Cisco RF Gateway 1 Software Release Notes, Release 3.01.06

Overview

Introduction

The Cisco RF Gateway 1 software version 3.01.06 provides IGMP-related enhancements to the 3.00.X code base, and fixes a synchronization issue in the interleaver logic that potentially results in an impairment, or spike, present on several RF channels. In SDV systems, 3.01.06 also provides a change in behavior between the RF Gateway 1 and the USRM when a bad card is detected.

The 3.X code provides double the QAM channel capacity without hardware changes. It remains fully SDV capable and also provides various stream management improvements. The new 3.X system releases are primarily intended for support of SDV applications. Other video deployments can continue to use 2.02.X as the preferred release.

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 3.01.06.

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

USRM Support

In earlier releases, QAM card failures on an RF Gateway 1 unit caused the USRM to take the entire RF Gateway 1 chassis out of service. This was due to inconsistent status information being provided to the USRM regarding aberrant QAM card initialization. RF Gateway 1 status reporting has been rectified and the condition handled appropriately by USRM revision 1.7.1 and later. The various behaviors depending on code revisions are summarized below.

- RF Gateway release 3.01.06 and USRM 1.7.1: When a QAM card fails during operation or at boot-up, the USRM continues to use all other QAM cards in the chassis, while the failed card is automatically taken out of service on the USRM.
- RF Gateway release 3.01.06 and USRM 1.6 or older: QAM card failure results in all QAM cards remaining in service on the USRM, including the failed card.
- RF Gateway release 3.01.01 or older and USRM 1.7.1: QAM card failure results in all QAM cards remaining in service on the USRM, including the failed card.
- RF Gateway release 3.01.01 or older and USRM 1.6 or older: QAM card failure results in the USRM taking all cards out of service.

Miscellaneous Improvements

- Release 3.01.06 enhanced IGMP version determination to prevent an incoming IGMP v2 Join from switching the RF Gateway 1 into IGMP v2 mode. With the changes to 3.01.06, only received IGMP v2 queries will cause the RF Gateway 1 to change from IGMP v3 mode to IGMP v2.
- Jitter alarm handling is now enhanced to prevent generating continuous PCRHI Jitter alarms. In release 3.01.06, PCRHI incidents will be written to the system log when Low Level Alarms is set to Verbose. In most cases, the alarm indicates a change of time base, such as due to ad insertion, and is not indicating a real impairment.

Operational Enhancements

The following features have been added between 3.00.18 and 3.01.01 and are also included in 3.01.06.

- Exponential Back-off of Multicast Source Switching. In 3.00.18, when a multicast stream stops arriving from the current source IP address, the RF Gateway 1 immediately switches to the next source. The RF Gateway 1 then waits for 1 second on that new source IP address before switching to the next source. Every subsequent second, another source switch is performed until the stream recovers.
  In Software Release 3.00.20 (and in 3.01.0X), an exponential back-off algorithm for the IGMP source switching was implemented to prevent the upstream switch or router from getting flooded with IGMP messages in cases of stream outage. In this algorithm, the RF Gateway 1 still switches immediately to the next source on the initial loss of input program, but it now waits 3 to 6 seconds for the stream to arrive from the new source before switching sources again. The RF Gateway 1 continues to use this 3 to 6 second wait time until all sources of the stream have been attempted. At that point, the RF Gateway 1 wraps back to the original source and doubles its wait time to 6 to 12 seconds. If the input does not recover, the RF Gateway 1 continues doubling its wait time on a source switch up to the maximum of 24 to 48 seconds.
  The new algorithm also has a random element to the wait times, hence the time ranges above. Each RF Gateway 1 on start-up calculates a random multiplier to use when calculating the back-off time. Thus, a group of RF Gateways connected to the same switch or router will spread their source switches over the timeout range to ease the spike of IGMP messages received by the switch.
- IGMP Report Bundling. This release of the RF Gateway 1 now bundles up to 120 IGMP group records into one IP packet upstream. The previous code would only send a maximum of 2 group records into a packet. This bundling drastically reduces the number of upstream IP packets in response to an IGMP general query, or in the case of a network outage causing many input streams to fail simultaneously.
- Support for 12 USRM RPC connections (and 3 DNCS connections). The RF Gateway 1 now supports up to 12 simultaneous USRM RPC connections and can also support up to 3 DNCS RPC connections.

