Cisco RF Gateway 1 Software Release 6.02.05 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software version 6.02.05 is a rebuild release for the 6.02.03 release.

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

There are no new features in this release.

Resolved Issues

Specific Issues

The following issue is resolved in this release.

ID	Description
CSCup78962	The RF Gateway 1 fails to encrypt the session due to a heavy burst after the system reboots.

Note: The following information applies to customers who have already upgraded to 6.01.02.

- The Broadcast Scrambling UI Flag was introduced in release 6.01.02 for controlling the GQI functionality of the RFGW-1. This flag was available on the System Page of the RFGW-1 web UI. This flag was removed to support the version compactness of GQI functionality from release 6.01.04 onward.
- The Dual Encryption Flag was introduced in 6.01.02 for controlling the total number of QAM channels. The flag was available on the System Page of the RFGW-1 in version 6.01.02. This flag was removed from release 6.01.04 onward.
- The default behavior for controlling the Audio and Video streaming during the encryption process, and in case of encryption failure, is *Clear*. If the previous release is 5.1.xx, and only then, the default value is *Black*.

Known Issues

ID	Severity	Description
CSCua16290	4	For simulcrypt applications, not all possible PID mismatch errors between the DNCS and the DCM will be detected. One such undetected error is when the DNCS and DCM PIDs are mismatched.
CSCub72868	5	The QAM output oversubscription firmware cannot detect bandwidth excursions above 170%, resulting in missed oversubscription alarms and failures to display, in red, the bandwidth horizontal bar graph on the GUI summary page. Once the bandwidth returns to less than 125%, the issue clears.
CSCuc30036	4	The display PIDs in hex function doesn't work consistently on the Scrambler/SCG Details page. Don't check the hex display function.
CSCuc32960	3	For continuous feed scrambling applications, if the DNCS qamManager process is stopped, the RFGW-1 is rebooted, and then after about 5 minutes, the qamManager process restarts, but the CF sessions don't restart on the RFGW-1. A reboot of the RFGW-1 clears the issue.
CSCuc35255	3	For applications with encrypted unicast continuous feed sessions, STB debug screens will periodically indicate stream errors even though the streams are error free.
CSCuc37103	3	For scrambling applications, scrambling alarms will be observed during bootup after rebooting the RFGW-1. The alarms are cleared shortly thereafter and the video will be properly delivered to and decoded by the STBs.
CSCud50641	3	For TBV applications, MPTS data PIDs are sometimes errorneously replicated and routed to another channel in addition to the intended channel. This is a very rare occurrence and has been observed by a single customer at a single site. A reboot of the RFGW-1 will clear the issue.
CSCud55505 CSCud55526 CSCud55562	4	For applications using sysLog, due to a issue with the sysLog server IP Address logic, it is necessary to disable and the reeanble sysLog when the IP address is entered for the first time or whenever it is changed thereafter. Please refer to System/Configuration/Logs/Syslog Configuration page on the GUI.
CSCud81461	5	The "Current Active Port" display on the IP Network page is not applicable and should be ignored in socket redundancy mode of operation. Please ignore it.

Known Issues

ID	Severity	Description
CSCud90203	3	For simulcrypt applications, if sessions are torn down, the RFGW-1 is rebooted, and then the sessions are rebuilt in a different order, an output PID mismatch issue will occur, usually on the audio PID. The issue can be cleared by rebooting RFGW-1 between one and two times.

Image Information

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

File Name	Size (in Bytes)
app_06.02.05.gz	4836476
becks_06.01.19_fw.gz	2645862
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_06_02_05.xml	1689
miller_lite_05.01.20_fw.gz	56807
superfly_04.04.06_fw.gz	1421717
CISCO-RFGW-1-MIB.my	228683
V06.02.05.zip (Compressed file containing all of the files above minus the MIB files)	17488125

Note:

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V06.02.05.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 V06.02.05.zip is 7848d8b3582c52defefb8a18ae930f60.

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 RFGW-1 unit running release 1.02.20 or higher can be upgraded directly to 6.01.07. Refer to Chapter 3, *General Configuration and Monitoring (Release Management)* of the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01, for more information.

The RFGW-1 reboots automatically at the end of the upgrade process. However, when upgrading to 6.02.05 from 1.02.09, an intermediate step is required: use bridge release 1.02.19 to upgrade to final release 1.02.20, and from there, to 6.02.05. The bridge release designated as 1.02.19 has been created to provide a secure and robust upgrade path. Bridge release 1.02.19 and final release 1.02.20 have identical user features and functionality.

WARNING:

Upgrading to 1.02.20 or 6.xx.xx directly from 1.02.09 must not be attempted. This may cause the RF Gateway 1 to be non-operational.

When upgrading an RFGW-1 unit running release 5.1.x to release 6.02.05, you must update through the intermediate bridge release designated as 5.01.11. Upgrading without the bridge release may cause errors when the QAM manager process runs on the DNCS.

WARNING:

Do not upgrade from any engineering release. Revert to the previous official release, save the configuration, and then perform an upgrade to the latest official release.

For example, if the active release is 6.1.2_C1 (Engineering build), revert to release 6.1.2, click SAVE (to save the configuration), and then download and activate release 6.1.6.

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

August 19, 2014