CISCO™

Cisco RF Gateway 1 Software Release 6.04.04 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software version 6.04.04 includes enhancements and also provides support for new features.

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

1. Socket Redundancy Enhancements

   a. When the stream's PCR PID's bitrate goes to zero, it will be treated as content loss and a stream switch will be initiated based on Socket Redundancy Priorities (Port switching has higher priority than source switching). This feature will work only for SPTS Streams with valid PCR reference in the PMT.

   b. An UI option is provided to manually switch a stream to the next port in the port pair (based on socket redundancy priorities).

   c. Please refer section GbE Interface Operation Modes in RFGW-1 configuration guide at the location http://www.cisco.com/c/dam/en/us/td/docs/video/OVP/RFGW _1/Cisco-RF-Gateway-1-Configuration-Guide.pdf

   d. This is implemented using the CDETS "CSCup51508 - SRE: Manual Stream Switching and Treat PCR zero bitrate as Content loss"

2. UDTA Enablement support.

   a. This feature contains the implementation for the in band control/PSIP/EAS support which is required in the UDTA environment to merge the PSIP and EAS information carried over the 0x1FFB PID. Please refer section "New Field in Stream map for UDTA enablement from V06.04.XX" in RFGW-1 configuration guide at the location http://www.cisco.com/c/dam/en/us/td/docs/video/OVP/RFGW _1/Cisco-RF-Gateway-1-Configuration-Guide.pdf

   b. This is implemented using the CDETS "CSCup09826 UDTA PSIP EAS aggregation support "

Resolved Issues

Specific Issues

The following issues are resolved in this release.

ID	Description
CSCup51508	This is a new feature request.SRE: Manual Stream Switching and Treat PCR zero bitrate as Content loss. For more details refer 'New Feature' Section.
CSCup09826	UDTA PSIP EAS aggregation support. This is a new feature request. For more details refer 'New Feature' Section.
CSCuo28537	Overrule Hint Bit Stop Delay setting in now provided in Advanced Page along SNMP Support .
CSCuo14126	QAM port control off - no CMs locking /RFGW1-Port control is not correct when channels are in Depi-Learn mode
CSCup56197	Streams not recovering when current active port is changed in Manual Red
CSCup65798	RFGW-1: PAT Pid index does not get de-allocated while stream shuts down. This could lead to PAT Pid Index Leak
CSCur30911	Upgrade to 6.3.x causes intermittent scrambling failure
CSCur30494	SSM Source Switching stops and stream is stuck in invalid state
CSCuo06033	Stream goes in clear for pk encrypted session on sending override when stream is not present and could lead result in stream getting stuck in un encrypted state.
CSCup71979	When updgrading software from 3.1.6 to 6.X.X the PAT / PMT repeat rate is not being retained and overriden with default value of 10.
CSCug76776	In Tier-based scrambling setup, all PID are expected to be scrambled. But when video PID is block, then scrambling fails & audio PIDS goes are clear.
CSCup78962	The RFGW-1 fails to encrypt sessions, when a voD churn is running and the RFGW-1 is rebooted. This cause the RFGW-1 to playout the ES pids in the clear without a PMT. The RFGW-1 issue is triggered when there is a burst of GQI commands issued by the DNCS, which are queued up in the DNCS by the RFGW-1 Reboot.

ID	Description
CSCtz50091	Manually selecting the PCR reference PID for dejittering incoming MPTS streams does not work. This functionality is now supported
CSCup15237	Multicast traffic over flows when changing redundancy mode from auto to manual. Streams configured on port pair 1 are shown in Non configured list
CSCuq73640	This issue is due to the route of PID 0 getting corrupted because of the source glitch. 2 PATs (one regenerated on rfgw , and another passed through from source) are played out. If the input source is stopped and started , PAT play out recoversDuplicate PAT play out when transient ES pid comes in with pid 0.
CSCuq85344	Stream switch not working for data stream in Socket Redundancy
CSCuq89802	Sock_red fails for data stream if stream is not present in primary port
CSCun07281	The details in 'ABOUT' page in RFGW-1 are old. This information is now corrected.
CSCul78114	In WebUI, Input program details shows zero bit rate for some streams No issues at RF output side, only issue in WebUI
CSCuo01277	After remove RFGW1 DVB License by uploading another license and leaving DVB license entry blank, the RFGW1 prints error logs. No functionality is affected only prints error message.
CSCuj55944	Wrong values on ifHCOutOctets. The problem is that the 64 bit counters are not updated correctly. This invloves changes in Duvel FPGA
CSCum34618	Input Bandwidth Overflow due to wrong IGMP joins
CSCue10169	AJAX - Unable to modify QAM freq from GUI when in manual + control DEPI
CSCud81461	Current active port is not applicable in socket redundancy mode and is hidden in this scenario.

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.
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.
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.
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	4	Sometimes logs are not written into syslog server when the IP address is either being entered the first time or has been changed.

Test Summary

Sanity Test

SNO	TEST	Automatic/Manual	Pass/Fail Status
1	Verification Pk Broadcast in DRACO headend	Manual	Passed
2	Verification of SDV in USRM headend	Manual	Passed
3	Verification of video using UDTA on DTACS setup	Manual	Passed
4	Verification of DVB scrambling using NDS CAS	Manual	Passed
5	DEPI head end verification	Manual	Passed

Functional 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, RF test, Configuration backup/Restore test)	Manual	Passed	150
3	Socket Redundancy & Stream redundancy test cases(manual redundancy, multicast redundancy, dual mc join)	Manual	Passed	39
4	PK Broadcast test	Manual	Passed	20
5	Table based video test	Manual	Passed	120
6	GQI Announce test	Manual	Passed	12
7	DVB Scrambling	Manual	Passed	189
8	GbE port redundancy test	Manual	Passed	20
9	Tier Based Scrambling test	Manual	Passed	32
10	PCR functional test	Manual	Passed	15
11	Socket Redundancy Enhancement with PCR based stream switching & support of Manual stream switching	Manual	Passed	85
12	ECM Load balancing	Manual	Passed	16
13	EAS-PSIP merge functional test (UDTA)	Manual	Passed	60

Migration Test

SNO	TEST	Automatic/Manual	Pass/Fail Status

1	Upgrade and downgrade test from V06.04.04to the releases below and reverted. (V02.02.24, V03.01.08, V06.01.07, V06.02.03, V06.03.01 and V06.03.03)	Manual	Passed

Automation Test

SNO	TEST	Feature	Automatic/Manual	Pass/Fail Status
1	Churn test GQI v3 PK encrypted using tools with 10 sessions/second	GQI V3	Automatic	Passed
2	Churn test GQI v2 clear using tools with 10 sessions/second	GQI V2	Automatic	Passed
3	Churn test GQI v2 PK encrypted using tools with 10 sessions/second	GQI V2	Automatic	Passed
4	Churn test GQI v3 VOD using tools with 13 sessions/second	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_06.04.04.gz	4906560
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_06.01.14_fw.gz	2630322
rfgw1_rel_06_04_04.xml	1689
miller_lite_05.01.21_fw.gz	54398
superfly_04.04.06_fw.gz	1421717
CISCO-RFGW-1-MIB.my	239767
V06.04.04.zip (Compressed file containing all of the files above minus the MIB files)	17468408

Note:

- The image files should be downloaded using the FTP Server in BINARY mode only.

- V06.04.04.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 V06.04.04.zip is c11c5093d297ebf8333587750f2322ee.

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 any 06.XX.XX release. (Example: 06.01.07, 06.03.03). 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 any release 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 any release. The bridge release 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.**

> ⚠️ **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.