Cisco RF Gateway 1 Software Release Notes, Release 1.03.11

Overview

Introduction

Software Release 1.03.11 is an SDV capable release for the Cisco® RF Gateway 1. This release provides support for a programmable dejitter buffer and OCAP STBs. An improved number of streams is supported. Miscellaneous fixes are also available including invalid input CC and jitter alarm improvements. SNMP (IF-MIB) MAC format and extended walk capability is also improved.

This release continues to support 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.

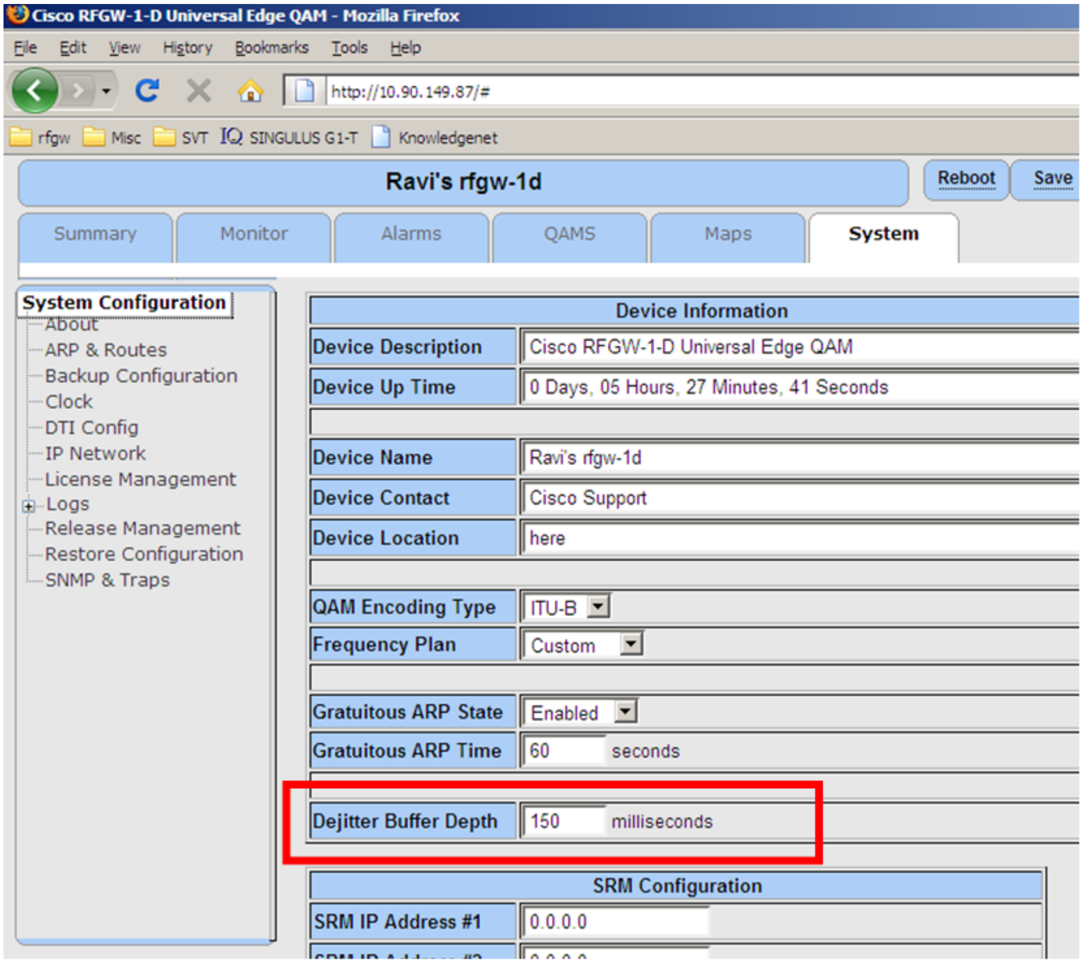
In This Document

Programmable Dejitter Buffer Support

The RF Gateway 1 dejitter buffer depth was fixed at 150 msec. This enhancement allows the dejitter buffer depth to be adjustable between 5 and 300 msec. The default value is still 150 msec to be compatible with existing systems.

