Cisco RF Gateway 1 Software Release Notes, Release 3.00.16

Overview

Introduction

The RF Gateway 1 software version 3.00.16 provides higher channel capacity with no hardware changes from its predecessor releases. The RF Gateway 1 remains fully SDV capable, and the new 3.00.16 system release is primarily intended for support of SDV applications. Other video deployments can continue to use 2.02.XX and so forth 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 3.00.16.

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

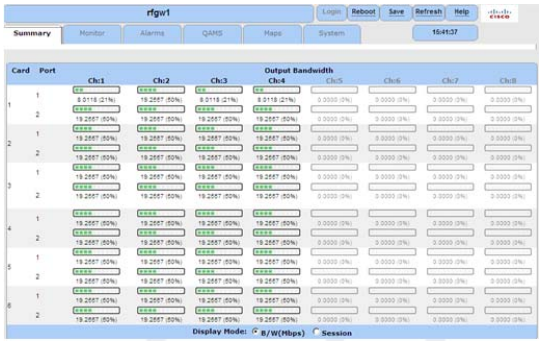
- 96 QAM Channels....3
- Miscellaneous Improvements....4
- Known Issues....5
- Licensing....6
- Upgrade Information....8
- IP Port Configuration Changes....9
- Upgrade Procedure for Customers Running 1.02.09....10
- IP Port Configuration Parameter Settings....12
- For Information....14

96 QAM Channels

The 3.00.16 release provides up to 96 licensed QAM channels or 8 channels per RF port. This feature is fully functional with no hardware changes from the predecessor RF Gateway 1 releases. The new 96 QAM channel capability is enabled by simply applying the 8 channels per port license to the 3.00.16 release.

The RF Gateway 1 continues to operate as earlier 48 QAM versions without applying the 8 channels per port license and upgrading to system release 3.00.16. There is no configuration and/or operational differences operating with system release 3.00.16 in this mode. QAM channel numbering follows the 4 channel per port predecessor.

Full backward compatibility is ensured with RF Gateway 1 configuration databases used under the 1.03.XX and 2.02.XX RF Gateway 1 system release branches. See the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112 for additional information about operating in the 8 channels per port mode.



(a) Unlicensed 8 channels per port

(b) Licensed 8 channels per port

Miscellaneous Improvements

- System release file transfers performed over the management network now include enhanced error checking for downloaded release verification.
- The RF Gateway 1 web management user interface for QAMS and Maps now implements faster loading web pages, providing the user with minimal page load times when accessing these configuration pages.
- Clicking Advanced Settings under Maps/Video Stream Map now includes a quaternary source specification capability. See Chapter 4 of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112 for detailed information about configuring the RF Gateway 1.
- Additional monitoring of QAM module health has been added, including monitoring alarms and traps for QAM module voltages. In addition to enhanced monitoring, software version 3.00.16 removes a QAM module from service if a critical failure occurs.

Known Issues

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

- The RF Gateway 1 has a known problem when an incoming stream is replicated via multiple sessions to multiple output carriers. The Multicast source address list will often be incorrectly appended with an extra source IP address. This address, in most cases, will be the same as the first source address in the list. However, it could also be any other source IP address that has been used for another stream. This extra source address will come into play if the real sources of the incoming video stream are not present. Once the correct sources have been tried and fail, the RF Gateway 1 will switch to the extra, possibly invalid source address for this stream.
- 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, the GbE ports will not respond to ICMP echo requests, nor will they properly resolve their link partner's MAC address via ARP. These limitations may adversely affect unicast operations when using /31 subnets.

Licensing

After an upgrade to 3.00.16, 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

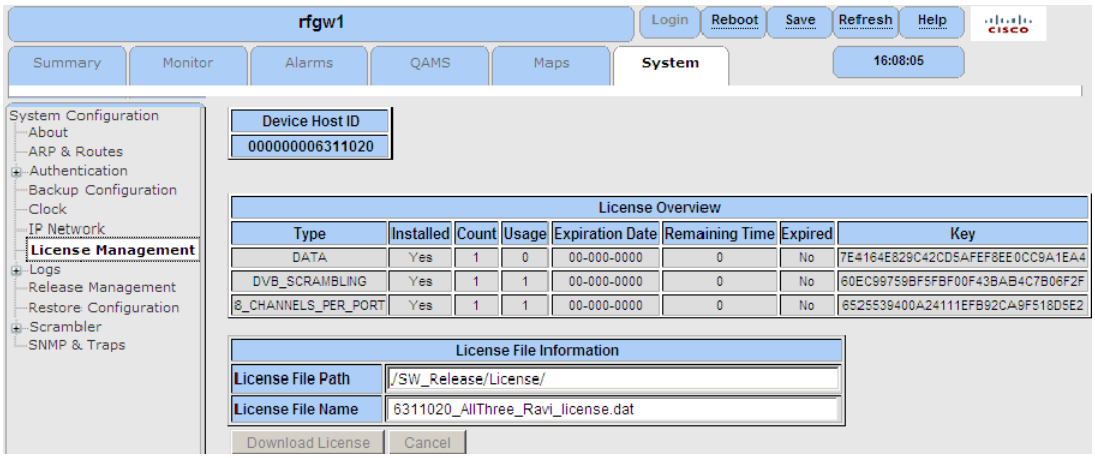
Most systems delivered with 1.02.20 or later using a data part number included a license file pre-installed at the factory. For these systems, an FTP transfer is not necessary.

