



Cisco RF Gateway 1 Software Release 2.02.24 Release Note

Overview

Introduction

Software Release 2.02.24 fixes seven bugs, two of which may affect output streams.

Purpose

The purpose of this document is to notify RF Gateway 1 users of the bug fixes, and special upgrade procedures needed for release 2.02.24.

Audience

This document is intended for system engineers and 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

- Bug Fixes 3
- Known Issues 4
- Licensing 6
- Upgrade Information 7
- IP Port Configuration Changes..... 8
- Upgrade Procedure for Customers Running 1.02.09 9
- IP Port Configuration Parameter Settings..... 11
- For Information 13

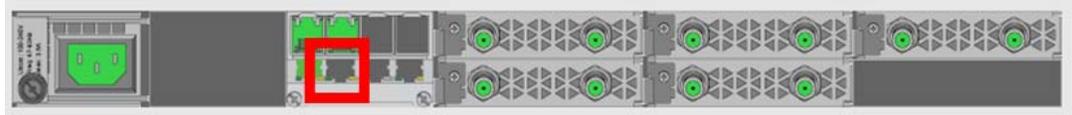
Bug Fixes

- Prior to release 2.02.24, a bug existed that could result in improper output bitrates and CC errors if there were too many VOD start/stops in a row. This bug is fixed in release 2.02.24.
- A bug was found in release 2.02.22 that caused memory corruption when a critical number of MPTS streams were present. This memory corruption caused the RF Gateway 1 to reboot anytime a stream map entry changed. This bug is fixed in release 2.02.24.

Known Issues

The following list identifies known limitations planned to be resolved as part of an upcoming GA release.

- The RF Gateway 1 web interface is not fully tested with IE-8 and Firefox 3.5 or newer. The RF Gateway 1 web management interface is tested with IE-6 or Firefox 2.0.0.14 and above. Use of Java 1.6.x is recommended.
- 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.



- The database restore feature requires disabling trap settings (in the "restore from database file" prior to release 2.01.09) before starting the restore procedure. This can be done before starting a restore configuration in 2.02.24. This step is needed for compatibility with the enhanced SNMPv1 and 2 trap support in this release.
- SNMP community strings are provided to support SNMPv1 and 2 traps. Prior to release 2.01.09, a single community string was applicable for all five trap receivers configurable for the operator. In release 2.02.11 and later, SNMPv1 and 2 traps are supported and each of the five trap receivers has a separate configurable trap community string. This may cause a possible loss of SNMP trap community strings during an upgrade or downgrade procedure. An operator should carefully verify their trap community strings when upgrading to or downgrading from 2.02.24, if they are being used.
- An upgrade to 2.02.24 from pre-release 2.01.09 automatically enables insertion of the Network PID into the PAT. If this is an issue in the user's system, it may be disabled on the *System/System Configuration* page.
- The system uptime counter rolls over to zero after approximately 49 days of continuous use. This behavior manifests on the web management GUI and via SNMP. The rollover does not cause any operational problems or side effects on active services.
Note: A power cycle or reboot of the RF Gateway 1 resets the system uptime counter as part of normal operation.
- The carrier bandwidth as reported by the GUI and SNMP agent may be incorrect up to +1 KHz. This could cause an external resource manager to not utilize all existing bandwidth on a QAM channel. Adjust the external SRM accordingly.
- If an MPTS stream is replicated more than 48 times and if the "Replicated" button on the *Monitor Input* page is clicked, the RF Gateway 1 reboots.
Do not click the "Replicated" button under these conditions.

