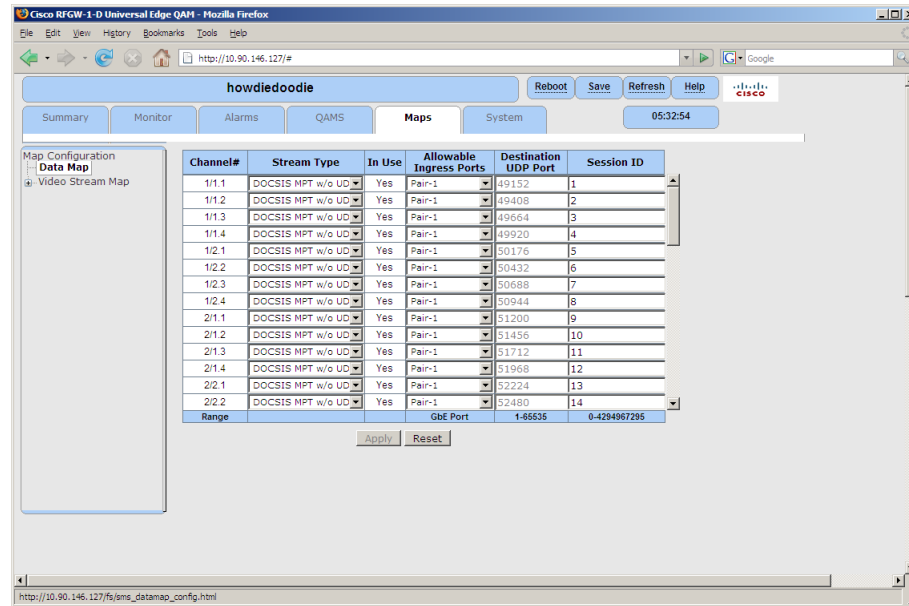
- Input Stream Type
- Allowable ingress port or port-pair
- Input stream DEPI Session ID port

Note: Once a carrier is in data mode, the Data Map becomes active for that carrier. The Data Map serves as a routing table which maps incoming data to unique output carriers.

To Configure the Data Map

- 1 Navigate to the *Maps* page.
- 2 In the tree menu, select **Data Map**.

Result: The following window is displayed.



- 3 Configure the Stream Type to be DOCSIS MPT without UDP for the desired carrier.

Note: The Stream Type setting of the RFGW-1-D is dependent upon the rf-channel configuration for the relevant controller modular-Cable in the CMTS. The following table lists the valid Stream Type settings for each of the rf-channel options in the uBR10K.

rf-channel (CMTS)	Stream Type (RFGW-1-D)
udp-port	MPEG
depi-remote-id	DOCSIS MPT w/o UDP

In DOCSIS 2.0 Cisco Wideband operation, the eQAM device carries only wideband channels (non-primary DOCSIS). For non-primary flows in DOCSIS 2.0 Cisco Wideband operation, rf-channels are typically configured as udp-ports in the CMTS, and the valid Stream Type is MPEG. For DOCSIS 3.0 Cisco Wideband operation, most operators are migrating to using depi-remote-id for all rf-channels. This is done primarily to provide flexibility in defining primary and non-primary channels. For flows defined as depi-remote-id in the CMTS, the valid Stream Type is DOCSIS MPT w/o UDP.

Chapter 7 Basic M-CMTS Data Specific Operation

- 4 Select the **Allowable Ingress Ports** which receives the flows from the CMTS. The correct GbE port (independent mode) or port pair (port-pair mode) will have its GbE port physical address (independent mode) or Video/Data IP address (port-pair mode) under the System/IP Network web view configured to match the eQAM IP address in the CMTS.
- 5 Enter the Destination UDP Port for the input stream to be mapped out to the relevant RF Gateway 1 carrier. The Destination UDP Port must match the udp-port of the corresponding rf-channel in the CMTS.

Notes:

- Session ID will automatically set to "N/A" when Stream Type is MPEG.
- For a given ingress port pair, the UDP port or session ID must be unique.

- 6 Click **Apply**.
- 7 Click **Save**.

Connecting to DTI Server

The RF Gateway 1 chassis provides redundant RJ-45 connections for connecting to DTI server devices. These connectors are located along the bottom row of RJ-45 connectors on the rear panel of the RF Gateway 1 chassis.

PS1	PS2	GbE1	GbE2	GbE3	GbE4	1/1	1/2	2/1	2/2	3/1	3/2
		mgmt	CA	DTI1	DTI2	4/1	4/2	5/1	5/2	6/1	6/2

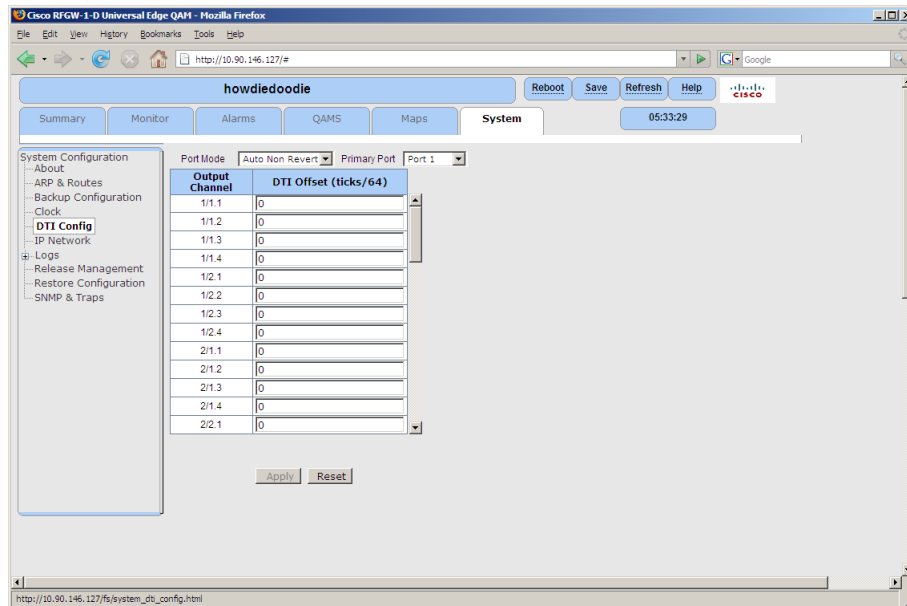
To Connect To DTI Server

- 1 Locate the DTI ports on the rear panel of the RF Gateway 1 chassis.
- 2 Connect the RF Gateway 1 to the timing server network using CAT5 cable.

To Configure DTI

- 1 Navigate to the *System* page.

2 In the tree menu, select **DTI Config**.



3 In the Port Mode drop-down box, select desired port mode (for DTI server redundancy).

Note: For proper interoperability with the Cisco uBR10K, the correct setting for Port Mode is *Auto Non Revert*.

4 In the Primary Port drop-down box, select **Primary Port**.

Note: For proper interoperability with the Cisco uBR10K, the correct setting for Primary Port is *Port 1*.

Note: Connection to the DTI Server can be verified using the DTI monitoring capability described in the next section.

5 Configure DTI Offset by entering the desired offset value in the row coincident with the desired carrier. (Units are DOCSIS ticks/64, which are the same units as the timing offset value calculated by the CMTS.)

Note: Calibration of the DTI Offset is typically necessary when RFGW-1-D carriers are added to existing service groups as additional primary channel capacity (i.e. to implement MxN mac-domains, where M>1). In such service groups, it is desirable that the CMTS "load-balance" cable modems among M primary channels. Using load-balancing, the CMTS has the ability to move cable modems among various DS primaries (statically or dynamically) when one or another primary channel becomes too heavily loaded. To implement load-balancing, it will likely be necessary to add DTI Offset values to RFGW-1-D carriers so that DTI timestamp values embedded in DOCSIS SYNC messages on these carriers are offset to match those carried on local 5x20 downstreams in the same mac-domain.

Generally, a service group will first be implemented using a single existing downstream primary from the CMTS RF linecard (i.e. the 5x20 linecard). When cable modems come online using the local 5x20 primary downstream, they will exhibit a timing offset value that is indicative of processing delays in the 5x20 and other characteristics of the physical plant (i.e. length of cables, temperatures, etc.). Incidentally, the processing delays in the 5x20 linecard are fixed - the user cannot add offsets to them. Therefore, the timing offset from the local 5x20 primary becomes the benchmark timing offset for the service group.

Timing offsets are critical because they are the mechanism by which the CMTS communicates the system time to cable modems. Cable modems need to know the system time so that they will only transmit in the upstream during specified timeslots (so that collisions are avoided on the shared upstream medium).

As a service group grows, operators may choose to add primary downstream capacity to improve the service level of the mac-domain (thus creating MxN domains). Primary downstream capacity can be added using additional 5x20 carriers, or, can be added using the M-CMTS architecture with one or more eQAM channels.

If the operator chooses to add primary downstreams from an eQAM, he or she will discover that the eQAM's own internal processing delays contribute to result in timing offsets (for cable modems that register online on eQAM primaries) that are different than the same cable modems that previously registered online on the local 5x20 primary. Therefore, eQAMs must implement a feature for offsetting the value of the DTI timestamp to calibrate eQAM primaries to match local 5x20 primaries in the service group. All eQAM primaries must be manually calibrated.

Generically, the calibration process to implement load-balancing in a mac-domain occurs as follows:

- Allow a test group of cable modems to register online on a benchmark local 5x20 primary downstream channel.
- Using the "show cable modem" command at the CMTS command line, record the average Timing Offset for all modems in the group.
- Add a primary downstream channel to an eQAM carrier in the service group. Allow the same group of cable modems to register online on it, so that the operator can record the difference in the average Timing Offset for the group.
- Manually calibrate out the timing offset difference using the DTI Offset feature of the eQAM.
- Finally, load-balancing can be configured and enabled for the service group.

6 Click **Apply**.

7 Click **Save**.

Status Monitoring

Introduction

This section provides information for status monitoring for DOCSIS compliant M-CMTS operation.

The RF Gateway 1 provides utilities for monitoring:

- Input streams (i.e., stream activity, input bitrate)
- Output streams (i.e., per carrier stream mapping, provisioned bitrate)
- Data specific monitoring (i.e., DOCSIS sync presence)
- DTI server connectivity and status

Monitoring

To View Input Monitoring

- 1 Navigate to the *Monitor* page.
- 2 In the tree menu, select the **Input/GbE** port.

Chapter 7 Basic M-CMST Data Specific Operation

Result: Input monitoring is shown for each GbE port.

The screenshot displays the Cisco RFGW-1-D Universal Edge QAM interface in Mozilla Firefox. The browser address bar shows `http://10.90.146.127/#`. The interface includes a navigation menu with options like Summary, Monitor, Alarms, QAMS, Maps, and System. The 'Monitor' tab is active, showing 'RFGW-1 Input Streams' for the selected GbE2 port. A table lists various input streams with columns for Type, GbE Port, Destination IP Address, UDP Port, Source IP Address, Status, Input Program Number, PMT PID, PCR PID, Total ES PIDs, Input Btrate (Mbps), and Replicated. The table contains 20 rows of data, all showing 'Stream Active' status and a replication count of 1.

Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Input Program Number	PMT PID	PCR PID	Total ES PIDs	Input Btrate (Mbps)	Replicated
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9114	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9126	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9111	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9099	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9084	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9090	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9084	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9102	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9099	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9078	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9078	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9093	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9096	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9096	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9093	1

To View Output Monitoring

- 1 Navigate to the Monitor page.
- 2 In the tree menu, select the Output/Card/RF Port.

Result: Output monitoring is shown for each QAM Card.

The screenshot shows the Cisco RFGW-1-D Universal Edge QAM web interface in Mozilla Firefox. The browser address bar shows 'http://10.90.146.127/#'. The interface has a navigation bar with 'Summary', 'Monitor', 'Alarms', 'QAMS', 'Maps', and 'System' tabs. The 'Monitor' tab is active. On the left, a tree menu shows 'Main' > 'Output' > 'Card 1' selected. The main content area displays 'RFGW-1 Output Sessions' with a table of data. The table has columns for Session ID, Type, Output QAM Channel, Output Bitrate (Mbps), Status, GbE Port, Destination IP Address, UDP Port, Program Number, PMT PID, PCR PID, and Input. There are 10 rows of data, all with 'N/A' for Session ID and 'Bound' for Status. Each row has a 'Details' link in the Input column.

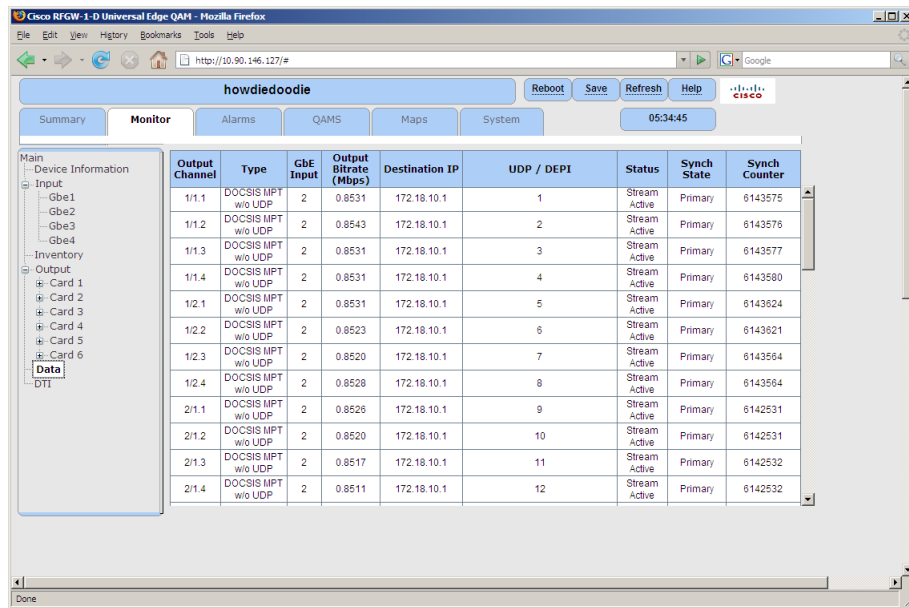
Session ID	Type	Output QAM Channel	Output Bitrate (Mbps)	Status	GbE Port	Destination IP Address	UDP Port	Program Number	PMT PID	PCR PID	Input
N/A	DMPT	1/1.1	0.9111	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.2	0.9126	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.3	0.9111	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.4	0.9105	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.1	0.9096	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.2	0.9093	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.3	0.9099	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.4	0.9099	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details

Chapter 7 Basic M-CMTS Data Specific Operation

To View Data Monitoring

- 1 Navigate to the Monitor page.
- 2 In the tree menu, select Data.

Result: Data monitoring is revealed for each GbE port.



The screenshot shows the Cisco RFGW-1-D Universal Edge QAM Monitor page in a Mozilla Firefox browser. The page title is "howdiedoodle" and the URL is "http://10.90.146.127/#". The page has a navigation bar with tabs for Summary, Monitor, Alarms, QAMS, Maps, and System. The Monitor tab is active, and the time is 05:34:45. On the left, there is a tree menu with "Data" selected. The main content area displays a table with the following columns: Output Channel, Type, GbE Input, Output Bitrate (Mbps), Destination IP, UDP / DEPI, Status, Synch State, and Synch Counter. The table contains 16 rows of data, all showing "Stream Active" status and "Primary" synch state.

Output Channel	Type	GbE Input	Output Bitrate (Mbps)	Destination IP	UDP / DEPI	Status	Synch State	Synch Counter
1/1.1	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	1	Stream Active	Primary	6143575
1/1.2	DOCSIS MPT w/o UDP	2	0.8543	172.18.10.1	2	Stream Active	Primary	6143576
1/1.3	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	3	Stream Active	Primary	6143577
1/1.4	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	4	Stream Active	Primary	6143580
1/2.1	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	5	Stream Active	Primary	6143624
1/2.2	DOCSIS MPT w/o UDP	2	0.8523	172.18.10.1	6	Stream Active	Primary	6143621
1/2.3	DOCSIS MPT w/o UDP	2	0.8520	172.18.10.1	7	Stream Active	Primary	6143564
1/2.4	DOCSIS MPT w/o UDP	2	0.8528	172.18.10.1	8	Stream Active	Primary	6143564
2/1.1	DOCSIS MPT w/o UDP	2	0.8526	172.18.10.1	9	Stream Active	Primary	6142531
2/1.2	DOCSIS MPT w/o UDP	2	0.8520	172.18.10.1	10	Stream Active	Primary	6142531
2/1.3	DOCSIS MPT w/o UDP	2	0.8517	172.18.10.1	11	Stream Active	Primary	6142532
2/1.4	DOCSIS MPT w/o UDP	2	0.8511	172.18.10.1	12	Stream Active	Primary	6142532

To View Input Details

Additional input information (for the output stream) can be retrieved by pressing the Input/Details button on the output monitoring screen.

Result: The following screen is displayed.

The screenshot shows a web browser window titled 'http://10.90.146.127 - RFGW-1 Input Details - Mozilla Firefox'. The page contains a checkbox 'Display PIDs in hex' which is unchecked. Below this is a table with the following data:

Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Input			Total ES PIDs	Input Bitrate (Mbps)
						Program Number	PMT PID	PCR PID		
Data	2	172.18.10.1	1	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.8949

Below the table is a section titled 'Input Program Details' containing a smaller table:

Program Number	ES PID	PID Bitrate(bps)

At the bottom of the page is another table with the following data:

Session ID	Output QAM Channel	Provisioned Bitrate(Mbps)	Output			
			Program Number	PMT PID	PCR PID	Output Bitrate (Mbps)
00000000000100000000	1/1.1	51253876	0	0	0	0.8940

The browser status bar at the bottom shows 'Done'.

To View DTI Monitoring

- 1 Navigate to the Monitor page.
- 2 In the tree menu, select DTI.

Result: DTI monitoring is shown for each DTI server port.

DTI Port Status		
	Port 1	Port 2
DTI Signal Detected	No	No
Server Device Type	0x0	0x0
Server Status	N/A	N/A
CRC Error Count	0x0	0x0
Cable Advance	0x0	0x0
TOD Count	0x0	0x0
Frame Error rate	< 2%	< 2%

DTI Statistics	
T3 State Transition Count	0x0
T4 State Transition Count	0x0
T6 State Transition Count	0x0
T7 State Transition Count	0x0
Normal Time Count	0x0
Holdover Time Count	0x0
Phase Error	0x0
Integral Frequency Term	0x73d
EFC Value	0xe04
DTI Client Specification Version	1
Firmware Revision	276
Port Switch Count	0

Note: DTI timestamp increments (updated ~5s) can be displayed using the Refresh button in the top right-hand corner of the page.

To View Tunnel Details

- 1 Navigate to the Monitor page.
- 2 In the tree menu, navigate to DEPI details and select tunnels

Result: DEPI tunnels are shown for each GbE port.

GbE	Local Tunnel ID	Remote Tunnel ID	Remote Name	State	Remote-Address	Sessions	Tunnel Details
3	2	1545842213	UBR10k	Established	13.1.1.1	24	Details
2	3	1936786046	UBR10k	Established	12.1.1.1	24	Details
4	4	3233929526	UBR10k	Established	15.1.1.1	24	Details

Note: The session Button would display the list of sessions pertaining to each tunnel. The statistics button would display the statistics for the sessions associated with each tunnel.

To View Session Details

- 1 Navigate to the Monitor page.
- 2 In the tree menu, navigate to DEPI details and select Sessions

Result: DEPI sessions is shown for QAM channel.

Local ID	Remote ID	Tunnel ID	QAM Channel	State	TS Id	Statistics
2	1252010029	2	5/1.3	Established	61698	Statistics
3	1252016805	2	5/1.7	Established	61702	Statistics
4	1252050401	2	5/1.6	Established	61701	Statistics
5	1252054909	2	5/1.8	Established	61703	Statistics
6	1252005796	2	5/1.2	Established	61697	Statistics
7	1252023168	2	5/1.5	Established	61700	Statistics
8	1252013049	2	5/1.1	Established	61696	Statistics
9	1252009314	2	5/1.4	Established	61699	Statistics
10	1252034850	2	4/2.7	Established	61694	Statistics
11	1252063778	2	4/2.6	Established	61693	Statistics

Note: The statistics button would display the statistics for this session.

To View DEPI QAM Statistics Details

- 1 Navigate to the Monitor page.
- 2 In the tree menu, navigate to DEPI details and select statistics.

Result: DEPI statistics is shown for each QAM channel.

Id	Qam Ch.	State	Sess. Type	#Out Ucast Pkts	#Out Octets	#Out Discards	#Out Errors	In Pkt. Rate	#Bad Seq. Errs	#DLM Pkts
36	2/2.1	ACTIVE	PRIMARY	592	1120856	0	0	594	0	10
43	2/2.2	ACTIVE	PRIMARY	5	940	0	0	1	0	0
47	2/2.3	ACTIVE	PRIMARY	5	940	0	0	1	0	0
42	2/2.4	ACTIVE	PRIMARY	5	940	0	0	1	0	0
46	2/2.5	ACTIVE	PRIMARY	5	940	0	0	1	0	0
30	2/2.6	ACTIVE	PRIMARY	5	940	0	0	1	0	0
27	2/2.7	ACTIVE	PRIMARY	5	940	0	0	0	0	0
31	2/2.8	ACTIVE	PRIMARY	5	940	0	0	1	0	0
38	3/1.1	ACTIVE	PRIMARY	5959	1120292	0	0	594	0	10
26	3/1.2	ACTIVE	PRIMARY	5	940	0	0	0	0	0
44	3/1.3	ACTIVE	PRIMARY	5	940	0	0	1	0	0
37	3/1.4	ACTIVE	PRIMARY	5	940	0	0	1	0	0
41	3/1.5	ACTIVE	PRIMARY	5	940	0	0	1	0	0
39	3/1.6	ACTIVE	PRIMARY	5	940	0	0	1	0	0
28	3/1.7	ACTIVE	PRIMARY	5	940	0	0	1	0	0
29	3/1.8	ACTIVE	PRIMARY	5	940	0	0	1	0	0
49	3/2.1	ACTIVE	PRIMARY	5959	1120292	0	0	594	0	10

Note: The statistics button displays statistics for this session.

8

M-CMTS Data DEPI-CP Operation

Introduction

This section provides information for provisioning the RF Gateway 1 for DOCSIS compliant M-CMTS operation using the DEPI control plane.

In This Chapter

- Provisioning..... 128
- Channel Application Mode 129
- Status Monitoring 131
- DEPI Feature Highlights..... 138

Provisioning

This section provides information for provisioning the RF Gateway 1 for M-CMTS operation using DEPI - Control plane.

Prerequisite configurations:

- GbE input ports, including Video/Data IP address
- QAM outputs
- Channel Application Mode

Channel Application Mode

To Verify Channel Application Mode

- 1 Navigate to the QAMs page and scroll to the bottom of the page.

Result: Channel Application Mode is revealed for each output carrier.

Note: The correct setting is "DEPI Remote / DEPI Learn".

RFQW QAM Channel	SRM QAM Channel	ON ID	TS ID	Mode	Spectrum Inversion	PRBS Stuffing	App Mode	Interleave Depth	PMT Rate (tables/sec)	PAT Rate (tables/sec)	DTI Offset (ticks/64)
1/1.1	1	1	1	Mute	Normal	On	DEPI-Learn	J=32,J=4	10	10	0
1/1.2	2	1	2	Mute	Normal	On	DEPI-Learn	J=32,J=4	10	10	0
1/1.3	3	1	3	Mute	Normal	On	DEPI-Learn	J=128,J=4	10	10	0
1/1.4	4	1	4	Mute	Normal	On	DEPI-Learn	J=128,J=4	10	10	0
1/1.5	5	1	5	Mute	Normal	On	DEPI-Learn	J=128,J=4	10	10	0
1/1.6	6	1	6	Mute	Normal	On	DEPI-Le	J=128,J=4	10	10	0
1/1.7	7	1	7	Mute	Normal	On	Video			10	0
1/1.8	8	1	8	Mute	Normal	On	Data			10	0
1/2.1	9	1	0	Mute	Normal	On	SDV	J=128,J=4	10	10	0
1/2.2	10	1	0	Mute	Normal	On	NGOD	J=128,J=4	10	10	0
							DEPI-Learn	J=128,J=4	10	10	0
							DEPI-Remg	J=128,J=4	10	10	0

DEPI-Remote

This is very similar to the DEPI remote static mode where the User can configure the QAM PHY parameters and only on match with the corresponding config on the M-CMTS would the session be set-up

Note: The RF-port 1/1 is now editable as all the QAM channels are in DEPI-Remote mode

RF Port	Spacing (MHz)	Modulation	Output Level (dBmV)	Symbol Rate (MS/s)	Port Control	Combined Carrier	ITU Carrier Number	Carrier Center Frequency (MHz)			
								Ch1 Ch5	Ch2 Ch6	Ch3 Ch7	Ch4 Ch8
1/1	5	QAM 256	45	5.361	On	Quad	37 38 39 40	303.000	309.000	315.000	321.000
						Quad	134 135 136 137	855.000	861.000	867.000	873.000
						Quad	146 147 148 149	927.000	933.000	939.000	945.000
1/2	5	QAM 64	50	5.057	Off	Quad	138 139 140 141	879.000	885.000	891.000	897.000

DEPI-Learn

This mode is similar to the DEPI remote learn mode where the QAM PHY parameters cannot be configured by the user and would be “learnt” from the configuration on the M-CMTS.

Chapter 8 M-CMTS Data DEPI-CP Operation

Note: The RF-port 1/1 is not editable as all the QAM channels are in DEPI-Learn mode.

RF Port	Spacing (MHz)	Modulation	Output Level (dBmV)	Symbol Rate (MS/s)	Port Control	Combined Carrier	ITU Carrier Number				Carrier Center Frequency (MHz)			
							Ch1 Ch5	Ch2 Ch6	Ch3 Ch7	Ch4 Ch8				
1/1	5	QAM 256	45	5.361	On	Quad	37	38	39	40	303.000	309.000	315.000	321.000
						Quad	134	135	136	137	855.000	861.000	867.000	873.000
1/2	5	QAM 64	50	5.057	Off	Quad	146	147	148	149	927.000	933.000	939.000	945.000
						Quad	138	139	140	141	879.000	885.000	891.000	897.000
2/1	5	QAM 256	50	5.361	Off	Quad	142	143	144	145	903.000	909.000	915.000	921.000
						Quad	134	135	136	137	855.000	861.000	867.000	873.000

Connecting to DTI Server

Please refer to *Connecting to DTI Server* (on page 116).

Status Monitoring

Introduction

This section provides information for status monitoring for DOCSIS compliant M-CMTS operation.

