



Cisco RF Gateway 1 Software Version 5.1.x Broadcast Simulcrypt Features Addendum

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. A listing of Cisco's trademarks can be found at 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. ^(1009R)

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

© 2010 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

Safe Operation for Software Controlling Optical Transmission Equipment	v
Chapter 1 Introduction	1
Software Enhancements	2
Chapter 2 Configuring the RF Gateway 1	3
QAM Annex and Frequency Plan Configuration	4
QAM Card Configuration.....	6
Global RF Port Configuration	6
QAM Card View	7
QAM RF Port Configuration.....	8
Global QAM Channel Configuration.....	9
Output Monitoring	11
Configuring System Logs	13
Configuring, Monitoring, and Fault Management via SNMP	15
Monitoring Capability.....	17
Chapter 3 Encryption and Scrambling	19
Simulcrypt Scrambling.....	20
Steps To Take.....	21
Configuring Scrambling General Settings.....	21
Configuring Scrambling Specific Parameters	22
Chapter 4 Customer Support Information	41
Support Telephone Numbers	42
Glossary	43
Index	47

Safe Operation for Software Controlling Optical Transmission Equipment

If this manual discusses software, the software described is used to monitor and/or control ours and other vendors' electrical and optical equipment designed to transmit video, voice, or data signals. Certain safety precautions must be observed when operating equipment of this nature.

For equipment specific safety requirements, refer to the appropriate section of the equipment documentation.

For safe operation of this software, refer to the following warnings.



WARNING:

- Ensure that all optical connections are complete or terminated before using this equipment to remotely control a laser device. An optical or laser device can pose a hazard to remotely located personnel when operated without their knowledge.
- Allow only personnel trained in laser safety to operate this software. Otherwise, injuries to personnel may occur.
- Restrict access of this software to authorized personnel only.
- Install this software in equipment that is located in a restricted access area.

1

Introduction

Overview

This document describes the Cisco RFGW-1 software version 5.1.x broadcast simulcrypt operation, including integrated PowerKEY® encryption, and NDS encryption. Broadcast sessions are setup using DNCS 4.4.1 and the scrambling operation is controlled by a NDS EIS operating in AC reference mode.

Who Should Use This Document

This document is intended for authorized service personnel who have experience working with the RFGW-1 or 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 first release of this guide.

In This Chapter

- Software Enhancements..... 2

Software Enhancements

The following enhancements are included in software version 5.1.x.

- Internal PowerKEY encryption
- Simulcrypt integration with NDS encryption

2

Configuring the RF Gateway 1

This chapter provides information needed to configure simulcrypt 5.1.x features.

In This Chapter

- QAM Annex and Frequency Plan Configuration 4
- QAM Card Configuration 6

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.

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

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	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.

QAM Card View

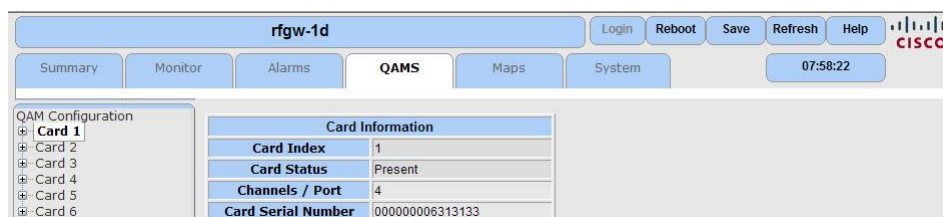
The RFGW-1 chassis can be populated with up to six QAM line cards.

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.



rfgw-1d		Login	Reboot	Save	Refresh	Help	CISCO
Summary	Monitor	Alarms	QAMS	Maps	System	07:58:22	

QAM Configuration	Card Information
Card 1	Card Index 1
Card 2	Card Status Present
Card 3	Channels / Port 4
Card 4	Card Serial Number 000000006313133
Card 5	
Card 6	

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.