- If MPTS streams are configured in the RF Gateway 1 and if the “Replicated” button is clicked, a new browser window pops up showing the Replication details. Clicking the “Display PIDs in hex” check box causes garbled data to be displayed. Closing and opening the browser window corrects the issue.
Do not click the “Display PIDs in hex” check box under these conditions.
- If MPTS stream(s) are configured in the RF Gateway 1 with “Ignore UDP Port” set to “True”, and if the “Details” button on the *Monitor Input* page is clicked, the MPTS values are not loaded.
- If a stream (with stream type set to Data) is replicated more than 48 times and if the “Data” node is clicked, the RF Gateway 1’s management port locks up, stopping all Telnet, Web (GUI), SNMP, and GQI services. You will need to power cycle to restore normal operation of the RF Gateway 1.
Do not click the “Data” node under these conditions.
- When rebooting an RF Gateway 1 servicing only multicast traffic, the primary GbE port sometimes ends up as the inactive port (it should be active). The RF Gateway 1 joins the multicast groups only on the current active port. It is possible that by the time (hardcoded to five seconds from the time of link up) the primary port has issued IGMP join and the streams are starting to arrive, the RF Gateway 1 has already switched to the backup port. Use a switch that responds faster than five seconds or switch back to the primary port manually after each boot up.
- When an RF Gateway 1 is configured in Dual Port Pair mode with "Revert to Primary" enabled and detection mode set to "Ethernet Link & UDP or L2TPv3 packets", switching to the primary port does not work. This behavior appears to occur only with this setting. You will need to switch back to the primary port manually under these conditions.
- Auto-refresh does not work for the *Monitor Resource Utilization* page. Refresh this page manually by clicking the "refresh" button.
- When a backup is performed by the ROSA EM, the MPTS stream map rows are transferred to the backup RF Gateway 1 with the output program numbers set to 0. If the user attempts to change the MPTS stream map row on the backup using the GUI, the change fails because 0 is not a valid program number. There’s no issue changing the row with SNMP because the program number is not used for MPTS streams. To change an MPTS stream map row on the backup, change the stream type to SPTS and then change the program number to any number other than zero, and click Apply. Change the stream type back to MPTS and make the other desired changes.

Licensing

After an upgrade to 2.02.24, a system license is required for the following features. Refer to Licensing in the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.

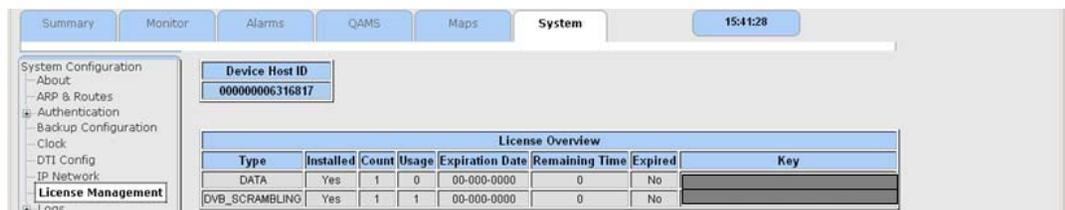
- Data streams requiring use of the DOCSIS® Timing Interface
- DVB® Encryption

Most systems delivered with 1.02.20 or later using a data part number included a license file pre-installed at the factory. For these systems, an FTP transfer is not necessary.

All systems delivered prior to 1.02.20 and some systems delivered with 1.02.20 require a license file. This can be obtained from Cisco after an upgrade to 2.02.24. Contact your account representative for details on obtaining your license files.

Note: Performing an upgrade without a license file will generate an alarm, informing the user that a license file is not present. The unit continues to function until configuration changes are made. However, performing the upgrade may impact functionality of licensed features.

For systems requiring a license upgrade, a licensing capable RF Gateway 1 provides the operator with a new tree menu item, *License Management* located under the **System** tab. See the following screen. The menu provides an FTP mechanism to transfer license files to the device. It is recommended that the operator monitor the file transfer status using feedback from the FTP server.



License Overview							
Type	Installed	Count	Usage	Expiration Date	Remaining Time	Expired	Key
DATA	Yes	1	0	00-000-0000	0	No	
DVB_SCRAMBLING	Yes	1	1	00-000-0000	0	No	

Upgrade Information

An RF Gateway 1 unit running release 1.02.20 can be upgraded directly to 2.02.24. 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 2.02.24 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 2.02.24 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. See *Upgrade Procedure for Customers Running 1.02.09* (on page 9).

**WARNING:**

Upgrading to 1.02.20 or above directly from 1.02.09 must not be attempted. This may cause the RF Gateway 1 to be non-operational.

Refer to Known Issues (on page 4) for SNMP related upgrade, downgrade and database restore considerations.

IP Port Configuration Changes

There is a bug in 1.02.09 that causes the following IP port configuration parameters to have inverted values saved in the configuration file.