- Release 3.01.06 corrects IGMP Query responses to send accurate IGMP group record information. This caused problems with the IGMP Query responses for all multicasts added after this particular multicast group. This problem also manifested due to the RF Gateway 1 treating a Source Specific Multicast group as a group with no sources. Also, IGMP Query responses were erroneously padding 4 bytes of data (for the source) in the case of an IGMP group with no sources. This handling is now corrected and resolves IGMP group record processing.
- Interoperability testing with one of BigBand's video servers revealed a problem where a maximum of 1024 sessions can be returned in the QueryBindings GQI response. This is now fully supported with Release 3.01.06 software.

RF Performance

- Rare RF impairment on even-numbered channels: On a very small percentage of units running 03.00.X, an RF impairment was discovered on even-numbered QAM channels on the top row of cards. The impairment appears as a "spike" on the top of the QAM carrier haystack on a spectrum analyzer. This impairment was caused by an out-of-sync condition at the input to the ITU encoder interleaver logic block. Handling for this error condition has been improved to prevent the RF impairment in version 3.01.01 and higher. (This fix is also in 3.00.21.)

Known Issues

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

- The RF Gateway 1 web management interface provides no events or alarms informing a user about a missing 8 channels per port license. The user can easily observe the Summary page to view greyed out channel frequencies and the System/License Management page to confirm an unlicensed unit.
- Over provisioning an unlicensed QAM channel causes an alarm condition on the RF Gateway 1.
- The RF Gateway 1 Web interface is not fully tested with IE-8 and FireFox-3.5.x 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.
- When using /31 IP addressing, although the RF Gateway 1 allows setting IP addresses and masks that correspond to this point-to-point protocol, it will not respond to ICMP ping requests.

Licensing

After an upgrade to 3.01.06, a new system license (8 channels per port) must be installed to access full 96 QAM channel support. For information regarding RF Gateway 1 licensing requirements and procedures, see the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.

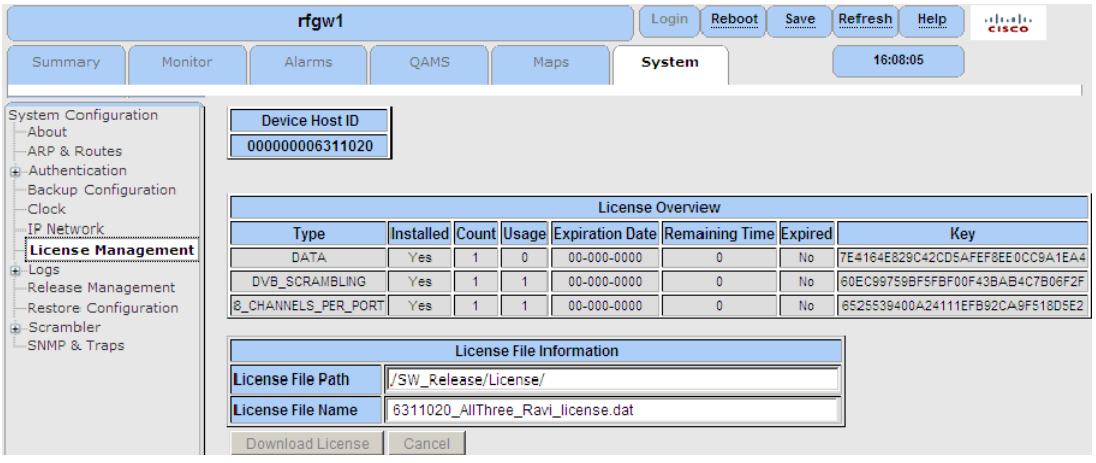
The following features require a system license:

- Third party encryption
- Data streams requiring use of the DOCSIS® timing interface
- DVB® encryption
- PowerKEY® encryption
- 8 channels per port

If licenses are not installed at the factory, activation of the features listed above will require that a license file be obtained from Cisco after an upgrade to 3.01.06. Contact your account representative for details on obtaining your license files.

Note: Performing an upgrade without a license file will not affect the configuration of a chassis already operating in release 1.03.X, 2.02.X, or 1.02.X. The unit continues to function as configured earlier until configuration or license changes are made. No alarms or warnings are currently present that indicate the absence of the 8 channel per port license.