The screenshot shows the 'rfgw-1d' configuration page with the 'QAMS' tab selected. The left sidebar shows a tree view under 'QAM Configuration' with 'Card 1' expanded, and 'RF Port 1/1' selected. The main panel displays the 'RF Port Configuration' for Card Index 1, Port Index 1. The parameters are as follows:

Parameter	Value
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
ITU Carrier Number	50
Carrier Center Frequency (MHz)	381.000

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 2 Configuring the RF Gateway 1

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.

Note: You can change values for one row and then update them all by clicking **Update All Rows**.

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.

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. ■ 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.

Parameter	Description
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.

SRM Details

In Release 5.1.x, the RFGW-1 has a new feature that allows the user to view details of any particular session.

Click the hyperlink under the Session ID field to view SRM parameters. See the following screen.

SRM Details	
Session ID	000000000000/1
SRM IP Address	64.100.109.200
Input Program Number	1
Output Program Number	2
Session Rate (bps)	3750000
No PID Remapping Flag	False
Total Number of PIDs	7
Total Number of Assigned PIDs	5
PowerKEY Encrypt Flag	True
Simulcrypt Flag	True
PID Assignment Error	No Error
PowerKEY CA Template Flag	True

Assigned PID Details		
PID Type	Input PID	Output PID
PMT	-	258
PCR	-	259
ECM	-	256
ECM	-	257
Video	101	259
Audio	102	260
Audio	103	261

Parameters

The following table describes SRM parameters.

Parameter	Description
Session ID	The unique number assigned by the SRM for the session.
SRM IP Address	The IP Address of the SRM that created the session.
Input Program Number	The Program Number of the source at the input.
Output Program Number	The Program number at the output.
Session rate (bps)	The provisioned bitrate of the session.
No PID Remapping Flag	True indicates that there are no PID changes between the input program and the output program.
Total Number of PIDs	This count indicates the number of output PIDs present.
Total Number of Assigned PIDs	This count indicates the number of provisioned output PIDs.
PowerKEY Encrypt Flag	True for PowerKEY or Simulcrypt JCAS operation.
Simulcrypt Flag	True for Simulcrypt JCAS operation.
PID Assignment Error	This field helps to reveal a detect PID error.
PowerKEY CA Template Flag	This field indicates that the SRM has exchanged encryption keys for this session.

The following table explains the PID parameters.

Parameter	Description
PID Type	The component type for the Program PIDs.
Input PID	The PIDs present in the input PMT.
Output PID	The provisioned PIDs.

Configuring System Logs

Follow the instructions below to configure system logs.

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

Result: The following screen is displayed.

System Configuration

- About
- ARP & Routes
- Authentication
 - Change Password
- Backup Configuration
- Clock
- IP Network
- License Management
- Logs
 - Configuration**
- Release Management
- Restore Configuration
- Scrambler
 - EIS Configuration
 - ECMG Configuration
 - SCG Details
 - SNMP & Traps

System Log Configuration

Module Name	Off	Terse	Verbose
Configuration	☒	☐	☐
Download, Backup & Restore	☐	☒	☐
DTI	☐	☒	☐
FTP License	☐	☒	☐
Hardware	☐	☒	☐
IGMP	☐	☒	☐
Initialization	☐	☒	☐
Input Ports	☐	☒	☐
Logging	☐	☒	☐
OLS Licensing	☐	☒	☐
QAM Cards	☐	☒	☐
PowerKEY	☐	☒	☐
Scrambler	☐	☒	☐
SDV Communications	☐	☒	☐
SNMP	☐	☒	☐
Stream Management	☐	☒	☐

Apply Reset Show Advanced Filters

- 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 following screen is displayed.

Advanced Filters			
Module Name	Off	Terse	Verbose
Calibration	☒	☐	☐
Data Plane Hardware	☒	☐	☐
Dejitter Buffer	☒	☐	☐
Factory	☒	☐	☐
Front Panel	☒	☐	☐
Input Stream Processing	☒	☐	☐
Low Level Alarms	☒	☐	☐
Output Stream Processing	☒	☐	☐
Packet Processor	☒	☐	☐
Resource allocator	☒	☐	☐
Scheduler Modulator	☒	☐	☐
SFP MAC	☒	☐	☐
Socket	☒	☐	☐
Web Server	☐	☒	☐

- 2 Select the desired filter levels for each category.