- The RF Gateway 1 provides utilities for monitoring:
- Input streams (i.e., stream activity, input bitrate)
- Output streams (i.e., per carrier stream mapping, provisioned bitrate)
- Data specific monitoring (i.e., DOCSIS sync presence)
- DTI server connectivity and status

Monitoring

To View Input Monitoring

- 1 Navigate to the *Monitor* page.
- 2 In the tree menu, select the **Input/GbE** port.

Result: Input monitoring is shown for each GbE port.

The screenshot shows the Cisco RFGW-1-D Universal Edge QAM Monitor interface. The main content area displays the 'RFGW-1 Input Streams' table. The table has columns for Type, GbE Port, Destination IP Address, UDP Port, Source IP Address, Status, Input Program Number, PMT PID, PCR PID, Total ES PIDs, Input Btrate (Mbps), and Replicated. The table contains 20 rows of data, all showing 'Stream Active' status for various input streams.

Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Input Program Number	PMT PID	PCR PID	Total ES PIDs	Input Btrate (Mbps)	Replicated
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9114	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9126	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9111	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9099	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9084	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9090	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9084	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9102	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9099	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9078	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9087	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9078	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9093	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9096	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9096	1
Data	2	172.18.10.1	DEPI	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.9093	1

To View Output Monitoring

- 1 Navigate to the Monitor page.
- 2 In the tree menu, select the Output/Card/RF Port.

Result: Output monitoring is shown for each QAM Card.

The screenshot shows the Cisco RFGW-1-D Universal Edge QAM web interface in Mozilla Firefox. The browser address bar shows 'http://10.90.146.127/#'. The interface has a navigation bar with 'Summary', 'Monitor', 'Alarms', 'QAMS', 'Maps', and 'System' tabs. The 'Monitor' tab is active. On the left, a tree menu shows 'Main' > 'Output' > 'Card 1' selected. The main content area displays 'RFGW-1 Output Sessions' with a table of data. The table has columns for Session ID, Type, Output QAM Channel, Output Bitrate (Mbps), Status, GbE Port, Destination IP Address, UDP Port, Program Number, PMT PID, PCR PID, and Input. There are 10 rows of data, all with 'Bound' status and 'DEPI' as the UDP Port. Each row has a 'Details' link in the Input column.

Session ID	Type	Output QAM Channel	Output Bitrate (Mbps)	Status	GbE Port	Destination IP Address	UDP Port	Program Number	PMT PID	PCR PID	Input
N/A	DMPT	1/1.1	0.9111	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.2	0.9126	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.3	0.9111	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/1.4	0.9105	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.1	0.9096	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.2	0.9093	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.3	0.9099	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details
N/A	DMPT	1/2.4	0.9099	Bound	2	172.18.10.1	DEPI	N/A	N/A	N/A	Details

To View Data Monitoring

- 1 Navigate to the Monitor page.
- 2 In the tree menu, select Data.

Result: Data monitoring is revealed for each GbE port.

The screenshot shows the Cisco RFGW-1-D Universal Edge QAM Monitor page in a Mozilla Firefox browser. The page title is "howdiedoodle" and the URL is "http://10.90.146.127/#". The page has a navigation bar with tabs for Summary, Monitor, Alarms, QAMS, Maps, and System. The Monitor tab is active, and the time is 05:34:45. On the left, there is a tree menu with "Data" selected. The main content area displays a table with the following columns: Output Channel, Type, GbE Input, Output Bitrate (Mbps), Destination IP, UDP / DEPI, Status, Synch State, and Synch Counter.

Output Channel	Type	GbE Input	Output Bitrate (Mbps)	Destination IP	UDP / DEPI	Status	Synch State	Synch Counter
1/1.1	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	1	Stream Active	Primary	6143575
1/1.2	DOCSIS MPT w/o UDP	2	0.8543	172.18.10.1	2	Stream Active	Primary	6143576
1/1.3	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	3	Stream Active	Primary	6143577
1/1.4	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	4	Stream Active	Primary	6143580
1/2.1	DOCSIS MPT w/o UDP	2	0.8531	172.18.10.1	5	Stream Active	Primary	6143624
1/2.2	DOCSIS MPT w/o UDP	2	0.8523	172.18.10.1	6	Stream Active	Primary	6143621
1/2.3	DOCSIS MPT w/o UDP	2	0.8520	172.18.10.1	7	Stream Active	Primary	6143564
1/2.4	DOCSIS MPT w/o UDP	2	0.8528	172.18.10.1	8	Stream Active	Primary	6143564
2/1.1	DOCSIS MPT w/o UDP	2	0.8526	172.18.10.1	9	Stream Active	Primary	6142531
2/1.2	DOCSIS MPT w/o UDP	2	0.8520	172.18.10.1	10	Stream Active	Primary	6142531
2/1.3	DOCSIS MPT w/o UDP	2	0.8517	172.18.10.1	11	Stream Active	Primary	6142532
2/1.4	DOCSIS MPT w/o UDP	2	0.8511	172.18.10.1	12	Stream Active	Primary	6142532

To View Input Details

Additional input information (for the output stream) can be retrieved by pressing the Input/Details button on the output monitoring screen.

Result: The following screen is displayed.

The screenshot shows a web browser window titled "http://10.90.146.127 - RFGW-1 Input Details - Mozilla Firefox". It contains a checkbox "Display PIDs in hex" which is unchecked. Below this is a table with input stream details:

Type	GbE Port	Destination IP Address	UDP Port	Source IP Address	Status	Input			Total ES PIDs	Input Bitrate (Mbps)
						Program Number	PMT PID	PCR PID		
Data	2	172.18.10.1	1	0.0.0.0	Stream Active	N/A	N/A	N/A	N/A	0.8949

Below the table is a section titled "Input Program Details" containing three buttons: "Program Number", "ES PID", and "PID Bitrate(bps)".

At the bottom is another table with output stream details:

Session ID	Output QAM Channel	Provisioned Bitrate(Mbps)	Output			
			Program Number	PMT PID	PCR PID	Output Bitrate (Mbps)
00000000000100000000	1/1.1	51253876	0	0	0	0.8940

The browser status bar at the bottom shows "Done".

To View DTI Monitoring

- 1 Navigate to the Monitor page.
- 2 In the tree menu, select DTI.

Result: DTI monitoring is shown for each DTI server port.

The screenshot shows the DTI monitoring interface for device rfgw-1d. The top navigation bar includes buttons for Login, Reboot, Save, Refresh, and Help. Below the navigation bar, there are tabs for Summary, Monitor, Alarms, QAMS, Maps, and System. The left sidebar shows a tree menu with 'DTI' selected under the 'Data' category. The main content area displays the following information:

Active Port	Neither	
State	Free run	
Client Status	10.24 MHz Activity-State	Present
Time Stamp	0x1E5114C0	

DTI Port Status	Port 1	Port 2
DTI Signal Detected	No	No
Server Device Type	0x0	0x0
Server Status	N/A	N/A
CRC Error Count	0x0	0x0
Cable Advance	0x0	0x0
TOD Count	0x0	0x0
Frame Error rate	< 2%	< 2%

DTI Statistics	
T3 State Transition Count	0x0
T4 State Transition Count	0x0
T6 State Transition Count	0x0
T7 State Transition Count	0x0
Normal Time Count	0x0
Holdover Time Count	0x0
Phase Error	0x0
Integral Frequency Term	0x73d
EFC Value	0xe04
DTI Client Specification Version	1
Firmware Revision	276
Port Switch Count	0

Note: DTI timestamp increments (updated ~5s) can be displayed using the Refresh button in the top right-hand corner of the page.

To View Tunnel Details

- 1 Navigate to the Monitor page.
- 2 In the tree menu, navigate to DEPI details and select tunnels

Result: DEPI tunnels are shown for each GbE port.

The screenshot shows the Tunnel Details interface for device Rowif. The top navigation bar includes buttons for Login, Reboot, Save, Refresh, and Help. Below the navigation bar, there are tabs for Summary, Monitor, Alarms, QAMS, Maps, and System. The left sidebar shows a tree menu with 'Tunnels' selected under the 'Depi Details' category. The main content area displays the following table:

GbE	Local Tunnel ID	Remote Tunnel ID	Remote Name	State	Remote-Address	Sessions	Tunnel Details
3	2	1545842213	UBR10k	Established	13.1.1.1	24	Details
2	3	1936786046	UBR10k	Established	12.1.1.1	24	Details
4	4	3233929526	UBR10k	Established	15.1.1.1	24	Details

Note: The session Button would display the list of sessions pertaining to each tunnel. The statistics button would display the statistics for the sessions associated with each tunnel.

To View Session Details

- 1 Navigate to the Monitor page.
- 2 In the tree menu, navigate to DEPI details and select Sessions

Result: DEPI sessions is shown for QAM channel.

Local ID	Remote ID	Tunnel ID	QAM Channel	State	TS Id	Statistics
2	1252010029	2	5/1.3	Established	61698	Statistics
3	1252016805	2	5/1.7	Established	61702	Statistics
4	1252050401	2	5/1.6	Established	61701	Statistics
5	1252054909	2	5/1.8	Established	61703	Statistics
6	1252005796	2	5/1.2	Established	61697	Statistics
7	1252023168	2	5/1.5	Established	61700	Statistics
8	1252013049	2	5/1.1	Established	61696	Statistics
9	1252009314	2	5/1.4	Established	61699	Statistics
10	1252034850	2	4/2.7	Established	61694	Statistics
11	1252063778	2	4/2.6	Established	61693	Statistics

Note: The statistics button would display the statistics for this session.

To View DEPI QAM Statistics Details

- 1 Navigate to the Monitor page.
- 2 In the tree menu, navigate to DEPI details and select statistics.

Result: DEPI statistics is shown for each QAM channel.

Id	Qam Ch.	State	Sess. Type	#Out Ucast Pkts	#Out Octets	#Out Discards	#Out Errors	In Pkt. Rate	#Bad Seq. Errs	#DLM Pkts
36	2/2.1	ACTIVE	PRIMARY	592	1120856	0	0	594	0	10
43	2/2.2	ACTIVE	PRIMARY	5	940	0	0	1	0	0
47	2/2.3	ACTIVE	PRIMARY	5	940	0	0	1	0	0
42	2/2.4	ACTIVE	PRIMARY	5	940	0	0	1	0	0
46	2/2.5	ACTIVE	PRIMARY	5	940	0	0	1	0	0
30	2/2.6	ACTIVE	PRIMARY	5	940	0	0	1	0	0
27	2/2.7	ACTIVE	PRIMARY	5	940	0	0	0	0	0
31	2/2.8	ACTIVE	PRIMARY	5	940	0	0	1	0	0
38	3/1.1	ACTIVE	PRIMARY	5959	1120292	0	0	594	0	10
26	3/1.2	ACTIVE	PRIMARY	5	940	0	0	0	0	0
44	3/1.3	ACTIVE	PRIMARY	5	940	0	0	1	0	0
37	3/1.4	ACTIVE	PRIMARY	5	940	0	0	1	0	0
41	3/1.5	ACTIVE	PRIMARY	5	940	0	0	1	0	0
39	3/1.6	ACTIVE	PRIMARY	5	940	0	0	1	0	0
28	3/1.7	ACTIVE	PRIMARY	5	940	0	0	1	0	0
29	3/1.8	ACTIVE	PRIMARY	5	940	0	0	1	0	0
49	3/2.1	ACTIVE	PRIMARY	5959	1120292	0	0	594	0	10

Note: The statistics button displays statistics for this session.

DEPI Feature Highlights

Data plane extension during PRE - SSO

DEPI control and session will be renegotiated on the secondary PRE after SO. The Dataplane on the RFGW1 should continue to forward data traffic, SYNC's, MAP/UCD for up for 60 seconds although the control plane is down, to allow traffic to flow during the PRE SO. . Note the sessions as observed on the Monitor->session page would be moved to Del-Wait state. Once the new DEPI control and session are established, the Data plane can be reprogrammed.

The idea is to make sure the modems stay online and there is no disruption in the traffic during a PRE SO.

DEPI Path Redundancy

DEPI Path Redundancy is a method for creation and management of redundant DEPI connections between the M-CMTS Core and the EQAM. The high availability requirements demands that the CMTS's architecture must avoid single points of failure through support for redundant sub-components involved in DEPI and the ability to operate with redundant DEPI connections.

DPR introduces two types of DEPI data sessions: primary sessions and secondary sessions. DPR provides redundancy at the data session level. Primary sessions are used to transport encapsulated DOCSIS data under normal conditions. Primary sessions are equivalent to generic DEPI sessions, when DPR is not supported. A secondary session serves as always-ready substitute for a primary session associated with the same QAM channel. A secondary session can be utilized to carry DEPI data when the associated primary session becomes unavailable as result of a failure or an operator action

Note: The Monitor->Depi details -> Statistics page indicates the session type that is currently active on a specific QAM channel.

9

Remapping Unreferenced PIDS

Introduction

This feature allows the operator to configure the RFGW-1-D such that it can insert SI data from the headend for the locally inserted channels which are carried in unreferenced PIDs and remap it to standard SI PIDs in the RFGW-1. The user can perform the following tasks:

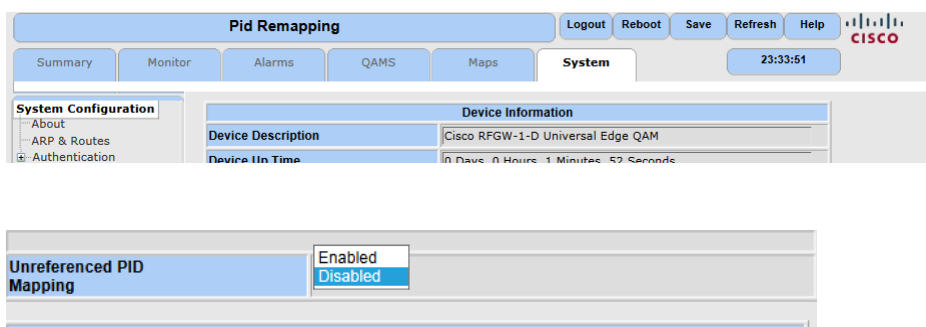
- Remap unreferenced PIDs from a data stream or MPTS stream.
- Block specific unreferenced PIDs from a data stream or MPTS stream.
- Block all the unreferenced PIDs from a data stream or MPTS stream.
- PID remapping is implemented on a QAM channel level.
- PMT PIDs from SPTS and MPTS streams on the QAM channels configured in “Video” mode.
- Blocking PMT PIDs in the SPTS and MPTS stream.
- Inserting PAT from the external data stream.

In This Chapter

- Enabling the Feature..... 140
- Feature Page 141
- Adding Entries to the Remap Table..... 142
- Blocked Unreferenced PIDS 143
- Enabling Insert External PAT..... 144
- Operator Responsibilities 145

Enabling the Feature

- 1 Login to the RFGW-1 and go to the *System/System Configuration* page.
- 2 Scroll down and set the Unreferenced PID Mapping feature to *Enabled*.
- 3 Click **Apply**.
- 4 Click **Save**.



Adding Entries to the Remap Table

- 1 In the Unreferenced PID Maps tree, select the QAM channel which requires PID mapping.
- 2 Click **Add row** in the Unreferenced PID Map Table and enter the value of Input PID and required Output PID. You can add multiple rows. The maximum number of remapping rows supported is 32 per QAM channel
- 3 If there is a need to block a specific PID in the stream, the operator can specify -1 at the Output PID Number column, effectively blocking the PID specified in the Input PID Number column.
- 4 Click **Apply**.
- 5 Click **Save**.
- 6 The color coding descriptions are shown below.
 - a Yellow - The existing row values were changed
 - b Green - New row is being added
 - c Red - The row will be deleted when you click Apply.

The screenshot shows the 'Unreferenced Pid Map Table' interface. On the left, a tree view shows 'Channel 4/2.2' selected. The table contains the following data:

Mark for Delete	Map Index	Row #	Output QAM Channel	Input PID Number	Output PID Number
<input type="checkbox"/>	0	0	4/2.2	17	-1
<input checked="" type="checkbox"/>	1	1	4/2.2	116	16
<input type="checkbox"/>	2	2	4/2.2	117	17
<input type="checkbox"/>	3	0	4/2.2	119	19
<input type="checkbox"/>	4	3	4/2.2	118	18

Buttons at the bottom: Add Row, Apply, Reset, Mark all rows for Delete

Blocked Unreferenced PIDS

Unreferenced PIDs in MPTS and Data streams can be blocked by checking the corresponding boxes of the QAM channels in the Block Unreferenced PID table.

By enabling the checkboxes in the PID table below, the following effects on the MPTS and Data streams configured on the QAM channel will occur.

- 1 Block all the unreferenced PIDs of the MPTS and Data streams on a QAM channel. This will include any standard SI PIDs coming along with the MPTS streams.
- 2 Will not block the PIDs mentioned in the PID remap table in any of the QAM channels.
- 3 If the operator needs to pass-through a specific Unreferenced PID after enabling this Block Unreferenced PID, an entry can be added in the remap table with the output PID values the same as the input PID value.

Block Unreferenced PID		
Row #	QAM Channel	Block Unreferenced PID
0	1/1.1	<input type="checkbox"/>
1	1/1.2	<input type="checkbox"/>
2	1/1.3	<input type="checkbox"/>
3	1/1.4	<input type="checkbox"/>
4	1/1.5	<input type="checkbox"/>
5	1/1.6	<input type="checkbox"/>
6	1/1.7	<input type="checkbox"/>
7	1/1.8	<input type="checkbox"/>
8	1/2.1	<input type="checkbox"/>
9	1/2.2	<input type="checkbox"/>
10	1/2.3	<input type="checkbox"/>

Apply Reset

Enabling Insert External PAT

Use the table below to enable/disable insertion of external PAT at the QAM channel level. This table is located on the Feature Page.

Insert External PAT PID		
Row #	QAM Channel	Enable Insert External PAT
0	1/1.1	<input type="checkbox"/>
1	1/1.2	<input type="checkbox"/>
2	1/1.3	<input type="checkbox"/>
3	1/1.4	<input type="checkbox"/>
4	1/1.5	<input type="checkbox"/>
5	1/1.6	<input type="checkbox"/>
6	1/1.7	<input type="checkbox"/>
7	1/1.8	<input type="checkbox"/>
8	1/2.1	<input type="checkbox"/>
9	1/2.2	<input type="checkbox"/>
10	1/2.3	<input type="checkbox"/>

Apply Reset

Below are the implicit effects of enabling insertion of external PAT on a channel.

- 1 All types of streams configured on this channel will be passed through.
- 2 PAT generated internally by RFGW will not be inserted in the QAM channel
- 3 Operator can insert PAT from an external data stream in the channel.

Operator can block/remap PMT PIDs on the channel to the value in (external) PAT manually by using the Unreferenced PID Map table.

Operator Responsibilities

PID Remapping

- 1 When specifying the PAT PID to be remapped, the operator should ensure that the PID comes only on one stream on that channel.
- 2 When remapping unreferenced PID / PMT PIDs, the operator should make sure that the desired output value of the remapping is not an existing ES or PMT PID of a stream on that channel. This will log output PID conflict in the System->Logs page.
- 3 When using the Block unreferenced PID option, the unreferenced PIDs of the MPTS stream and data stream will be blocked. This might include NIT, SDT, BAT, etc., on an MPTS stream so use this with caution. In case there is a pressing need to use this option and the NIT, SDT, BAT needs to be inserted at the output, specify this in the PID remap table with the same input and output PID values.
- 4 When remapping the PMT from the data stream, the operator should make sure that the output PID value is not the same as any existing PMT on the channel.

Inserting External PAT

- 1 Operator should take care of input PID conflicts i.e. ES and PMT PIDs of each stream should be unique within a given QAM channel. This is applicable for SPTS and MPTS stream with the Insert external PAT enabled as the streams are passed through when this option is enabled.
- 2 Operator should ensure that the unreferenced PID remapped should appear on only one stream on a QAM channel at any given point of time. If the same PID appears on two different channels, there will be CC errors at the output.
- 3 The Insert External PAT is supported only on the channels in the table based video mode.
- 4 When specifying the PAT PID to be remapped, the operator should ensure that that the PID appears only on one stream on that channel.
- 5 When remapping an unreferenced PID/PMT PID, the operator should make sure that the desired output value of the remapping is not an existing ES or PMT PID of a stream on that channel. This will cause an output PID conflict in the System->Logs in the RFGW.
- 6 When remapping PMT from the data stream, the operator should make sure that the output PID value is not the same as any existing PMT on the channel.

10

Alarm Configuration

Introduction

A new Alarm Configuration page has been added to the Web user interface to allow for editing of the alarm configuration.

In This Chapter

- Configuring Alarm Settings 148

Configuring Alarm Settings

This new page is accessible from the System tab, and appears as shown in the following example:

Alarm Name	Enable	Log Enable	Severity	Set Threshold	Clr Threshold	Units
Pwr Up Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Critical			
Gbe Port Link	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Critical			
UDP Traffic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Critical			
Fan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
FPGA Temp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
Power Supply	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Critical			
DTI Fail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Critical			
Mgmt Port Link	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
DC Voltage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
Stream Rate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
Cont Count	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major	5	0	counts/sec
Dejitter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
QAM Temp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
Rel Invalid	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
DTI Bkup Fail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
QAM Over B/W	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
License	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
QAM Gen Fail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
QAM Init	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
EIS ChanClosed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
EIS ConnLost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
ECMG NoChan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
ECMG ConnLost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
CW ClearExt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
CW CPEExtNoComp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
CW CPEExtNoEcm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
ECM PIDNoAlloc	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
QAM Incompat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
GbE port CRC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major	10	0	errors/5 min
Bind Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
QAM Voltage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
QAM Summary	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
IIPIDConflict	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major			
Cont Count A/V	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Major	5	0	counts/sec

Alarm Details

- Alarm Name – Name of the Alarm for which the row settings apply.
- Enable – Enables the Alarm notification for a particular alarm type; this will enable the log by default.
- Log Enable – Enables the log for particular alarm; editable only when the Alarm

is disabled.

- Severity - Enables the user to set the severity of alarms (Minor, Major, Critical, Warning).
- Set Threshold/Clear Threshold/Units - Helps to generate or clear alarms based on threshold values specified for some alarms.

This page also contains three additional settings:

- Apply - Sets any changes made in the Alarm Configuration page (either Enable/Severity/Threshold).
- Reset - Cancels any changes made in the Alarm Configuration page but not yet applied.
- Defaults - Returns any applied changes in the Alarm Configuration page to their default values.
- Users are not permitted to edit certain critical alarm settings. Examples include hardware alarms such as Pwr Up Test, Fan, and so on. In these cases, the corresponding fields on the page are dimmed.

11

Variable Fan Speed

Introduction

Variable Fan Speed is based on the temperature. Currently, the fan runs at full speed (setting is 255) irrespective of temperature. When this feature is enabled, the fan speed changes based on the measured temperature.

In This Chapter

- GUI Feature Option..... 152
- Feature Design Details 153

GUI Feature Option

GUI option "Smart Fan Control" is added on the System page of the RFGW-1.

It has two options:

- Enabled: The Fan speed changes based on the measured temperatures.
- Disabled: The Fan always runs at FULL Speed.

Note: This feature is DISABLED by default.

Feature Design Details

When Smart Fan Control changes to "Enable" there will be a 30 second delay before changing the FAN Speed to avoid any FAN related alarms.

Disabling the Smart Fan Control will make all fans operate at full speed immediately.

This feature flag is unit specific and will not be carried forward to other units when using the backup configuration file.

Based on the temperature, the fan control settings will vary from 150<->175<->255. GUI logs indicate these changes.

Fan Control Settings	Highest Temperature (in Centigrade)
150	< 65
175	> = 65 and < 74
255	> = 74

During RFGW-1 boot up, the fan will run at full speed (setting 255) for at least 5 minutes. This allows the boot process to be complete and the RFGW-1 to be configured completely.

Temperature readings are taken every 10 seconds from various measuring points. Out of these readings, the highest temperature will be recorded.

If temperature increases, the fan speed will increase immediately to the specified setting (see above).

Lowering the fan speed will be applied after 10 minutes from the point of increase in fan speed. This design is intended to reduce toggling of the fan speed thereby increasing the life of the fan.

Alarms will be raised based on the speed/rpm out of tolerance (existing design)

When there is any fan failure or fan running at a very low speed, the software will kick start all the fans at full speed (255).

There are fail safe mechanisms in place when the software fails/hangs.

12

Licensing

Introduction

To utilize certain software features, a software license is required in software releases after 01.02.20. The license is resident on the chassis, and is easy to install using an FTP server. No license server is required after installation. This section describes various applications that require a license file and also explains how to install, activate and verify the license file on the RF Gateway 1.

Note: The screens in this section are representative of software release 02.01.09 licensed features. The Authentication login button will not be present on software releases earlier than 02.01.09.

In This Chapter

- Applications Requiring a Software License 156
- Installing and Activating a License 161
- Secure License Transfer..... 163

Applications Requiring a Software License

To access the following features, a license is required after software release 01.02.20.

- Data streams requiring use of the DOCSIS Timing Interface
- DVB Encryption
- PowerKey Encryption

Note: It is recommended that the user backup the configuration of the RF Gateway 1 before performing any software upgrade, including license file installation.

RFGW Licenses

All of the licenses on the RFGW-1 can be ordered individually or together depending on the application. The available licenses are:

Video - No license required – capability exists on the device when shipped.

Data - Enables DOCSIS DEPI functionality. One Data license enables functionality on 4 QAMs per port. If an octal license is applied to the RFGW-1, two data licenses are needed to use 8 QAMs per port.

PowerKEY - Enables PowerKEY scrambling. One PowerKey license enables functionality on 4 QAMs per port. If an octal license is applied to the RFGW-1 two PowerKEY licenses are needed to use 8 QAMs per port.

DVB - Enables DVB scrambling. One DVB scrambling license enables functionality on 4 QAMs per port. If an octal license is applied to the RFGW-1, two DVB licenses are needed to use all 8 QAMs per port.

Octal License Option:

The Octal license enables 8 QAMs per port. When ordering an Octal license as an upgrade, one license type is required – L-RFGW1-OCTAL

When ordering the Octal license to be pre-installed at the factory, the Octal license is based upon the number of QAM cards. The Octal license can be purchased. Refer to the following table for the PID details.

