



Cisco RF Gateway 1 Software Release Notes, Release 1.03.18

Overview

Introduction

The RF Gateway 1 software version 1.03.18 introduces a new feature to display RF port information on the front panel display. Release 1.03.18 remains fully SDV capable, and provides various stream management improvements and bug fixes. It continues to support Motorola DigiCipher streams (C0/C1 tables), and also continues to support a programmable de-jitter buffer depth and OCAP STBs.

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 1.03.18.

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

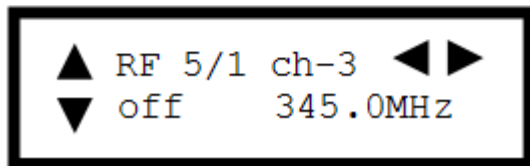
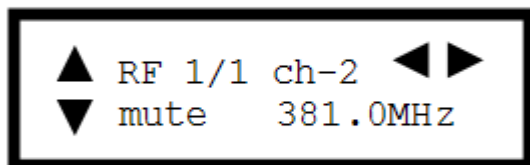
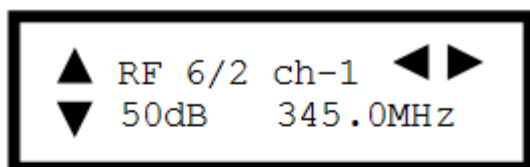
■ Front Panel Enhancements	3
■ Stream Management Improvements.....	4
■ Miscellaneous Improvements	5
■ Known Issues	6
■ Licensing	7
■ Upgrade Information	9
■ IP Port Configuration Changes.....	10
■ Upgrade Procedure for Customers Running 1.02.09.....	11
■ IP Port Configuration Parameter Settings.....	13
■ For Information.....	15

Front Panel Enhancements

Software Release 1.03.18 provides the operator the ability to view frequency and output power levels of the carriers on the front panel LCD. This allows easy access for users interested in confirming RF port status directly from a unit.

The front panel *Info* submenu now includes an *RF* selection for entry into the RF port/channel display screens. The up and down arrow keys on the front panel keypad can be used to move from one RF port to the next, and the left and right arrow keys from one carrier to the next. All carriers on an RF port have the same output level. If a carrier is muted or if the RF port is off, the string *mute* or *off*, respectively, will be displayed instead of the power level. To exit these screens, the user must press the middle select button on the front panel keypad from any RF menu screen. Refer to examples below of the front panel display.

Note: The limited area of the LCD display does not allow the power level and frequency to be presented with the same precision with which they can be set.



Stream Management Improvements

The following improvements have been made to stream management on the RF Gateway 1.

- Improved recovery of streams marked as "Input Loss."
- Improved handling of starting and stopping MPTS streams with an unblocked PAT. Also, PAT generation handling is enhanced when multiple streams are routed to an output.
- Improved handling of Null PAT to allow streams to remain successfully bound.
- Recovery from streams marked as "Bad Input" (due to incoming PAT or PMT table thrashing) is now reliable, with PAT and unreferenced PID mappings getting recreated correctly.
- Improved handling of blocked PID array differences on multiple replications of an incoming stream.

Miscellaneous Improvements

- RPC QueryBindingInfo handling is now correctly returning bit rate from the bind and not from the session. This is necessary for interoperability with non-Cisco SDV servers.

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 1.03.18, 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 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 1.03.18. 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 item, *License Management*, located under the **System** tab. Refer to the screen below. It provides an FTP mechanism to transfer license files to the device.

Licensing

Note: In Release 1.03.18, 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.

The screenshot displays the web interface for RFGW-1-D. The top navigation bar includes 'Reboot', 'Save', 'Refresh', and 'Help' buttons, along with the Cisco logo and the time '18:28:24'. The main content area is divided into several sections:

- System Configuration:** A sidebar menu with options like 'About', 'ARP & Routes', 'Backup Configuration', 'Clock', 'DTI Config', 'IP Network', 'License Management' (highlighted), 'Logs', 'Release Management', 'Restore Configuration', and 'SNMP & Traps'.
- Device Host ID:** A field showing '00000006311020'.
- License Overview:** A table with the following data:

Type	Installed	Count	Usage	Expiration Date	Remaining Time	Expired	Key
THIRD PARTY ENCRYPTION	No	--	--	--	--	--	--
M-CMITS DATA	Yes	1	1	00-000-0000	--	No	7E4164E829C42CD5AFEF8EE0CC9A1EA4
DVB ENCRYPTION	No	--	--	--	--	--	--
PowerKEY ENCRYPTION	No	--	--	--	--	--	--
- License File Information:** A form with fields for 'License File Path' and 'License File Name', and buttons for 'Download License', 'Cancel', and 'Show FTP Settings'.