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

- 3 Click **Apply**.

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.

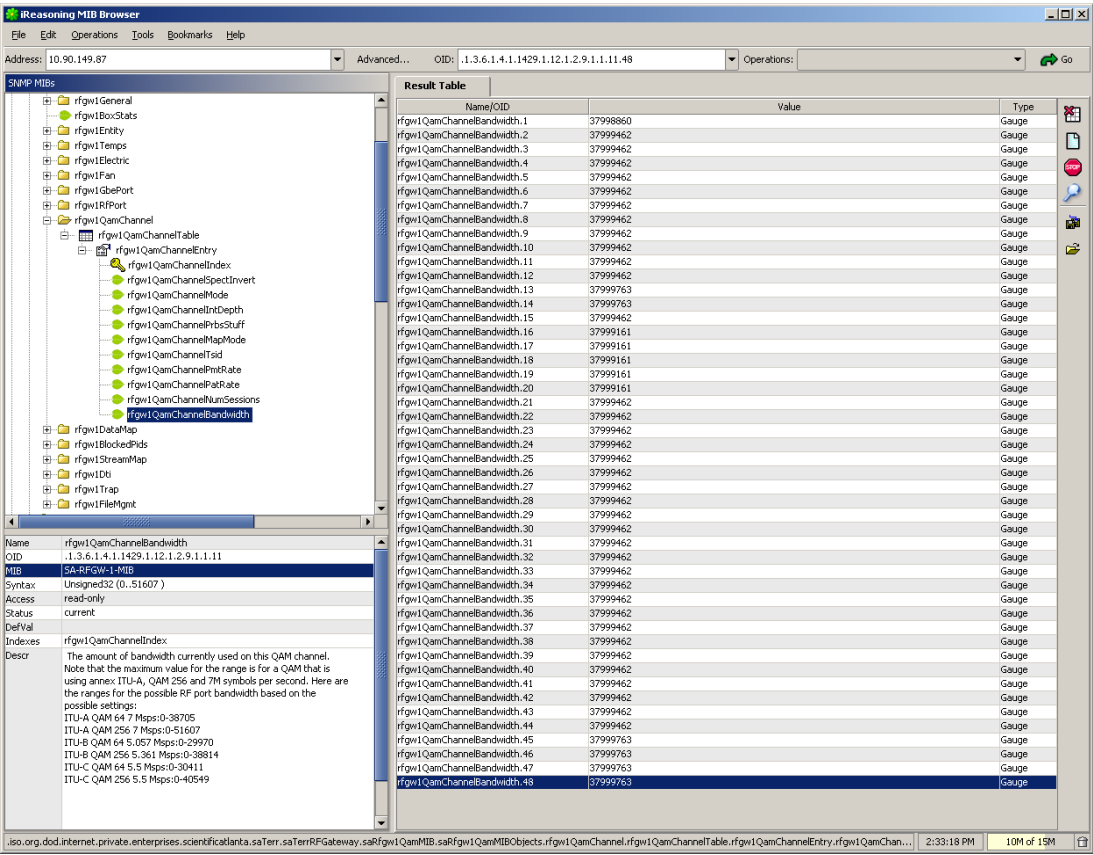
The following table shows the MIBs supported.

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.

MIB Name	Description
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.