SWLIC-RFGW1-OCTAL1
SWLIC-RFGW1-OCTAL2
SWLIC-RFGW1-OCTAL3
SWLIC-RFGW1-OCTAL4
SWLIC-RFGW1-OCTAL5
SWLIC-RFGW1-OCTAL6

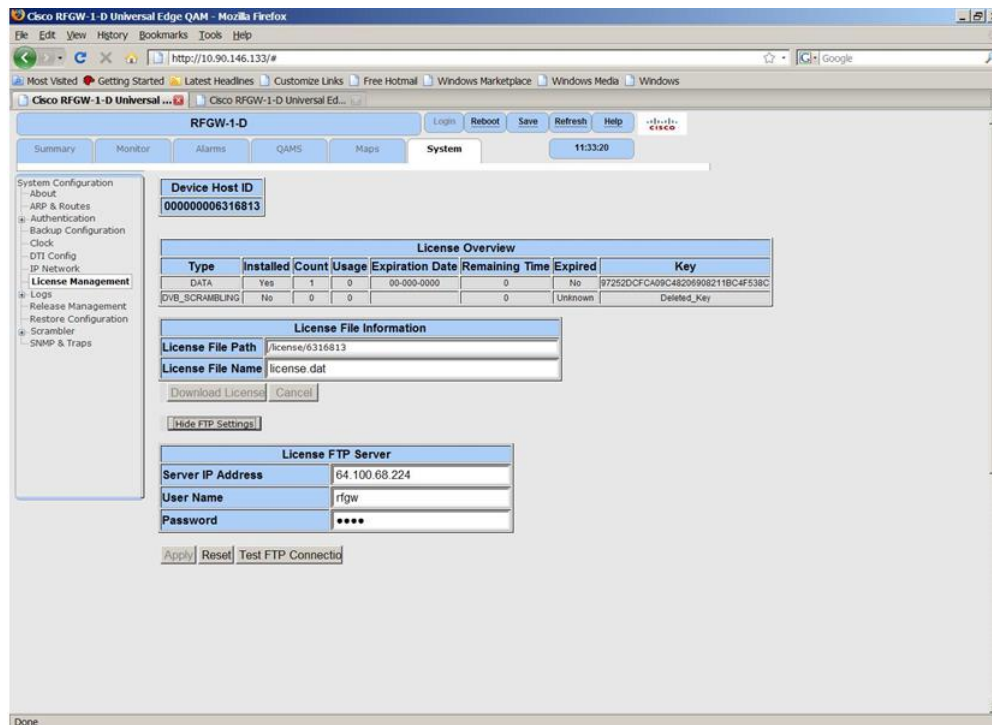
Obtaining a License File

The following section describes the steps to obtain a license file.

For customers who purchased an RF Gateway 1 using a part number that includes a license feature, the following license will be pre-installed at the factory.

SWLIC-RFGW1-DATA	RFGW-1 DATA License must configure with RFGW1
<ul style="list-style-type: none"> ■ SWLIC-RFGW1-OCTAL1 ■ SWLIC-RFGW1-OCTAL2 ■ SWLIC-RFGW1-OCTAL3 ■ SWLIC-RFGW1-OCTAL4 ■ SWLIC-RFGW1-OCTAL5 ■ SWLIC-RFGW1-OCTAL6 	RFGW-1 OCTAL LICENSE: MUST CONFIGURE WITH RFGW1
SWLIC-RFGW1-PKEY	RFGW-1 PowerKey Scrambling License: Must configure with RFGW-1
SWLIC-RFGW1-DVB	RFGW-1 DVB Scrambling License: Must configure with RFGW-1

You can verify installation by accessing the *System/License Management* page of the GUI. An example of this page with an installed data license is shown below.



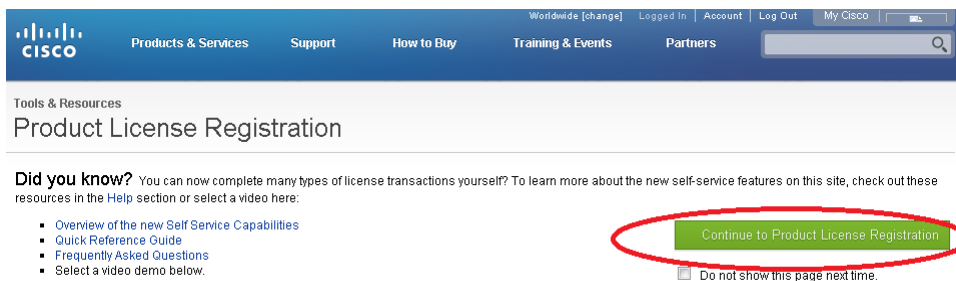
Chapter 12 Licensing

For customers who purchased an RF Gateway 1 without a license and want to upgrade, you will have to purchase the license file. A PAK number (used for obtaining license files to upgrade for specific functionality) may be purchased by contacting your Cisco account team.

To Obtain a License File

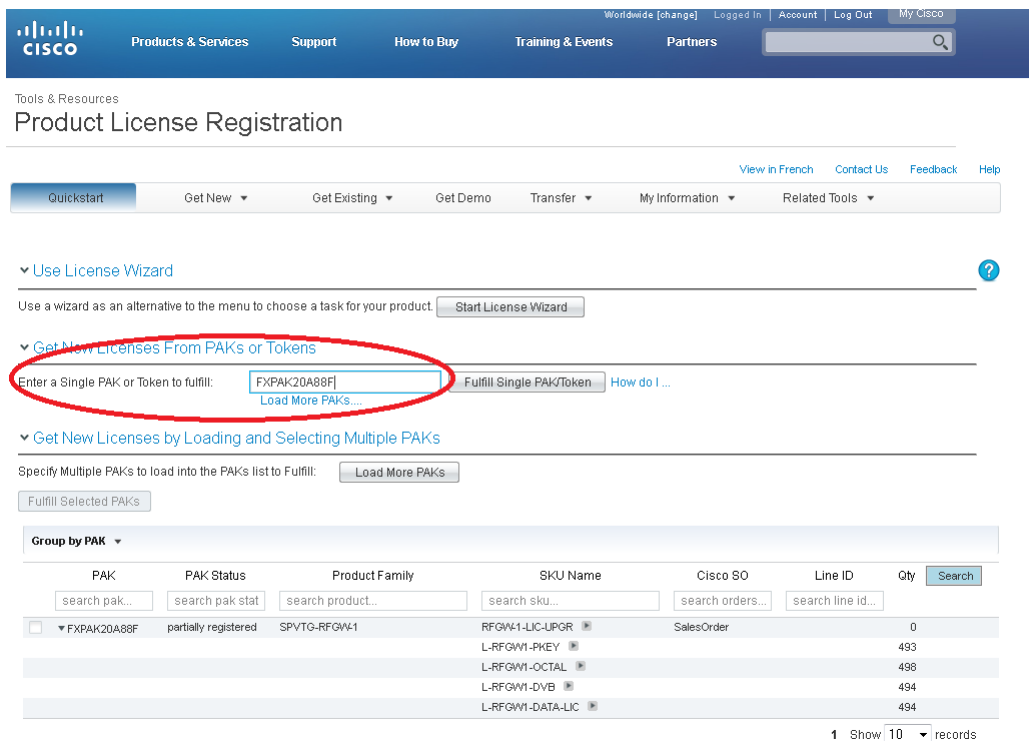
- 1 Obtain a PAK number from Cisco.
- 2 Using the PAK number and device serial number, obtain the license file from the Cisco license web application.
- 3 Proceed to the license administration portal at <https://tools.cisco.com/SWIFT/LicensingUI/Home>.

Result: The following page is displayed.



- 4 Click **Continue to Product License Registration**.

Result: The following page is displayed.



- 5 Enter the PAK number, then click **Fulfill Single PAK/Token**.

Result: The following page is displayed.

Quickstart **Get New** Get Existing Get Demo Transfer My Information Related Tools

Get New Licenses From PAKs or Tokens

✓ 1. Specify PAK **2. Assign SKUs to Devices** 3. Review

SPVTG-RFGW1
Product Authorization Key (PAK):

FXPAK20A88F

SKU	Quantity Available	Quantity to Assign
PAK:FXPAK20A88F		
RFGW1-LIC-UPGR		
L-RFGW1-DVB	492	0
L-RFGW1-PKEY	493	0
L-RFGW1-OCTAL	496	1
L-RFGW1-DATA-LIC	493	0

Clear Quantities

Serial Number:

Back **Next** Cancel

1 Enter the serial number of the RF Gateway 1 you wish to license.

Note: The serial number can be found on the System\About page of the RF Gateway GUI.

2 Click Next.

Result: The following page is displayed.

Quickstart **Get New** Get Existing Get Demo Transfer My Information Related Tools

Get New Licenses From PAKs or Tokens

✓ 1. Specify PAK ✓ 2. Assign SKUs to Devices **3. Review**

The license information that will be submitted.

HostId
AAK\WHJ

PAK	SKU Name	Qty
1	FXPAK20A88F	
2	RFGW1-LIC-UPGR	-2
3	L-RFGW1-DVB	0
4	L-RFGW1-PKEY	0
5	L-RFGW1-OCTAL	1
6	L-RFGW1-DATA-LIC	0

Your License Key will be emailed within the hour to these email addresses and connected with the specified end user.

* Send To:

* End User:

* License Agreement: I agree with the Terms of the License
[View License Agreement...](#)

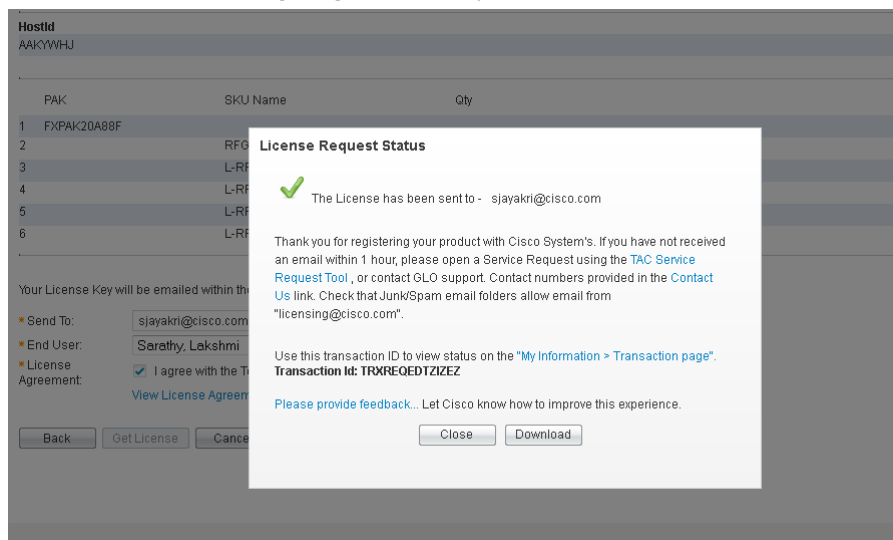
Back **Get License** Cancel

This page shows Octal licenses obtained from PAK that are to be assigned to a particular device. In this example, the RF Gateway 1 has been licensed for "DATA", however in most cases, licensed features will be displayed as "None".

Chapter 12 Licensing

- 3 Enter the mail id where the license should be sent.
- 4 Agree to the terms of the license and click **Get License**.

Result: The following page is displayed. The file will also be emailed to you.



- 5 Click **Close**.

Upgrading a License

Customers can upgrade or configure the license under the PAK PID L-RFGW1-SWLIC. Customers must have an octal license that can be combined with Data, Powerkey, and DVB scrambling for 8 QAMs per port to enable respective functionalities.

L-RFGW1-DATA-LIC	RFGW-1 DATA LICENSE (2 REQUIRED WHEN COMBINED WITH OCTAL LICENSE)
L-RFGW1-OCTAL	RFGW-1 OCTAL UPGRADE
L-RFGW1-PKEY	RFGW-1 POWERKEY SCRAMBLING LICENSE (2 REQUIRED WHEN COMBINED WITH OCTAL LICENSE)
L-RFGW1-DVB	RFGW-1 DVB SCRAMBLING LICENSE (2 REQUIRED WHEN COMBINED WITH OCTAL LICENSE)

Installing and Activating a License

To Install a License

The license file will be installed via FTP. An external FTP server will be required.

1 Click System/License Management

Result: The *License Overview* window is displayed.

The screenshot shows the Cisco RFGW 1-D configuration interface. The 'License Overview' table is as follows:

Type	Installed	Count	Usage	Expiration Date	Remaining Time	Expired	Key
DATA	Yes	2	0	00-000-0000	0	No	5FA3A71EB45ACB5CAB1C58FF2B41EADF
DVB_SCRAMBLING	Yes	2	0	00-000-0000	0	No	1C10BA8E6C00CD475C0959D907EB636D
B_CHANNELS_PER_PORT	No	0	0	00-000-0000	0	No	Deleted_Key
POWERKEY	Yes	2	0	00-000-0000	0	No	3D919FC10990B66FAB3D399394FE4481

The 'License File Information' section shows:

- License File Path: .
- License File Name: license.dat.00000000AAKYWHJ.txt

Buttons for 'Download License' and 'Cancel' are visible below the fields. A 'License Status' message at the bottom reads: 'License File download completed. Click refresh to get the validation key and license details.'

2 Click Show FTP Settings.

Result: The *Configuration FTP Server* window is displayed.

3 Enter the FTP Server IP Address.

4 Enter the FTP User Name.

5 Enter the FTP Password.

6 Click Apply.

7 Click Test FTP Connection. Verify your connection with the FTP login success popup.

Note: If a failure occurs, recheck the IP address, user name and password.

8 Click Save.

9 In the "License File Path" text box, enter the path on the FTP server to the license file.

Example: /rfgw-1-d/data_license/AAKYWHJ

10 In the "License File Name" text box, enter the name of the license file.

Example: license.dat.00000000AAKYWHJ.txt

11 Click Download License to initiate download of the license file.

Note: If download failure occurs, recheck the path to the license directory and the filename.

To Activate a License

- 1 Click the reboot button in the upper right corner. (Reboot is required to activate the license file.)

Result: The RF Gateway 1 will reboot and activate the license file.

Secure License Transfer

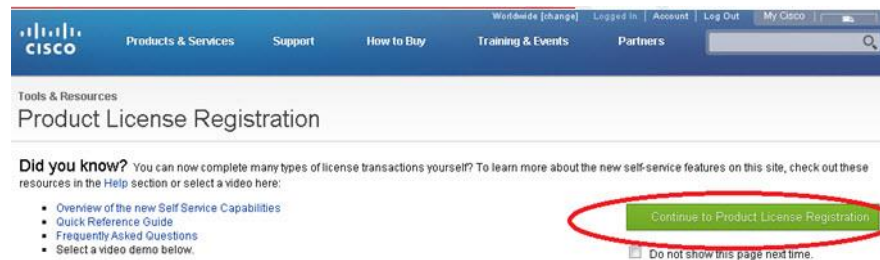
The Secure License Transfer feature allows you to transfer unused licenses from one RFGW-1 (source device) to another RFGW-1 (destination device).

Start License Transfer

Follow the steps below to start a license transfer.

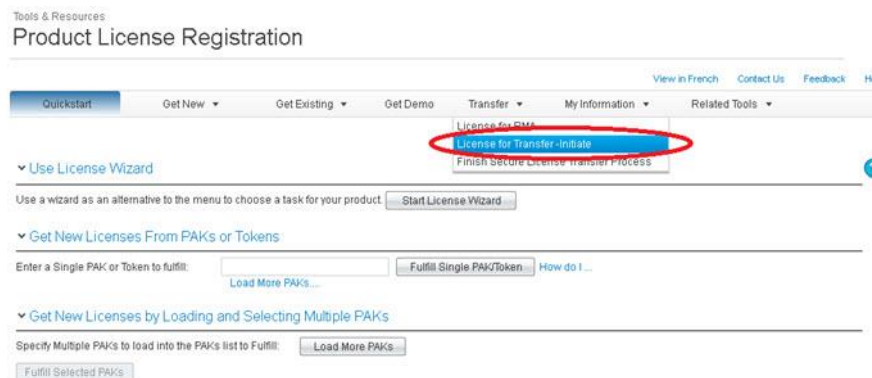
- 1 Log in to the license administration portal at <https://tools.cisco.com/SWIFT/LicensingUI/Home>

Result: The following screen is displayed.



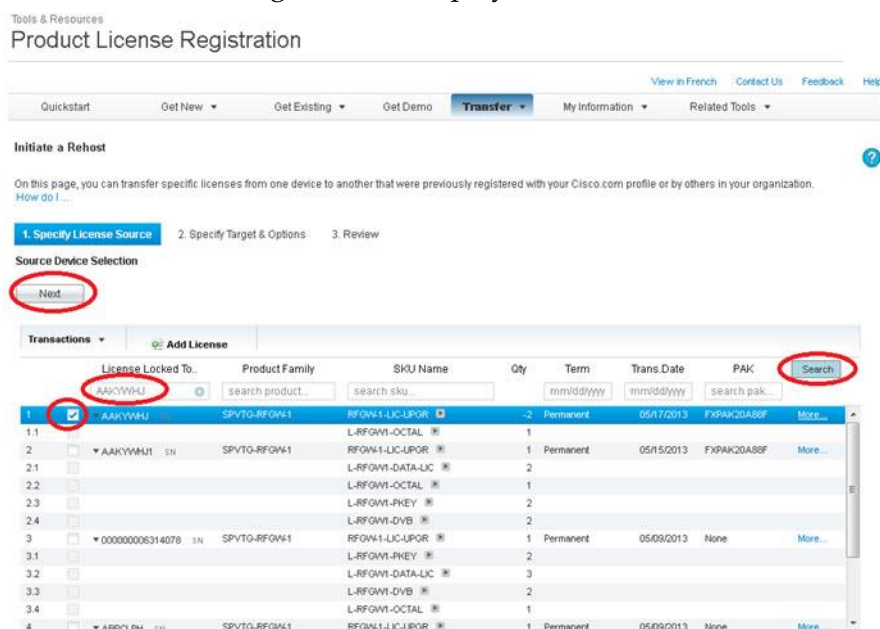
- 2 Click **Continue to Product License Registration**.

Result: The following screen is displayed.



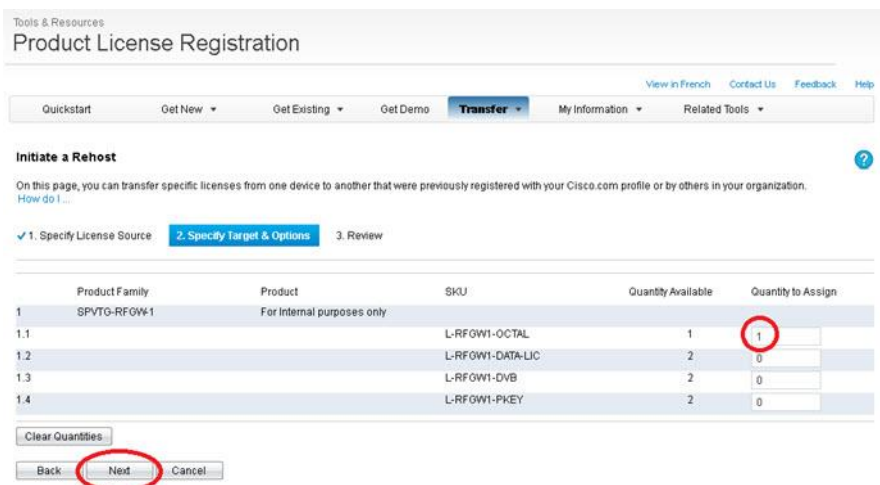
- 3 Select the Transfer tab and click **License for Transfer –Initiate**.

Result: The following screen is displayed.



- Select the device serial number from list or click **Next** and enter the serial number. Click **Search**.

Result: The following screen is displayed.



- Enter the quantity to be assigned and click **Next**.

Result: The following confirmation page is displayed.

Product License Registration

Quickstart Get New Get Existing Get Demo **Transfer** My Information Related Tools

View in French Contact Us Feedback Help

Initiate a Rehost

On this page, you can transfer specific licenses from one device to another that were previously registered with your Cisco.com profile or by others in your organization.

How do I ...

✓ 1. Specify License Source ✓ 2. Specify Target & Options **3. Review**

	Serial Number	Product ID
1 Source	AAKYWHJ	
Target	Token	

	Skus Name	Quantity
1.1	L-RFGWI-OCTAL *	1

Your License Key will be emailed within the hour to these email addresses and connected with the specified end user.

Send To: sjayakri@cisco.com

End User: Sarathy, Lakshmi

License Agreement: I agree with the Terms of the License [View License Agreement...](#)

Back **Submit** Cancel

6 Enter the mandatory details and click **Submit**.

Result: The following page is displayed.

Initiate a Rehost

On this page, you can transfer specific licenses from one device to another that were previously registered with your Cisco.com profile or by others in your organization.

How do I ...

✓ 1. Specify License Source ✓ 2. Specify Target & Options

	Serial Number	Product ID
1 Source	AAKYWHJ	
Target	Token	

	Skus Name	Quantity
1.1	L-RFGWI-OCTAL *	1

Your License Key will be emailed within the hour to these email addresses and connected with the specified end user.

Send To: sjayakri@cisco.com

End User: Sarathy, Lakshmi

License Agreement: I agree with the Terms of the License [View License Agreement...](#)

Back Submit Cancel

License Request Status

✓ The License has been successfully sent to the email address below: sjayakri@cisco.com

Use this transaction ID to view status on the "My Information > Transaction page".

Transaction id: TXREOEDTZIEH

If you have not received an email within 1 hour, please open a Service Request using the TAC Service Request Tool Please have your valid Cisco.com user Id and password available. As an alternative, you may also call our main Technical Assistance Center at 800-553-2447. Please be sure to check your Junk/Spam email folders for this email from licensing@cisco.com with your license key attached.

Please provide feedback... Let Cisco know how to improve this experience.

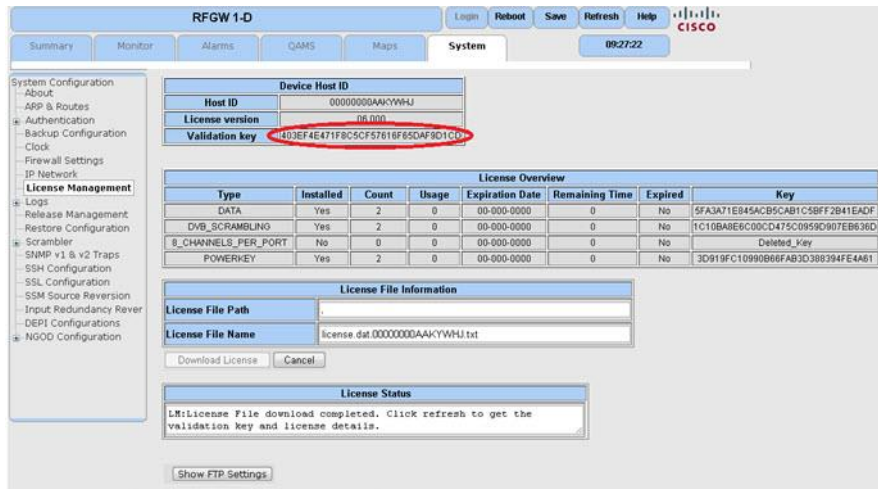
Close Download

Installing/Activating the License

- 1 To install the license, refer to *Installing and Activating a License* (on page 161).
- 2 Once the license is installed, click the **Refresh** button to activate the license.

Result: Validation key information is displayed. See screen below.

Note: The Validation key is needed to complete the license transfer.

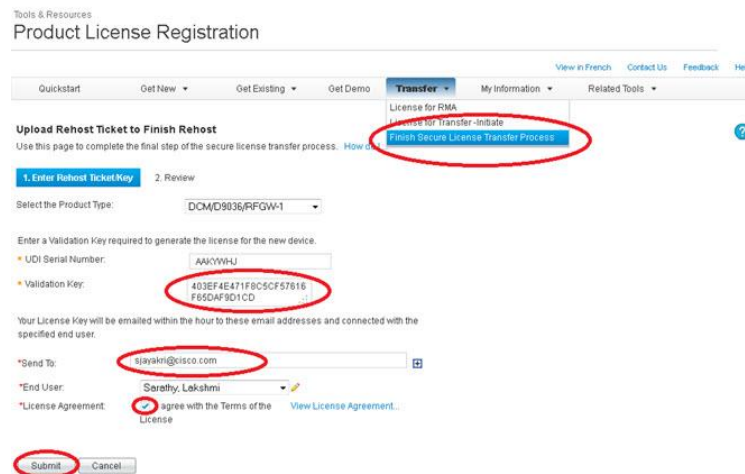


Complete License Transfer

To complete the License transfer, follow the instructions below.

- 1 Navigate to the Cisco license administration portal application @ <https://tools.cisco.com/SWIFT/LicensingUI/Home>
- 2 Select the Transfer tab and click **Finish Secure License Transfer Process**.

Result: The following screen is displayed.



- 3 Enter the validation key obtained after downloading the license to the source RFGW-1.
- 4 Agree to the terms of the license and Click **Submit**.

Result: The following email will be sent with the generated token.

Token Generated

licensing@mailers list

Sent: Fri 5/17/2013 12:26 PM

To: Selvakumar Jayakrishnan (sjayakri)

DO NOT DISCARD THIS EMAIL.

You have received this email because your email address was provided to Cisco Systems Technical Assistance Center due to the Transfer of Licenses of your Device. Please read this email carefully and forward it with any attachments to the proper system administrator if you are not the correct person.

Below you will find a corrected Token that will allow you to successfully register for and receive a license key/file for your purchase. Additionally, you should keep a copy of this email with your software product for future reference.

Token : TOK1F24RRU

Please log in to the following web site to complete your registration and receive your license key/file.

<http://www.cisco.com/go/license>

We apologize for any inconvenience this delay has caused you.

Note: The case is closed and you will now be able to use this license for another device. Refer to *Obtaining a License File* (on page 157).

13

Encryption and Scrambling

Introduction

This chapter describes how to integrate the RFGW-1 into scrambling applications.

In This Chapter

■ Introduction.....	170
■ Scrambling, Control Word, and Cryptoperiod.....	171
■ Access Criteria and Access Rights.....	172
■ Entitlement Control Messages	173
■ Event Information Scheduler	174
■ Scrambling Levels.....	175
■ Simulcrypt Scrambling.....	177
■ Timing Parameters.....	178
■ Steps To Take.....	180

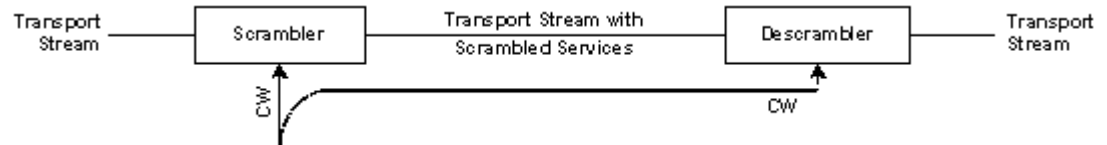
Introduction

The RF Gateway 1 is provided with a DVB Simulcrypt compliant scrambler designed to meet DVB Simulcrypt Conditional Access (CA) specifications ETSI TS 103 197. There are many CA Systems in use and the goal of the RF Gateway 1 is to integrate the devices in as many CA Systems as possible. To achieve this, a common set of protocols and interfaces between scramblers and CA Systems is required.