- Negotiation Mode (On/Off) - one for each port (total 4)
- Redundancy Mode (Auto/Manual) - one for each port pair (total 2)
- Revert Mode (Enable/Disable) - one for each port pair (total 2)

For details on these parameters, see Chapter 3, *General Configuration and Monitoring* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.

This bug has been corrected in the configuration file in 1.02.19. Upon upgrade to 1.02.19, these three parameters will appear to have changed values as seen in the *System/IP Network* page of the web GUI. As a result, the IP ports may not be configured properly for operation immediately after upgrade (after the subsequent reboot that follows activation.)

See *Upgrade Procedure for Customers Running 1.02.09* (on page 9).

Upgrade Procedure for Customers Running 1.02.09

**WARNING:**

Upgrading to 2.02.24 directly from 1.02.09 must not be attempted. This may cause the RF Gateway 1 to become non-operational.

- 1 Before starting the upgrade, backup the system configuration. Refer to Chapter 3, *General Configuration and Monitoring (Configuration Backup)* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112. Name the file appropriately to identify it as a configuration that corresponds to 1.02.09. This file will be necessary later if the user decides to revert back to 1.02.09.
- 2 Record the IP port configuration parameters by saving a screen capture of the *System/IP Network* page. See *Recording IP Port Configuration Settings* (on page 12).
- 3 Download and activate 1.02.19. Refer to Chapter 3, *General Configuration and Monitoring (Release Management)* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112. The RF Gateway 1 reboots automatically at the end of the upgrade process.
- 4 After reboot, display the *System/IP Network* page. See *Displaying IP Port Configuration Settings* (on page 11).
- 5 Verify the IP port configuration parameters by checking them against those recorded in step 2 (prior to the upgrade as done in step 3). The Negotiation Mode, Redundancy Mode, and Revert Mode parameter values are inverted. See *Displaying IP Port Configuration Settings* (on page 11). Change the differing parameter values to match those recorded before download and activation. Be sure to click **Apply** after making your changes.
- 6 Once step 5 is completed, save the configuration which includes the IP port configuration parameters. Going forward, these values will not change.
- 7 Validate/qualify/soak release 1.02.19 in its application to establish confidence the release is operating at the same level as 1.02.09. In the very unlikely event that service is impacted by 1.02.19, reverting back to 1.02.09 may be done to re-establish operations. If reverting back to 1.02.09 is necessary, the IP port configuration parameters must be swapped back and the configuration saved in step 2 restored.

Upgrade Procedure for Customers Running 1.02.09

- 8 After satisfactory completion of step 7, upgrade from 1.02.19 to 1.02.20. These two releases have identical performance and behavior. Release 1.02.20 includes a boot code upgrade that readily supports future roadmap features/releases without the need for subsequent two-step bridge upgrade processes.
- 9 Download and activate 2.01.09. Refer to Chapter 3, *General Configuration and Monitoring (Release Management)* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112. The RF Gateway 1 reboots automatically at the end of the upgrade process.

IP Port Configuration Parameter Settings

The RF Gateway 1 has four physical GbE input ports that receive video and data streams from the upstream network. These ports may be used independently (in software releases 2.02.22 or later) or configured to implement input redundancy. See Chapter 3, *General Configuration and Monitoring of the Cisco RF Gateway 1 Configuration Guide*, part number 4025112 for specific details.

Displaying IP Port Configuration Settings

Follow these instructions to display the *System/IP Network* page.

- 1 Launch your web browser.
- 2 In the IP Address field, enter the RF Gateway 1 IP address.
- 3 Click **Enter**.
- 4 Click the *System/IP Network* tab and review the IP settings. Refer to the following screen.

The screenshot displays the configuration page for the RF Gateway 1, specifically the *System/IP Network* section. The page is organized into several tables and sections:

- 10/100 Ports:** A table with columns for Management and Conditional Access. It includes fields for Part Control, Address Selection Mode, MAC Address, IP Address, Subnet Mask, and Default Gateway.
- Part Pair Configuration:** A table with columns for Part Pair 1 and Part Pair 2. It includes fields for Video/Data IP, Redundancy Mode (set to 'Auto'), Primary Port, Current Active Port, Redundancy Configuration, Detection Mode, LOS Timeout (h), Revert To Primary (set to 'Enabled'), and Revert Check Time (h).
- GbE Input Ports:** A table with columns for Part 1, Part 2, Part 3, and Part 4. It includes fields for Part Configuration, MAC Address, IP Address, Subnet Mask, and Negotiation Mode (set to 'On' for all ports).

