Cisco RF Gateway 1 Software Release 6.01.06 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software version 6.01.06 is a rebuild release of 6.01.02 which addresses field and interoperability issues found during a new DRACO (DNCS) release. This release also introduces the Variable Fan speed 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 4025112
- *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

Variable Fan Speed

Variable Fan Speed based on the temperature: Currently, the fan runs at full speed (setting is 255) irrespective of temperature. Some customers informed us that the noise level is on the higher side. Hence this feature was introduced.

Below are the key design elements:

- GUI option "Smart Fan Control" is added on the System page of the RFGW-1.
- It has two options:
  - Enabled: The FAN speed will change based on the measured temperatures.
  - Disabled: The FAN will always run at FULL Speed..
- This feature is DISABLED by default.
- When Smart Fan Control changes to "Enable," there will be a 30 second delay before changing the FAN Speed to avoid any FAN related alarms.
- Disabling the Smart Fan Control will make all fans operate at full speed immediately.
- This feature flag is unit specific and will not be carried forward to other units when using the backup configuration file.
- Based on the temperature, the fan control settings will vary from 150<->175<->255. GUI logs indicate these changes.

Fan Control Settings	Highest Temperature (in Centigrade)
150	< 65
175	> = 65 and < 74
255	> = 74

- During RFGW-1 boot up, the fan will run at full speed (setting 255) for at least 5 minutes. This allows the boot process to be complete and the RFGW-1 to be configured completely.
- Temperature readings are taken every 10 seconds from various measuring points. Out of these readings, the highest temperature will be recorded.
- If temperature increases, the fan speed will increase immediately to the specified setting (see above)
- Lowering the fan speed will be applied after 10 minutes from the point of increase in fan speed. This design is intended to reduce toggling of the fan speed thereby increasing the life of the fan.
- Alarms will be raised based on the speed/rpm out of tolerance (existing design)

- When there is any fan failure or fan running at very low speed, the software will kick start all the fans at full speed (255).
- There are fail safe mechanisms in place when the software fails/hangs.

This feature is addressed in CSCui14544

Resolved Issues

The following issues are resolved in version 6.01.06:

ID	Description
CSCug46530	The non-cable Card STB running the Rovi Application reboots when it is descrambling the encrypted VOD content that is streamed by the RFGW-1. The 'Hint Bit' would now be cleared in the PowerKEY ECM's based on the value of the 'Hint Bit Stop Delay' field in the DB. The default value would be -600 msecs. **Note:** If the encrypted content is to be streamed for the Rovi STB's: It must set 'Hint Bit Stop Delay' as -400 msecs The 'Overrule Hint Bit Stop Delay' flag must be set to 'True' for the STB's to descramble the content without any issues. This field is configurable from the GUI. ['Scrambler->ECMG Configuration' Page for the Internal PK ECMG]
CSCuh27821	When a program is removed from an MPTS stream, the RFGW output stream still holds the program that was removed in PAT.
CSCzk50477/ CSCuh48603	System uptime is observed to be incorrect over time. The system uptime in system configuration page rolls over after 49 days of continuous usage.
CSCuc17414	Session IDs are longer and are missing source IDs in the WEB GUI.
CSCui04198	RFGW - 1 GUI shows incorrect values for rx/tx bytes, unicast packets. Total number of packets and number of unicast packets found to increase but it wraps around after a certain value.
CSCuf44668	The STB is not able to descramble services when the software version of the RFGW-1 operating in the 'Tier-based' Scrambling Mode is upgraded from version 03.02.06 to 06.01.02.
CSCug26833	The Active Core Encryption Algorithm field in the **System->Scrambler** Page does not always display the current Active Core Encryption Algorithym that the RFGW-1 actually supports.
CSCug45803/ CSCud52927	Revert to primary should not work in redundancy mode but its reverting to primary when traffic is received.
CSCug42900	When Both unicast & mulitcast are configured with same UDP port nuThe 'tCpuResrcMonitor' task crashed due to a data storage exception and the Watchdog rebooted the RFGW-1. The issue was reported by CVC.mber, session getting configured only for multicast stream & not unicast.