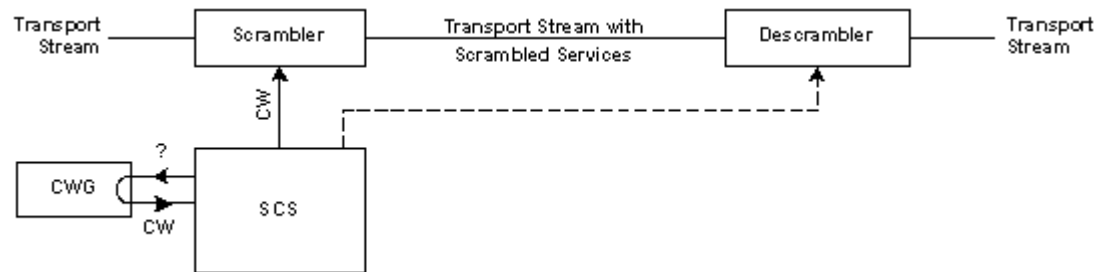
The RF Gateway 1 scrambler works on a license basis. For more information concerning licenses, refer to *Chapter 12: Licensing* (see "*Licensing*" on page 155).

Scrambling, Control Word, and Cryptoperiod

At the transmission site of a CA System, services multiplexed into a Transport Stream can be scrambled using a DVB common scrambling algorithm with a scrambling/descrambling key called Control Word (CW). At the receiver site, the scrambled services can be descrambled by an appropriate descrambling algorithm using the same CW.



To increase the security of a CA System, the CW used to scramble and descramble services changes periodically (typically every 10 seconds). The duration of scrambling by one CW is called Crypto Period. CWs, typically 64 bits long, are generated by a Control Word Generator (CWG) and requested by the Simulcrypt Synchronizer (SCS).



CWs cannot be delivered from the transmitter to the receiver site in the clear. They need to be encrypted. The algorithm used to encrypt the CW is unique to each CA System and implemented in a secure device of the descrambler and uses the smart card of the customer's Conditional Access Module (CAM).

Access Criteria and Access Rights

When a subscriber is only interested in particular services, i.e. sports and nature, he only wants to pay for those services. Unpaid services must remain unintelligible. Therefore, two parameters are defined, Access Criteria (AC) and Access Rights.

- Access Criteria is vendor specified information and specifies service-related criteria applied to a package of services or elementary streams. These subscriptions (also called theme or product) are encapsulated into Entitlement Control Messages (ECMs). Refer to *Entitlement Control Messages* (on page 173).
- Access Rights are stored on the smart card of the descrambler and determines which services the subscriber can access. These Access Rights are periodically reconfirmed using Entitlement Management Messages (EMMs). When Access Rights for a particular subscriber are changed, EMMs are sent to the descrambler with the new Access Rights.

Example:

AC 1 subscription = Football ECM1

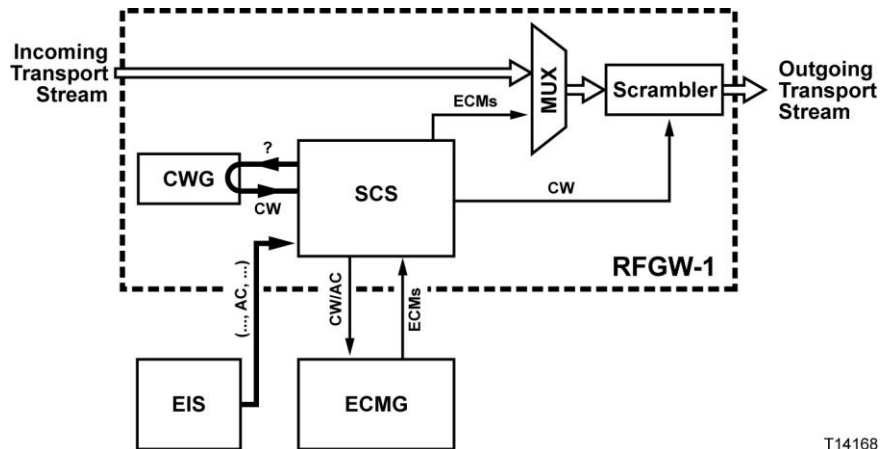
AC 2 subscription = Tennis ECM2

AC 3 subscription = Golf ECM3

A subscriber pays to view football and golf programs. His set top box receives all ECM packets that contain the appropriate CWs. The set top box also receives EMM packets that contain Access Rights for this box. These rights are compared with the AC and the set top box is only allowed to decipher the ciphered CWs of the ECMs for which the subscriber has Access Rights (ECM1 and ECM3).

Entitlement Control Messages

The SCS triggered from the EIS to start a CA event will get every Crypto Period a CW for this event from the CWG. For more information, refer to *Event Information Scheduler* (on page 174).



T14168

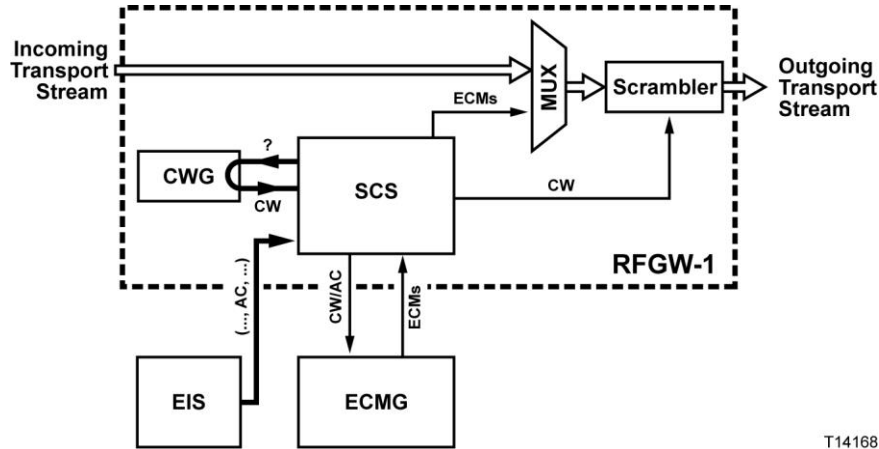
The SCS extracts the AC from the Scrambling Control Group (SCG) information received from the EIS. The synchronizer sends this AC together with the CW for the corresponding Crypto Period to the Entitlement Control Message Generator (ECMG). The ECMG encrypts both the AC and the CW using a particular cryptographic algorithm with a specific Service Key. This encrypted data is encapsulated into an ECM and sent to the SCS.

Before the first Crypto Period for this event begins, the SCS starts sending ECMs for this event to the multiplexer (typically every 200 msec). This start time is necessary to give the descrambler time to decrypt the encrypted CW and AC. The multiplexer multiplexes this stream of ECMs with the outgoing Transport Stream. When the event begins, the SCS sends the CW to the scrambler, which starts scrambling the service(s) associated with this event.

Before the end of the Crypto Period, the SCS requests a new CW from the CWG, then sends it together with the AC to the ECMG, and receives a new ECM for this event from the ECMG. This new generated ECM is multiplexed in the outgoing Transport Stream. When the Crypto Period is ended, the new CW is sent to the scrambler, which starts scrambling the service(s) using the new CW. This occurs for every Crypto Period until the end of the event.

Event Information Scheduler

The EIS is the functional unit in the CA System that holds the schedule, configuration, and other information required for the complete CA system.

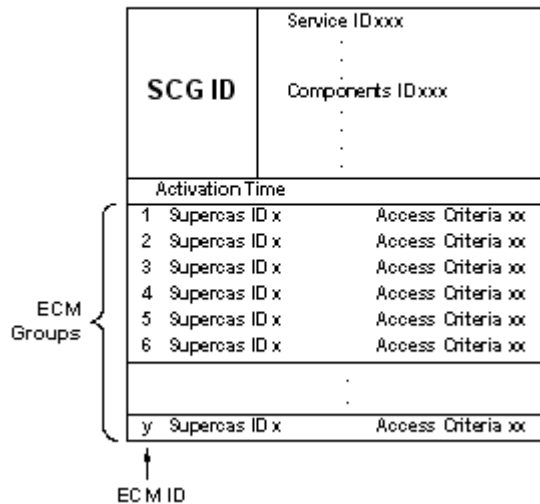


T14168

To start a scrambling event, the EIS provides the SCS with a SCG provisioning message. The message contains a list of services and/or elementary streams that must be scrambled at the same time with the same CW and a list with ECM groups for which ECMs must be generated. An ECM group contains the necessary information, like Super_Cas_ID, ECM_ID, and AC, to bind an ECM stream to a CA provider.

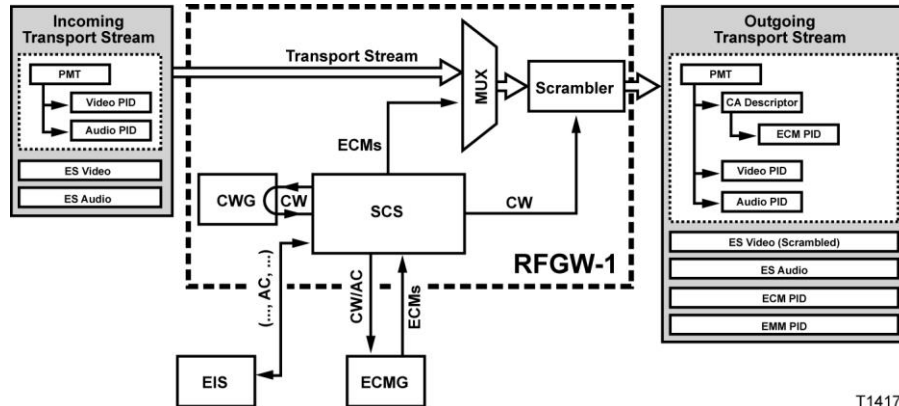
To stop a scrambling event, the EIS sends a SCG provisioning message update to the SCS. The ECM group for the event of which scrambling must be stopped is removed from the SCG provisioning message. The following illustration shows a SCG provisioning message.

SCG Provisioning Message



Service Level Scrambling

The alternative to elementary stream level scrambling is to scramble all components that make up a service with the same CW. In this case, there is only one stream of ECM messages associated with the service as a whole.



When scrambling at the service level, all elementary streams within the service are scrambled using the same CW. Only one ECM is required for each service. The CA descriptor is inserted near the top of the PMT.

Note: Elementary stream level scrambling and service level scrambling can be mixed within the scrambler but not within the same service.

Simulcrypt Scrambling

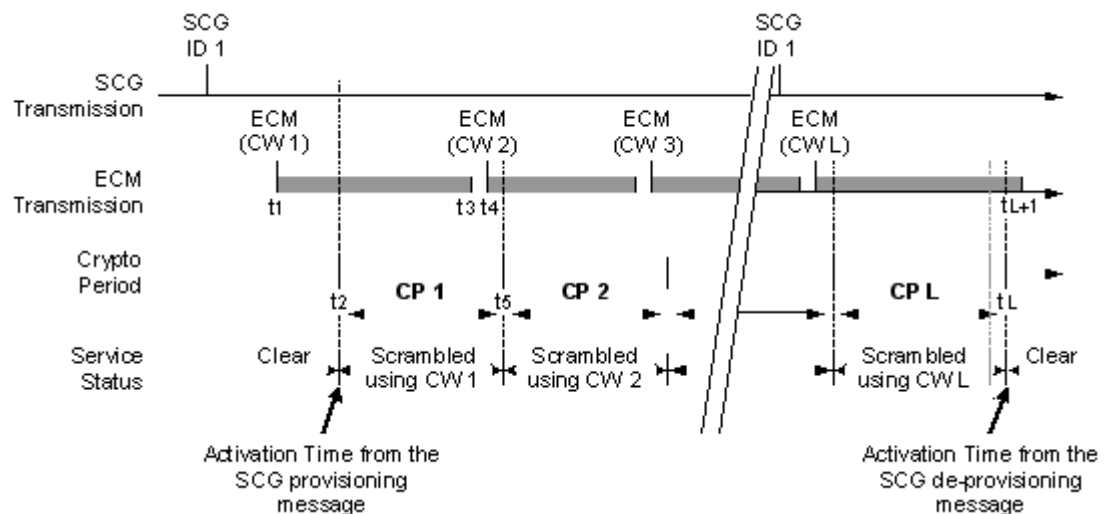
Simulcrypt scrambling is a scrambling method whereby a single transport stream contains ECMs from different CA Systems. Each CA system uniquely scrambles the same CW in the ECM so that elementary stream bandwidth is not increased. This enables different CA decoder populations to receive and correctly decode the same video and audio streams.

Timing Parameters

When the EIS triggers the SCS to start a new CA event using a SCG (ID 1) provisioning message, the SCS requests a CW (CW 1) from the CWG. Once the SCS receives the CW from the CWG, the SCS sends the CW together with the AC and ECM ID extracted from the SCG provisioning message to the ECMG. The ECMG encrypts the CW and AC and encapsulates this data into an ECM. The ECMG sends this ECM to the SCS. At a certain time before (t_1-t_2) starting the CA event (activation time), the SCS starts sending ECMs for the first Crypto Period at regular times to the multiplexer.

- Transition Start Delay (t_1-t_2): represents the amount of time between the start of the first Crypto Period following a clear to scrambled transition, and the start of the broadcasting of the ECM attached to this period.

The multiplexer multiplexes these ECMs directly into the outgoing Transport Stream. At the same time, a CA descriptor containing the ECM Packet Identifier (PID) is inserted into the PMT of the transport stream.



The Transition Start Delay must match the time the descrambler needs to decapsulate the ECM PID from the PMT and to decrypt the CW and AC. At the start (t_2) of the first Crypto Period (CP 1), the set top box starts descrambling the scrambled service using CW 1.

At a certain time (t_3-t_5) before the end of running Crypto Period (CP 1), the SCS stops transmitting ECMs attached to this CP and at a certain time (t_4-t_5) before the next Crypto Period (CP 2), the SCS starts transmitting ECMs for CP 2.

- Stop Delay (t_3-t_5): represents the amount of time between the end of a Crypto Period and the end of the broadcasting of the ECM attached to this period.
- Start Delay (t_4-t_5): represents the amount of time between the start of a Crypto Period and the start of the broadcasting of the ECM attached to this period.

When the SCS receives an SCG provisioning message update from the EIS indicating the end of the running CA event, the synchronizer extends the last Crypto Period until the end of the activation time extracted from the SCG provisioning message update.

Once the activation time (t_l) is reached, the set top box stops descrambling the service. The SCS stops transmitting ECMs attached to this last Crypto Period at time (t_l+1).

- Transition Stop Delay (t_l-t_l+1): represents the amount of time between the end of last Crypto Period preceding a scrambled to clear transition, and the end of the broadcasting of the ECM attached to this period.

When the SCS receives a SCG provisioning message containing another AC for the service(s), the synchronizer stops sending ECMs containing the previous AC at time t_6 in the last Crypto Period and starts sending ECMs with the new AC at time (t_7).

- AC Start Delay (t_7-t_8): represents the amount of time between the start of the first Crypto Period following a change in the AC and the start of the broadcasting of the ECM attached to this period.
- AC Stop Delay (t_6-t_8): represents the amount of time between the end of the last Crypto Period preceding a change in AC and the end of the broadcasting of the ECM attached to this period.

During the connection setup between the SCS and the ECMG, the SCS receives a Channel Status Message containing particular timing parameters. When timing parameters are missing or inaccurate, the Scrambler ECMG settings allow overruling these parameters.

When a subscriber tunes into a scrambled service in a particular Crypto Period, the scrambler is not able to scramble the service during the rest of this Crypto period because he has only the CW for the next period. To solve this problem, an ECM can be provided with more than one CW. CA Systems allow 1 or 2 CWs in an ECM, for example, the CW of the current Crypto Period and the CW of the next period.

Steps To Take

Before scrambling can be used, the following steps must be completed.

1 Prerequisite Configurations

- a Configure the GbE input ports, including Video/Data IP address. For information regarding GbE Interface Configuration, see the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01.
- b Configure the QAM outputs. For information regarding Enabling QAM Ports, see the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01.
Note: ONID and TSID must match EIS settings for CVC simulcrypt.
- c Configure Channel Application Mode (SDV for CVC simulcrypt operation, Video for VOD map mode). For information regarding Channel Application Mode, see the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01.

2 Simulcrypt Controller Configurations

- a Configure Scrambling General Parameters. Refer to *Configuring Scrambling General Settings* (on page 182).
Note: For CVC simulcrypt, Core Encryption should be set to DVB CSA.
- b Configure Scrambling Specific Parameters. Refer to *Configuring Scrambling Specific Parameters* (on page 183).
- c Assign one or multiple ECMG(s) to the RFGW-1 and configure the ECMG-specific parameters. Refer to *Entitlement Control Message Generators* (on page 183).
Note: CVC Simulcrypt should use "ECM ID" instead of "Auto" to satisfy reference AC requirements.
- d Assign one or multiple EIS(s) to the RFGW-1 and configure the EIS-specific parameters. Refer to *Event Information Schedulers* (on page 198).

Configuring Broadcast Scrambling and Dual Encryption Broadcast

Follow instructions below to select scrambler parameters.

- 1 Navigate to the System Configuration page.

Result: The following page is displayed.

System Configuration		Device Information	
Device Description	Cisco RFGW-1-D Universal Edge QAM	Device Up Time	3 Days, 17 Hours, 57 Minutes, 54 Seconds
Device Name	rfgw1d	Device Contact	Cisco Support
Device Location	here	QAM Encoding Type	MU-B
Frequency Plan	Standard	Gratuitous ARP State	Enabled
Gratuitous ARP Time	60 seconds	Def jitter Buffer Depth	150 milliseconds
Network PID	0108	Insert Network PID reference in PAT	Enabled
Ingress All Option for VOO	Disabled	Gle Part CRC Alarm Set Threshold	10
Gle Part CRC Alarm Clear Threshold	0	Begin Scrambler Alarm Debounce	10 seconds
End Scrambler Alarm Debounce	10 seconds	Automatic Configuration Save	Enabled
Pre Encrypted Type	Predefined	Broadcast Scrambling	Enabled
Dual Encryption Broadcast	Enabled	MPTS Defaults	Pass Input PAT

- 2 Configure Broadcast Scrambling parameter as Enabled/Disabled.

Result: The following pop-up message is displayed.

Changing the Broadcast Scrambling setting and clicking on Apply button will trigger a database save and reboot. Click Ok to continue or Cancel to abort.

- 3 Configure Dual Encryption Broadcast as Enabled/Disabled. This parameter is editable, only if the Broadcast Scrambling parameter is set as Enabled.

Result: The following pop-up message is displayed.

Changing the Dual Encryption Broadcast setting and clicking on Apply button will trigger a database save and reboot. Click Ok to continue or Cancel to abort.

Prevent this page from creating additional dialogs

- 4 Click **Apply** to accept or Reset to abort.

Note: Changing the broadcast scrambling parameter is allowed only if there are no active sessions. Any change to these two parameters will trigger an automatic configuration save and will reboot the RF Gateway.

Configuring Scrambling General Settings

General Settings Parameters

The following table describes the General Settings parameters.

Parameter	Description
Scramble Video and Audio	The RFGW-1 can scramble all components of a service or only the video and audio component of a service (in case of service level scrambling).
Check SCG at Provision Time	When this parameter is on and the SCS receives a SCG provisioning message from the EIS, the RFGW-1 checks the presence of the elementary streams/service(s) in the incoming transport stream with the service(s) listed in the SCG provisioning message. If the incoming transport stream contains the service(s), the SCS accepts the SCG. If not, the SCS refuses the SCG and returns an error message to the EIS. When switched off, the RFGW-1 checks the transport stream for service(s) present (activation time). The scrambler starts the scrambling process for service(s).
Strong Pairing Enforcement	Switches on or off the NDS strong pairing enforcement.
SCG Persistence	Allows the SCGs to be stored on the device so that they are available after reboot.
Active Core Encryption	Shows the correct firmware encryption algorithm.
Core Encryption Algorithm	Selects DES (PowerKEY), or DVB-CS for simulcrypt.
Scrambled ECMG Streams	Displays the scrambled stream count on the RFGW-1.

Selecting Scrambler Parameters

Follow instructions below to select scrambler parameters.

- 1 Navigate to the *System/Scrambler* page.

Result: The following page is displayed.



- 2 Click the check box next to the parameter you want to activate.
- 3 Click **Apply** to accept or **Reset** to abort.

Configuring Scrambling Specific Parameters

About the SCS Configuration GUI

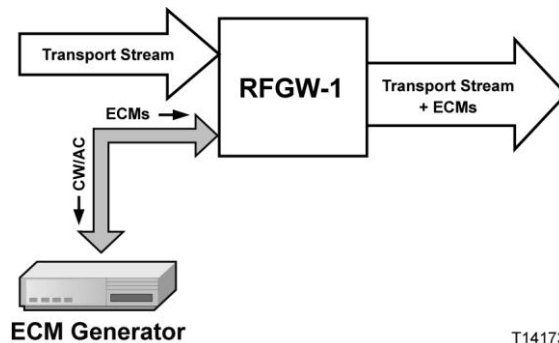
The SCS allows configuring the scrambling specific parameters and assigning the following CA interfaces:

- ECMG interfaces
- EIS interfaces

Note: The number of CA interfaces that can be assigned to a RF Gateway 1 using the SCS configurator is restricted to 40.

Entitlement Control Message Generators

To establish communication between the SCS of the RFGW-1 and an ECMG, a TCP connection has to be made followed by a channel set up. During the connection process, the SCS requires the IP address and port number of the ECMG to establish the TCP connection, and needs a channel identifier to set up a channel. The operator can determine this channel identifier or the SCS can pick a channel identifier from the free channel identification pool.



The SCS also requires mapping between the Super CAS ID, which is a concatenation of the CA system identifier, subsystem identifier, and the communication parameters. Once the channel is established and the EIS triggers the SCS to request ECMs from the ECMG, an ECM stream is set up.

The number of ECM streams that can be set up between the SCS and the ECMG within one channel is limited and depends on the CA System.

Load Balancing

For backup and/or load sharing purposes, several ECMGs can be connected to the RFGW-1. The priority assigned to the communication channel determines if the ECMGs are used in load balancing or in backup mode. When the channel priorities of the ECMGs are equal, the ECMGs work in load sharing mode. When the priority differs, the ECMG with highest priority (= lowest number) acts as the main ECMG and the ECMG with the lowest priority acts as backup.

Whenever the RFGW-1 sets up a new ECM stream, it selects a connected ECMG. It then selects the ECMG connection with the highest priority that has available ECM capacity. If the generators have an equal priority, the one with available ECM capacity and the least open streams will be selected. When the load on an ECMG decreases, ECM streams will not automatically spread over equal priority ECMGs.

As soon as the channel connection with an ECMG is broken, or the ECMG runs out of ECMG capacity, a new ECMG is selected according to the criteria above.

The ECMG working modes can be combined. For example, two generators with the same priority (load sharing mode) can be combined with a generator that has a lower priority (backup mode).

Note: If capacity is unavailable, the ECM stream will not be set up and the service(s) can not be scrambled.

Examples

■ Load Sharing

Suppose an application has two ECMGs (IP A and B) with the same priority (prio 1), and has a capacity of 10 streams. During stream setup, the streams are spread over the ECMGs as follows:

- IP A: streams 1, 3, 5, 7, 9
- IP B: streams 2, 4, 6, 8, 10

When the RFGW-1 stops scrambling a number of services (corresponding streams 5, 7, and 9), no stream balancing is done.

- IP A: streams 1, 3
- IP B: streams 2, 4, 6, 8, 10

■ ECMG backup

In our application, ECMG IP A has priority 1 and IP B priority 2. The streams are shared as follows:

- IP A: streams 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
- IP B: streams

If IP A fails, IP B takes over the load.

- IP A: streams
- IP B: streams 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

If IP A restores:

- IP A: streams 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
- IP B: streams

When an additional stream is required, capacity will be taken from IP B.

- IP A: streams 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
- IP B: streams 11

■ **Load Sharing and ECMG Backup**

Suppose an application has three ECMGs (IP A, B, and C) with a capacity of 10 streams. IP A and B have priority 1 and IP C priority 2. During stream setup, the streams are spread over the ECMGs as follows:

- IP A (prio 1): streams 1, 3, 5, 7, 9, 11
- IP B (prio 1): streams 2, 4, 6, 8, 10
- IP C (prio 2): streams

If IP A fails, the full capacity of IP B will be used and the remainder of the capacity of IP C will be used.

- IP A (prio 1): streams
- IP B (prio 1): streams 2, 4, 6, 8, 10, 1, 3, 5, 7, 9
- IP C (prio 1): streams 11

Adding an ECMG

Follow the instructions below to add an ECMG.

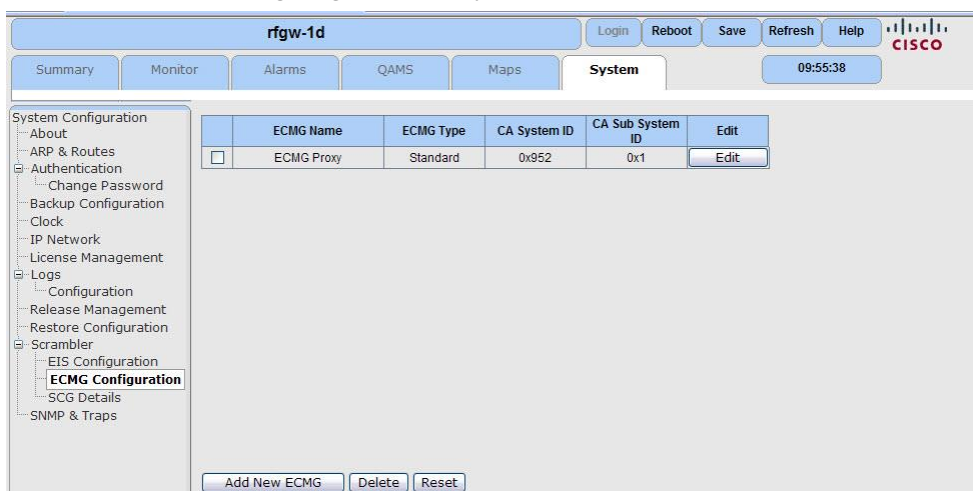
- 1 Navigate to the *System/Scrambler* page.

Result: The following page is displayed.



- 2 Click the + to expand the window and select **ECMG Configuration**.

Result: The following page is displayed.



- 3 To add a new ECMG, click **Add New ECMG**.

Note: To select an ECMG you have already created, click **Edit**.

Result: The following page showing the ECMG parameters is displayed.

The screenshot shows the configuration page for rfgw-1d. The left sidebar lists various configuration categories, with 'ECMG Configuration' selected. The main area displays the following parameters:

ECMG Name	ECMG Proxy
ECMG Type	Standard
CA System ID (Hex)	0x0
CA Sub System ID (Hex)	0x0
ECMG PID Source	Auto
ECMG PID Lower Limit (Hex)	0x30
ECMG PID Upper Limit (Hex)	0x1ff6
ECMG Streams / ECMG	0
Open ECMG Streams / ECMG	0
Automatic Channel ID Selection	<input checked="" type="checkbox"/>
Enable Hot Backup	<input type="checkbox"/>

Buttons: Apply, Reset

Radio buttons: Advanced, Connection, Descriptor Rules

Priority	IP Address	Port	ECMG Port Selection	Channel Id	ECM Channel Id	Connection Status	Open Streams

- To add ECMG connections, refer to *Adding ECMG Connection Entries* (on page 188).