Each time a new stream is started, two FPGA registers will be set according to the dejitter depth. The depth is specific to the RF Gateway 1 or applicable to the entire RF Gateway 1 box. It is recommended that the depth be set on the System Configuration Page or the RF Gateway 1 General MIB folder. This object is persistent. Granularity is one msec.

If the dejitter buffer depth setting is changed, a warning will appear informing the user of a momentary disruption in service. Once this pop-up is acknowledged, the user must apply the change for it to take effect.



http://10.90.149.87/#

Ravi's rfgw-1d

Device Information

Device Description	Cisco RFGW-1-D Universal Edge QAM
Device Up Time	0 Days, 05 Hours, 27 Minutes, 41 Seconds
Device Name	Ravi's rfgw-1d
Device Contact	Cisco Support
Device Location	here
QAM Encoding Type	ITU-B
Frequency Plan	Custom
Gratuitous ARP State	Enabled
Gratuitous ARP Time	60 seconds
Dejitter Buffer Depth	150 milliseconds

SRM Configuration

SRM IP Address #1	0.0.0.0

OCAP STB Support

In previous releases, the default PAT was not inserting a reference to the NIT PID. Therefore, OCAP STBs were not finding the TSID. In Release 1.03.11, a network PID (0x1ffc) has been added to the PAT, allowing proper operation of OCAP STBs.

Stream Support

Up to 2046 streams are now supported. In prior releases, only 1024 streams could be activated.

Improved CC and Jitter Alarms

False CC and jitter alarms recorded during stream start and shutdown is now fixed. This was noticed in the SDV mode of operation and under heavy loads. This allows customers better network troubleshooting by alleviating false CC alarms and extraneous log file entries.

Improved SNMP Capability

The following improvements have been made.

- An extended SNMP walk operation on the RF Gateway 1 initiated by MRTG tools such as Cacti was experiencing problems with the walk completing. This has been improved and now the RF Gateway 1 allows the MIB to be queried properly.
- IF-MIB support improvements include improper MAC address (ifPhyAddress MIB object) display format correction.

Miscellaneous Fixes

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

- Web GUI stability fixes include a very slow memory leak correction on the *Summary* page.
- Web GUI unresponsiveness was observed over long periods of web user inactivity.
- Log manager design improvements to reduce delays in transferring large log files.
- SNMP updates resulting in automatic database persistence capability is now available.
- Setting the RF port center frequency with floating point values resulted in possible rounding errors such that the values retained in the system database could have erroneous frequency values.
- IGMPv3 specific query handling is now improved to handle the isolated case where a router sends IGMP queries when a multicast stream is active on both gigabit ethernet ports and they are configured on the same VLAN. The queries arise upon leaving the multicast group on any one GbE port. The RF Gateway 1 now responds promptly, allowing no momentary video anomalies.
- Under some scenarios, it is advantageous for the RF Gateway 1 to have gratuitous ARP implemented for the management port. For example, when a unit is replaced by another unit with the same IP address without a reboot, the default ARP-cache timeout on the router port is 4 hours. It could take up to 4 hours for the MAC address to be updated if no gratuitous ARPs are present on the management port. During this time, there is no communication with the RF Gateway 1. With gratuitous ARP enabled, the router's ARP table is immediately updated and management traffic flows as expected.
- GbE Port redundancy is improved to prevent an inactive port staying inactive when switched to the primary port (of the pair).

