Cisco RF Gateway 1 Software Release Notes, Release 1.03.17

Overview

Introduction

Software Release 1.03.17 is an SDV capable release for the RF Gateway 1 which supports Motorola DigiCipher streams (C0/C1 tables). It also features support for a programmable de-jitter buffer and OCAP STBs. Other miscellaneous fixes are included, for example, improved multicast source switching and stream map capabilities.

This release continues to support Software Licensing, Table Based Video, Wideband Data Specific and the Basic M-CMTS Data applications.

Purpose

The purpose of this document is to notify RF Gateway 1 users of data applications supported and enhanced capabilities. This document also provides upgrade procedures from the bridge release to the final release.

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

Motorola DigiCipher Stream Support

Software Release 1.03.17 supports pre-encrypted Motorola DigiCipher streams (C0/C1 tables). These streams contain SI tables on the incoming PMT PID. The additional tables have a Table ID of either 0xC0 or 0xC1. These tables are now extracted and reinserted at the output along with the remapped PMT. The ECM table may also arrive on the PMT PID. This table may be remapped and passed through to the output by the RF Gateway 1.

Stream Map Muxing

The following improvements have been made to the Stream Map feature.

- The RF Gateway 1 Stream Map feature is improved to resolve issues with MPTS de-multiplexing. Scenarios addressed include when mapping multiple programs of an MPTS to an output, removing one row often caused the incorrect map entry to get removed from the stream map.
- Also, when multiplexing an MPTS with an SPTS, if the SPTS was replacing an MPTS program that was being blocked, the output would often not have the correct SPTS program. These stream map configurations are now verified to operate as expected.

Improved Source Switching

In releases earlier than 1.03.17, the content detection mechanism had an issue which, depending on the number of input streams, resulted in undesired source switching away from valid sources. When approximately 50 or more input streams were active, it was possible to have rare occurrences of these unnecessary source switches on new stream startup. These source switches result in brief video glitches that occur 10 seconds after stream creation. As the number of input streams increase, the likelihood of a newly created stream having the source switch problem increases. At around 200 or more input streams, almost all newly created streams will suffer from a source switch on creation and thus have the glitch. This behavior is addressed in V01.03.17 so that the RF Gateway 1 will not switch sources and will correctly stay on a good primary input source, or will stay on the first good input source.

Miscellaneous Fixes

Varying severity bug fixes have been included in the following areas:

- Under heavy SDV load conditions, the RF Gateway 1 was not recovering its sessions as required. Some sessions could be lost after reboot. This has been addressed and recovery is tested.
- Dropped video packets were observed during heavily loaded SDV replication tests. This anomaly was resolved by fine tuning design aspects of the RF Gateway 1 firmware, but was only occurring in tests with unusual amounts of replication, hence not expected to be observed in the field.

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.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 1.03.11, a system license must be installed to access certain features. For information regarding RF Gateway 1 licensing requirements and procedures, refer to 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

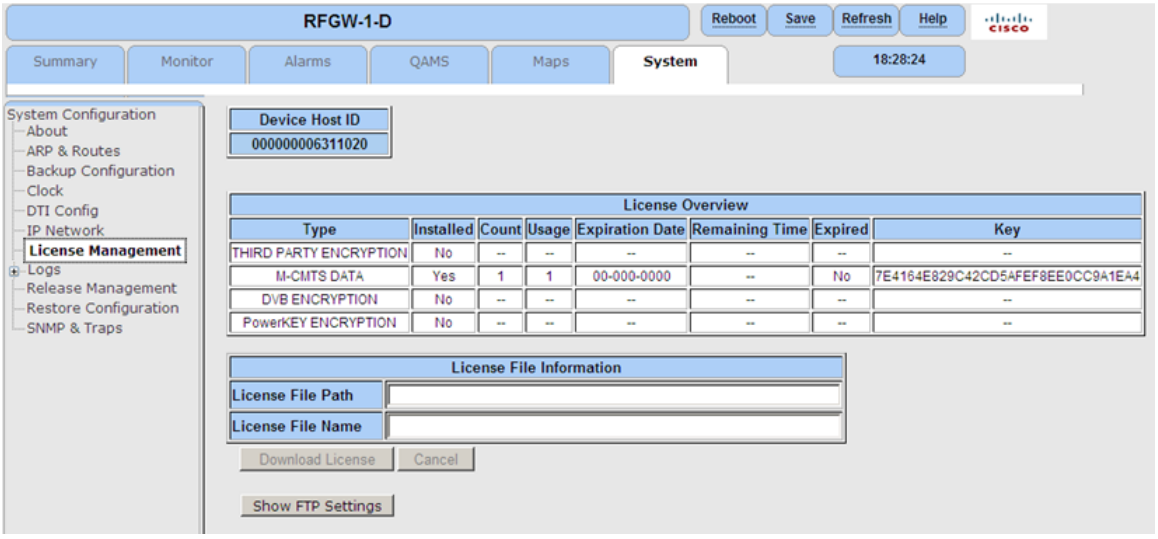
Most systems delivered with 1.02.20 or later using a data part number included a license file pre-installed from the factory. For these systems, an FTP transfer as described below will not be necessary.