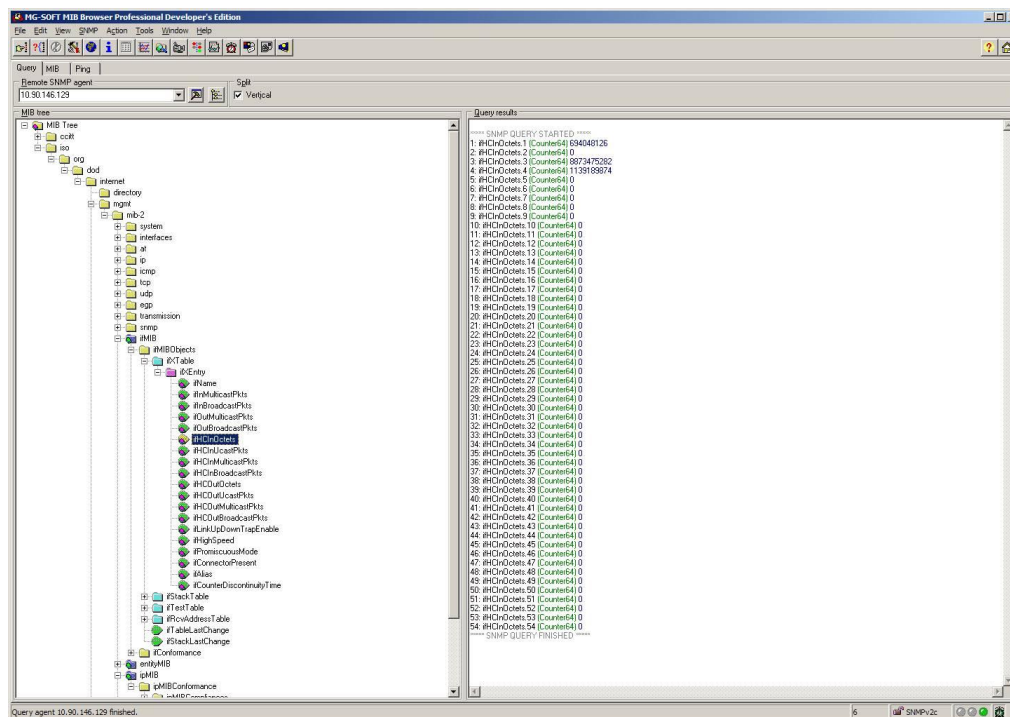
Monitoring Capability

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.



Chapter 2 Configuring the RF Gateway 1

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



3

Encryption and Scrambling

Introduction

This chapter describes how to integrate the RFGW-1 into scrambling applications.

In This Chapter

- Simulcrypt Scrambling..... 20
- Steps To Take..... 21

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.

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 4025112.
- b Configure the QAM outputs. For information regarding Enabling QAM Ports, see the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.
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 4025112.

2 Simulcrypt Controller Configurations

- a Configure Scrambling General Parameters. Refer to *Configuring Scrambling General Settings* (on page 21).
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 22).
- 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 23).
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 37).

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).

Parameter	Description
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

SCS Configuration GUI

The SCS Configuration GUI allows configuring the scrambling specific parameters and assigning the following CA interfaces:

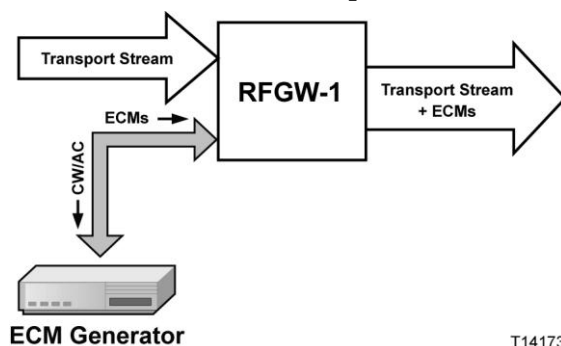
- ECMG interfaces

■ EIS interfaces

Note: The number of CA interfaces that can be assigned to a RFGW-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

Steps to Take

- 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.

The screenshot shows the 'rfgw-1d' web interface. The top navigation bar includes 'Login', 'Reboot', 'Save', 'Refresh', and 'Help'. The 'System' tab is selected, and the 'Scrambler' sub-tab is active. The left sidebar shows the 'System Configuration' tree with 'Scrambler' expanded. The main content area displays the 'Scrambler General Settings' form.

