# Cisco RF Gateway 1 Software Release 6.01.07 Release Note

## Overview

### Introduction

Cisco RF Gateway 1 (RFGW-1) software release 6.01.07 contains several enhancements relative to RFGW-1 software release 6.01.06.

### 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 4024958

### 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

## Summary of Defects

This release mainly addresses the following issues:

- Several problems were noted when the RFGW-1 was operating in Socket redundancy mode.
- The RFGW-1 stopped responding to new sessions after a few hours of operation when encrypted VOD sessions (very short sessions) were churned at a very high rate with DNCS Draco (6.0.x).
- Input stream processing in the RFGW-1 became corrupted when the RFGW-1 received **create session** requests with the UDP port number specified as 0, and the states of the input streams are inconsistent from that point onward.

## Specific Issues

The following issues are resolved in this release.

| ID | Description |
|---|---|
| CSCui19630 | When the RFGW-1 receives **create session** requests with the UDP port number specified as 0, the Input Stream Processing in the RFGW-1 becomes corrupted and the states of the input streams are inconsistent from that point onward.<br>Even if subsequent session creation requests have valid UDP port numbers, scrambling does not start because the RFGW-1 is in an inconsistent state. |
| CSCui45129 | When using link, UDP, and TS socket loss detection mode and switching manually to input port 2, some incoming multicast streams are not being mapped to the output from input port 2. Instead, the software continues trying to take them from port 1. |
| CSCui45252 | Loss of PAT and PMT occurs when switching to the backup port at the output. |
| CSCui34704 | Data multicast stream fails on Socket redundancy. After configuring for Socket redundancy, the data stream pumped in multicast IP fails to switch to the backup port. |
| CSCuh27908 | An intermittent problem occurs with oversubscribed channels reported by one customer. It appears that the PIDs from the input are misrouted to the output, causing this overload. |
| CSCuj00674 | Loss of output occurs with SPTS replication on socket switching. |
| CSCuj06000 | An unreferenced program occurs in PAT after socket switching. |

| ID | Description |
|---|---|
| CSCuj09953 | After encrypted VOD usage for 150,000+ sessions during a churn test, VOD failures result and cause an internal software error response from the RFGW-1. |

**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

The following table lists the issues found during system verification testing. These issues will be fixed in subsequent releases.

**Note:** These issues can be viewed using the Bug Toolkit. For more information, see ***Bug Toolkit*** (on page 9).

| ID | Severity | Description |
|---|---|---|
| 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. |
| 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. |
| CSCud50641 | 3 | For TBV applications, MPTS data PIDs are sometimes erroneously 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. |
| 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. |
| 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 is restarted, the CF sessions don't restart on the RFGW-1. A reboot of the RFGW-1 will clear the issue. |
| CSCub47068 | 3 | For DOCSIS applications, Depi Latency Measurement doesn't work with the 3G60 line card. The delay remains at the default value of 550 microseconds and, depending on network latency, will need to be manually adjusted. |
| CSCud55562<br>CSCud55505<br>CSCud55526 | 4 | For applications using sysLog, due to an issue with the sysLog server IP Address logic, it is necessary to disable and the re-enable sysLog when the IP address is entered for the first time or whenever it is changed thereafter. Refer to System/Configuration/Logs/Syslog Configuration page on the GUI. |
| 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 the case where the DNCS and DCM PIDs are mismatched. |

| ID | Severity | Description |
|---|---|---|
| CSCud69623 | 4 | For TBV applications, the PMV entry validation logic has an issue which permits entry of values exceeding 255. It is the user's responsibility to limit the PMV entry to 255 or less to prevent invalid output PID assignments. |
| CSCub67221 | 4 | The "Change Password" link at the lower left corner of the RFGW1-D Login popup doesn't work. To change the password, log in as an administrator. |
| 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. |
| 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. |
| 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 will clear. |

# Image Information

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

| File Name | Size (in Bytes) |
|---|---|
| app_06.01.07.gz | 4812504 |
| becks_06.01.16_fw.gz | 2731945 |
| 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_01_06.xml | 1689 |
| miller_lite_05.01.20_fw.gz | 56807 |
| superfly_04.04.06_fw.gz | 1421717 |
| CISCO-RFGW-1-MIB.my | 223,243 |
| V06.01.07.zip (Compressed file containing all of the files above minus the MIB files) | 17,521,110 |

**Note:**

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V06.01.07.zip is the compressed file of all the image components excluding the MIB files. If using this compressed file, you must uncompress it before uploading into RFGW-1.
- The calculated MD5 checksum for V06.01.07.zip is db271b645309f9478113d49232fa2d2d.

# Bug Toolkit

Follow these instructions to log on to the Bug Toolkit. After you have logged on, you can search for all bugs in this release, search for a specific bug or search, for bugs using specific criteria.

1. Go to **http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl**.
2. When prompted, log on with your user name and password. The Bug Toolkit page opens.

   **Note**: If you have not set up an account on Cisco.com, click **Register Now** and follow the on-screen instructions to register.

## Search for a Specific Bug

1. In the **Search for Bug ID** field, enter the ID of the bug you want to view and click **Go**.
2. The Bug Toolkit displays information about the bug in the **Search Bugs** tab.

## Search for All Bugs in This Release

1. To search for all the bugs in this release, enter the following search criteria in the **Search Bugs** tab:
   - Select Product Category: Select **Video**.
   - Select Products: Select **Cisco RF Gateway Series**.
   - Software Version: Select **6.1** to view the list of bugs in this release.
2. Click **Search**. The Bug Toolkit displays the list of bugs for this release.

# 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 6.01.07 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 6.01.07. 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 6.01.04 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 6.01.07, you must update through the intermediate bridge release designated as 5.01.13. 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, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

**Americas Headquarters**
Cisco Systems, Inc. http://www.cisco.com
170 West Tasman Drive Tel: 408 526-4000
San Jose, CA 95134-1706 800 553-6387
USA Fax: 408 527-0883

October 2013 Part Number OL-30670-01