Cisco RF Gateway 1 Software Release Notes, Release 2.02.15

Overview

Introduction

Software Release 2.02.15 contains a number of minor enhancements not available in the previous release, 2.02.11, which supports four independent input GbE ports and up to four multicast source IP addresses in Table mode. Release 2.02.11 retains DVB Simulcrypt Scrambling capability for the RF Gateway 1 platform and supports license-upgradeable data features and a user authentication feature for security of the RF Gateway 1 management interface.

Purpose

The purpose of this document is to notify RF Gateway 1 users of the enhancements included in the current release and inform users of any special upgrade procedures needed for using Release 2.02.15.

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

MPTS Pass-Through Enhancements

The following miscellaneous bugs have been addressed in 2.02.15.

- Under certain circumstances in MPTS pass-through mode, the RF Gateway 1 was erroneously reporting continuity count errors on the incoming null PID.
- A feature was added to support PID blocking on data (engineering) streams so that MPTS muxing in broadcast applications can pass SI tables.
- When adding a MPTS stream to map, defaults for PID blocking list include the PAT and stuffing packets which causes PAT regeneration on the outputs. A setting was added so that when adding a MPTS entry, the default can be to pass the PAT. In either case, the user can still go into the advanced settings and manipulate the block list.
- Corrected a problem with passing an incoming MPTS PAT through to the output. If multiple streams were multiplexed to the output, a PAT would sometimes get generated and sent to the output, along with the passed through PAT.
- Corrected a problem recovering an MPTS from the 'Bad Input' state. If an MPTS gets into 'Bad Input' state, it will now properly recover once the condition clears. ('Bad Input' is caused by too many PSI/SI table changes in one second on the input to the RF Gateway 1.)

Miscellaneous Improvements

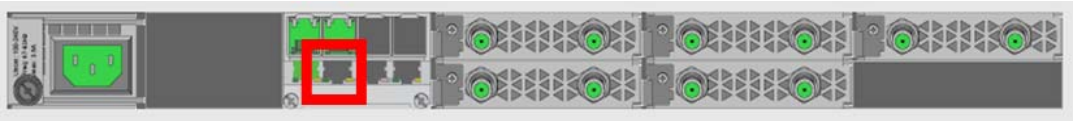
The following miscellaneous improvements have been made in release 2.02.15.

- An erroneously reported error that appeared in the RF Gateway 1 log at start-up has been addressed. The log entries suggested an issue reading EEPROMs on the I/O boards.
- PCR discontinuities could be inserted on the wrong TS Index when PCR discontinuity insertion is enabled and an event on an input stream required insertion of a PCR discontinuity flag. Some settop boxes may exhibit a brief audio or video glitch when a discontinuity flag is present.
- Fix problems handling IGMP queries and sending IGMP reports on the second GbE pair in GbE dual-port pair mode.
- A problem related to replicated unicast streams not streaming properly when the input is disrupted, and then recovers has been addressed.
- When an established stream received an empty PAT (one with no referenced programs), the stream was sometimes getting stuck in "Content Loss" or "Wait For Content" state. Now, when the proper SPTS or MPTS PAT arrives, the stream recovers correctly.
- In GbE Independent mode, the Monitor/Main page now correctly shows active and primary for all 4 GbE ports.
- Support has been added to allow IP addresses conforming to /31 networks. This will allow the setting IP addresses with the last octet of 0 or 255. A popup message box will appear to notify the user that one of these values has been entered.

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 also recommended.
- The Summary page displays the unit rear panel with Conditional Access (CA) port enabled/disabled as green/grey. The CA port indication represents the on/off setting and does not represent actual link status.



- The database Restore feature in 2.02.15 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 2.02.15. The procedure is needed to allow compatibility with the enhanced SNMP version 1 and 2 trap support in 2.02.15.
- SNMP community strings are provided in 2.02.15 to support SNMP v1 and v2 traps. Prior to release 2.01.09, there was a single community string applicable to all five trap receivers configurable for the operator. In release 2.02.11 and beyond, in addition to supporting SNMPv1 and v2 traps, 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 2.02.11 or later releases or downgrading from 2.02.11 or later releases, if they are being used.
- An upgrade to 2.02.11 from pre-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.

Licensing

After an upgrade to 2.02.15, 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 01.02.20 require a license file. This can be obtained from Cisco after an upgrade to 2.02.15. 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, located under the System tab, *License Management*. It 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.

Upgrade Information

An RF Gateway 1 unit running release 1.02.20 can be upgraded directly to 2.02.15. 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 2.02.15 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 2.02.15 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. Refer to Upgrade Procedure for Customers Running 1.02.09.

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 for SNMP related upgrade, downgrade and database restore considerations.

IP Port Configuration Changes

There is a bug in 1.02.09 that results in 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, refer to 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 value as seen in the *System/IP Network* page of the web GUI, and as a result, the IP ports may not be configured properly for operation immediately after upgrade (after the subsequent reboot that follows activation).

Refer to Upgrade Procedure for Customers Running 1.02.09.

