Cisco RF Gateway 1 Software Release 6.01.02 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software version 6.01.02 consolidates all the existing RFGW-1 branches into one release, and adds new features, such as, Downstream External PHY Interface Control Plane, Socket Redundancy, and Next Generation On Demand.

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

The following new features are included in software version 6.01.02:

- Downstream External PHY Interface - Control Plane (DEPI - CP)

  In the past, the DEPI sessions were statically mapped in RFGW-1. Now, with the introduction of DEPI-CP, the DEPI sessions are configured from M-CMTS, in addition to learning QAM channel parameters.
- New configuration option for source selection based on multicast stream status, in addition to the existing Port Level Redundancy in all the RFGW-1 software versions.
- Next Generation On Demand (NGOD)
- Enhanced reporting features, such as, the RFGW-1 web GUI that displays the non-configured streams to the GbE port.
- New UDP alarms are added for managing RFGW-1 from ROSA.

Resolved Issues

The following issues are resolved in version 6.01.02:

ID	Description
CSCtq76123	If a time zone offset from UTC is selected on the RFGW-1 system/clock web GUI page, the encrypted PowerKEY sessions result in black screens on the DHCT. Also, when provisioning the SCG, the SCS uses the system time, not the UTC time.
CSCtz24940	RFGW1:Revert option does not restore all the streams to the primary port. During Socket Redundancy mode, when the Revert To Primary option is selected, only part of the sessions (which are bound to the backup port) recovers back to the primary port. The remaining sessions are still bound to the backup port. To revert all the sessions back to the primary port, you must apply the Revert To Primary option four or five times.
CSCtx79319	QAM bandwidth is incorrectly calculated, leading to throughput issues for DATA streams.
CSCuc71421	The RFGW-1 does not scramble VoD services if the SCG is provisioned with the activation time set to the future, and if the Input UDP Stream is detected at the RFGW-1 between the SCG Provision Time and the Activation Time.
CSCtz13043	The web GUI locks up when a movie ends.
CSCty14370	After reboot, PAT is played out with invalid CRC when NIT is referenced in PAT.

Known Issues

The RFGW-1 version 6.01.02 has moderate severity issues that were found during Cisco System Verification testing. They will be fixed in a subsequent release. The issues can be viewed using the Bug Toolkit. For more information, see ***Bug Toolkit*** (on page 6).

The following table describes minor issues in version 6.01.02:

ID	Severity	Description
CSCud55562 CSCud55505 CSCud55526	4	For applications using sysLog, due to an issue with the sysLog server IP Address validation logic, it is necessary to disable and then re-enable sysLog when the IP address is entered initially or changed by the web GUI (**System > Configuration Logs > Syslog Configuration**).
CSCua16290	4	For simulcrypt applications, not all possible PID mismatch errors between the DNCS and the DCM are detected.
CSCud69623	4	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.
CSCub67221	4	The "Change Password" link at the lower left corner of the RFGW1-D Login screen is non-operational. To change the password, log in as an administrator.
CSCuc30036	4	The display PIDs in hex function does not display consistently on the Scrambler/SCG Details web GUI page. Do not use the hex display function.
CSCud52927	5	The revert to primary option only works in the Link Only redundancy mode, not in the Link + UDP redundancy mode.
CSCud81461	5	The "Current Active Port" display on the IP Network page is not applicable and should be ignored in the socket redundancy mode.
CSCub72868	5	The QAM output oversubscription firmware cannot detect bandwidth excursions above 170%, resulting in missed oversubscription alarms and a failure to display, in red, the bandwidth horizontal bar graph on the Summary web GUI page. Once the bandwidth returns to less than 125%, normal operation resumes.

Bug Toolkit

The Bug Toolkit is an online tool that allows registered users to search for bugs by release or by a bug number.

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 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.

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 Bugs Using Specific Criteria

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 the desired software version number.
   - Select Version Type: Select one of the following options:
     - **Known Affected Version (KAV):** the software version/release assumed to contain this bug
     - **Fixed-in:** the software version/release in which the bug has been fixed

- – **Found-in:** the software version/release in which the bug was first reported
- Search for Keyword(s): Enter desired key words in this field. Separate search phrases with Boolean expressions (**AND**, **NOT**, **OR**) to search within the bug title and details.
- Advanced Options: You can perform a search using the default search criteria, or define custom criteria for an advanced search. To customize the advanced search, select **Use custom settings for severity, status, and others** and provide the following information:
  - – Severity—Select the severity level.
  - – Status—Select any combination of **Terminated**, **Open**, or **Fixed**.
    - Select **Terminated** to view terminated bugs. To filter terminated bugs, clear the Terminated check box and select the appropriate sub-options that appear below the terminated check box. The sub-options are **Closed**, **Junked**, and **Unreproducible**.
    - Select **Open** to view all the open bugs. To filter the open bugs, clear the Open check box and select the appropriate sub-options that appear below the Open check box. The sub-options are **Assigned**, **Forwarded**, **Held**, **Information Required**, **More**, **New**, **Open**, **Postponed**, **Submitted**, and **Waiting**. Select multiple sub-options as required.
    - Select **Fixed** to view fixed bugs. To filter fixed bugs, clear the Fixed check box and select the appropriate sub-options that appear below the fixed check box. The sub-options are **Resolved** and **Verified**.
  - – Advanced—Select the **Show only bugs containing bug details** check box to view only those bugs that contain detailed information, such as symptoms and workarounds.
  - – Modified Date—Select this option if you want to filter bugs by the date they were last modified.
  - – Results Displayed Per Page—Select the appropriate option from the list to restrict the number of results that appear per page

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 6.01.02. 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 6.01.02 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 6.01.02 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 6.01.02 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 6.01.02 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.

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.

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

January 2013 Part Number OL-28796-01