Removing an ECMG

Follow the instructions below to remove an ECMG.

- Click the box next to the ECMG entry to be removed.

Result: The entry is highlighted as shown in the following screen.

The screenshot shows the configuration page for rfgw-1d. The left sidebar lists various configuration categories, with 'ECMG Configuration' selected. The main area displays a table of ECMG entries:

	ECMG Name	ECMG Type	CA System ID	CA Sub System ID	Edit
<input checked="" type="checkbox"/>	ECMG Proxy	Standard	0x952	0x1	Edit

Buttons: Add New ECMG, Delete, Reset

- Click **Delete** to delete the entry or **Reset** to abort.

Tip: To remove more than one entry, click the check box of the first row, press and hold the **SHIFT** key, and click the check box of the last row.

ECMG Parameters

The following table describes the ECMG parameters.

Parameter	Description
ECMG Name	ECMG name (max 20 characters) acts as a label to facilitate the identification of the ECMG in the CA system.
ECMG Type	<ul style="list-style-type: none"> ■ Standard: DVB Simulcrypt. ■ M_Crypt: (DVB Simulcrypt) allows empty ECMs to reset scrambling. ■ Nagra: (DVB Simulcrypt) prefetch less ECMs in advance to enable quicker use of updated AC.
CA System ID (Hex)	Used to indicate the type of CA system applicable for the associated ECM stream. Contact your CA vendor for more information. CA System identifier is defined in table 3 CA_system_ID of ETR 162.
CA Sub System ID (Hex)	Used to differentiate multiple ECMGs from the same CA vendor in the CA application. Contact your CA vendor for more information.
ECMG PID Source	<p>Select the desired ECM PID source.</p> <ul style="list-style-type: none"> ■ ECM ID: SCG Provisioning message is used to determine the ECM PID. ■ Auto: The multiplexer of the RFGW-1 chooses the ECM PID from the list of free PIDs. <p>Note: The list of free PIDs, determined by the multiplexer can be limited by defining limits (ECM PID Lower Limit, and ECM PID Upper Limit).</p>
ECMG PID Lower Limit (Hex)	Lower limit for ECMG PID.
ECMG PID Upper Limit (Hex)	Upper limit for ECMG PID.
ECMG Streams/ECMG	Number of ECMG streams required.
Open ECMG Streams/ECMG	Number of open ECMG streams to the ECMG of the CA system.
Automatic Channel ID Selection	Enable/disable automatic channel ID selection.
Enable Hot Backup	Not supported at this time (future use).

Follow the instructions below to change ECMG parameters.

- 1 Highlight the parameter to be changed and modify.
- 2 Click **Apply**.

Changing ECMG Parameters

Follow the instructions below to change ECMG parameters.

- 1 Highlight the parameter to be changed and modify.
- 2 Click **Apply**.

Adding ECMG Connection Entries

Follow the instructions below to add ECMG connection entries.

- 1 Navigate to the *System/Scrambler* page.

Result: The following page is displayed.

The screenshot shows the 'System' configuration page for 'rfgw-1d'. The left sidebar lists various configuration categories, with 'Scrambler' expanded. The main content area displays the 'Scrambler General Settings' form. The settings are as follows:

Setting	Value
Scramble Only Video and Audio	<input type="checkbox"/>
Check SCG at Provision Time	<input type="checkbox"/>
Strong Pairing Enforcement	<input type="checkbox"/>
SCG Persistence	<input type="checkbox"/>
Active Core Encryption Algorithm	DES
Core Encryption Algorithm	DES
Scrambled ECMG Streams	0

Buttons for 'Apply' and 'Reset' are located below the settings table.

- 2 Click the + to expand the window and select **ECMG Configuration**.

Result: The following page is displayed.

The screenshot shows the 'System' configuration page for 'rfgw-1d'. The left sidebar lists various configuration categories, with 'Scrambler' expanded and 'ECMG Configuration' selected. The main content area displays a table of ECMG configurations:

	ECMG Name	ECMG Type	CA System ID	CA Sub System ID	Edit
<input type="checkbox"/>	ECMG Proxy	Standard	0x952	0x1	Edit

Buttons for 'Add New ECMG', 'Delete', and 'Reset' are located below the table.

- 3 Click **Add New ECMG**.

Result: The following page is displayed.

The screenshot shows the configuration page for 'rfgw-1d'. The left sidebar contains a tree view with 'ECMG Configuration' selected. The main area displays the following configuration fields:

- ECMG Name: ECMG Proxy
- ECMG Type: Standard
- CA System ID (Hex): 0x0
- CA Sub System ID (Hex): 0x0
- ECMG PID Source: Auto
- ECMG PID Lower Limit (Hex): 0x30
- ECMG PID Upper Limit (Hex): 0x1ff6
- ECMG Streams / ECMG: 0
- Open ECMG Streams / ECMG: 0
- Automatic Channel ID Selection:
- Enable Hot Backup:

Buttons for 'Apply' and 'Reset' are present. Below the form are radio buttons for 'Advanced', 'Connection' (selected), and 'Descriptor Rules'. At the bottom, a table header is visible:

Priority	IP Address	Port	ECMG Port Selection	Channel Id	ECM Channel Id	Connection Status	Open Streams
----------	------------	------	---------------------	------------	----------------	-------------------	--------------

4 Click **Connection**.

Result: The *Connection* table is displayed.

○ Advanced ○ Connection ○ Descriptor Rules

Priority	IP Address	Port	ECMG Port Selection	Channel Id	ECM Channel Id	Connection Status	Open Streams
1	10.0.0.1	8500	CA	0	1	Closed	0

Buttons: Add New Connection, Reset

5 Click **Add New Connection**.

Result: A new row is added to the *Connection* table.

- In the **Priority** box of this entry, enter a channel priority number to determine the ECMG working mode.
- In the **IP Address** box, enter the IP address of the ECMG. The octets of the IP address must be separated by dots.
- In the **Port** box, enter the port number of the ECMG used for this channel.
- In the **ECMG Port Selection** box, enter the Ethernet port to use for communication with the ECMG.

10 In the **Channel Id** box, enter the channel Id number. A number between 0 and 65535 is allowed. If **Automatic Channel ID Selection** is supported, the ID is automatically set. Make sure the check box is selected.

Note: All CA vendors do not support Automatic Channel ID Selection.

11 Click **Apply** to accept change or **Reset** to abort.

Removing ECMG Connection Entries

Follow the instructions below to remove ECMG connection entries.

1 In the Connections table, click the check box(es) of the entry that must be removed.

Result: The entry is highlighted.

2 Click **Apply** to remove the entry.

Tip: To remove more than one entry, click the check box of the first row, press and hold the [SHIFT] key, and then click the check box of the last row.

Overruling ECMG Channel Status Messages Parameter Values

In normal circumstances, the values in the Channel Status Message generated by the ECMG are used by the SCS to determine the ECM transmit timings. When particular values are missing, inaccurate, and cannot be changed on the ECMG, these values can be overruled using the SCS Configuration GUI. The table below describes the parameters that can be overruled.

Parameter	Description
Override Max. Comp. Time (ms)	The worst-case time needed by an ECM Generator to compute an ECM when all the streams in a channel are in use. This parameter determines the ECM Request Interval parameter used by the Simulcrypt Synchronizer. This parameter should be changed if the ECM Generator indicates that the ECMG is out of computational resources.
Override Min. CP Duration (ms)	The minimum amount of time a control word can be active before it can be changed. Note: For normal CVC simulcrypt, this setting should remain at 4 seconds.
Override Transition Start Delay (ms)	The amount of time between the start of the first cryptoperiod following a clear to scrambled transition and the start of the broadcasting of the ECM attached to this period.
Override Transition Stop Delay (ms)	The amount of time between the end of the last cryptoperiod preceding a scrambled to clear transition and the end of broadcasting the ECM attached to this period.
Override Start Delay (ms)	The amount of time between the start of a cryptoperiod and the start of broadcasting the ECM attached to this period.
Override Stop Delay (ms)	The amount of time between the end of a cryptoperiod and the end of broadcasting the ECM attached to this period.
Override AC Start Delay (ms)	The amount of time between the start of the first cryptoperiod following a change in the Access Criteria and the start of broadcasting the ECM attached to this period.

Chapter 13 Encryption and Scrambling

Override AC Stop Delay (ms)	The amount of time between the end of the last cryptoperiod preceding a change in Access Criteria and the end of broadcasting the ECM attached to this period.
Override Repetition Period (ms)	The amount of time between two ECM packets at the output of the scrambler.
Override Max. Streams:	The maximum number of simultaneous open streams supported by an ECMG on a channel. If the ECMG returns 0, no maximum is known. The scrambler will not limit the amount of streams on a channel and no ECMs will be requested from the ECMG backup when maximum capacity is reached on the ECMG. To make sure an ECMG is not overloaded, the maximum number of streams can be overruled.
Override Hint Bit Start Delay (ms)	[Visible only for the Internal PowerKEY ECMG] The amount of time before the start of the new cryptoperiod from which the Hint Bit should be set in the PowerKEY ECM's.
Override Hint Bit Stop Delay (ms)	[Visible only for the Internal PowerKEY ECMG] The amount of time before the start of the new cryptoperiod from which the Hint Bit should be cleared in the PowerKEY ECM's.

The following table shows the minimum, maximum, and default values of these parameters.

Parameter	Minimum Value	Maximum Value	Default Value
Override Max Comp Time (ms)	0	60,000	5,000
Override Min CP Duration (ms)	1,000	3,600,000	10,000
Override Transition Start Delay (ms)	-30,000	0	-2,000
Override Transition Stop Delay (ms)	0	30,000	2,000
Override Start Delay (ms)	-30,000	30,000	-2,000
Override Stop Delay (ms)	-30,000	30,000	-2,000
Override AC Start Delay (ms)	-30,000	30,000	-2,000
Override AC Stop Delay (ms)	-30,000	30,000	-2,100
Override Repetition Period (ms)	0	30,000	100
Override Max. Streams	0	30,000	512

Independent of the active/inactive state of a RFGW-1 participating in a CA application, the RFGW-1 will be connected to the ECMG by default.

Changing Channel Status Message Parameter Values

Follow the instructions below to change message parameter values.

- 1 Click **Advanced**.

Steps To Take

Result: The following table is displayed for all the ECMG's other than the Internal PowerKEY ECMG.

Advanced	
Override Max. Comp. Time (ms)	<input type="checkbox"/> 5000
Override Min. CP Duration (ms)	<input type="checkbox"/> 10000
Override Transition Start Delay (ms)	<input type="checkbox"/> -2000
Override Transition Stop Delay (ms)	<input type="checkbox"/> 2000
Override Start Delay (ms)	<input type="checkbox"/> -2000
Override Stop Delay (ms)	<input type="checkbox"/> -2000
Override AC Start Delay (ms)	<input type="checkbox"/> -2000
Override AC Stop Delay (ms)	<input type="checkbox"/> -2000
Override Repetition Period (ms)	<input type="checkbox"/> 100
Override Max. Streams	<input type="checkbox"/> 512

- 2 Click the check box next to the parameter you want to change.
Result: The parameter box becomes active.
- 3 Modify the setting.
- 4 Click **Apply** to accept change or **Reset** to abort.

Chapter 13 Encryption and Scrambling

When the 'Advanced' radio button is clicked for the Internal PowerKEY ECMG, the following table is displayed.

<input type="button" value="Apply"/> <input type="button" value="Reset"/>	
<input checked="" type="radio"/> Advanced <input type="radio"/> Connection <input type="radio"/> Descriptor Rules	
Override Max. Comp. Time (ms)	<input type="checkbox"/> 550
Override Min. CP Duration (ms)	<input checked="" type="checkbox"/> 4000
Override Transition Start Delay (ms)	<input type="checkbox"/> -600
Override Transition Stop Delay (ms)	<input type="checkbox"/> 0
Override Start Delay (ms)	<input type="checkbox"/> -600
Override Stop Delay (ms)	<input type="checkbox"/> -600
Override AC Start Delay (ms)	<input type="checkbox"/> -600
Override AC Stop Delay (ms)	<input type="checkbox"/> -600
Override Repetition Period (ms)	<input type="checkbox"/> 100
Override Max. Streams	<input type="checkbox"/> 2048
Override Hint Bit Start Delay	<input type="checkbox"/> -1000
Override Hint Bit Stop Delay	<input type="checkbox"/> -600

If the encrypted content is to be streamed for the non-Cable Card STB's running the Rovi Application, the 'Hint Bit Stop Delay' parameter must be set as -400 msecs and the 'Override Hint Bit Stop Delay' flag must be set to 'True' for the STB's to descramble the content without any issues.

ECMG Descriptor Rules

CA descriptors are data structures used to carry CA specific information for services or elementary streams. The RFGW-1 is able to update PMTs with CA descriptors according to the user configurable CA descriptor rules. The SCS configurator allows configuring CA descriptor rules and applying these rules to descriptors.

Note: When the RFGW-1 scrambles a service or components within a service, CA descriptors in the PMT are sorted using the values of the ECM PIDs to which the CA descriptors apply. CA descriptors with the lowest value appear first. When a scrambled service is passed from input to output of the RFGW-1, the CA descriptor order is not changed.

Adding a Descriptor Rule

Follow the instructions below to add a descriptor rule.

- 1 Navigate to the *System/Scrambler* page.

Result: The following page is displayed.

The screenshot shows the configuration page for 'rfgw-1d'. The left sidebar contains a tree view with 'Scrambler' expanded to 'ECMG Configuration'. The main content area displays 'Scrambler General Settings' with the following options:

Setting	Value
Scramble Only Video and Audio	<input type="checkbox"/>
Check SCG at Provision Time	<input type="checkbox"/>
Strong Pairing Enforcement	<input type="checkbox"/>
SCG Persistence	<input type="checkbox"/>
Active Core Encryption Algorithm	DES
Core Encryption Algorithm	DES
Scrambled ECMG Streams	0

Buttons for 'Apply' and 'Reset' are located below the settings.

- 2 Click the + to expand the window and select **ECMG Configuration**.

Result: The following page is displayed.

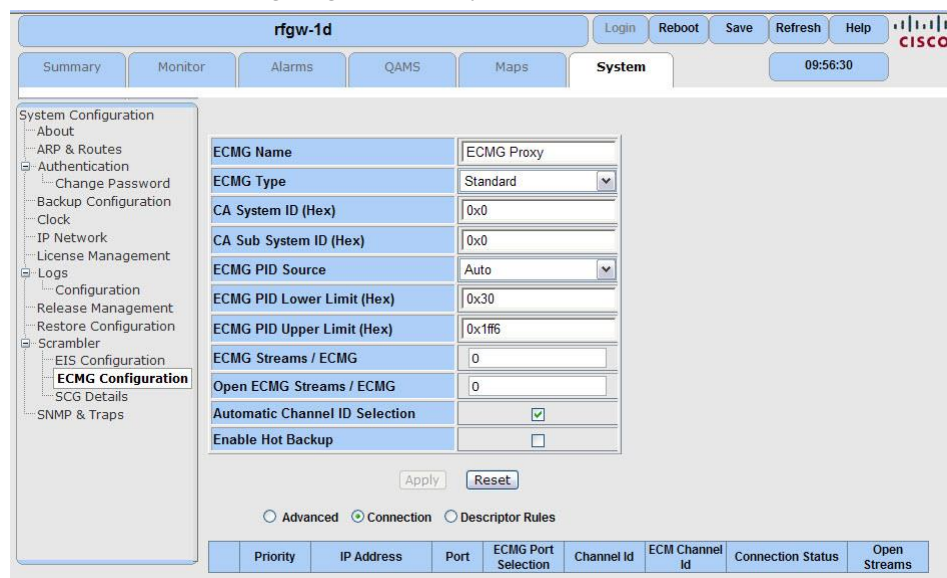
The screenshot shows the configuration page for 'rfgw-1d' with 'ECMG Configuration' selected in the sidebar. The main content area displays a table of ECMG configurations:

	ECMG Name	ECMG Type	CA System ID	CA Sub System ID	Edit
<input type="checkbox"/>	ECMG Proxy	Standard	0x952	0x1	Edit

Buttons for 'Add New ECMG', 'Delete', and 'Reset' are located below the table.

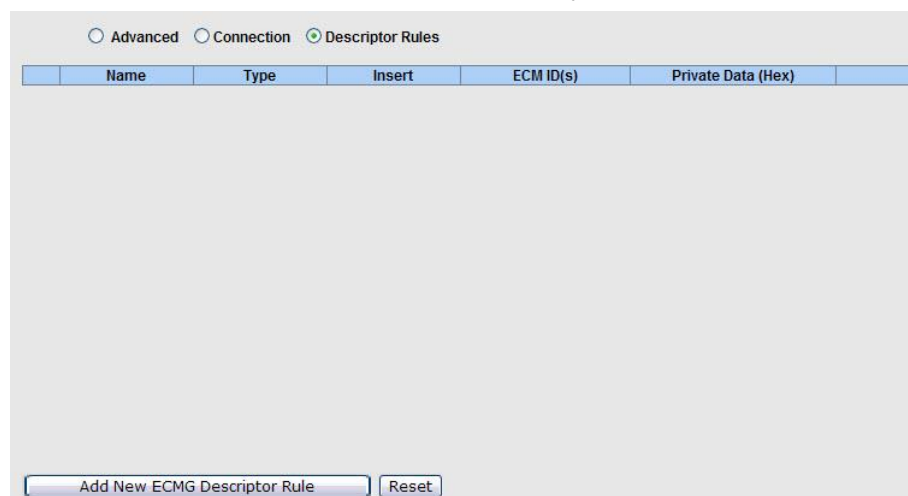
- 3 Click **Add New ECMG**.

Result: the following page is displayed.



4 Click **Descriptor Rules**.

Result: The Descriptor Rules table is displayed.



5 Click **Add New ECMG Descriptor Rule**.

Result: The rule is added to the table.

6 Click **Apply** to accept change or **Reset** to abort.

7 To make changes to any of the parameter settings, highlight and modify. Click **Apply** to accept changes.

Removing a Descriptor Rule

Follow the instructions below to remove a descriptor rule.

1 Select the check box next to the rule you want to remove.

Result: The entry is highlighted as shown in the following screen.

2 Click **Apply** to accept change or **Reset** to abort.

Descriptor Rule Parameters

The following table describes the Descriptor Rule parameters.

Parameter	Description
Name	Identification of the descriptor rule.
Type	Allows you to select the rule type. <ul style="list-style-type: none"> ■ Add Private Data - add data to the standard descriptor. ■ Do Not Insert - prevents updating the CA descriptor in the PMT if the PSI/SI information is generated by an external PSIG. <p>Notes:</p> <ul style="list-style-type: none"> ■ If the rule type is set to <i>Do Not Insert</i>, the <i>Insert</i> and <i>Private Data [Hex]</i> parameters are unavailable. ■ Private data is CA Vendor proprietary.
Insert	Select the insertion level mode for the private data part. <ul style="list-style-type: none"> ■ According to EIS - EIS determines insertion level. ■ At ES Level - insertion is performed at ES level (even if service level scrambling is defined by the EIS).
ECM ID(s)	ECM ID(s) to which the CA descriptor rule must be applied. Multiple IDs must be separated by a comma.
Private Data (Hex)	Private data of the descriptor rule.

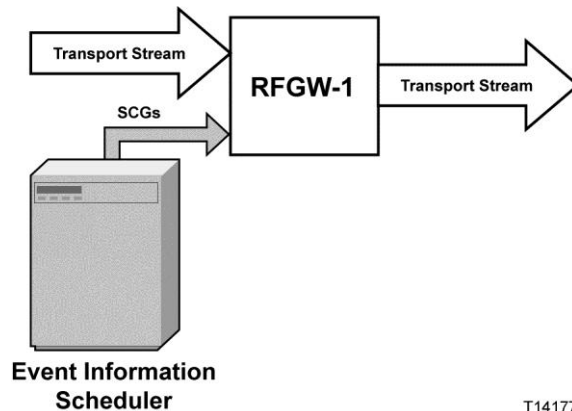
Notes:

- The RFGW-1 adds a standard CA descriptor to the PMTs of scrambled services, or elementary streams.
- When no IDs are added into the Data ID(s) box, the descriptor rule is applied to all ECMs. Since only one rule with empty Data ID(s) box is allowed, this rule overrules the standard CA descriptor.
- When IDs are added, the rule is only applied to the ECM IDs appearing in the ECM ID(s) box. Only one rule can be effective for a certain ECM ID.
- ECM IDs added must be unique over all descriptor rules for a certain ECMG.

Chapter 13 Encryption and Scrambling

Event Information Schedulers

The EIS provides the SCS with SCGs containing relevant information to scramble services. To establish communication between the EIS and the SCS, a TCP connection should be made followed by a channel set up. Once the connection is made, the SCS of the RFGW-1 receives SCGs from the EIS. To set up a TCP connection between the EIS and the RFGW-1, the EIS requires the knowledge of the IP address and TCP port of the RFGW-1 used to establish the connection.



T14177

Adding an EIS

Follow the instructions below to add an EIS.

- 1 Navigate to the *System/Scrambler* page.

Result: The following page is displayed.



- 2 Click the + to expand the window and select **EIS Configuration**.

Result: The following page is displayed.



- 3 Click **Add New EIS**.

Result: The new EIS is added to the table.



- 4 Click **Apply** to accept change, or **Reset** to abort.

Removing an EIS

Follow the instructions below to remove an EIS.

- 1 Select the check box next to the Rule you want to remove.

Result: The row is highlighted.

- 2 Click **Apply** to accept change or **Reset** to abort.

EIS Parameters

The following table describes the EIS parameters.

Parameter	Description
EIS Name	Identifies the EIS in the CA System.
TCP Port	Listening port number used by the RFGW-1 to establish TCP connection with the EIS. Note: The TCP listening port number must be unique and cannot be used by an EMM Generator or a PSI Generator.
EIS Port Selection	The Ethernet port to use for communication with the EIS.
Overrule	When the Cryptoperiod parameter is encapsulated into Scrambling.
CP Duration	When control groups are missing or inaccurate, this parameter can be overruled.
EIS Type	The following EIS types are available. <ul style="list-style-type: none"> ■ General - Third party EIS ■ SA Specific EIS of ROSA NMS Note: Only one SA EIS can be assigned to a RFGW-1.
Connection Status	Status of the connection to the EIS.
Peer IP	IP address of the EIS.

Changing EIS Parameters

Follow the instructions below to change EIS parameters.

- 1 Click the drop down box to select the parameter to change.
Result: The **Apply** and **Reset** buttons are now active.
- 2 Click **Apply** to accept change and **Reset** to abort.

14

Security Features

This chapter describes the Cisco RF Gateway 1 security features including GUI authentication, HTTPS and SFTP support.

In This Chapter

■ Security Features Overview	202
■ Authentication.....	203
■ Enabling HTTPS on the RF Gateway 1	210
■ SFTP Support.....	218
■ Firewall Settings.....	223

Security Features Overview

The following features are supported in software version 6.1.x.

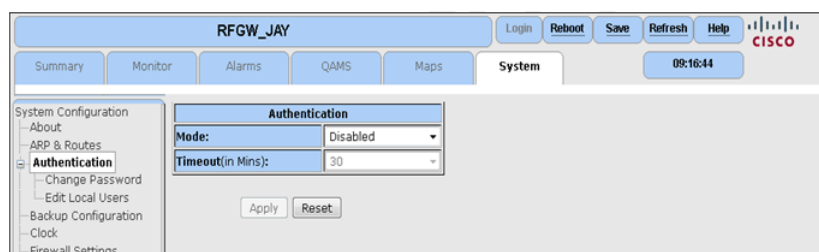
- Local and remote authentication for accessing RFGW GUI.
- HTTPS support
- SFTP support (SSHv2 with DSA key supported).
- DSA key download for SFTP.
- SFTP client support to perform release management, backup/restore configuration, license management, and SSL/SSH key download.
- Firewall settings to enable or disable SFTP, FTP, HTTPS, HTTP, and Telnet ports.

Authentication

Password-based authentication is available for RF Gateway 1 users operating software release 06.1.x. This chapter describes how to configure user authentication capabilities. The unit can be operated without authentication enabled (default factory setting) or enabled in two user-settable (Local and Remote) modes of operation.

Authentication Configuration

The RF Gateway 1 is shipped to customers with the authentication default factory setting set to disabled as shown in the following screen. A unit in this state allows the user full read and write access to all configurable parameters. The RF Gateway 1 web management page appears with the login tab grey and un-selectable. Local and remote authentication modes are available. To enable Local Authentication, refer to *To Set up Local Authentication* (on page 203). To enable Remote Authentication, refer to *To Setup Remote Authentication* (on page 207). Once the authentication mode is enabled, the user must provide a password to make any new authentication mode changes. While operating in either mode, the RF Gateway 1 management interface allow users alphanumeric passwords of 4 to 16 characters in length.



Local Authentication

The RF Gateway 1 supports five read only users (rfgw1, rfgw2, rfgw3, rfgw4, rfgw5, and one read-write user (admin). All these users have the default password (factory setting) "0000". Additional login ids cannot be provisioned in Local mode. Refer to *To Change Default Password* (on page 205).

To Set up Local Authentication

- 1 Navigate to the *System/Authentication* page.

Result: The following page is displayed.

- 2 In the *Mode* drop-down window, select **Local** as the mode of operation.

The default timeout value is 30 minutes. The timeout value can be changed, if required.

- 3 Click **Apply**.

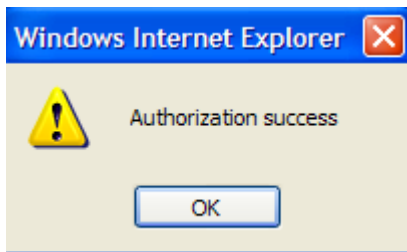
Result: The login UI screen is displayed.



Local user names can be entered as one of the following: admin, rfgw1, rfgw2, rfgw3, rfgw4 and rfgw5. Note: admin is a read-write user. The other users are read-only users.

- 4 Enter 0000 as the default password.
- 5 Click **Login**.

Result: The following screen is displayed.

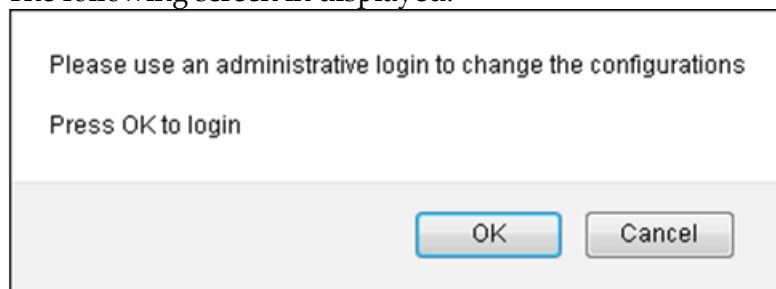


- 6 Click **OK**.

