Cisco RF Gateway 1 Software Release 5.02.02 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software version 5.02.02 provides feature additions /enhancements to the Simulcrypt Broadcast version of the RFGW software (Release 5.01.XX) and also addresses some of the field issues reported by 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.

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

CP Boundary Separation for NDS only broadcast sessions

This feature addition is targeted at the NDS only broadcast sites, to minimize the effects of time aligned crypto periods on multi tuner STB's. This feature is disabled by default and can be enabled with a setting on the advanced page GUI.

This feature ensures that the crypto periods are separated out for sessions as per the maximum number of sessions to be supported, the crypto period and the crypto period boundary separation that is required.

This feature should be disabled in the Simulcrypt setup.

Unicast Stream/Session Redundancy for Simulcrypt Sessions

This feature enhances redundancy options available in the RFGW to input streams with missing services/programs. This feature enables RFGW

1. To switch to an alternate input stream, if the complete MPTS fails.
2. To switch to another MPTS carrying the program number if only a specific program fails on the input.

The RFGW also sends the traps and logs the session switch.

Resolved Issues

Specific Issues

The following issues are resolved in this release.

ID	Description
CSCum66938	Feature Request: Unicast Stream/Session Redundancy for Simulcrypt Sessions
CSCum08884	Feature Request: CP Boundary Separation for NDS only broadcast sessions
CSCum46243	RFGW1 sending null public key during DiscoverEncryption and causing a crash in the DNCS QAM Manager process.
CSCud89547	The WatchDog Task does not reboot the RFGW-1 after certain exceptions
CSCun18011	RFGW-1:Streaming Encrypted content in Clear in case of no CABlob
CSCuo14234	Pointers to the SI extractor buffer could get corrupted while processing large tables (PAT/PMT).
CSCup37390	RFGW-1 (5.1.x) creates stale SCG in PK broadcast setup. (Disabling PK only broadcast sessions)
CSCup70922/ CSCuo06033	Some sources remain clear for pk gqi session RFGW1 on rare scenario
CSCue65591/ CSCuh48603	UPTIME reset issue though system rebooting was not happened
CSCug68098	'tCpuResrcMonitor' Task crashed due to a data storage exception and the Watchdog rebooted the RFGW-1.
CSCur55481	The bad PMT descriptor such as missing CRC from the upstream device causes RFGW to exhaust memory while parsing PMT and leads to new VOD session in Waiting for PMT state. Rebooting RFGW-1 is the only workaround.

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

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	Broadcast input redundancy test cases	Manual	Passed	14
5	PID conflict test cases	Manual	Passed	28
6	Session Refresh test cases	Manual	Passed	14
7	CP boundary tests	Manual	Passed	11

Migration Test

SNO	TEST	Automatic/Manual	Pass/Fail Status
1	Upgrade from below releases to V05.02.02 and reverted. (V05.01.11, V05.01.15, V05.02.00_E6)	Manual	Passed

Automation Test

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

Image Information

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

File Name	Size (in Bytes)
app_05.02.02.gz	3589816
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_06.01.12_fw.gz	2584181
rfgw1_rel_05_02_02.xml	1689
miller_lite_05.01.20_fw.gz	56807
superfly_04.04.06_fw.gz	1421717
CISCO-RFGW-1-MIB.my	208737
V05.02.02.zip (Compressed file containing all of the files above minus the MIB files)	15986171

Note:

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V05.02.02.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 V05.02.02.zip is 23c01f1311bf85177f5b26b970512190.

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

January 2015