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

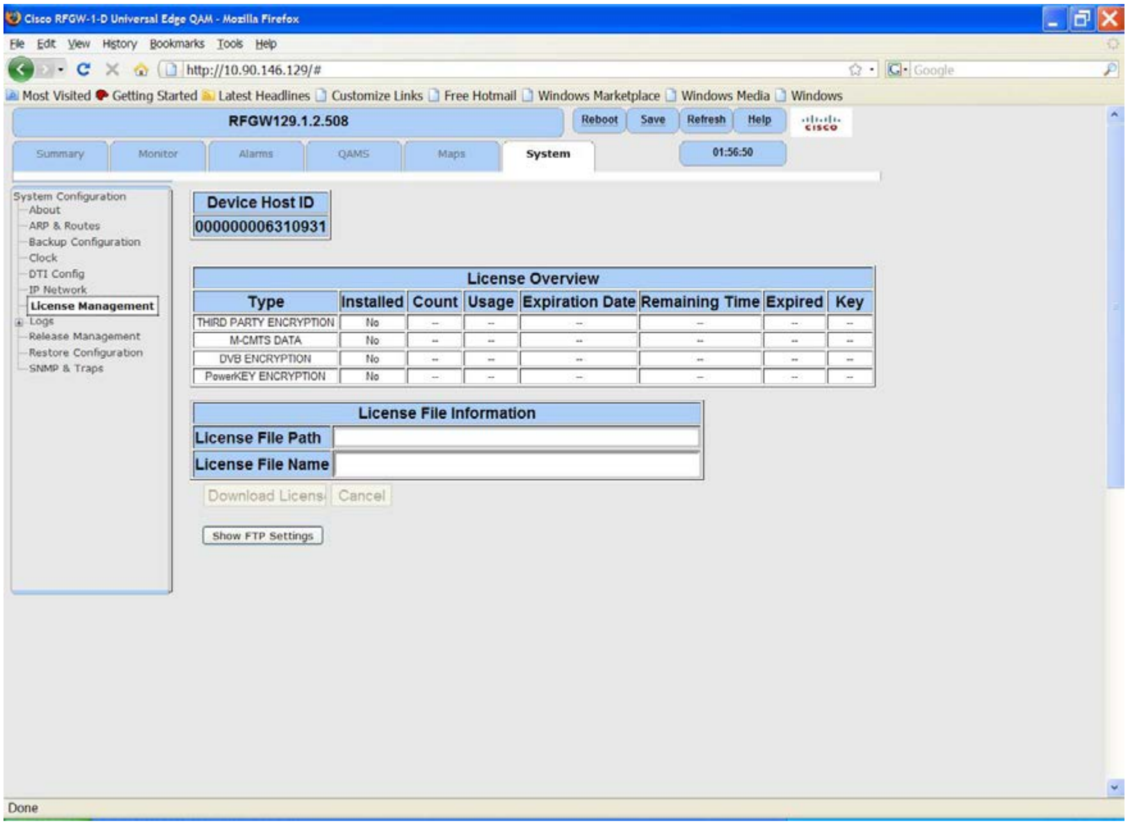
Most systems delivered with release 1.02.20 or later using a data part number included a license file pre-installed at the factory. For these systems, an FTP transfer is not necessary.

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

Note: The RF Gateway 1 will not immediately warn the operator if the FTP transfer fails due to an incorrect filename. It is recommended that the operator monitor the file transfer status using feedback from the FTP server.



Device Host ID
000000006310931

License Overview

Type	Installed	Count	Usage	Expiration Date	Remaining Time	Expired	Key
THIRD PARTY ENCRYPTION	No	--	--	--	--	--	--
M-CMTS DATA	No	--	--	--	--	--	--
DVB ENCRYPTION	No	--	--	--	--	--	--
PowerKEY ENCRYPTION	No	--	--	--	--	--	--

License File Information

License File Path	
License File Name	

Upgrade Information

An RF Gateway 1 unit running 1.02.20 can be upgraded directly to 1.03.11. 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. In order to upgrade from 1.02.09 to 1.02.20 and finally 1.03.11, 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 13).

⚠ **WARNING:**

Upgrading to 1.02.20 or 1.03.11 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 13).

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 16).

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 15).