Upgrade Information

An RF Gateway 1 unit running release 1.02.20 can be upgraded directly to 1.03.18. 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 1.03.18 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 1.03.18 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* (on page 11).

**WARNING:**

Upgrading to 1.02.20 or 1.03.18 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 11).

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. 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 14).
- 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 13).
- 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 13). 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.

Upgrade Procedure for Customers Running 1.02.09

- 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 1.03.18. 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.

The screenshot displays the Cisco RF Gateway 1 System Configuration page. The left sidebar shows the navigation menu with 'IP Network' selected. The main content area is divided into several sections:

- 10/100 Ports:** A table with columns for Management and Conditional Access. Settings include Port Control (Off), Address Selection Mode (Static), MAC Address (00:50:48:11:30:94), IP Address (10.90.149.60), Subnet Mask (255.255.255.0), and Default Gateway (10.90.149.1).
- Part Pair Configuration:** A table with columns for Part Pair 1 and Part Pair 2. Settings include Video/Data IP (10.90.149.60), Redundancy Mode (Auto for Part 1, Manual for Part 2), Primary Port (1 for Part 1, 3 for Part 2), Current Active Port (1 for Part 1, 3 for Part 2), Redundancy Configuration, Detection Mode (Ethernet Link), LOS Timeout (s) (1 for Part 1, 1 for Part 2), Revert To Primary (Enabled for Part 1, Enabled for Part 2), and Revert Check Time (s) (1 for Part 1, 1 for Part 2).
- GME Input Ports:** A table with columns for Part 1, Part 2, Part 3, and Part 4. Settings include GME Data Port Mode (Dual Port Pairs), Port Configuration, MAC Address (00:50:48:11:30:98), IP Address (10.1.1.140), Subnet Mask (255.255.255.0), and Negotiation Mode (On for all parts).

Red boxes highlight the Redundancy Mode and Negotiation Mode settings in the Part Pair Configuration and GME Input Ports sections, respectively.

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	For <i>Technical Support</i> , call:
	Atlanta, Georgia United States	<ul style="list-style-type: none"> ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press 2 at the prompt) For <i>Customer Service</i> , call: <ul style="list-style-type: none"> ■ 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 <i>Technical Support</i> , call: <ul style="list-style-type: none"> ■ Telephone: 32-56-445-197 or 32-56-445-155 ■ Fax: 32-56-445-061 For <i>Customer Service</i> , call: <ul style="list-style-type: none"> ■ Telephone: 32-56-445-444 ■ Fax: 32-56-445-051 ■ Email: service-elc@cisco.com
Japan	Japan	<ul style="list-style-type: none"> ■ Telephone: 81-3-5908-2153 or +81-3-5908-2154 ■ Fax: 81-3-5908-2155
Korea	Korea	<ul style="list-style-type: none"> ■ Telephone: 82-2-3429-8800 ■ Fax: 82-2-3452-9748 ■ Email: songk@cisco.com
China (mainland)	China	<ul style="list-style-type: none"> ■ Telephone: 86-21-2401-4433 ■ Fax: 86-21-2401-4455 ■ Email: xishan@cisco.com
All other Asia Pacific countries & Australia	Hong Kong	<ul style="list-style-type: none"> ■ Telephone: 852-2588-4746 ■ Fax: 852-2588-3139 ■ Email: saapac-support@cisco.com
Brazil	Brazil	<ul style="list-style-type: none"> ■ Telephone: 11-55-08-9999 ■ Fax: 11-55-08-9998 ■ Email: fattinl@cisco.com or ecavalhe@cisco.com
Mexico, Central America, Caribbean	Mexico	For <i>Technical Support</i> , call: <ul style="list-style-type: none"> ■ Telephone: 52-3515152599 ■ Fax: 52-3515152599 For <i>Customer Service</i> , call: <ul style="list-style-type: none"> ■ Telephone: 52-55-50-81-8425 ■ Fax: 52-55-52-61-0893 ■ Email: sa-latam-cs@cisco.com

For Information

Region	Centers	Telephone and Fax Numbers
All other Latin America countries	Argentina	For <i>Technical Support</i> , call: <ul style="list-style-type: none">■ Telephone: 54-23-20-403340 ext 109■ Fax: 54-23-20-403340 ext 103 For <i>Customer Service</i> , call: <ul style="list-style-type: none">■ Telephone: 770-236-5662■ Fax: 770-236-5888■ Email: keillov@cisco.com



5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678.277.1000

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.

© 2010 Cisco Systems, Inc. All rights reserved.
February 2010

Printed in United States of America
Part Number 7019570 Rev A