



# Cisco RF Gateway 1 Software Release 6.03.01 Release Note

## Overview

### Introduction

Cisco RF Gateway 1 (RFGW-1) software version 6.03.01 contains several improvements from release 6.02.01. This release also includes the PID Remapping feature.

### 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 Issues ..... 4
- Known Issues ..... 7
- Image Information..... 8
- Bug Toolkit ..... 9
- Upgrade Information ..... 10

## New Features

PID Remapping is a new feature described in this release.

### PID Remapping

#### Unreferenced PID map

This feature allows the operator to

- 1 Remap unreferenced PIDs from a data stream or a MPTS stream.
- 2 Block specific unreferenced PIDs from a data stream or a MPTS stream.
- 3 Block all the unreferenced PIDs from a data stream or a MPTS stream.
- 4 PID remapping is implemented on a QAM channel level.

This feature can be used to insert SI data from an external data stream which carries the SI data on different PIDs and then can be remapped to standard PIDs

Addressed as part of CSCum87960: Unreferenced PIDs remapping for MPTS and data streams

#### External PAT Insertion

This feature enables the operator to insert an external PAT from a data stream to account for the locally inserted channels or channels from different sources. This feature can be enabled for the channel configured as "Video" in the QAMs page in RFGW Web UI.

This feature supports the functions below.

- 1 SI PIDs (NIT, SDT, BAT, PAT, PMT) from the data stream
- 2 PMT PIDs from SPTS and MPTS streams
- 3 Blocking PMT PIDs in the SPTS and MPTS stream
- 4 Blocking PAT from the input stream and Blocking PAT generated by the RFGW-1
- 5 This feature is implemented at the QAM channel level

Addressed as part of CSCun31168:- Support Insertion on External PAT

Refer to the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01 for details on configuring these features.

## Resolved Issues

### Summary of Defects

This release addresses the following issues:

- In the Tier-based scrambling setup, the STB is unable to descramble the encrypted AC-3 Audio streamed by the RFGW-1.
- Ingress All setting on RFGW-1 (UDP Pass through code) duplicate output sessions are seen.
- RFGW1 sending null public key. This was noticed during the CVC DNCS crash analysis. The RFGW-1 sends null public key and therefore causes the dnscs qamManager process to crash.
- Some of the UI issues are addressed in this release.

### Specific Issues

The following issues are resolved in this release.

ID	Description
CSCuf50763	Summary Page shows Invalid Status for the CA Port is a UI issue and the functionality is not broken. This issue is observed in RFGW 03.02.06 as well. The only difference between 03.02.06 and 06.01.xx build is that CA port is always set to "ON: i.e. linkup" by default in 03.02.06 and in 06.01.xx it is "Off:Link down" by default.
CSCun78489	STB unable to descramble the encrypted AC-3 Audio streamed by RFGW-1  In the Tier-based scrambling setup, when the Customer orders VoD content, the RFGW-1 would stream it in the Clear until the CryptoPeriod Boundary and then starts scrambling the content in the next CryptoPeriod after updating the CA Descriptor in the PMT. The STB is having a problem with the 'Clear -> Encrypted' transition
CSCum79899	In Simulcrypt HE PK sessions are created using DNCS CW ClearExt Alarms not cleared
CSCul68518	Wrong interaction between Ingress all and VOD session timeout features
CSCum46243	RFGW1 sending null public key This was noticed during CVC DNCS crash analysis. The RFGW1 sends null public key and it causing to crash the dnscs qamManager process and under the condition :RFGW1 powered on and DNCS bounce qamManager, runs auditqam query, toggle SRM IP

ID	Description
CSCum62252	User is able to modify changes to Alarm Configuration. Alarm Configuration applied successfully even without admin login
CSCty26751	Monitor Output table should be sorted by Output port/channel
CSCum93042	Refresh All Sessions button should be removed from non Simulcrypt sessions and for 6.x.x branch. It is applicable only for 5.x.x branch
CSCum34691	When DCM sources to create over-subscription in RFGW1 i.e. create an over-subscription in many (as many as 30-40) channel of RFGW1 output. RFGW1 goes for a continuous reboot since most of process time is wasted in logging 'stream_log.txt'
CSCuh31956	Stream map rules entries reset when Reset in stream map table is clicked.
CSCuc95302	When the the CA port is disconnected from the cable, there should be an alarm generated. The Summary page displays the unit rear panel with the conditional access (CA) port enabled/disabled as green/gray. This represents the on/off setting and not the actual link status.
CSCug99124	RFGW1 always return MSK error from CreateSessionV3 although it's a VoD session in Draco
CSCtz67108	RFGW-1 A6 fails to launch 80% of sessions if one bad udp port number present in session list such as udp Port 65536 or Port 0.
CSCun13536	RFGW1 passthrough duplicate output sessions. If you disable (or remove) the input source the RFGW will loss it output, which is to be expected. If you then re-enable the source, the RFGW1 will ingest both at the same time.
CSCun18011	The Encrypted content streaming in clear if the GQI session is created without CA Blob.
CSCun01822	RFGW1: MAPS tab, Stream Map table: After selecting any entry, the navigation bar on the right overlaps the content of the last column.
CSCun01844 CSCuc30036	The display PIDs in hex function doesn't work consistently on the Scrambler/SCG Details page. SCG Details shows -1 for ES PIDs after checking Display in hex checkbox.
CSCuj28641	Recent issues with USRM disconnects to gateways brought to light we do not log the loss of the Management port connection on the RFGW-1. Added this port connection loss to Terse logs
CSCun32660	Data sessions are in Stream active state when content has stopped flowing. Also data sessions don't switch to the backup port in redundancy configuration.
CSCum99606	D6 Comm Setting Ping is both Successful and Unsuccessful. A ping sent to the same device shows both successful and unsuccessful. Expected unsuccessful because there is no IP Address and it is not enabled.

## Resolved Issues

ID	Description
CSCty27051 CSCtz86709	GbE port LED not lit and GbE Absent indication on Summary page
CSCub64406	NonConfiguredStreams UI display not consistent with other pages
CSCuc17411	RFGW-1 WUI - Monitor input/output tables not in correct position
CSCuo03848	When there is a Bulk Change of AppMode from SDV to Video, RFGW-1 crashes randomly when ingress all feature is enabled.

**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
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 usecs and, depending on network latency, will need to be manually adjusted.
CSCud55562 CSCud55505 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. 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.
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_06.03.01.gz	4877680
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_03_01.xml	1689
miller_lite_05.01.20_fw.gz	56807
superfly_04.04.06_fw.gz	1421717
CISCO-RFGW-1-MIB.my	238364
V06.03.01.zip (Compressed file containing all of the files above minus the MIB files)	17502587

**Note:**

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V06.03.01.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 V06.03.01.zip is 8859c3cd82965795d4b46bd31f978531.



## 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 6.03.01 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 6.03.01. 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 6.03.01, 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

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](http://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.

© 2014 Cisco and/or its affiliates. All rights reserved.

April 2014

Part Number OL-31942-01