Scrambler General Settings	
Scramble Only Video and Audio	☐
Check SCG at Provision Time	☐
Strong Pairing Enforcement	☐
SCG Persistence	☐
Active Core Encryption Algorithm	DES
Core Encryption Algorithm	DES
Scrambled ECMG Streams	0

Buttons: Apply, Reset

- 2 Click the + to expand the window and select **ECMG Configuration**.

Result: The following page is displayed.

The screenshot shows the 'rfgw-1d' web interface. The top navigation bar includes 'Login', 'Reboot', 'Save', 'Refresh', and 'Help'. The 'System' tab is selected, and the 'ECMG Configuration' sub-tab is active. The left sidebar shows the 'System Configuration' tree with 'ECMG Configuration' selected. The main content area displays a table of existing ECMG entries.

	ECMG Name	ECMG Type	CA System ID	CA Sub System ID	Edit
☐	ECMG Proxy	Standard	0x952	0x1	Edit

Buttons: Add New ECMG, Delete, Reset

- 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 'rfgw-1d' System Configuration page. 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)	0x1fff
ECMG Streams / ECMG	0
Open ECMG Streams / ECMG	0
Automatic Channel ID Selection	☒
Enable Hot Backup	☐

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 28).

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 'rfgw-1d' System Configuration page. The left sidebar lists various configuration categories, with 'ECMG Configuration' selected. The main area displays the following table:

	ECMG Name	ECMG Type	CA System ID	CA Sub System ID	Edit
☒	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	■ 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	Select the desired ECM PID source. ■ 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. 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).
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**.

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 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 form includes several checkboxes and dropdown menus for configuring scrambling options.

Scrambler General Settings	
Scramble Only Video and Audio	☐
Check SCG at Provision Time	☐
Strong Pairing Enforcement	☐
SCG Persistence	☐
Active Core Encryption Algorithm	DES
Core Encryption Algorithm	DES
Scrambled ECMG Streams	0

Buttons: Apply, Reset

- 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 left sidebar. The main content area displays a table of existing ECMG configurations.

	ECMG Name	ECMG Type	CA System ID	CA Sub System ID	Edit
☐	ECMG Proxy	Standard	0x952	0x1	Edit

Buttons: Add New ECMG, Delete, Reset

- Click **Add New ECMG**.

Result: The following page is displayed.

The screenshot shows the 'rfgw-1d' System Configuration page. The left sidebar lists various configuration categories, with 'ECMG Configuration' selected. The main area displays the 'ECMG Configuration' form with the following 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 located below the form. At the bottom, there are radio buttons for 'Advanced', 'Connection' (selected), and 'Descriptor Rules'. Below these is a table with the following columns: Priority, IP Address, Port, ECMG Port Selection, Channel Id, ECM Channel Id, Connection Status, and 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

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.

Parameter	Description
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.

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**.

Result: The following table is displayed.

Apply Reset	
☒ Advanced ☐ Connection ☐ Descriptor Rules	
Override Max. Comp. Time (ms)	☐ 5000
Override Min. CP Duration (ms)	☐ 10000
Override Transition Start Delay (ms)	☐ -2000
Override Transition Stop Delay (ms)	☐ 2000
Override Start Delay (ms)	☐ -2000
Override Stop Delay (ms)	☐ -2000
Override AC Start Delay (ms)	☐ -2000
Override AC Stop Delay (ms)	☐ -2000
Override Repetition Period (ms)	☐ 100
Override Max. Streams	☐ 512

- Click the check box next to the parameter you want to change.

Result: The parameter box becomes active.

- Modify the setting.
- Click **Apply** to accept change or **Reset** to abort.

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.

- Navigate to the *System/Scrambler* page.

Chapter 3 Encryption and Scrambling

Result: The following page is displayed.

The screenshot shows the 'rfgw-1d' System Configuration page. The left sidebar lists various configuration categories, with 'Scrambler' expanded. The main content area displays the 'Scrambler General Settings' form. The form includes several checkboxes and two dropdown menus.