Read-Only/Read-Writer User

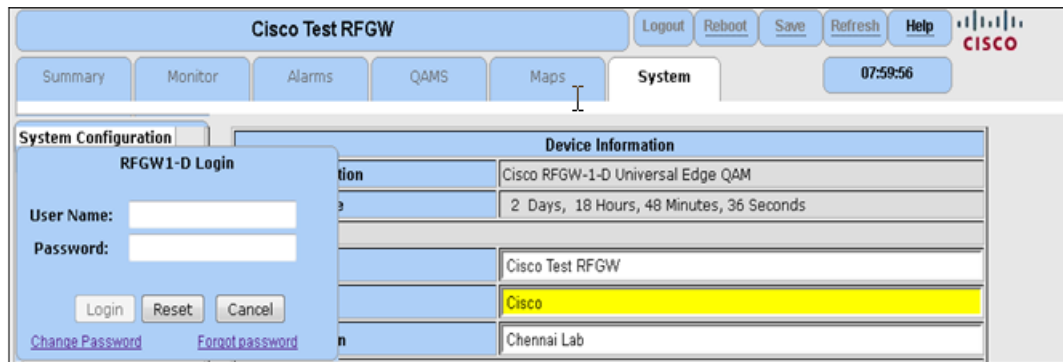
- 1 In the Login UI, login as rfgw1 (local user).
- 2 Edit the configurations in RF Gateway 1 web pages and click **Apply**.

The following screen is displayed.



- 3 Click **OK**.

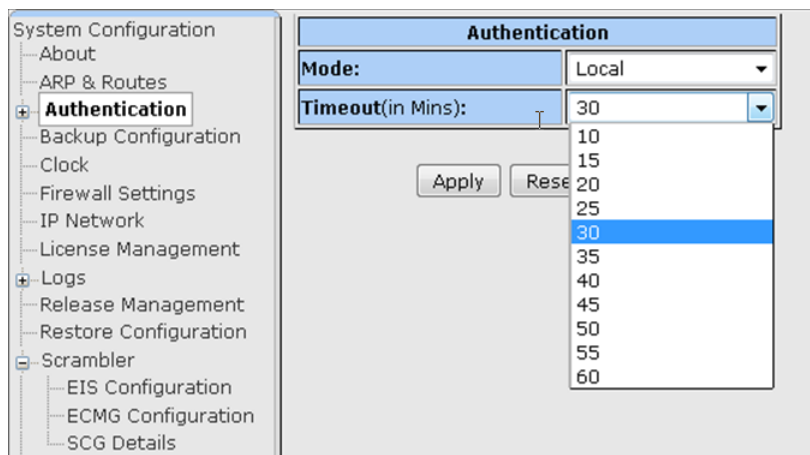
The following screen is displayed.



- 4 Login as admin.
- 5 Edit the configurations in RF Gateway 1 web pages and click Apply. Note: Only admin user can make changes to RF Gateway 1 configurations, save the configuration or reboot the RF Gateway 1.
- 6 The settings are applied.

To Change Timeout

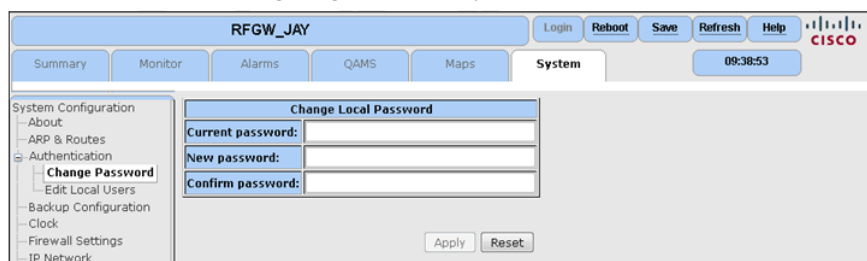
- 1 Navigate to the System/Authentication page.
- 2 Click the dropdown box for Timeout and select the appropriate timeout value.



To Change Default Password

- 1 Navigate to the *System/Authentication* page.
- 2 Click the + sign and select **Change Password**.

Result: The following page is displayed.



- 3 Change your password.
- 4 Click **Apply**.
- 5 Click **Save** on the main menu bar to save your settings.

To Edit Local Users

- 1 Login as admin.
- 2 Navigate to the *System/Authentication* page.
- 3 Click the + sign and select Edit Local Users.

Result: The following page is displayed.

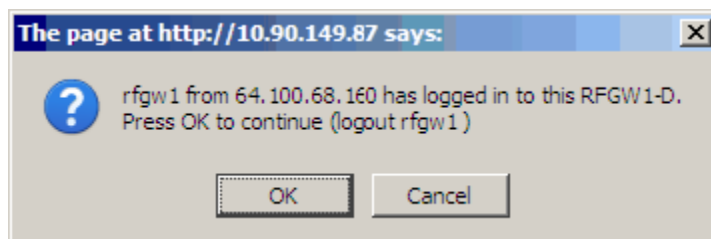


- 4 Select the Login-id to edit.
- 5 Enter the value for Rename login-id to.
- 6 Enter New password and Confirm password.
- 7 Click **Apply**.

Local User Management

- When a user is logged in as "admin" (Local mode), the user can access all configurable RF Gateway 1 web pages and has full read and write access.
- When a user is logged in as "rfgw1", "rfgw2", "rfgw3", "rfgw4" or "rfgw5" (Local mode), the user can access all configurable RF Gateway 1 web pages and has read only access.

- Single user access is supported and a successful login attempt from a different network web client IP address results in terminating the previous session, allowing one RF Gateway user at a time. The following message provides a warning before this action is taken.



Remote Authentication

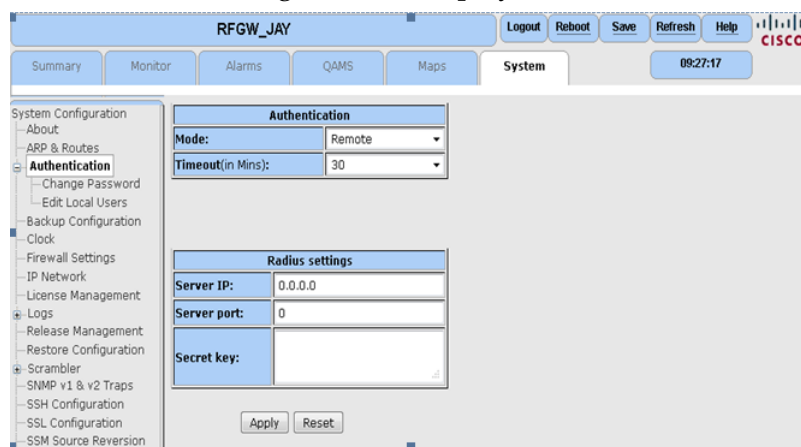
Multiple-user authentication is provided using the RADIUS protocol for network authentication. A RADIUS server needs to be accessible on the RF Gateway 1 management network for multiple user authentications. Standard RADIUS servers are readily available. For example, WinRadius and FreeRADIUS.

To Setup Remote Authentication

Follow the instructions below to setup remote authentication.

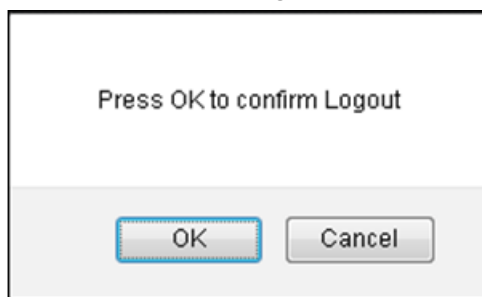
- Navigate to the *System/Authentication* page.
- In the *Mode* drop-down box, select **Remote**.

Result: The following screen is displayed.

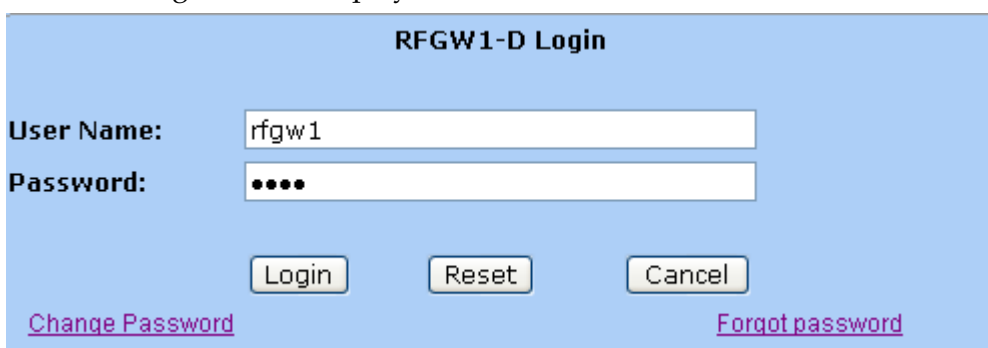


- Enter *Server IP*, *Server port* and *Secret key*.
- Click **Apply**.
- Click **Save** on the main menu bar to save your settings.
- Click **Logout** on the main menu bar.

Result: The following window is displayed.



- 7 Click **OK**.
 - 8 Click **Login** on the main menu bar.
- The following screen is displayed.



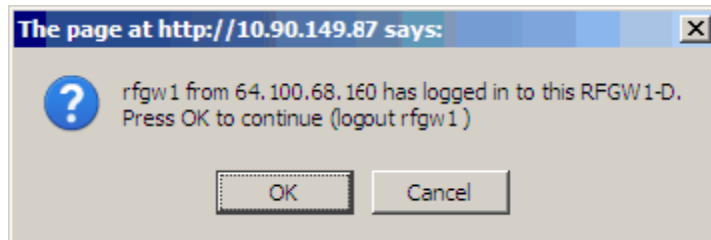
- 9 Enter *User Name* and *Password* provisioned on the RADIUS server.

Remote User Management

- When logged in as "rfgw1" or any RADIUS user (in *Remote* mode), the user can access all configurable RF Gateway 1 web pages.
- In the Radius users configuration file in RADIUS server, set the cisco-avpair as cisco-avpair = "shell:priv-lvl=15" in order to allow read-write access of the RFGW1 web pages for that Radius user.
- Operators can configure the default user ID ("rfgw1") as a Local and/or RADIUS user. The RF Gateway 1 uses one or the other for its authentication credentials.
- Operators use their RADIUS server interface to setup and change RADIUS based users and passwords.
- Local password capability is also enabled in *Remote* (multi-user) mode. Hence, the Local user and its password are still valid. For this reason, it is essential to change the factory default password as soon as possible. Also, while in *Remote* mode, System/Authentication/Change Password feature can be used to change a *Local* user password only. The RF Gateway 1 operator must use the RADIUS server interface to make changes to its remote user credentials. This cannot be performed using the RF Gateway 1 management interface.
- If remote authentication does not succeed using the user credentials entered,

then local authentication will be tried with the same user credential details entered.

- Single read-write user access is supported and a successful login attempt from a different network web client IP address results in terminating the previous session, allowing one user at a time to be logged in and make changes. The following message box provides a warning before action is taken.



Password Recovery

A password reset and recovery feature is available using the RF Gateway 1 front panel.

To Reset the Default Password

- 1 On the front panel, press the **LEFT & UP** buttons together.
- 2 On the front panel, press the **LEFT & DOWN** buttons together.

Result: The following screen is displayed.



- 3 Select **Yes**.

Note: This procedure resets the default password to *1111*. To change your password, refer to *To Change Default Password* (on page 205).

Enabling HTTPS on the RF Gateway 1

Steps for Enabling HTTPS

The following steps for enabling HTTPS are explained in detail in the following sections.

- Create a CA
- Create a unique key and CSR for each RF Gateway 1 unit required to support HTTPS
- Sign each CSR with the CA
- Download each key and certificate from the FTP server to each RF Gateway 1 unit
- Import the CA certificate into each browser that you plan to use with your RF Gateway 1 unit

In the following steps, the command prompt is shown in italics, the user input is shown in bold, and the computer response is shown in normal typeface.

Creating a CA Certificate

Create a CA certificate named ca.crt:

```
OpenSSL> req -new -x509 -days 365 -key ca.key -out ca.crt
```

Enter pass phrase for ca.key:

Loading 'screen' into random state - done

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:Kentucky

Locality Name (eg, city) []:LaRue

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Sinking Spring Farm

Organizational Unit Name (eg, section) []:Log Cabin

Common Name (eg, YOUR name) []:Abraham

Email Address []:honest@abe.com

OpenSSL>

Creating a Server Key

Create a server.key and an unprotected server key name server.pem.

Server.pem, which you'll create below, is not password protected. Guard it well because it contains your private RSA key in the clear for all to see.

OpenSSL> genrsa -des3 -out server.key 4096

Loading 'screen' into random state - done

Generating RSA private key, 4096 bit long modulus

.....

.....

.....++

.....++

e is 65537 (0x10001)

Enter pass phrase for server.key:

Verifying - Enter pass phrase for server.key:

OpenSSL> rsa -in server.key -out server.pem

Enter pass phrase for server.key:

writing RSA key

OpenSSL>

Creating a CSR

Create a Certificate Signing Request named server.csr:

Recall that when using HTTPS, your browser requires that the site name match the Common Name on the certificate. Therefore you must use the IP Address of the RFGW-1 as the certificate Common Name below.

OpenSSL> req -new -key server.key -out server.csr

Enter pass phrase for server.key:

Chapter 14 Security Features

Loading 'screen' into random state - done

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:Indiana

Locality Name (eg, city) []:West Lafayette

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Purdue University

Organizational Unit Name (eg, section) []:Delta Chi Fraternity

Common Name (eg, YOUR name) []:10.90.149.80

Email Address []:amelia@purdue.edu

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:

An optional company name []:Boilermakers Inc.

OpenSSL>

Sign the CSR

Sign the Certificate Signing Request with the self-created CA made earlier and name it public.crt: Browsers such as Firefox are very picky about serial numbers and check for duplicates. Serial numbers must be unique for each signing.

```
OpenSSL> x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out public.crt
```

Loading 'screen' into random state - done

Signature ok

```
subject=/C=US/ST=Indiana/L=West Lafayette/O=Purdue University/OU=Delta Chi Frate
```


munity/CN=10.90.149.80/emailAddress=amelia@purdue.edu

Getting CA Private Key

Enter pass phrase for ca.key:

OpenSSL>

Downloading Key and Certificate Files to the RF Gateway 1

The SSL Configuration menu is used to set the FTP server IP address, user name, and password. It is also used to set the path to the key and certificate file and the key and certificate filename. The Server Key(server.pem) must not be password protected.

Follow the instructions below to configure the SSL settings.

- 1 Navigate to the System/SSL Configuration page.

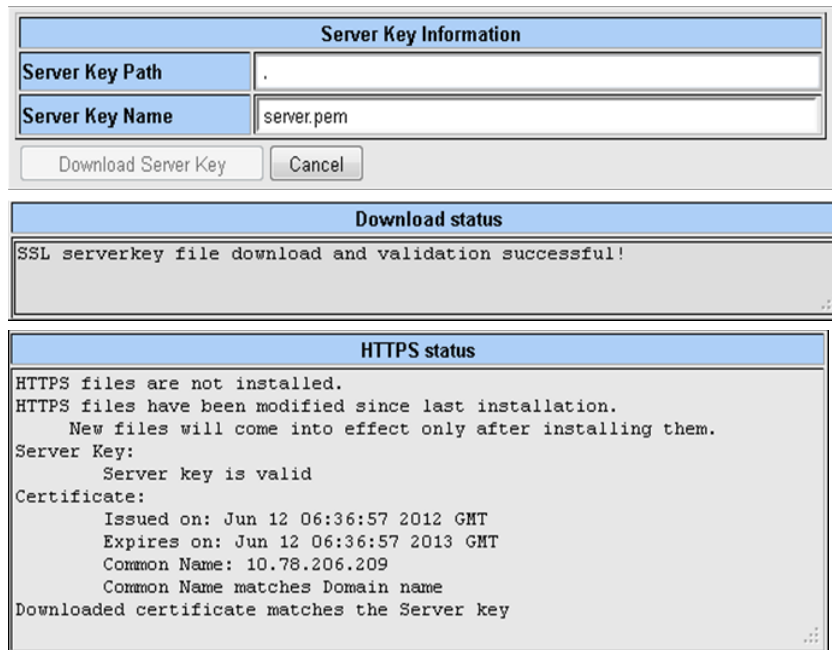
Result: The following screen is displayed.

- 2 In the Server Key Information box, enter the Server Key Path and Server Key Name.

Note: It is recommended that the Server Key be named "server.pem".

- 3 Click Download Server Key.

Result: The following details can be noted.

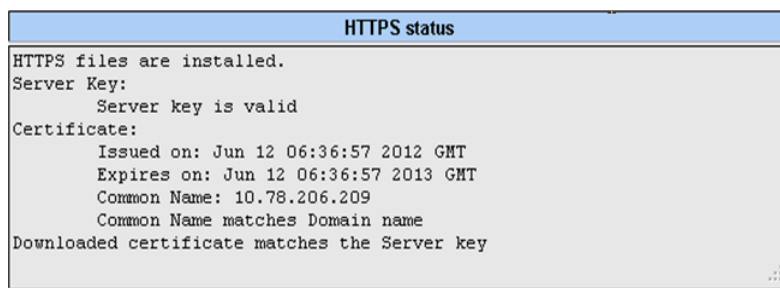
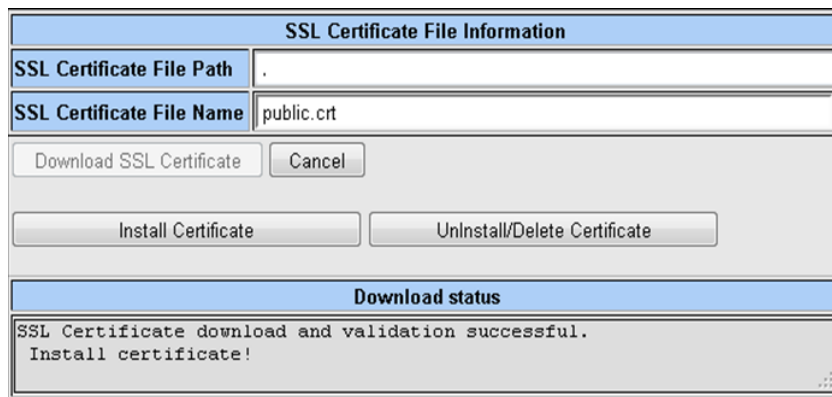


- 4 In the SSL Certificate File Information box, enter SSL Certificate File Path and the SSL Certificate File Name.

Note: It is recommended that the file be named "public.crt".

- 5 Click Download SSL Certificate.

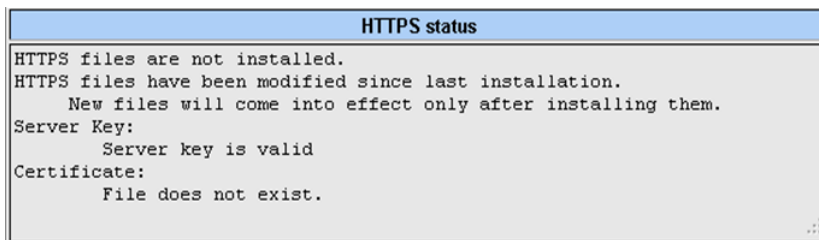
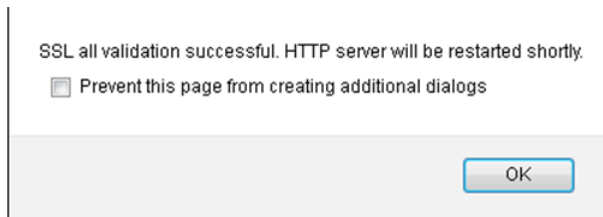
Result: The status window indicates whether the files are valid or invalid.



- 6 Once the files are validated, click Install Certificate to restart the server.

Result: After a few seconds, firewall permitting, the server responds to both HTTP and HTTPS requests.

Note: Invalid files are automatically deleted.



7 Click **UnInstall/Delete Certificate** to disable HTTPS.

Result: The key and certificate files are deleted and the web server restarts.

Importing the CA Certificate

Follow the instructions below to import the CA certificate into Firefox.

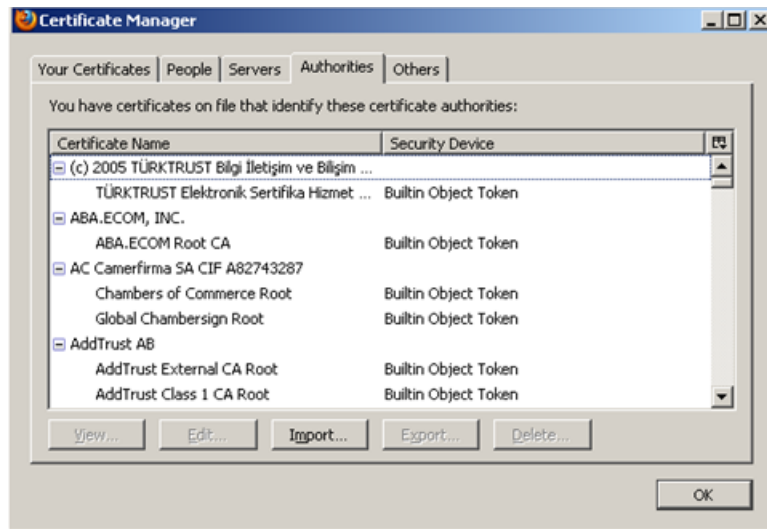
1 Launch Firefox.

Result: The following screen is displayed.



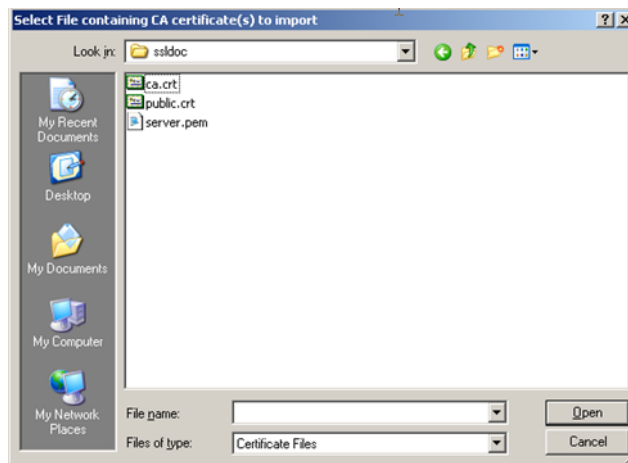
- 2 Click Tools - Options - Advanced - Encryption - View Certificates - Authorities.

Result: The following screen is displayed.



- 3 Click **Import**.

Result: The following screen is displayed.



- 4 Search for and select your ca.crt file.

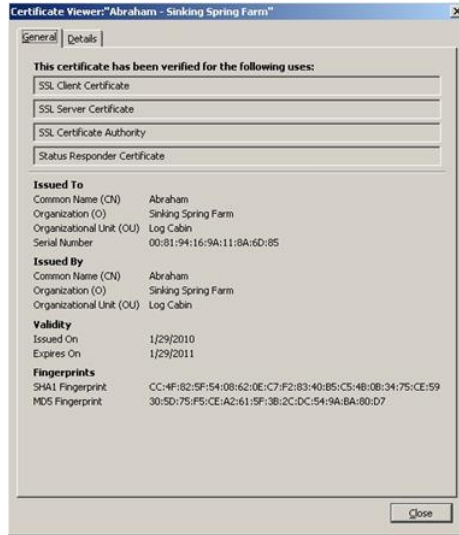
- 5 Click **Open**.

Result: The following screen is displayed.



- 6 Check the Trust this CA to identify web sites box.
- 7 Click **View** to examine your CA certificate.

Result: The following screen is displayed.



SFTP Support

For SFTP client and server, SSHv2 with DSA key is used as the security protocol. SFTP client and server will be operational only after the DSA key is downloaded and installed (firewall permitting for SFTP server) and provided the transfer mode is set to SFTP (for SFTP client).

Note: By default, the firewall for FTP and SFTP is enabled and the default file transfer method is set to FTP

GUI Changes for SFTP

The following GUI changes have been added for SFTP support.

System Tab Changes

- 1 System Configuration page now includes an option to select FTP or SFTP for file download/upload.
- 2 Firewall Settings now include an option to enable/disable the SFTP port.
- 3 SSH Configuration page has been added to provide access to the new security features. See screen below.

Device Information	
Device Description	Cisco RFGW-1-D Universal Edge QAM
Device Up Time	3 Days, 13 Hours, 19 Minutes, 31 Seconds
Device Name	RFGW_JAY
Device Contact	Cisco Support
Device Location	here
QAM Encoding Type	ITU-B
Frequency Plan	Standard
Gratuitous ARP State	Enabled
Gratuitous ARP Time	60 seconds
Dejitte Buffer Depth	150 milliseconds
Network PID	8188
Insert Network PID reference in PAT	Enabled

Generating a DSA Key

Overview

The RFGW-1 is shipped from the factory with SFTP disabled. To enable SFTP, you will need the following:

- FTP server to download the required DSA key

- Open Source toolkit for SSH to generate the DSA key
- Software containing SSH/SFTP kernel support such as 2.6.x or 6.1.x.

Important: It is recommended that you consult your IT and security departments before installing on live RFGW-1 systems. The key files you'll be creating contain a private key and must be handled in accordance with your company's security procedures, especially the unprotected key known as `dsa_key.pem`.

Creating an Unprotected DSA Key:

The `dsa_key.pem` is not password protected. It contains your private DSA key in the open for all to see. Generating a DSA key requires an openssh shell (Cygwin is used in our example). Follow the instructions below to create a DSA key.

- 1 Enter the following command at the shell prompt:

`ssh-keygen -t dsa` (the "-t" flag is used to specify the key type).

Result: You will be prompted for the location to save the file. The default location is `~/.ssh/id_dsa`.

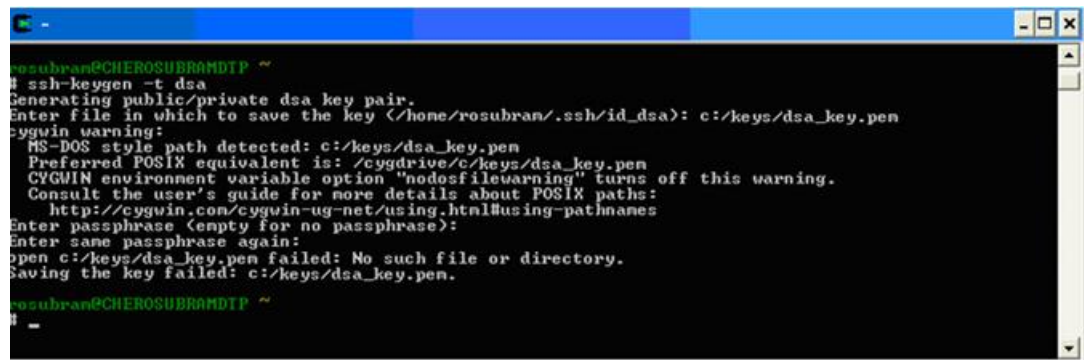
- 2 Click **Enter** to save the file to the default location, or specify a different location.

