Cisco RF Gateway 1 Software Release 06.04.09 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software version 06.04.09 mainly addresses few issues reported from the field and minor software enhancement.

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

SNMP support for Enabling/Disabling smart fan control

This enhancement request is addressed as part of **CSCuw55304** - Adding SNMP support for smart fan control. This is the SNMP OID addition for enabling/disabling Smart fan feature.

Configuration support to turn on/off NCS CAM events

When there are unexplained short sessions in GQI VOD or overloading of multicast IP addresses in a broadcast, there are lots of NCS CAM Trap messages flood the monitoring system of customers. This feature will provide GUI option to turn on/off NCS CAM events and is addressed as part of **CSCus98261**.

Resolved Issues

Specific Issues

The following issues are resolved in this release.

ID	Description
CSCuv62774	RFGW1 reboots for a specific stream when the session ends. The reboot is triggered by watchdog after stream manager crashes. This is very rare condition.
CSCuu69887	EIS Override SCG is not persistent across reboot.
CSCuy21249	GUI allows incorrect changing of interleaver settings in ITU A
CSCuy24776	Radius login disable telnet and FTP access to the RFGW1 after performing some >1000 login/logout
CSCuv56815	The RFGW1 6.4.4 version alarms “CW for CP 65535 not found “is seen this is due to session’s overrides and short sessions.
CSCur37696	Issue in enabling "Insert External PAT PID" for specific QAM channels
CSCuy88545	IPPV encrypted sessions not working. Mainly for Powerkey only sessions are not working due to over rides

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.
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

HE Verification 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

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, RF test, Configuration backup/Restore test)	Manual	Passed	65
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	DVB Scrambling	Manual	Passed	10
7	GbE port redundancy test	Manual	Passed	20
8	PCR functional test	Manual	Passed	15
9	Socket Redundancy Enhancement with PCR based stream switching & support of Manual stream switching	Manual	Passed	5
10	EAS-PSIP merge functional test (UDTA)	Manual	Passed	30
11	Alarm filter	Manual	Passed	32
12	DEPI	Manual	Passed	17
13	Authentication	Manual	Passed	4
14	Configure Session time out	Manual	Passed	3
15	Unreferenced PID remap / External PAT insertion	Manual	Passed	4
16	SNMP test	Manual	Passed	3

Migration Test

SNO	TEST	Automatic/Manual	Pass/Fail Status
1	Upgrade and downgrade test from V06.04.09 to the releases below and reverted. (V02.02.26, V03.01.08, V06.01.07, V06.02.03, V06.03.03 and V06.04.05)	Automatic	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

Image Information

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

File Name	Size (in Bytes)
app_06.04.09.gz	4904500
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_09.xml	1689
miller_lite_05.01.21_fw.gz	54398
superfly_04.04.06_fw.gz	1421717
CISCO-RFGW-1-MIB.my	240329
V06.04.09.zip (Compressed file containing all of the files above minus the MIB files)	17468837

Note:

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V06.04.09.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 V06.04.09.zip is 2be48d3a84174f34f72c99999f38feea.

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.

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

First Published: August 2016