ID	Description
CSCug68098	The 'tCpuResrcMonitor' task crashed due to a data storage exception and the Watchdog rebooted the RFGW-1. The issue was reported by CVC.
CSCtx89720:	The upper four center frequencies of each RF port are reported incorrectly by the DOCSIS-IF-MIB. Occurs only when the 8 channel per license is installed and only when the DOCSIS-IF-MIB is used to read the center frequencies of the upper [5-8] RF channels.
CSCud55197	Inventory Page displays incorrect SW Version of QAM Card during Page Refresh. This issue was reported by one customer.
CSCua02831	A single QAM channel on an RFGW-1 fails in a manner such that it can no longer deliver VOD streams that STBs can decrypt. The frequency of occurrence is rare, about once a week for several hundred RFGW-1's. The issue occurred with one customer.
CSCud65293:	Broadcast scrambling disabled, no sessions can be setup on GQIv3 DNCS. This "seems" to only affect DNCS that has GQIv3 capability (4.4.1 and 6.0.). For non-GQIv3 capable DNCS such as DNCS 5.0, it is possible to build source definitions with broadcast scrambling disabled
CSCuc74154	GQI V3 Encrypted VOD session streaming in clear, if VOD and clear broadcast sessions configured in same RFGW-1
CSCuf01534/ CSCuf16523:	The STB is unable to descramble the content intermittently for a few seconds and the 'not authorized' message appears on the STB with V6.02.01 upgraded units.
CSCud69623	For TBV applications, the PMV entry validation logic has an issue which permits the entry of values exceeding 255. The user must limit the PMV entry to 255 or less to prevent invalid output PID assignments.

Note: The information below is applicable to customers who have already upgraded to 6.01.02.

- Broadcast Scrambling UI Flag was introduced in 6.01.02, for controlling the GQI functionality of RFGW-1. The flag was available on the System Page of the RFGW-1 web UI. The GUI flag “Broadcast Scrambling” has been removed for supporting the version compactness of GQI in the 6.01.04 release.
- 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. In version 6.01.06, the flag is removed.
- The default behavior for controlling the Audio and Video streaming during the encryption process and in case of encryption failure will be *Clear*. Only if the previous release is 5.1.xx, will the default value be *Black*.

Known Issues

Below is a list of issues found during system verification testing. The issues can be viewed using the Bug Toolkit. For more information, see Bug Toolkit.

The following table is a list of issues that will be fixed in subsequent releases:

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 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.
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 wil 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 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.
CSCua16290	4	For simulcrypt applications, not all possible PID mismatch errors between the DNCS and the DCM wiil 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

Below are the details of files and its size for V06.01.06 release.

File Name	Size (in Bytes)
app_06.01.06.gz	4,814,120
becks_06.01.16_fw.gz	2,731,945
bootrom_V5_02.05.00.bin	2,097,152
coors_05.00.27_fw.gz	2,845,585
dual_moretti_07.01.04_06.01.05_fw.gz	5,440,797
duvel_06.01.13_fw.gz	2,681,608
rfgw1_rel_06_01_06.xml	1,689
miller_lite_05.01.20_fw.gz	56,807
superfly_04.04.06_fw.gz	1,421,717
CISCO-RFGW-1-MIB.my	223,243
V06.01.06.zip (Compressed file of above files)	17,417,730

NOTE:

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V06.01.06.zip is the compressed file of all the image components excluding the Mib files. If using this compressed file, the user needs to un-compress it before uploading into RFGW-1.

Log On to the 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 RF Gateway 1 unit running release 1.02.20 or higher can be upgraded directly to 6.01.04. Refer to Chapter 3, *General Configuration and Monitoring (Release Management)* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112, for more information. The RF Gateway 1 reboots automatically at the end of the upgrade process. However, when upgrading to 6.01.04 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 6.01.04 must be followed. The bridge release designated as 1.02.19 has been created to provide a secure and robust upgrade path. Releases 1.02.19 (bridge) and 1.02.20 (final) 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.

An RF Gateway unit running release 5.1.x upgrading to 6.01.04 must update through an 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 back 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) follow the procedure below:

Revert back to release 6.1.2, click SAVE (to save the configuration) 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.
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 2013 Part Number OL-29933-01