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 screen below. It provides an FTP mechanism to transfer license files to the device.



Upgrade Information

An RF Gateway 1 unit running release 1.02.20 or higher can be upgraded directly to 3.01.06. 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 3.01.06 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 3.01.06 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 3.01.06 directly from 1.02.09 must not be attempted. This may cause the RF Gateway 1 to be non-operational.

IP Port Configuration Parameter Settings

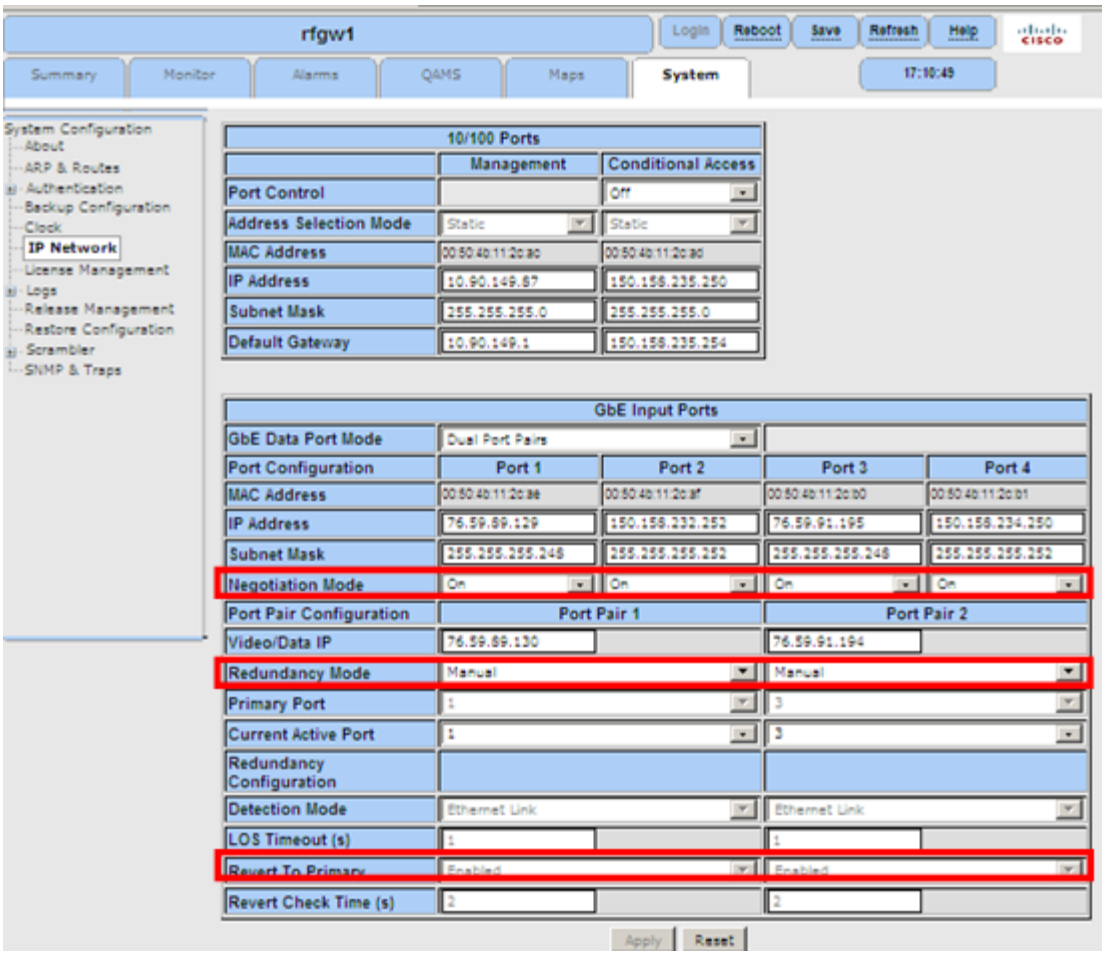
The RF Gateway 1 has four physical GbE input ports that receive video and data streams from the upstream network. These ports may be used independently (in software releases 02.02.11 or later) or configured to implement input redundancy. See Chapter 3, *General Configuration and Monitoring* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112 for 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. See 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 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 *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

Printed in United States of America
April 2010 Part Number 7020535 Rev A