Scrambler General Settings	
Scramble Only Video and Audio	☐
Check SCG at Provision Time	☐
Strong Pairing Enforcement	☐
SCG Persistence	☐
Active Core Encryption Algorithm	DES
Core Encryption Algorithm	DES
Scrambled ECMG Streams	0

Buttons: Apply, Reset

- 1 Click the + to expand the window and select **ECMG Configuration**.

Result: The following page is displayed.

The screenshot shows the 'rfgw-1d' System Configuration page with 'ECMG Configuration' selected in the left sidebar. The main content area displays a table with one row of configuration data.

	ECMG Name	ECMG Type	CA System ID	CA Sub System ID	Edit
☐	ECMG Proxy	Standard	0x952	0x1	Edit

Buttons: Add New ECMG, Delete, Reset

- 2 Click **Add New ECMG**.

Result: the following page is displayed.

The screenshot shows the 'rfgw-1d' System Configuration page. The left sidebar lists various configuration categories, with 'ECMG Configuration' selected. The main area displays the following settings:

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: Apply, Reset

Radio buttons: ☐ Advanced, ☒ Connection, ☐ Descriptor Rules

Priority	IP Address	Port	ECMG Port Selection	Channel Id	ECM Channel Id	Connection Status	Open Streams
----------	------------	------	---------------------	------------	----------------	-------------------	--------------

3 Click Descriptor Rules.

Result: The Descriptor Rules table is displayed.

The screenshot shows the 'Descriptor Rules' section. At the top, there are radio buttons: ☐ Advanced, ☐ Connection, and ☒ Descriptor Rules. Below is a table with the following columns:

	Name	Type	Insert	ECM ID(s)	Private Data (Hex)
--	------	------	--------	-----------	--------------------

Buttons: Add New ECMG Descriptor Rule, Reset

4 Click Add New ECMG Descriptor Rule.

Result: The rule is added to the table.

5 Click Apply to accept change or Reset to abort.

6 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.

	Name	Type	Insert	ECM ID(s)	Private Data (Hex)	
☒	ECMG Rule	Add Private Data	According to EIS			Edit

2 Click **Apply** to accept change or **Reset** to abort.

Descriptor Rule Parameters

The following table describes the Descriptor Rule parameters.

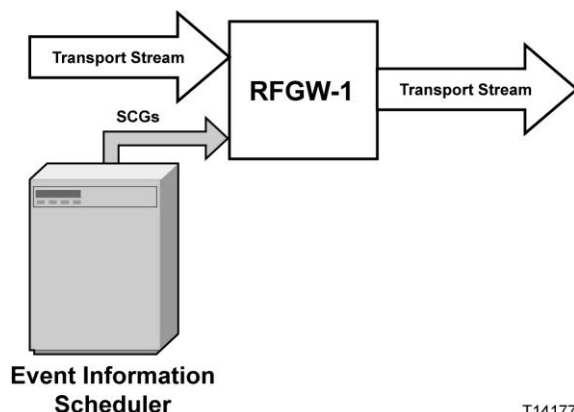
Parameter	Description
Name	Identification of the descriptor rule.
Type	Allows you to select the rule type. ■ Add Private Data - add data to the standard descriptor. ■ Do Not Insert - prevents updating the CA descriptor in the PMT if the PSI/SI information is generated by an external PSIG. Notes: ■ If 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. ■ 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.

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.

The screenshot shows the 'EIS Configuration' page. On the left is a tree view with the following items: Backup Configuration, Clock, IP Network, License Management, Logs, Configuration, Release Management, Restore Configuration, Scrambler, **EIS Configuration**, ECMG Configuration, SCG Details, and SNMP & Traps. The main area contains a table with one row. Below the table are four buttons: 'Add New EIS', 'Apply', 'Delete', and 'Reset'.

☒	EIS Proxy	9501	CA	No	10	General	No	N/A	N/A
☒	EIS Proxy	9501	CA	No	10	General	No	N/A	N/A

3 Click **Add New EIS**.

Result: The new EIS is added to the table.