Result: You will then be prompted for a passphrase.

- 3 Click **Enter** twice to generate an unprotected file.

Result: The following 2 files are created:

- `dsa_key.pem` - the private key (to be downloaded to the RFGW-1)
- `dsa_key.pem.pub` - the public key (may be downloaded to the server)



```

rosubran@CHEROSUBRANDTP ~
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/rosubran/.ssh/id_dsa): c:/keys/dsa_key.pem
cygwin warning:
MS-DOS style path detected: c:/keys/dsa_key.pem
Preferred POSIX equivalent is: /cygdrive/c/keys/dsa_key.pem
CYGWIN environment variable option "nodosfilewarning" turns off this warning.
Consult the user's guide for more details about POSIX paths:
  http://cygwin.com/cygwin-ug-net/using.html#using-pathnames
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
open c:/keys/dsa_key.pem failed: No such file or directory.
Saving the key failed: c:/keys/dsa_key.pem.

rosubran@CHEROSUBRANDTP ~
#

```

Note: You can specify the filename on the command line by inserting an "-f". This flag forces the path for storing the key file. See example below.

```
ssh-keygen -t dsa -f /path/to/my_dsa
```

Installing SFTP

By default, SFTP is disabled and FTP is used as the default file transfer method.

Follow the steps below to enable and configure SFTP.

Chapter 14 Security Features

Step 1:

- Download DSA Key to RFGW-1
- Navigate to the System/SSH Configuration page. Set the FTP Server IP Address, User Name, and Password. You can also enter the DSA Key Path and DSA Key Name for downloading the DSA key file. The key file must not be password protected.
- Once all the parameters have been set, click Download DSA Key to download and validate the files.

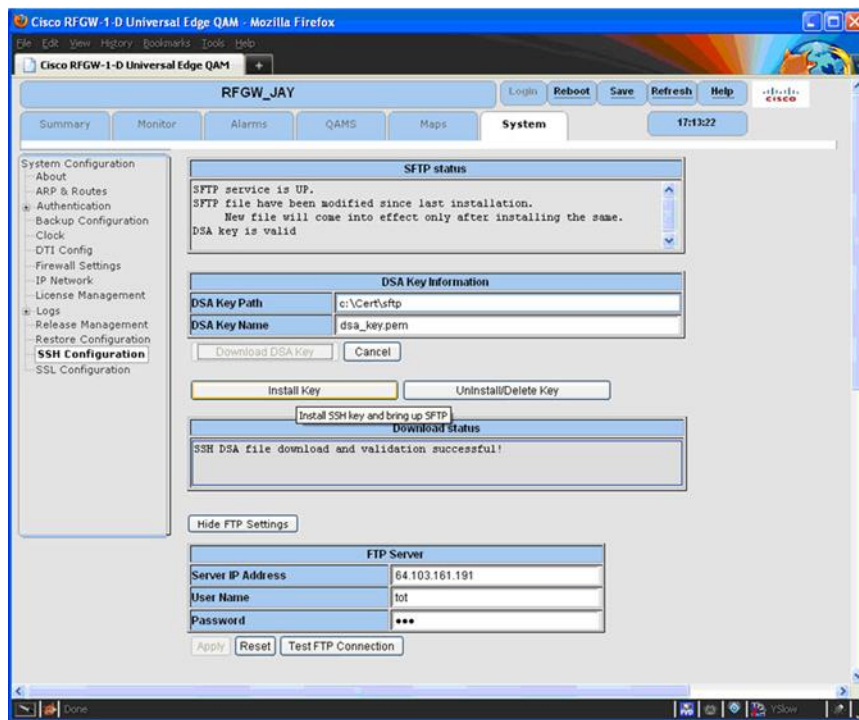
Result: The status window indicates whether the download and validation was successful.

Step 2: Install SFTP in RFGW-1

- Once the files are validated, click Install Key to install the files. Invalid key files are automatically deleted.

Results:

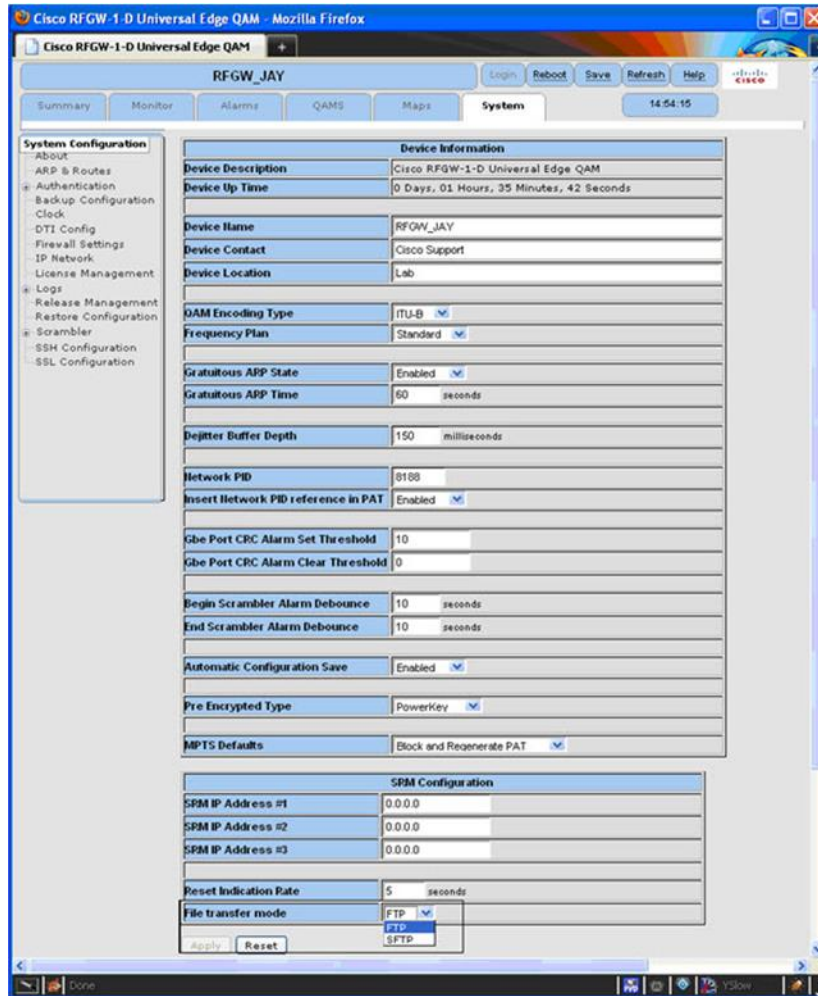
- SFTP Server: Once the key is installed (firewall for SFTP port must be set to enable), the RFGW-1 responds to both SFTP and FTP requests.
- SFTP client: Once the key is installed (file transfer mode must be set to SFTP), all further download/upload operations (such as release, license download, configuration backup, etc.) are done using SFTP.



Step 3: Select SFTP as File Transfer mode

- The user can switch between FTP and SFTP client for file transfer.

Note: When the SFTP is selected as the file transfer mode, before downloading and installing the DSA key, a message appears indicating that the configuration will not be allowed.



Uninstalling SFTP

To uninstall SFTP, follow the step below.

Step 1: Uninstall SFTP in RFGW-1

On the SSH Configuration page, click Uninstall.

Results:

The key is deleted

All existing SFTP connections are closed

Chapter 14 Security Features

SFTP server and client are disabled

Note: The File transfer method remains unaltered. If set to SFTP, change to FTP manually.

Firewall Settings

The various ports can be enabled/disabled using the following screen.

Firewall Settings	
FTP Port	Enabled
SFTP Port	Enabled
HTTP Port	Enabled
HTTPS Port	Enabled
Telnet Port	Enabled

Apply Reset

Notes:

- HTTP port cannot be disabled when HTTPS port is disabled.
- HTTPS port cannot be disabled when HTTP port is disabled

15

96 QAM Channel Software

The Cisco RF Gateway 1 Chassis supports 96-QAM channel software upgradeability with no changes to its existing hardware configuration. Users considering this mode of operation continue to receive full support of all features and backward compatibility as with the 48-QAM channel operation.

In This Chapter

■ Licensing	226
■ Release Management.....	227
■ Configuration Management	229
■ Operational Considerations	230
■ Network Management	235

Licensing

The RF Gateway 1 can be licensed for 96-QAM channel support by applying a license that can be procured using the procedures detailed in *Chapter 8: Licensing* (see "Licensing" on page 155).

When the user successfully applies a 96-QAM channel license, the license information is displayed under the System/License Management menu.

The screenshot shows the Cisco configuration interface for device **rfgw1**. The **System** menu is selected, and the **License Management** option is highlighted in the left-hand navigation pane. The **Device Host ID** is **00000006311020**.

The **License Overview** table displays the following information:

Type	Installed	Count	Usage	Expiration Date	Remaining Time	Expired	Key
DATA	Yes	1	0	00-000-0000	0	No	7E4164E829C42CD5AFEF8EE0CC9A1EA4
DVB_SCRAMBLING	Yes	1	1	00-000-0000	0	No	80FC99759BF5FB00E43BAB4C7B06F2F
8_CHANNELS_PER_PORT	Yes	1	1	00-000-0000	0	No	6525539400A24111EFB92CA9F518D5E2

Below the table is the **License File Information** section, which includes input fields for **License File Path** and **License File Name**, and **Download License** and **Cancel** buttons.

A reboot is necessary after applying the 96-QAM channel license to activate the license. Users can verify the application of a valid license by viewing the **8_CHANNELS_PER_PORT** license entry as displayed above. Currently, software release V03.00.XX and above support the 96-QAM channel license.

Release Management

Installation of the 96-QAM channel aware releases V03.00.XX and above follow the same guidelines and procedures outlined in *Chapter 3: General Configuration and Monitoring* (see "General Configuration and Monitoring" on page 25).

Upgrades

Simply applying a 96-QAM channel license to a RF Gateway 1 release that is not capable of 96-Channel operation (in other words, less than V03.00.XX) will have no effect on the operation of that chassis. The license will become active when a 96-QAM channel software release (V03.00.XX and above) is used to upgrade the chassis.

Conversely, upgrading the RF Gateway 1 to V03.00.XX and above without a 96-QAM channel license allows the RF Gateway 1 user to continue to operate in the existing mode (48-QAM channel) without any changes to the chassis configurations or settings.

The Summary page clearly identifies all unlicensed channels as greyed-out. The following graphics illustrate the absence (and presence) of the 96-QAM channel license.

Non-licensed 96-QAM channels on the RF Gateway 1 Summary page appear as follows:

		Output Bandwidth							
Card	Port	Ch:1	Ch:2	Ch:3	Ch:4	Ch:5	Ch:6	Ch:7	Ch:8
1	1	11.1358 (28%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
2	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
3	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
4	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
5	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
6	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)	0.0000 (0%)

Chapter 15 96 QAM Channel Software

Fully licensed 96 QAM channels on the RF Gateway-1 Summary page appear as follows:

rfgw-1d									Login	Reboot	Save	Refresh	Help	
Summary	Monitor	Alarms	QAMS	Maps	System						08:57:24			
Card	Port	Output Bandwidth												
		Ch:1	Ch:2	Ch:3	Ch:4	Ch:5	Ch:6	Ch:7	Ch:8					
1	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
2	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
3	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
4	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
5	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
6	1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					
	2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)					

Revert

A RF Gateway 1 user can exercise the Revert capability to switch from the 96-QAM channel aware V03.00.XX release to V01.03.XX, V02.02.XX release branches.

Configuration Management

Configuration management of the 96-QAM channel aware releases, for example, V03.00.XX and above, follow the guidelines and procedures outlined in *Chapter 3: General Configuration and Monitoring* (see "*General Configuration and Monitoring*" on page 25).

Backup

No additional information or procedures are needed to perform 96-QAM channel backups offline. As before, frequent backups are highly recommended for all operators.

Restore

Performing configuration database restoration of 48-QAM channel chassis at the 96-QAM channel capable V03.00.XX and above is allowed. RF Gateway 1 software V01.03.XX, and V02.02.XX release branch configuration databases are backward compatible and tested with the 96 QAM-Channel aware V03.00.XX release.

Operational Considerations

Operating in 96-QAM channel mode provides an increased capacity with no additional hardware or operational costs. Users will be provided with new power level ranges and two combined channel banks capable of up to Quad channels configured per RF port available.

QAM Configuration

All 96 QAM channels are configurable from the *QAMS/QAM Configuration* sub menus. Two sets of four combined channels are now available.

Note: Channels 1 and 5 (QAM channel center frequencies) are configurable by the user. Carrier frequencies within one RF port must not overlap.

Important: Port control will turn **On** or **Off** an entire RF port (physical F-connector). If a user intends to turn off only a group of four channels, an additional option "None" under combined channels has been provided for that function. As always, individual channels may be muted using the individual channel controls.

Global QAM Configuration Example

RF Port	Spacing (MHz)	Modulation	Output Level (dBmV)	Symbol Rate (MS/s)	Port Control	Combined Channels	Channel Center Frequency (MHz)			
							Ch1 Ch5	Ch2 Ch6	Ch3 Ch7	Ch4 Ch8
1/1	6	QAM 256	50.0	5.361	On	Quad	345.000	351.000	357.000	363.000
						Quad	405.000	411.000	417.000	423.000
1/2	6	QAM 256	50	5.361	On	Quad	369.000	375.000	381.000	387.000
2/1	6	QAM 256	50	5.361	Off	None				
						None				

RF Port Sub-Menu Example

QAM Configuration

- Card 1
 - RF Port 1/1
 - Channel 1/1.1
 - Channel 1/1.2
 - Channel 1/1.3
 - Channel 1/1.4
 - Channel 1/1.5
 - Channel 1/1.6
 - Channel 1/1.7
 - Channel 1/1.8
 - RF Port 1/2
- Card 2
- Card 3
- Card 4
- Card 5
- Card 6

RF Port Configuration

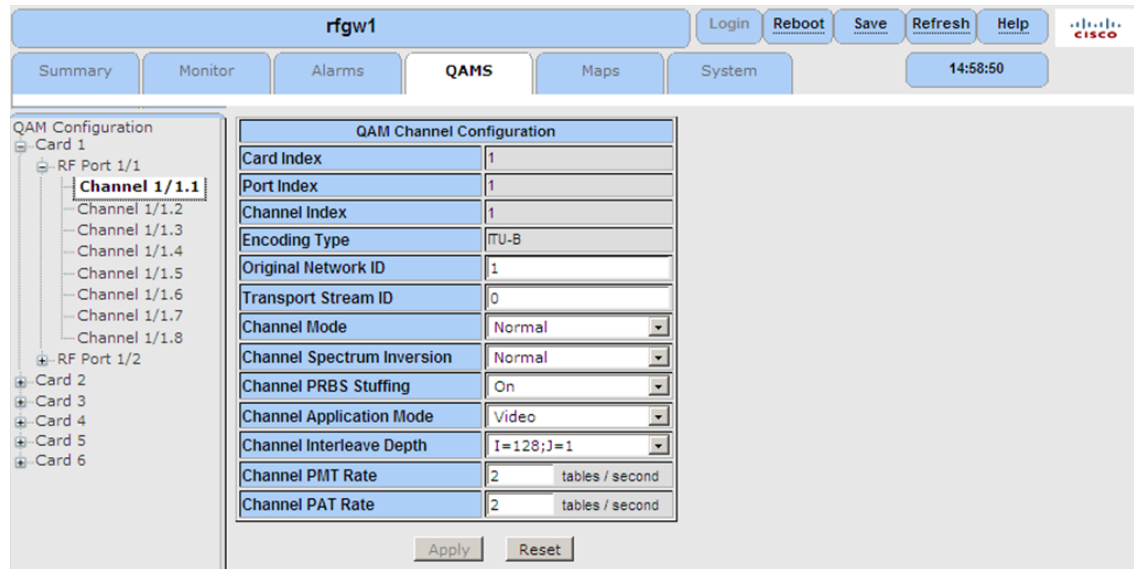
Card Index	1
Port Index	1
Encoding Type	ITU-B
Service Group ID	0
Channel Spacing (MHz)	6
Modulation	QAM 256
Channel Output Level (dBmV)	50.0
Channel Symbol Rate (MS/s)	5.361
Port Control	On
Combined Channels	Quad
Channel Center Frequency (MHz)	345.00C 351.00C 357.00C 363.00C 405.00C 411.00C 417.00C 423.00C

Apply Reset

RF Port output power ranges are based on the total number of combined channels selected by the user. Refer to the table below.

Combined Channels	Range
1	52-62
2	48-58
3	46-56
4	44-54
5	43-53
6	42-52
7	41-52
8	41-52

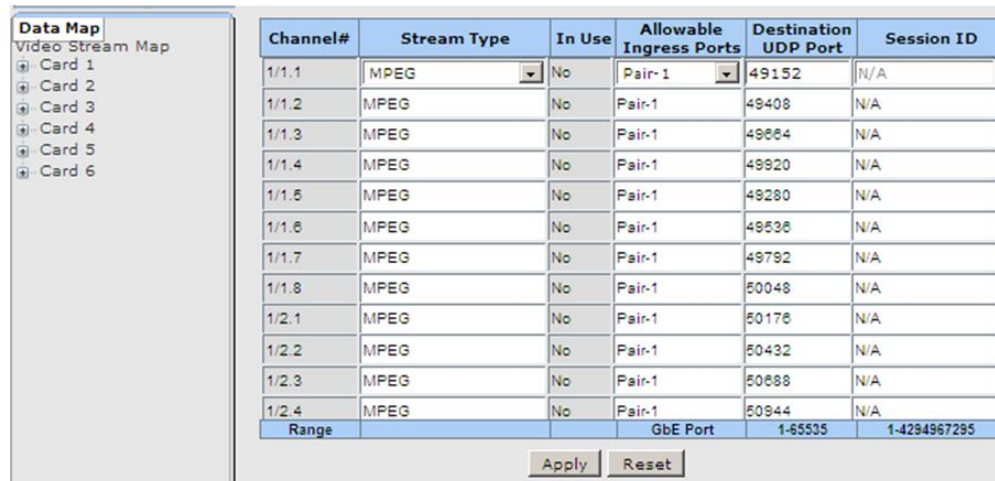
Channel Configuration sub-menu Example



Map Configuration

The RF Gateway 1 Map editor now allows the user to provision the additional available channels for services. Video and Data map entry in the 96-QAM channel capable V03.00.XX and above releases is shown below. Selecting a particular map row allows the user to view the appropriate pull-down menus and data fields. The same principle is applied to Video stream map Advanced Settings. Base and Advanced Rules for map manipulation are described in *Chapter 4: Table-Based Video Specific Operation* (see "Table-Based Video Specific Operation" on page 83).

Data Map Editor



Video Stream Map Editor

Data Map

Video Stream Map

- Card 1
- Card 2
- Card 3
- Card 4
- Card 5
- Card 6

Stream Map Table

Row #	Output QAM Channel	Destination IP Address	UDP Port	Active	Allowed Ingress Ports	Stream Type	Program Number		PMV	Data Rate (kbps)
							Input	Output		
0	1/1.1	0.0.0.0	49156	True	Pair-1	SPTS	0	2	2	0
1	1/1.1	0.0.0.0	49158	True	Pair-1	SPTS	0	3	3	0
2	1/1.1	0.0.0.0	49160	True	Pair-1	SPTS	0	4	4	0
3	1/1.1	0.0.0.0	49162	True	Pair-1	SPTS	0	5	5	0
4	1/1.1	0.0.0.0	49164	True	Pair-1	SPTS	0	6	6	0
5	1/1.1	0.0.0.0	49166	True	Pair-1	SPTS	0	7	7	0
6	1/1.1	0.0.0.0	49168	True	Pair-1	SPTS	0	8	8	0
7	1/1.1	0.0.0.0	49170	True	Pair-1	SPTS	0	9	9	0
8	1/1.1	0.0.0.0	49172	True	Pair-1	SPTS	0	10	10	0
9	1/1.1	0.0.0.0	49174	True	Pair-1	SPTS	0	11	11	0
10	1/1.1	0.0.0.0	49176	True	Pair-1	SPTS	0	12	12	0

Video Map Advanced Settings

Advanced Settings

Row #	Source IP Address				Ignore UDP Port	PCR PID Select	MPTS Dejitter		Blocked PIDs
	Primary	Secondary	Tertiary	Quaternary			Mode	Ref	
0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
3	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
4	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
5	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
6	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
7	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
8	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
9	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
10	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1

Monitoring

The RF Port output monitoring now includes the ability to monitor all 8 outputs per RF port.

The screenshot shows the Cisco NMS interface for a device named 'rfgw-1d'. The top navigation bar includes buttons for 'Login', 'Reboot', 'Save', 'Refresh', and 'Help', along with the Cisco logo and a clock showing '01:52:42'. The main content area is titled 'RFGW-1 Output Sessions' and features a table with the following data:

Session ID	Type	Output QAM Channel	Output Bitrate (Mbps)	Status	GbE Port	Destination IP Address	UDP Port	Output			Input
								Program Number	PMT PID	PCR PID	
Video Map Session	SPTS	1/1.1	9.8877	Bound	1	10.1.1.29	49174	11	192	193	Details

The left navigation tree shows a hierarchy starting with 'Main', followed by 'Device Information', 'Input', 'Inventory', 'Output', 'Card 1', 'RF Port 1/1', and 'Channel 1/1.1' (which is selected). Other channels listed include 1/1.2 through 1/1.8, 'RF Port 1/2', 'Card 2' through 'Card 6', 'Data', 'DTI', and 'Resource Utilization'.

Network Management

Operating in the 96-QAM channel mode provides SNMP monitoring and management as in the 48-channel mode. The following proprietary MIBs are now fully 96 QAM-channel compatible:

- 1 CISCO-RFGW-1-MIB.my
- 2 CISCO-RFGW-1-MIB.Support
- 3 CISCO-RFGW-1-OLS-MIB.mib
- 4 CISCO-RFGW-1-PROD-MIB.mib
- 5 CISCO-RFGW-1-SCRAMBLING-MIB.mib
- 6 CISCO-RFGW-1-TRAP-MIB.mib

16

NGOD Specific Operation

This chapter provides information for provisioning the RF Gateway 1 for NGOD operation. The reader is assumed to have knowledge of the NGOD protocol.

In This Chapter

■ Provisioning.....	238
■ Status Monitoring	241
■ Troubleshooting.....	242
■ Logs.....	243

Provisioning

This section provides information for provisioning the RF Gateway 1 for NGOD operation.

Prerequisite configurations:

- GbE input ports, including Video/Data IP address
- QAM outputs
- Channel Application Mode

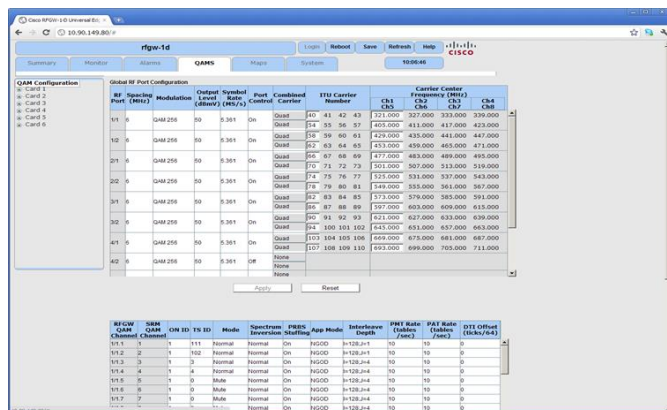
Channel Application Mode

To Verify Channel Application Mode

Navigate to the Qams page.

- 1 Select the QAM channels and set the App Mode to NGOD.
- 2 Set the TSID appropriately

Result: App Mode is displayed for each output carrier.



NGOD Settings

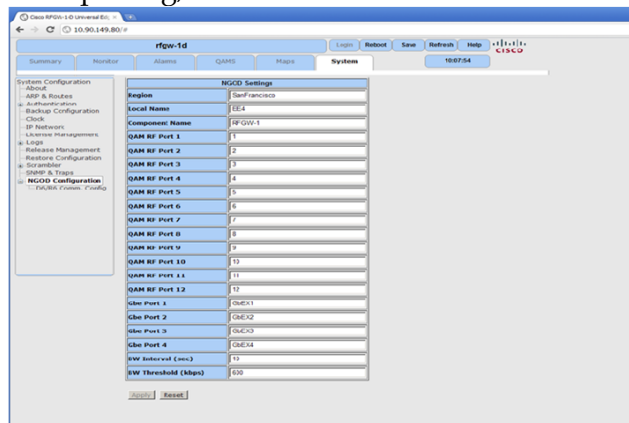
Navigate to the System tab and from there to the NGOD configuration on the left hand side of the tab.

RFGW-1 is Configured with the following NGOD Settings

- VREP Version – This should be set to 2.
- Region Name – This is the Region Name that this RFGW-1 belongs to.

Local Name – This is the local name of the RFGW-1. When the region and local name is appended together, this identifies the RFGW-1 location.

- Component Name
- Local – Region Name and Local Name Component Name – The Name of the RFGW-1
- QAM RF Port 1-12 names - These are used to advertise the QAM Ports to the ERM
Names of the GigE ports
- Bw Interval and Bw Threshold The RFGW-1 checks every QAM to see if during a Bw Interval, there was a change in the bandwidth that is equal to or greater than the Threshold. This is used by the ERM to maintain Bandwidth. To disable the reporting, one should set the Bw Interval to 0.



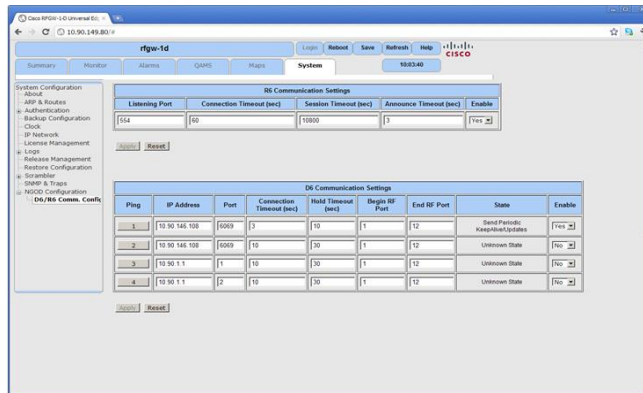
D6/R6 Communication

Provide the information of the ERM and the ports that they are listening on

- 1 Navigate to the System Tab.
- 2 Select D6/R6 Comm. Config under the NGOD configuration menu.
- 3 Setup ERM IP Address, Port, Timeouts, R6 Listening Port etc.
 - a IP Address and Port – ERM IP Address and Port. Up to 4 different ERMs can be configured with one RFGW-1
 - b Connection Timeout – Time out in secs to accommodate network delays
 - c Hold Time out – Keep Alive messages are sent 3 times during a Hold time and no faster than once every 3 seconds
 - d BEGIN and END RF ports – These are the port numbers/QAM channels that the ERM can configure
 - e State – Read only Field – Provides the current state information of the RFGW-1
 - f Listening Port – R6 Listening Port. This is the port where the RFGW is listening for R6 messages.