Red boxes highlight the following settings:

- Redundancy Mode: Auto
- Revert To Primary: Enabled
- Negotiation Mode: On (for all four GbE input ports)

Recording IP Port Configuration Settings

Follow these instructions to record the IP port configuration settings.

- 1 Navigate to the *System/IP Network* page.
- 2 Click the **Alt-PrtScrn** keys to copy the IP Network parameter settings to the clipboard.
- 3 Launch Microsoft Word (or WordPad if you don't have Microsoft Word) and paste the clipboard contents to page 1.
- 4 Save the Microsoft Word document as ipsettings.doc.

For Information

Support Telephone Numbers

This table lists the Technical Support and Customer Service numbers for your area.

Region	Centers	Telephone and Fax Numbers
North America	Cisco Services Atlanta, Georgia United States	For <i>Technical Support</i> , call: <ul style="list-style-type: none"> ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press 2 at the prompt) For <i>Customer Service</i> , call: <ul style="list-style-type: none"> ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press 3 at the prompt) ■ Fax: 770-236-5477 ■ Email: customer-service@cisco.com
Europe, Middle East, Africa	Belgium	For <i>Technical Support</i> , call: <ul style="list-style-type: none"> ■ Telephone: 32-56-445-197 or 32-56-445-155 ■ Fax: 32-56-445-061 For <i>Customer Service</i> , call: <ul style="list-style-type: none"> ■ Telephone: 32-56-445-444 ■ Fax: 32-56-445-051 ■ Email: service-elc@cisco.com
Japan	Japan	<ul style="list-style-type: none"> ■ Telephone: 81-3-5908-2153 or +81-3-5908-2154 ■ Fax: 81-3-5908-2155
Korea	Korea	<ul style="list-style-type: none"> ■ Telephone: 82-2-3429-8800 ■ Fax: 82-2-3452-9748 ■ Email: songk@cisco.com
China (mainland)	China	<ul style="list-style-type: none"> ■ Telephone: 86-21-2401-4433 ■ Fax: 86-21-2401-4455 ■ Email: xishan@cisco.com
All other Asia Pacific countries & Australia	Hong Kong	<ul style="list-style-type: none"> ■ Telephone: 852-2588-4746 ■ Fax: 852-2588-3139 ■ Email: saapac-support@cisco.com
Brazil	Brazil	<ul style="list-style-type: none"> ■ Telephone: 11-55-08-9999 ■ Fax: 11-55-08-9998 ■ Email: fattinl@cisco.com or ecavalhe@cisco.com
Mexico, Central America, Caribbean	Mexico	For <i>Technical Support</i> , call: <ul style="list-style-type: none"> ■ Telephone: 52-3515152599 ■ Fax: 52-3515152599 For <i>Customer Service</i> , call: <ul style="list-style-type: none"> ■ Telephone: 52-55-50-81-8425 ■ Fax: 52-55-52-61-0893 ■ Email: sa-latam-cs@cisco.com

For Information

Region	Centers	Telephone and Fax Numbers
All other Latin America countries	Argentina	For <i>Technical Support</i> , call: <ul style="list-style-type: none">■ Telephone: 54-23-20-403340 ext 109■ Fax: 54-23-20-403340 ext 103 For <i>Customer Service</i> , call: <ul style="list-style-type: none">■ Telephone: 770-236-5662■ Fax: 770-236-5888■ Email: keillov@cisco.com



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

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

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.

DOCSIS is a registered trademark of Cable Television Laboratories, Inc.

DVB is a registered trademark of the DVB Project.

Other 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. (1009R)

Product and service availability are subject to change without notice.

© 2011 Cisco and/or its affiliates. All rights reserved.
March 2011

Printed in USA
Part Number 7019749 Rev A