The screenshot shows the 'EIS Configuration' page after adding a new entry. The table now has two rows. The buttons 'Add New EIS', 'Apply', 'Delete', and 'Reset' are still present at the bottom.

☒	EIS Proxy	9501	CA	No	10	General	No	N/A	N/A
☒	EIS Proxy	9501	CA	No	10	General	No	N/A	N/A
☒	EIS Proxy	9501	CA	No	10	General	No	N/A	N/A

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.
Override	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. ■ 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.

SCG Details

The following screen shows SCG details.

System Configuration

- About
- ARP & Routes
- Authentication
- Backup Configuration
- Clock
- IP Network
- License Management
- Logs
- Release Management
- Restore Configuration
- Scrambler
 - EIS Configuration
 - ECMG Configuration
 - SCG Details**
 - SNMP & Traps

☐ Display ON ID, TS ID and ES PIDs in hex

SCG Details [View all SCGs](#)

SCG ID	ON ID	TS ID	SCG Ref. ID	Activation Time	CP Duration (ms)	Service IDs	ES PIDs	ECM Groups
1	1	1	4294967295	1970/1/1 0:0:0	4000		259, 260, 261	Show
2	1	1	4294967295	1970/1/1 0:0:0	4000		275, 276, 277	Show
3	1	1	4294967295	1970/1/1 0:0:0	4000		291, 292, 293	Show
4	1	1	4294967295	1970/1/1 0:0:0	4000		307, 308, 309	Show
5	1	1	4294967295	1970/1/1 0:0:0	4000		323, 324, 325	Show
6	1	1	4294967295	1970/1/1 0:0:0	4000		339, 340, 341	Show
7	1	1	4294967295	1970/1/1 0:0:0	4000		355, 356, 357	Show
8	1	1	4294967295	1970/1/1 0:0:0	4000		371, 372, 373	Show

SCG Parameters

The following table describes the SCG parameters.

Parameter	Description
SCG ID	Scrambling Control Group Identifier.
ON ID	Original Network Identifier.
TS ID	Transport Stream Identifier.
SCG Ref ID	Scrambling Control Group Reference Identifier.
Activation Time	The scrambling start time.
CP Duration (ms)	The EIS provisioned cryptoperiod.
Service IDs	If the SCG contains service-level scrambling, this field will contain the services to be scrambled.
ES PIDs	If the SCG contains component-level scrambling, this field will contain the ES components to be scrambled.
ECM Groups	The SCG groups showing the ECM PID value and Access Criteria.

4

Customer Support Information

Introduction

This chapter contains information on obtaining product support.

Obtaining Product Support

IF...	THEN...
you have general questions about this product	contact your distributor or sales agent for product information or refer to product data sheets on www.cisco.com .
you have technical questions about this product	call the nearest Technical Support center.
you have customer service questions about this product	call the nearest Customer Service center.

In This Chapter

- Support Telephone Numbers..... 42

Support Telephone Numbers

This table lists the Technical Support and Customer Service numbers for your area.