Upgrade Procedure for Customers Running 1.02.09

WARNING:

Upgrading to 2.01.09 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. Refer to ***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. Refer to ***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. Refer to ***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 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.

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 2.02.15. 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.

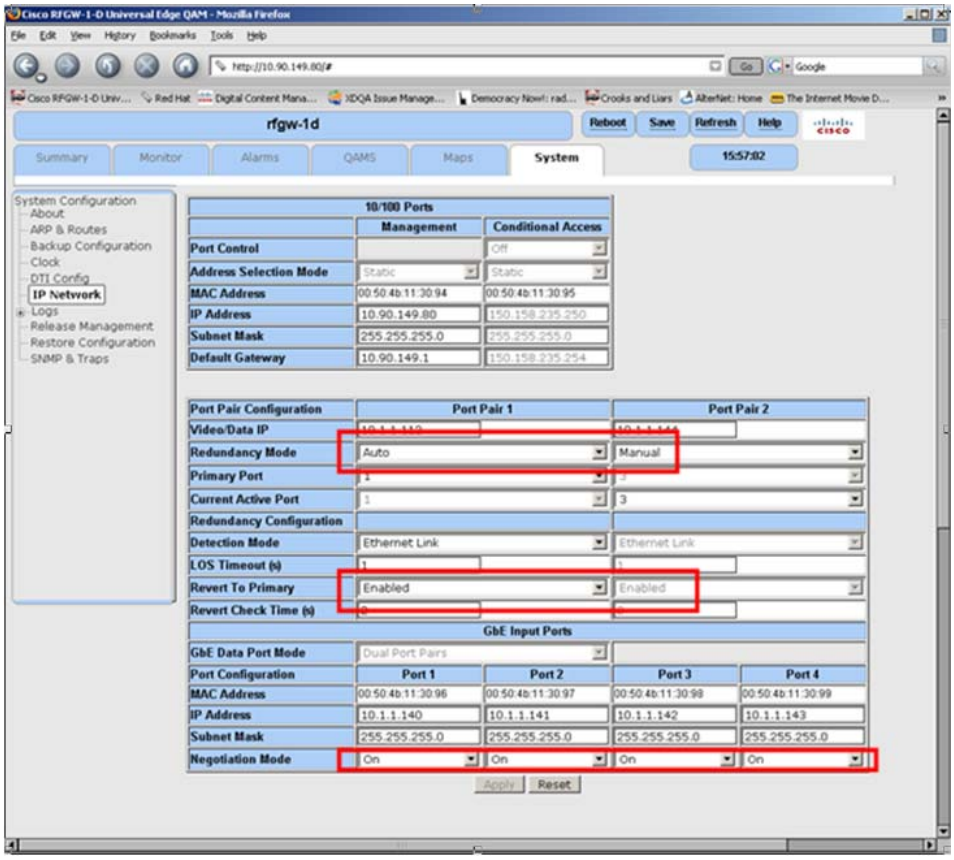
IP Port Configuration Parameter Settings

Refer to 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.



Recording IP Port Configuration Settings

Follow these instructions to record 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 Word Pad 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 *Technical Support*, call: ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press **2** at the prompt) For *Customer Service*, call: ■ 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 *Technical Support*, call: ■ Telephone: 32-56-445-197 or 32-56-445-155 ■ Fax: 32-56-445-061 For *Customer Service*, call: ■ Telephone: 32-56-445-444 ■ Fax: 32-56-445-051 ■ Email: service-elc@cisco.com
Japan	Japan	■ Telephone: 81-3-5908-2153 or +81-3-5908-2154 ■ Fax: 81-3-5908-2155
Korea	Korea	■ Telephone: 82-2-3429-8800 ■ Fax: 82-2-3452-9748 ■ Email: songk@cisco.com
China (mainland)	China	■ Telephone: 86-21-2401-4433 ■ Fax: 86-21-2401-4455 ■ Email: xishan@cisco.com
All other Asia Pacific countries & Australia	Hong Kong	■ Telephone: 852-2588-4746 ■ Fax: 852-2588-3139 ■ Email: saapac-support@cisco.com
Brazil	Brazil	■ Telephone: 11-55-08-9999 ■ Fax: 11-55-08-9998 ■ Email: fattinl@cisco.com or ecavalhe@cisco.com
Mexico, Central America, Caribbean	Mexico	For *Technical Support*, call: ■ Telephone: 52-3515152599 ■ Fax: 52-3515152599 For *Customer Service*, call: ■ Telephone: 52-55-50-81-8425 ■ Fax: 52-55-52-61-0893 ■ Email: sa-latam-cs@cisco.com

Region	Centers	Telephone and Fax Numbers
All other Latin America countries	Argentina	For *Technical Support*, call: ■ Telephone: 54-23-20-403340 ext 109 ■ Fax: 54-23-20-403340 ext 103 For *Customer Service*, call: ■ Telephone: 770-236-5662 ■ Fax: 770-236-5888 ■ Email: keillov@cisco.com

5030 Sugarloaf Parkway, Box 465447 678.277.1000
Lawrenceville, GA 30042

September 2009 Part Number 7019262 Rev A