Chapter 16 NGOD Specific Operation

- g Connection Time out – This is how long the RFGW-1 waits for an R6 message before resetting the connection.
- h Session Time out – This is how long a session is kept alive by the RFGW-1 without receiving a R6 session refresh (Ping) from the ERM
- i Announce Time out – This is how long the RFGW-1 waits before resending an Announce Message.



Status Monitoring

Status monitoring of the R6/D6 messages between the ERM and the RFGW-1 is shown on the Monitor tab of the RFGW-1.

The types of messages and the protocol are shown in the tab. The IP Address in the first column is the address of the ERM and the number with a dash represents the time the connection has been on. For e.g. in the figure below 10.90.146.108 ERM has been in the connected state for the last 4555 minutes.

The screenshot shows the 'Monitor' tab of the RFGW-1 interface. It displays two tables of connection data. The top table is titled 'R6 IP Addresses, Connection Duration (minutes) and Packet Counts' and the bottom table is titled 'D6 IP Addresses, Connection Duration (minutes) and Packet Counts'. Both tables have columns for IP Address / Duration (minutes), Dir, Open, Update, Keepalive, Notification, and Unknown.

R6 IP Addresses, Connection Duration (minutes) and Packet Counts						
IP Address / Duration (minutes)	Dir	Open	Update	Keepalive	Notification	Unknown
10.90.146.108 -3	Rx	1	0	51	0	0
10.90.146.108 -3	Tx	1	204	49	0	0
-0	Rx	0	0	0	0	0
-0	Tx	0	0	0	0	0
-0	Rx	0	0	0	0	0
-0	Tx	0	0	0	0	0
-0	Rx	0	0	0	0	0
-0	Tx	0	0	0	0	0

D6 IP Addresses, Connection Duration (minutes) and Packet Counts						
IP Address / Duration (minutes)	Dir	Setup	Forward	Get Params	Ping	Options
10.90.146.108 -4555	Rx	249	0	2	18000	5311
10.90.146.108 -4555	Tx	0	0	0	0	0
-0	Rx	0	0	0	0	0
-0	Tx	0	0	0	0	0
-0	Rx	0	0	0	0	0
-0	Tx	0	0	0	0	0
-0	Rx	0	0	0	0	0
-0	Tx	0	0	0	0	0

NGOD LOG Messages

Under the System tab, System Configuration menu and Log submenu, Logs Configuration can be set. NGOD Manager logs can be set to different levels. When selecting the Logs submenu, you can see the logs from the NGOD module. The logs can be used to troubleshoot NGOD issues.

The screenshot shows the 'System Logs' tab of the RFGW-1 interface. It displays a table of log entries with columns for Time, Source, and Description. The logs are filtered by 'All Logs' and show a list of events from the NGOD module.

Time	Source	Description
25 SEP 11 10:17:21.161	NGOD	DE: Record Keepalive IP 10.90.146.108
25 SEP 11 10:17:16.161	NGOD	DE: Record Keepalive IP 10.90.146.108
25 SEP 11 10:17:16.161	NGOD	DE: Send Keepalive IP 10.90.146.108
25 SEP 11 10:17:16.171	NGOD	DR: Update(10.90.146.108) BVI Update Cam 25 TSD:55 Available 9005
25 SEP 11 10:17:16.171	NGOD	DR: Update(10.90.146.108) BVI Update Cam 24 TSD:44 Available 16405
25 SEP 11 10:17:16.171	NGOD	DR: Update(10.90.146.108) BVI Update Cam 19 TSD:38 Available 11062
25 SEP 11 10:17:16.171	NGOD	DR: Update(10.90.146.108) BVI Update Cam 17 TSD:34 Available 9005
25 SEP 11 10:17:16.161	NGOD	DR: Update(10.90.146.108) BVI Update Cam 9 TSD:18 Available 3005
25 SEP 11 10:17:16.161	NGOD	DR: Update(10.90.146.108) BVI Update Cam 8 TSD:17 Available 16405
25 SEP 11 10:17:16.161	NGOD	DR: Update(10.90.146.108) BVI Update Cam 7 TSD:10 Available 9005
25 SEP 11 10:17:16.161	NGOD	DR: Update(10.90.146.108) BVI Update Cam 9 TSD:11 Available 16405
25 SEP 11 10:17:16.161	NGOD	DE: Record Keepalive IP 10.90.146.108
25 SEP 11 10:17:14.161	NGOD	DE: Send Keepalive IP 10.90.146.108
25 SEP 11 10:17:11.161	NGOD	DE: Record Keepalive IP 10.90.146.108
25 SEP 11 10:17:16.161	NGOD	DE: Record Keepalive IP 10.90.146.108
25 SEP 11 10:17:16.161	NGOD	DE: Record Keepalive IP 10.90.146.108
25 SEP 11 10:17:20.161	NGOD	DE: Record Keepalive IP 10.90.146.108
25 SEP 11 10:17:16.161	NGOD	DE: Send Keepalive IP 10.90.146.108
25 SEP 11 10:17:20.161	NGOD	DR: Update(10.90.146.108) BVI Update Cam 28 TSD:51 Available 22980
25 SEP 11 10:17:16.161	NGOD	DR: Update(10.90.146.108) BVI Update Cam 19 TSD:38 Available 11018
25 SEP 11 10:17:20.165	NGOD	DR: Update(10.90.146.108) BVI Update Cam 18 TSD:35 Available 20445

Troubleshooting

- RFGW-1 QAMs are not recognized by the ERM.
- Check the “State” on the D6/R6 comm. Config page. If it is in StartUp/Establish connection state for more than a few minutes, the RFGW-1 is unable to communicate with the ERM. Check the TCP connections between the RFGW-1 and the ERM.
- Check if the Streaming Zone (RegionName.LocalName) is correct. Ensure that the ERM is configured in the same Streaming Zone as the RFGW-1.
- Make sure that QAMs on the RFGW-1 are configured for NGOD and are enabled
- If the RFGW-1 “State” is in Send Periodic Keep Alives then its connected to the ERM and ready
- If it still does not recognize the QAMs, check the RFGW-1 logs.
- RFGW-1 QAMs are recognized by the ERM but no sessions are created
- Check R6 Connection is established at the ERM if there is a provision to do so.
- Check the R6 Listening port and make sure the ERM is requesting a connection on that port.
- Check RFGW-1 logs for any errors during R6 communication.

Logs

- NGOD System logs allow the operator to determine the correct behavior of the RFGW-1. Following is the list of some of the important logs.
- R6[<IP Address of USRM>] Session creation failed: Bad id format:<Passed in ID>
- Session creation from the USRM failed due to bad id provided by the USRM during session creation
- R6[<IP Address of USRM>] Session creation failed: Bad destipaddr
Output:<QAM Id> ProgNo.:<Prog No.> DestIp:<Ip Address> for
ERM:<Resource Manager IP>
- Destination IPAddress used to create the session by the USRM is invalid causing the Session Creation to fail.
- R6[<IP Address of USRM>] Session creation failed: Could not add session
Output: :<QAM Id> ProgNo.: <Prog No.> for ERM: <Resource Manager IP>
- Generic session creation failed message
- R6[<IP Address of USRM>] Session creation failed, TSId not found:
Output:<QAM Id> TsId:<TsId> ERM: <Resource Manager IP>
- TSID specified by the USRM to create a session was invalid.
- R6[<IP Address of USRM>] CreateSession Invalid number of multicast addresses
<Count>
- More than two multicast sources were specified during session creation
- R6[<IP Address of USRM>] CreateSession Invalid dest multicast address. Can not have different dest for multiple mc address. MC Count:<Count>
- Dest multicast addresses were different for each of the multicasts specified.
- R6[<IP Address of USRM>]: <Send Buffer> - Send Failed. Length:<Length of Buf> ReturnVal:<Sent Bytes> Error:<ErrorNum>
- Generic TCP send to the USRM failed. Typically occurs if the network connection is down.
- R6[<IP Address of USRM>]: Teardown failed. Sess not found. Sess:<Sess No>
SessId:<OnDemand SessionId> IP:<Src IP Address>
- Teardown was requested for a session that does not exist.
- R6 Opened a new connection for ERM: [<IP Address of USRM>]
- A new connection the Resource Manager was made.
- R6MsgRecv[<IP Address of USRM>]: %s - Unknown Message ==><Message

Received>

- An unknown message was received from the USRM
- R6[<Worker Num>]: <IP Address of USRM> - Connection Timed out.
Now:<Now Time> LastMsgTime:<Last message time> Timeout:<Connection Time Out>
- No messages were received for a period of time. Last message time received is mentioned in the log. Connection time out is also shown in the log.
- R6[<Worker Num>] Closing connection for ERM:< IP Address of USRM>
- There are 4 worker threads processing the ERM connections for a max of 4 different ERMs. This message indicates that a connection is being closed. Once a worker thread has closed the connection, the worker thread will become available for a new connection.
- R6 GenIPsrvr:Got a new Accept:<Socket Num> from <IP Address>
- A new connection was accepted.
- R6[<IPAddress>] No worker available
- All the 4 worker threads are in use and there are no working threads available to process the connection from the USRM.
- NGOD session timeout reached for sessionID = <Session Id>
- Session Timeout on the session is reached and the session is closed.
- D6State[<ERM Instance>]: ESTABLISH IP:<ERM IpAddress> SZ:<Streaming Zone>
- D6 connection is established. ERM instance number, there are 4 of them.
- D6State[<ERM Instance>]: RECVOPEN IP: <ERM IpAddress>
- Waiting for receiving an OPEN message from the ERM
- D6State[<ERM Instance>]: SENDFIRSTKEEPALIVE IP: <ERM IpAddress>
- Starting to send the First Keep Alive message.
- D6State[<ERM Instance>]: RECVFIRSTKEEPALIVE IP: <ERM IpAddress>
- Sent the first Keep Alive message, waiting to receive the First Keep Alive message
- D6State[<ERM Instance>]: INITUPDATE IP: <ERM IpAddress>
- First update message is being sent to the ERM
- D6State[<ERM Instance>]: ERRORNOTIFICATION IP: <ERM IpAddress>
- There was an error during the message exchange with the ERM

- D6[<ERM Instance>]: Error (sent != tx bytes) errno:<Error Num>
- TCP IP connection failure would cause the sent bytes to not match what was intended to be transmitted.
- D6[<ERM Instance>]: Error receiving errno:<Error Num>
- Error while receiving the data from the ERM.
- D6 Error[<ERM Instance>]: SendOpen Failed
- This means that the RFGW failed to send the OPEN message to the ERM
- D6 Error[<ERM Instance>]: ReceiveOpen Failed
- RFGW did not receive an OPEN message from the ERM
- D6 Error[<ERM Instance>]: Waiting for ReceiveOpen timedout. Hold time expired.
- Receive open was not received from the ERM. Hold timer expired.
- D6 Error[<ERM Instance>]: ReceiveOpen parsing open message Failed
- Parsing the OPEN message that was received from the server failed.
- D6 Error[<ERM Instance>]: SendKeepAlive Failed
- Sending Keep Alive message failed.
- D6 Error[<ERM Instance>]: ReceiveKeepAlive -- Error receiving message
- Error while receiving the Keep Alive message from the ERM
- D6 Error[<ERM Instance>]: ReceiveKeepAlive -- Nothing received
- While waiting for a Keep Alive nothing was received.
- D6 Error[<ERM Instance>]: ReceiveKeepAlive -- HoldTime Expired
- While waiting for a Keep Alive Hold timer expired.
- D6 Error[<ERM Instance>]: SendInitialUpdate -- Send failed
- Sending initial update failed
- D6 QAMUPDATE[<ERM Instance>]: ADD QAM:<QAM Id> Freq: <Freq> Mod <Modulation Mode> TSID <TsId>
- Adding QAMs to the ERM.
- D6[<ERM Instance>] QAMUPDATE: WITHDRAW QAM:<QAM Id> TSID <TsId>
- Removing QAMs from the ERM
- D6Update[<ERM Instance>]: BW Update ERROR Qam:<QAM Id>

Chapter 16 NGOD Specific Operation

- BW updates are sent periodically to the ERM if enabled. This message indicates that there was an error while sending these messages.
- D6[<ERM Instance>]: ERROR no keepAlives (<Keep Alive time>) seen, now holdTime (<Remaining Hold Time>) <= 0 too
- No Keep Alive seen and the Hold time is expired.

17

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

Technical Specifications

About This Appendix

This appendix provides system specifications for the RF Gateway 1.

Note: Technical specifications are subject to change without prior notice.

In This Appendix

- General Specifications 250
- Electrical Specifications..... 252

General Specifications

Introduction

The following table lists the general specifications of the RF Gateway 1 equipment.

Environmental Specifications

Item	Specification
Ambient temperature range	
■ Within specs	0 to 50°C (32 to 122°F)
■ Operation	0 to 50°C (32 to 122°F)
■ Storage	-40 to 70°C (-40 to 158°F)
Operating humidity	5% to 95%, non-condensing

Chassis Mechanical Specifications

Item	Specification
Height	1.75 in. (44.5 mm) (1 RU)
Width	19 in. (482.6 mm)
Depth	21 in. (533.4 mm)
Weight	27.5 lbs (12.5 kg)

Physical

Item	Specification
Dimension	
■ In mm (H x W x D)	44.5 mm x 482.6 mm x 533.4 mm
■ In inch (H x W x D)	1.75" x 19" x 21"
Weight	
■ Fully loaded	12.5 kg (27.5 lbs)
■ Empty housing	6.6 kg (14.5 lbs)

Power Supply Specifications

Item	Specification
Power supply (nominal)	100 - 240 V AC \pm 10% -48 V DC (voltage range -38 to -58 V DC)
Power consumption (nominal)	Typical < 345 Maximum < 410 W

Electrical Specifications

GbE Input Interface

Item	Specification
Number of inputs	2 + 2 (for redundancy)
Connector	Electrical and optical small form factor pluggable (SFP)
Interface type	Gigabit Ethernet according to IEEE 802.3ab (electrical) or IEEE 802.3z (optical)
Data rate	Full line rate
Syntax	VBR and CBR MPEG SPTS and MPTS on UDP (RFC-768), RTP, L2TPv3, IGMPv3
Dejitter Buffering	150 ms

Management Interface

Item	Specification
Interface type	Ethernet 10/100Base-T
Connector	1 x RJ 45
Protocols	HTTP, SNMP, FTP, RPC

DTI Interface

Item	Specification
Interface type	Ethernet 10/100Base-T
Connector	2 x RJ 45 Primary and Redundant

RF Outputs

Item	Specification
Number of outputs	Max. 12 (each with 4 adjacent QAM channels)
Connector	F-type, 75 Ω
Frequency	

Electrical Specifications

■ Range	Channel edges between 45 and 1000 MHz (tunable)
■ Step size	1 kHz
■ Stability	± 3 ppm
■ Accuracy	± 3 ppm
Channel bandwidth	6, 7 or 8 MHz depending on QAM standard
Level	
■ Range	Quad Mode: 54 dBmV RMS Max per QAM channel in 0.1 dB steps Triple Mode: 55 dBm V RMS Max per QAM channel on 0.1 dB steps Dual Mode: 57 dBmV RMS Max per QAM channel in 0.1 dB steps Single Mode: 61 dBmV RMS Max per QAM channel in 0.1 dB steps
■ Stability	± 1 dB
■ Accuracy	± 1 dB
Return loss	> 14 dB 45-750 MHz > 13 dB 750-870 MHz > 12 dB 870-1000 MHz Per DOCSIS 3.0 DRFI specification CM-SP-DRFI-103-060106

Signal Specifications

Item	Specification
Channel encoding	Randomization, Reed-Solomon, Trellis and Interleaving according to ITU-T Annex A, B or C
MER (before equalizer)	≥ 40 dB (at RF)
MER (after equalizer)	≥ 45 dB (at RF)
BER (256 QAM)	≤ 5x10 ⁻⁹ (ITU-A/C pre FEC) ≤ 1x10 ⁻¹³ (ITU-B pre FEC/post trellis)
Bandwidth	6, 7 or 8 MHz (transmission standard depending)
QAM constellation	64 & 256 QAM

Specifications Optical Types SFP Modules

The following table describes the Prisma branded optical type SFP transceivers available.

Part Number	Type	Distance	Wave Length	Mode
4002019	WDM	Up to 500m	850 nm	Multi-mode
4002020	WDM	Up to 5km	1310 nm	Single-mode

The following table describes the Cisco branded optical type SFP transceivers available.

Part Number	Type	Distance	Wave Length	Mode
GLC-SX-MM	WDM	Up to 500m	850 nm	Multi-mode
GLC-LH-SM	WDM	Up to 5km	1310 nm	Single-mode

Electrical GbE SFP Transceiver

The following table describes the Prisma branded electrical GbE SFP transceiver available.

Part Number	Description
4006222	GbE SFP copper

The following table describes the Cisco branded electrical GbE SFP transceiver available.

Part Number	Description
GLC-T	GbE SFP copper

Glossary

ECM

Entitlement Control Messages.

ECMG

Entitlement Control Message Generator.

EIS

Event Information Scheduler.

EMM

Entitlement Management Messages.

ES

Elementary Stream.

FTP

File Transfer Protocol. Allows users to transfer text and binary files to and from a personal computer, list directories on the foreign host, delete and rename files on the foreign host, and perform wildcard transfers between hosts.

GUI

graphical user interface. A program interface that takes advantage of a computer graphics capabilities to make the program visually easier to use.

HTML

Hypertext Markup Language.

HTTP

Hypertext Transfer Protocol.

IP

Internet Protocol. A standard that was originally developed by the United States Department

Glossary

of Defense to support the internetworking of dissimilar computers across a network. IP is perhaps the most important of the protocols on which the Internet is based. It is the standard that describes software that keeps track of the internetwork addresses for different nodes, routes, and outgoing/incoming messages on a network. Some examples of IP applications include email, chat, and web browsers.

IP address

Internet protocol address. A 32-bit sequence of numbers used for routing IP data. Each IP address identifies a specific component on a specific network. The address contains a network address identifier and a host identifier.

ISO

International Organization for Standardization. An international body that defines global standards for electronic and other industries.

PC

personal computer.

QAM

quadrature amplitude modulation. An amplitude and phase modulation technique for representing digital information and transmitting that data with minimal bandwidth. Both phase and amplitude of carrier waves are altered to represent the binary code. By manipulating two factors, more discrete digital states are possible and therefore larger binary schemes can be represented.

RADIUS

Remote Authentication Dial-In User Service. A networking protocol that provides centralized Authentication, Authorization and Accounting (AAA) management for computers to connect and use a network service.

RF

radio frequency. The frequency in the portion of the electromagnetic spectrum that is above the audio frequencies and below the infrared frequencies, used in radio transmission systems.

RMA

return material authorization. A form used to return products.

RPU

Remote Provisioning Utility.

RU

rack unit. RU is the measuring unit of vertical space in a standard equipment rack. One RU equals 1.75" (44.5 mm).

SCG

Scrambling Control Group.

SCS

Simulcrypt Synchronizer.

UDTA

Universal Digital Transport Adapter.

Index

9

96 QAM Channel Software • 225

A

About the SCS Configuration GUI • 183
Access Criteria and Access Rights • 172
Adding an ECMG • 186
Adding an EIS • 198
Adding ECMG Connection Entries • 188
Adding Entries to the Remap Table • 142
Advanced Rules for Advanced Settings • 93
Advanced Settings • 89
Alarm Configuration • 147
Alarm Details • 148
Applications Requiring a Software License • 156
ARP and Route Configuration • 48
Authentication • 203
Authentication Configuration • 203
Automated Video Stream Map Configuration • 87

B

Backup • 229
Basic M-CMTS Data Specific Operation • 113
Blocked Unreferenced PIDS • 143

C

Card Presence • 16
Carrier Parameters • 17
Changing Device Settings • 6
Changing ECMG Parameters • 188
Changing EIS Parameters • 200
Channel Application Mode • 20, 84, 100, 106, 114, 129, 238
Clock Configuration • 49
Complete License Transfer • 166
Configuration Backup • 74
Configuration Management • 74, 229
Configuration Restore • 75
Configuration Save • 74
Configuring Alarm Settings • 148

Configuring Broadcast Scrambling and Dual Encryption Broadcast • 180
Configuring GbE Interface Settings • 42
Configuring GbE Port Operational Mode • 42
Configuring IP Network Settings • 10
Configuring Management Port (10/100) IP Address, Subnet Mask and Default Gateway • 10
Configuring QAM Output • 15
Configuring Redundancy for Port Pair Mode • 45
Configuring Reversion of Multicast Streams to Primary Port • 46
Configuring Scrambling General Settings • 182
Configuring Scrambling Specific Parameters • 183
Configuring Static Routes • 14
Configuring the Annex • 7
Configuring the Clock • 8
Configuring the Device Name • 6
Configuring the IP Address Through the Front Panel • 4
Configuring the Video/Data IP Address for GbE Port Pair Mode • 43
Configuring VOD Parameters • 21
Configuring, Monitoring, and Fault Management via SNMP • 80
Connecting the RF Gateway 1 Using a Web Browser • 5
Connecting to DTI Server • 116
Creating a CA Certificate • 210
Creating a CSR • 211
Creating a Server Key • 211
Customer Information • 247

D

D6/R6 Communication • 239
Data Map Configuration • 106, 114
Data Monitoring • 61
DEPI Feature Highlights • 138
DEPI-Learn • 129
Depi-Remote • 129

Device Information • 56
Downloading Key and Certificate Files to the RF Gateway 1 • 213
Downloading System Release Images • 78
DTI Monitoring • 62

E

ECM • 255
ECMG • 255
ECMG Descriptor Rules • 194
ECMG Parameters • 188
EIS • 255
EIS Parameters • 200
Electrical Specifications • 252
EMM • 255
Enabling HTTPS on the RF Gateway 1 • 210
Enabling Insert External PAT • 144
Enabling QAM Port • 16
Enabling the Feature • 140
Enabling UDTA • 96
Encryption and Scrambling • 169
Entitlement Control Message Generators • 183
Entitlement Control Messages • 173
ES • 255
Event Information Scheduler • 174
Event Information Schedulers • 198

F

Fault Management of the RF Gateway 1 • 65
Feature Design Details • 153
Feature Page • 141
Firewall Settings • 223
FTP • 255

G

GbE Interface Configuration • 35
GbE Interface Operation Modes • 35
General Configuration and Monitoring • 25
General Specifications • 250
Global QAM Channel Configuration • 31
Global RF Port Configuration • 28
GUI • 255
GUI Changes for SFTP • 218
GUI Feature Option • 152

H

HTML • 255
HTTP • 255

I

important safety instructions • ix
Importing the CA Certificate • 215
Ingress All VoD • 21
Input Monitoring • 54
Inserting External PAT • 145
Installing and Activating a License • 161
Installing SFTP • 219
Introduction • 1, 170
Inventory • 57
IP • 255
IP address • 256
ISO • 256

L

Legacy Mode • 101
Licensing • 155, 226
Load Balancing • 183
Local Authentication • 203
Local User Management • 206
Logs • 243

M

Map Configuration • 232
M-CMTS Data DEPI-CP Operation • 127
Monitor Tab • 54
Monitoring • 97, 109, 119, 131, 234
Monitoring the RF Gateway 1 • 53
MPTS Pass-Through Mode of Operation • 95

N

Network Connectivity Testing • 14
Network Management • 235
NGOD Settings • 238
NGOD Specific Operation • 237

O

Obtaining a License File • 157
Operational Considerations • 230
Operator Responsibilities • 145
Output Monitoring • 58
Overruling ECMG Channel Status Messages
Parameter Values • 191

P

Password Recovery • 209
PC • 256
PID Remapping • 145
Provisioning • 84, 100, 106, 114, 128, 238

Q

QAM • 256
 QAM Annex and Frequency Plan Configuration • 26
 QAM Card Configuration • 28
 QAM Card View • 29
 QAM Channel Configuration • 101
 QAM Channel Level Configuration • 33
 QAM Configuration • 230
 QAM RF Port Configuration • 30

R

RADIUS • 256
 Read-Only/Read-Writer User • 204
 Real -Time Clock Setup • 49
 Release Management • 77, 227
 Remapping Unreferenced PIDS • 139
 Remote Authentication • 207
 Remote User Management • 208
 Removing an ECMG • 187
 Removing an EIS • 199
 Removing ECMG Connection Entirely • 191
 Resource Utilization • 63
 Restore • 229
 Revert • 228
 RF • 256
 RF Gateway 1 Configuration Quick Start • 3
 RMA • 256
 RPU • 256
 RU • 257

S

SCG • 257
 Scrambling Levels • 175
 Scrambling, Control Word, and Cryptoperiod • 171
 SCS • 257
 Security Features • 201
 Secure License Transfer • 163
 Security Features Overview • 202
 Selecting Scrambler Parameters • 182
 Session Refresh • 59
 SFTP Support • 218
 Sign the CSR • 212
 Simple Network Time Protocol (SNTP) • 50
 Simulcrypt Scrambling • 177
 SNMP Configuration • 63
 SRM Configuration • 100
 Start License Transfer • 163

Status Monitoring • 97, 103, 109, 119, 131, 241
 Steps for Enabling HTTPS • 210
 Steps To Take • 180
 Summary Tab • 53
 Switched Digital Video Specific Operation • 99
 System Alarms • 65
 System Events • 67
 System Tab Changes • 218

T

Table-Based Video Specific Operation • 83
 Timing Parameters • 178
 To Change Default Password • 205
 To Edit Local Users • 206
 To Reset the Default Password • 209
 To Set up Local Authentication • 203
 To Setup Remote Authentication • 207
 Troubleshooting • 242

U

Uninstalling SFTP • 221
 Upgrades • 227
 User Notification of Alarms and Events • 68

V

Variable Fan Speed • 151
 Video Session Timeout • 22
 Video Stream Map Configuration • 84

W

Wideband Data Specific Operation • 105



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-6387

Fax: 408 527-0883

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.

Product and service availability are subject to change without notice.

© 2008 - 2014 Cisco and/or its affiliates. All rights reserved.

Part Number 78-4025112-01 Rev H0

October 2014 Printed in USA