Region	Centers	Telephone and Fax Numbers
North America	Cisco Services Atlanta, Georgia United States	For <i>Technical Support</i> , call: ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press 2 at the prompt) For <i>Customer Service</i> , call: ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press 3 at the prompt) ■ Fax: 770-236-5477 ■ Email: customer-service@cisco.com
Europe, Middle East, Africa	Belgium	For <i>Technical Support</i> , call: ■ Telephone: 32-56-445-197 or 32-56-445-155 ■ Fax: 32-56-445-061 For <i>Customer Service</i> , call: ■ Telephone: 32-56-445-444 ■ Fax: 32-56-445-051 ■ Email: service-elc@cisco.com
Japan	Japan	■ Telephone: 81-3-5908-2153 or +81-3-5908-2154 ■ Fax: 81-3-5908-2155
Korea	Korea	■ Telephone: 82-2-3429-8800 ■ Fax: 82-2-3452-9748 ■ Email: songk@cisco.com
China (mainland)	China	■ Telephone: 86-21-2401-4433 ■ Fax: 86-21-2401-4455 ■ Email: xishan@cisco.com
All other Asia Pacific countries & Australia	Hong Kong	■ Telephone: 852-2588-4746 ■ Fax: 852-2588-3139 ■ Email: saapac-support@cisco.com
Brazil	Brazil	■ Telephone: 11-55-08-9999 ■ Fax: 11-55-08-9998 ■ Email: fattinl@cisco.com or ecavalhe@cisco.com
Mexico, Central America, Caribbean	Mexico	For <i>Technical Support</i> , call: ■ Telephone: 52-3515152599 ■ Fax: 52-3515152599 For <i>Customer Service</i> , call: ■ Telephone: 52-55-50-81-8425 ■ Fax: 52-55-52-61-0893 ■ Email: sa-latam-cs@cisco.com
All other Latin America countries	Argentina	For <i>Technical Support</i> , call: ■ Telephone: 54-23-20-403340 ext 109 ■ Fax: 54-23-20-403340 ext 103 For <i>Customer Service</i> , call: ■ Telephone: 770-236-5662 ■ Fax: 770-236-5888 ■ Email: keillov@cisco.com

Glossary

CA

Conditional Access.

CM

cable modem

CMTS

cable modem termination system.

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.

Glossary

HTML

hypertext markup language.

HTTP

hypertext transfer protocol.

IP

Internet protocol. A standard that was originally developed by the United States Department 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.

MIB

management information base.

MPTS

multiprogram transport streams

PC

personal computer.

PID

packet identifier.

PMT

program map table.

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 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.

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.

SDV

Switched Digital Video.

SNMP

simple network management protocol.

SPTS

single-program transport streams.

Glossary

TCP

Transmission Control Protocol.

Index

A

Adding an ECMG • 26
Adding an EIS • 37
Adding ECMG Connection Entries • 28

C

CA • 43
Changing EIS Parameters • 39
CM • 43
CMTS • 43
Configuring Scrambling General Settings • 21
Configuring Scrambling Specific Parameters • 22
Configuring System Logs • 13
Configuring the RF Gateway 1 • 3
Configuring, Monitoring, and Fault Management via SNMP • 15
customer support information • 41
Customer Support Information • 41

E

ECM • 43
ECMG • 43
ECMG Descriptor Rules • 33
ECMG Parameters • 28
EIS • 43
EIS Parameters • 39
EMM • 43
Encryption and Scrambling • 19
Entitlement Control Message Generators • 23
ES • 43
Event Information Schedulers • 37

F

FTP • 43

G

Global QAM Channel Configuration • 9
Global RF Port Configuration • 6
GUI • 43

H

HTML • 44
HTTP • 44

I

Introduction • 1
IP • 44
IP address • 44
ISO • 44

L

Load Balancing • 23

M

MIB • 44
MPTS • 44

O

Output Monitoring • 11
Overruling ECMG Channel Status Messages
Parameter Values • 31

P

PC • 44
PID • 44
PMT • 44

Q

QAM • 45
QAM Annex and Frequency Plan Configuration • 4
QAM Card Configuration • 6
QAM Card View • 7
QAM RF Port Configuration • 8

R

RADIUS • 45
Removing an ECMG • 27
Removing an EIS • 38
Removing ECMG Connection Entries • 31
RF • 45

Index

RMA • 45

RU • 45

S

SCG • 45

SCG Details • 40

SCG Parameters • 40

SCS • 45

SCS Configuration GUI • 22

SDV • 45

Selecting Scrambler Parameters • 22

Simulcrypt Scrambling • 20

SNMP • 45

Software Enhancements • 2

SPTS • 45

SRM Details • 12

Steps To Take • 21

Support Telephone Numbers • 42

T

TCP • 46



Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678.277.1000
www.cisco.com

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.

© 2010 Cisco and/or its affiliates. All rights reserved.

October 2010 Printed in United States of America

Part Number 4038589 Rev A