All systems delivered prior to 1.02.20 and some systems delivered with release 01.02.20 will require that a license file is obtained from Cisco after an upgrade to 1.03.17. 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 will continue to function until configuration changes are made.

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

Note: In Release 1.03.17, 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 1.02.20 can be upgraded directly to 1.03.17. 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 1.03.17 from 1.02.09, an intermediate step of using the bridge release (1.02.19) to arrive at 1.02.20 must be followed. In order to upgrade from 1.02.09 to 1.02.20 and finally 1.03.17, a 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*** (on page 12).

WARNING:

Upgrading to 1.02.20 or 1.03.17 directly from 1.02.09 must not be attempted. This may cause the RF Gateway 1 to become non-operational.

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*** (on page 12).

Upgrade Procedure for Customers Running 1.02.09

WARNING:

Upgrading to 1.02.20 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 15).
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 IP Port Configuration page. Refer to ***Displaying IP Port Configuration Settings*** (on page 14).
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 14). 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 1.03.11. 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.

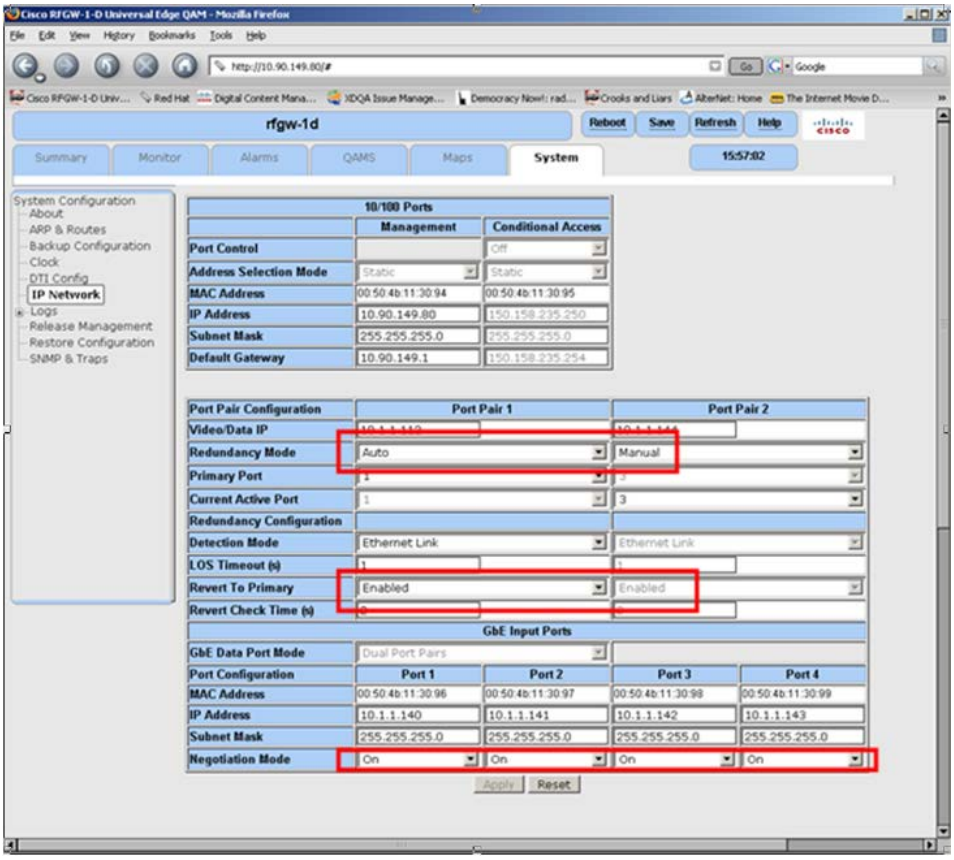
IP Port Configuration Parameter Settings

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

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

September 2012 Printed in USA Part Number 7019013 Rev B