



Cisco RF Gateway 1 Software Release 5.02.06 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software version 5.02.06 provides feature additions /enhancements to the Simulcrypt Broadcast version of the RFGW software (Release 5.01.XX) for 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.

New Features

 **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 Issues7
- Known Issues8
- Test Summary9
- Image Information.....10
- Bug Toolkit11
- Upgrade Information12

New Features

Broadcast Redundancy Enhancement

This feature is addressed as part of CSCuu29952 - CVC - Enhancements to broadcast input redundancy.

This feature provides input redundancy for GQIv3 sessions using unicast streams in the following cases:

Session creation:

When a new session is created using an **SPTS** on a Gbe port pair, and if the session doesn't become active in Y seconds, the session will be switched to next port pair. This is accomplished by deleting the sessions bound to that stream and creating it in next Gbe port pair on the same UDP port.

When new sessions are created using an **MPTS** on a Gbe port pair and only if none of the sessions on that MPTS become active, then all those sessions will be switched to next Gbe port pair on the same UDP port.

Input loss for an active session:

When the RFGW1 detects **stream loss** (SPTS/MPTS) on a Gbe port pair, the sessions bound to that stream will be switched to next Gbe port pair on the same UDP port.

When one or more programs in MPTS are lost, the sessions bound to those programs will remain in the same Gbe port pair. When the RFGW1 detects a **program loss** in a MPTS, only a trap is sent.

NOTE: Before and after switching the status of the session will be logged and trap is also sent.

Configuration details

The feature can be enabled/disabled in the advanced page. The advanced page can be accessed using the URL "<RFGW1-IP>/fs/advanced.html".

NOTE: The advanced page has features, which alter the functioning of the RFGW-1 drastically. Please handle this page with caution.

New Features

| Advanced Configuration | |
|---|------------------|
| Dejitter Discontinuity Insertion | Disabled |
| Dejitter Discontinuity Persistence | Enabled |
| Dejitter Buffer Start Delay | 0 milliseconds |
| Packet Delay Discontinuity Insertion | Disabled |
| Discontinuity Delay Threshold | 5 milliseconds |
| | |
| Stream Hold Delay | 2 seconds |
| | |
| Digicipher table change detection threshold | 20 |
| SI change detection threshold | 6 |
| SI change detection interval | 2 seconds |
| Stream Map PIDs per PMV | 32 |
| CP Boundary Separation | Disabled |
| CP Separation Interval | 250 milliSeconds |
| CP Separation Max Sessions | 50 Sessions |
| Auto Session Refresh | Enabled |
| | |
| Input Redundancy | Disabled |
| Input Loss trigger duration | 5 seconds |
| Zero bit-rate trigger duration | 10 seconds |
| Revert to primary | |

Apply Reset

The configuration of feature can be found at the bottom of the page as highlighted by the yellow window in the above figure.

1. **Input Redundancy** controls the enabling or disabling of the feature.
2. **Input Loss trigger duration** specifies the number of seconds to wait on current port after an active session goes to loss state, before switching that session to the next port.

3. **Zero bit-rate trigger duration** specifies the number of seconds to wait on current port where the session is created and the session doesn't become active before switching the session to the next port.
4. **Revert to primary** will switch the sessions to the port where the session was initially created.

To make the changes done in 1, 2, 3 to become effective, apply button has to be clicked.

| | |
|--|------------|
| Input Redundancy | Enabled ▾ |
| Input Loss trigger duration | 5 seconds |
| Zero bit-rate trigger duration | 10 seconds |
| <input type="button" value="Revert to primary"/> | |

To manually switch a stream to the next port pair, go to **Monitor** -> **output**. Click **details** for any session that is bound to this stream. In the bottom of the pop-up window, click **Display session list/ show session list**.

| Session ID | RFGW QAM Channel | SRM QAM Channel | Provisioned Bitrate(Mbps) | Output | | | |
|-------------------------|------------------|-----------------|---------------------------|----------------|---------|---------|-----------------------|
| | | | | Program Number | PMT PID | PCR PID | Output Bitrate (Mbps) |
| 0000000000000000104/260 | 2/1.2 | 18 | 5.0000 | 4 | 320 | 321 | 1.7446 |

| Session ID |
|---------------------|
| 0000000000000000102 |
| 0000000000000000103 |
| 0000000000000000104 |
| 0000000000000000105 |
| 0000000000000000106 |

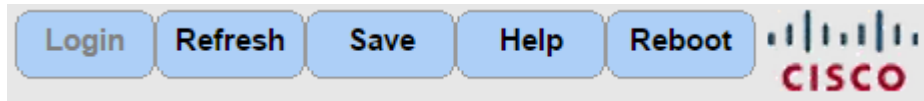
Click **Switch to Port Pair 1/ Switch to Port Pair 2** to switch the streams between port pairs.

New Features

Logout and reboot button to be at a distant from each other

The log out button is right next to the reboot button. There is risk here with someone accidentally clicking reboot instead of log out. Hence CVC requested for this GUI change. This request is addressed in CSCuu82517.

Below is the modified location of these buttons:



Resolved Issues

Specific Issues

There are no field issues resolved in this release.

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 |

Migration Test

| SNO | TEST | Automatic/Manual | Pass/Fail Status |
|-----|--|------------------|------------------|
| 1 | Upgrade from below releases to V05.02.06 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_05.02.06.gz | 3593664 |
| 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_06.xml | 1689 |
| miller_lite_05.01.20_fw.gz | 56807 |
| superfly_04.04.06_fw.gz | 1421717 |
| CISCO-RFGW-1-MIB.my | 208737 |
| V05.02.06.zip (Compressed file containing all of the files above minus the MIB files) | 15987994 |

Note:

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V05.02.06.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 V05.02.06.zip is 38f0963bd874df1bd5c89bd9b95406e4.

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.

© 2015 Cisco and/or its affiliates. All rights reserved.

June 2015