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 15). 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

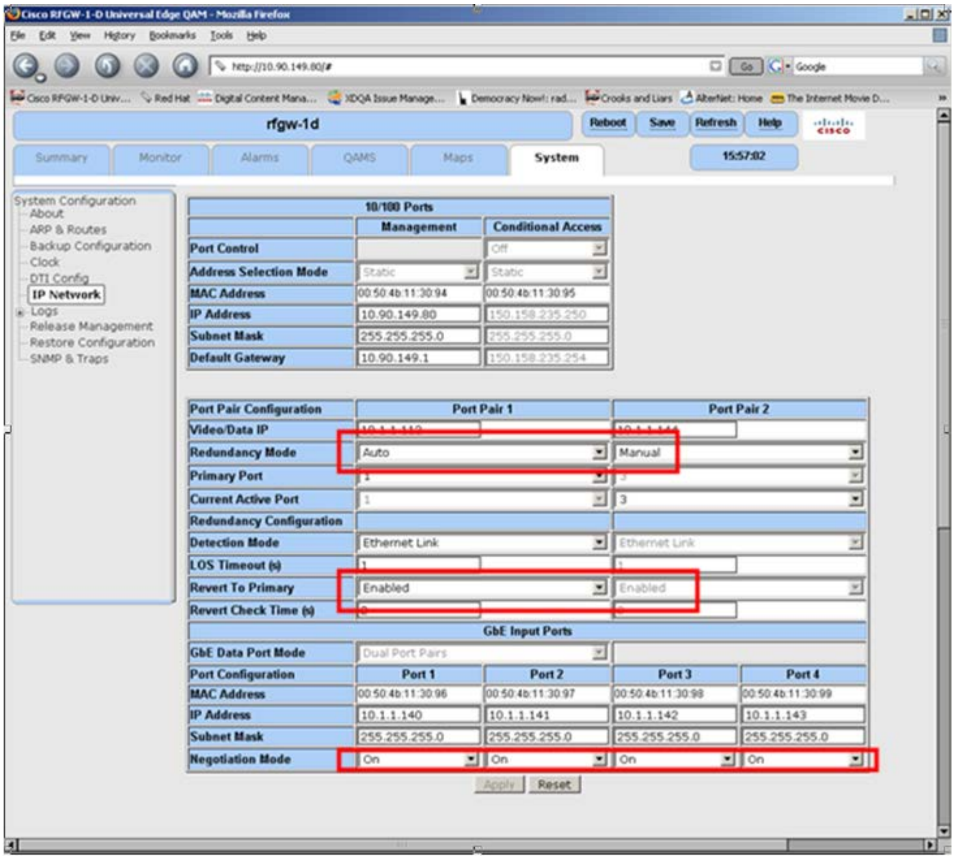
Follow these instructions to display the *System/IP Network* page.

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.



10/100 Ports		
	Management	Conditional Access
Port Control		Off
Address Selection Mode	Static	Static
MAC Address	00:50:4b:11:30:94	00:50:4b:11:30:95
IP Address	10.90.149.80	150.158.235.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	10.90.149.1	150.158.235.254

Port Pair Configuration	Port Pair 1		Port Pair 2	
Video/Data IP	10.1.1.112		10.1.1.144	
Redundancy Mode	Auto		Manual	
Primary Port	1		3	
Current Active Port	1		3	
Redundancy Configuration				
Detection Mode	Ethernet Link		Ethernet Link	
LOS Timeout (s)	1		1	
Revert To Primary	Enabled		Enabled	
Revert Check Time (s)	0		0	
GbE Input Ports				
GbE Data Port Mode	Dual Port Pairs			
Port Configuration	Port 1	Port 2	Port 3	Port 4
MAC Address	00:50:4b:11:30:96	00:50:4b:11:30:97	00:50:4b:11:30:98	00:50:4b:11:30:99
IP Address	10.1.1.140	10.1.1.141	10.1.1.142	10.1.1.143
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On

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

August 2012 Printed in USA Part Number 7018116 Rev B