



Cisco RF Gateway 1 Software Release 5.03.02 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software version 5.03.02 provides feature additions /enhancements to the Simulcrypt Broadcast version of the RFGW software (Release 5.01.XX) for Altice USA (earlier known as Cablevision Systems Corporation (CVC)).

Purpose

The purpose of this document is to notify users of the enhancements included in this release, and to identify known issues.

Audience

This document is intended for system engineers or managers responsible for operating and/or maintaining this product.

Related Publications

Refer to the following documents for additional information regarding hardware and software.

- *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01
- *Cisco RF Gateway 1 System Guide*, part number 78-4024958-01


Safe Operation for Software Controlling Optical Transmission Equipment

If this document 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 should be observed when operating equipment of this nature.

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

New Features

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

 **WARNINGS:**

- 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.

In This Document

- New Features.....3
- Resolved Issues4
- Known Issues5
- Test Summary6
- Image Information.....8
- Bug Toolkit9
- Upgrade Information10

New Features

RFGW1 changes for supporting 3 ECM groups for LSM based simulcrypt broadcast environment.

This feature enables RFGW1 to support simulcrypt broadcast with Linear Session Manager (LSM). Below is the list of changes to RFGW1 software done as part of CDET CSCvc72163.

1. The discover encryption message in the GQI protocol has been modified to send the encryption modes based on the license present and scrambling configuration on the chassis.

PK License	DVB License	Current scrambler	Modes sent
No	No	Don't care	None
Yes	No	DES	PKEY, DES
Yes	No	DVB-CSA	PKEY
Yes	Yes	DVB_CSA	PKEY,DVB_CSA
No	Yes	DES	none
No	Yes	DVB_CSA	DVB_CSA

2. Sending traps when the user initiates "Switch sessions to next port" and "Revert All sessions to primary".
3. Modified debug APIs for the assigned PID verification to include third ECM
 - a. qpiderrors
 - b. qpiderrorsall
 - c. qscgerrors
 - d. qscgerrorsall

Resolved Issues

Specific Issues

ID	Description
CSCvd50428	Duplicate input program numbers in GQIv3 is not handled correctly.

Known Issues

- The RF Gateway 1 Web interface is not fully tested with IE-8 and FireFox 3.5.x or newer. The RF Gateway 1 web management interface is tested with IE-6 or FireFox 2.0.0.14 and above. Use of Java 1.6.x is also recommended.
- When using /31 IP addressing, although the RF Gateway 1 allows setting IP addresses and masks that correspond to this point-to-point protocol, it will not respond to ICMP ping request.

Test Summary

Feature Test

SNO	TEST	Automation/Manual	Pass/Fail Status	Test Cases executed
1	Input Redundancy with SNMP for Broadcast	Manual	Passed	25

HE Verification Test

SNO	TEST	Automatic/Manual	Pass/Fail Status
1	Verification of Simulcrypt sessions in CVC headend	Manual	Passed

Sanity Test

SNO	TEST	Automation/Manual	Pass/Fail Status	Test Cases executed
1	GUI test cases (exploring and verifying all the GUI pages)	Manual	Passed	200
2	Platform test functional-(Release management, Backup/Restore, Configuration backup/Restore test)	Manual	Passed	65
3	Simulcrypt test cases	Manual	Passed	78
4	PID conflict test cases	Manual	Passed	28
5	Session Refresh test cases	Manual	Passed	14
6	Authentication	Manual	Passed	30
7	Scrambler Test case	Manual	Passed	40

Migration Test

SNO	TEST	Automatic/Manual	Pass/Fail Status
1	Upgrade from below releases to V05.03.02 and reverted. (V05.01.11, V05.01.15, V05.02.02, V05.02.06, V05.02.09)	Manual	Passed

Automation Test

SNO	TEST	Feature	Automatic/Manual	Pass/Fail Status
1	Simulcrypt Churn	GQI V3	Automatic	Passed

Test Summary

2	SNMP based stream switch	Input Redundancy	Automatic	Passed
---	--------------------------	------------------	-----------	--------

Image Information

The following table lists the files included in this release and their file sizes.

File Name	Size (in Bytes)
app_05.03.02.gz	3597252
becks_06.01.14_fw.gz	2490139
bootrom_V5_02.05.00.bin	2097152
coors_05.00.27_fw.gz	2845585
dual_moretti_07.01.04_06.01.05_fw.gz	5440797
duvel_06.01.13_fw.gz	2681608
rfgw1_rel_05_03_02.xml	1689
miller_lite_05.01.20_fw.gz	56807
superfly_04.04.06_fw.gz	1421717
CISCO-RFGW-1-MIB.mib	218269
V05.03.02.zip (Compressed file containing all of the files above minus the MIB files)	16063151

Note:

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V05.03.02.zip is the compressed file of all the image components excluding the MIB files. The file must be uncompressed before uploading into the RFGW-1.
- The calculated MD5 checksum for V05.03.02.zip is 59b6de0c378636c0d0bb923657de6a06.

Bug Toolkit

If you need information about a specific caveat that does not appear in this release note, you can use the Cisco Bug Toolkit to find caveats of any severity. Use the following URL to access the Bug Toolkit:

<http://tools.cisco.com/Support/BugToolKit/>

If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.

Upgrade Information

An RF Gateway 1 unit running release 1.02.20 or higher can be upgraded directly to 5.XX.XX. Refer to Chapter 3, *General Configuration and Monitoring (Release Management)* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112, for more information. The RF Gateway 1 reboots automatically at the end of the upgrade process. However, when upgrading to 5.XX.XX from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 5.XX.XX must be followed. The bridge release designated as 1.02.19 has been created to provide a secure and robust upgrade path. Releases 1.02.19 (bridge) and 1.02.20 (final) have identical user features and functionality.



WARNING:

Upgrading to 1.02.20 or 5.XX.XX directly from 1.02.09 must not be attempted. This may cause the RF Gateway 1 to be non-operational.

For Information

If You Have Questions

If you have technical questions, contact Cisco Services for assistance. Follow the menu options to speak with a service engineer.



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

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. (1110R)

Product and service availability are subject to change without notice.

© 2017 Cisco and/or its affiliates. All rights reserved.

April 2017