All systems delivered prior to 1.02.20 and some systems delivered with release 01.02.20 will require that a license file be obtained from Cisco after an upgrade to 3.00.16. 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 V01.03.XX, V02.02.XX, or V01.02.XX. The unit will continue to function as configured earlier until configuration or any 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.

Note: In Release 3.00.16, the RF Gateway 1 will not immediately warn the operator if the FTP transfer fails due to an incorrect filename. It is strongly 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 1.03.19. See 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 1.03.19 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 3.00.16 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 10).

WARNING:

Upgrading to 1.02.20 or 3.00.16 directly from 1.02.09 must not be attempted. This may cause the RF Gateway 1 to be non-operational.

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 value 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 10).

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, back up the system configuration. See 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 13).
3. Download and activate 1.02.19. See 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 12).
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 12). 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 3.00.16. See 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.

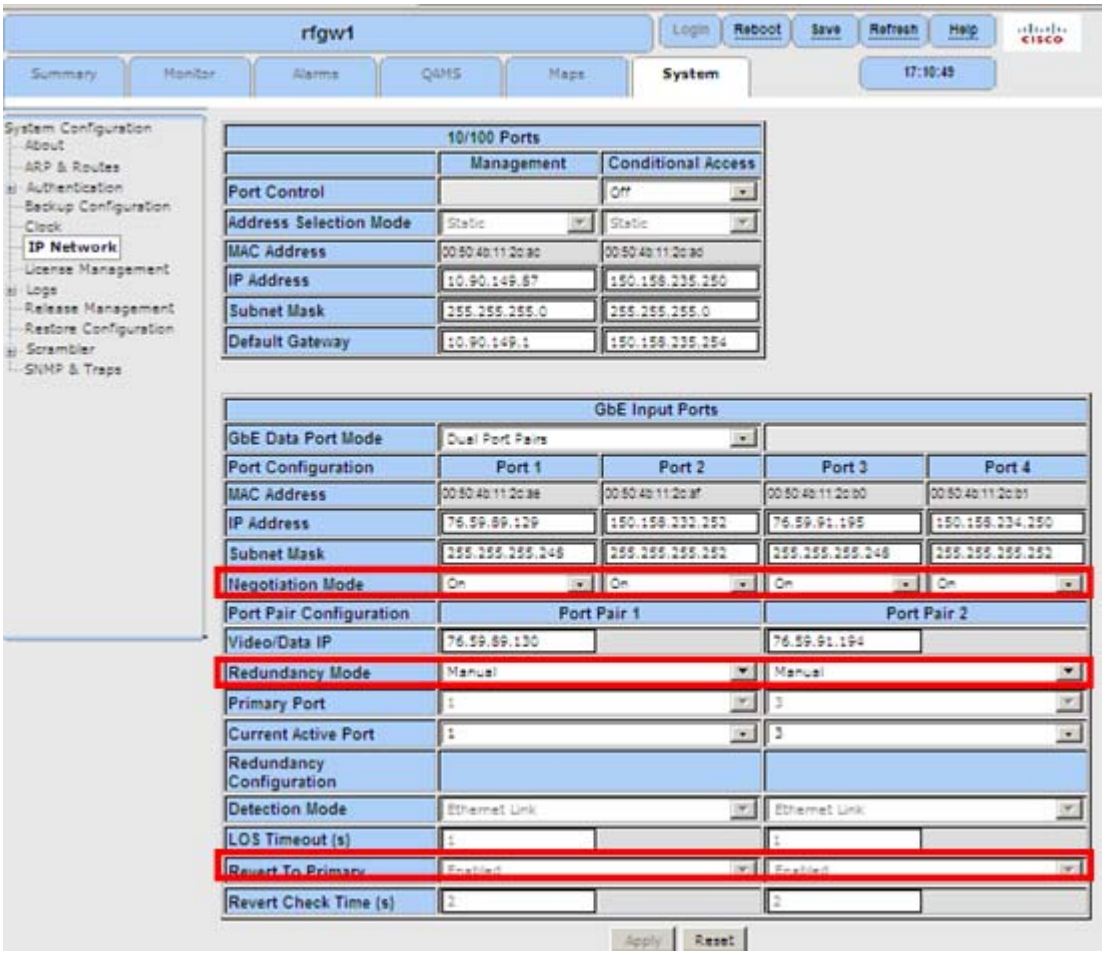
IP Port Configuration Parameter Settings

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 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 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. 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

Cisco, Cisco Systems, the Cisco logo, the Cisco Systems logo, and PowerKEY are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
DOCSIS is a registered trademark of Cable Television Laboratories, Inc.
DVB is a registered trademark of the DVB project.
All other trademarks mentioned in this document are the property of their respective owners.
Product and service availability are subject to change without notice.

© 2009 Cisco Systems, Inc. All rights reserved. Printed in United States of America

November 2009 Part Number 7019486 Rev A