



Cisco RF Gateway 1 Software Release Notes, Release 2.02.11

Overview

Introduction

Software Release 2.02.11 has the capability to support four independent input GbE ports. In addition, users are now allowed to specify up to four multicast source IP addresses for Video Map configuration. Release 2.02.11 retains the DVB Simulcrypt Scrambling and user authentication features introduced from Release 2.01.09.

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 2.02.11.

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.

Overview

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

■ Independent GbE Ports.....	3
■ Multicast Sources.....	4
■ SNMP Improvements.....	5
■ Miscellaneous Improvements	6
■ Known Issues	7
■ Licensing	8
■ 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

Independent GbE Ports

The RF Gateway 1 now supports two separate GbE data port modes called "Dual Port Pairs" and "Four Port Independent" that are user configurable using the *System/IP Network/Gbe Data Port Mode* drop down list.

- **Dual Port Pairs:** While operating in Dual Port Pairs mode, the RF Gateway 1 allows configuration of two port pairs with port redundancy and a Video/Data IP address, which was shared by the port pair. The total input bandwidth is limited to 2 Gbps in this mode. This mode of operation has been supported in all previous releases of the RF Gateway 1. Refer to Chapter 3, General Configuration and Monitoring of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.
- **Four Port Independent:** In Four Port Independent mode, the RF Gateway 1 has a greater overall input capacity (4 Gbps) but no physical link redundancy options. Refer to Chapter 3, General Configuration and Monitoring of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.

Note: Four Port Independent mode does not use the Video/Data IP address.

GbE Input Ports				
GbE Data Port Mode	Four Port Independent			
Port Configuration	Port 1	Port 2	Port 3	Port 4
MAC Address	00:50:4b:11:2c:ae	00:50:4b:11:2c:af	00:50:4b:11:2c:b0	00:50:4b:11:2c:b1
IP Address	10.1.1.165	10.1.1.166	10.1.1.167	10.1.1.168
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Negotiation Mode	On	On	On	On

Multicast Sources

The RF Gateway 1 now supports an additional (quaternary) source multicast IP address defined in *Maps/Video Stream Map/Show Advanced Settings*. The default entry "0.0.0.0" implies "don't care" for undefined sources. As with previous releases, the RF Gateway 1 cycles through the four defined source addresses for an MPTS multicast stream until it detects a good stream from one of its specified source addresses.

Hide Advanced Settings

Advanced Settings

Row #	Source IP Address				Ignore UDP Port	PCR PID Select	MPTS Dejitter		Blocked PIDs
	1	2	3	4			Mode	Ref	
0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	One Stream	0	0, 8191, -1, -1
1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	Break Into SPTS	0	0, 8191, -1, -1
2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	False	From PMT	Break Into SPTS	0	0, 8191, -1, -1

SNMP Improvements

The following list identifies miscellaneous 2.02.11 SNMP and RF Gateway 1 proprietary MIB enhancements.

- SNMP access now includes additional fields that can be provisioned like SRM IP addresses, System Clock settings, ARP and Route settings.
- The FTP settings for Configuration Backup, Restore and Licensing were not accessible via SNMP. Release 02.02.11 now allows the setting of FTP server IP address, user name and password for all these operational modes.
- Extraneous errors were logged when using SNMP-WALK operations on IF-MIB or the RF Gateway 1 proprietary MIB (even in terse logging mode). This has been corrected in Release 2.02.11.
- Logging filters can now be configured via SNMP.
- Scrambler Alarm Debounce (System/System Configuration) values are now configured from SNMP.
- Insert Network PID reference in PAT (System/System Configuration) is now configured from SNMP.
- Miscellaneous bug fixes relating to SNMP are available. E.g., clock SNTP mode setting is restricted to unicast (instead of multicast/unicast); GbE port CRC alarm set threshold upper limit value (4294967295) is now settable correctly.

Miscellaneous Improvements

The following list identifies miscellaneous 2.02.11 improvements.

- The RF Gateway 1 Web GUI interface and SNMP capabilities now support /31 networks. The IP address validation is now fixed to allow a zero for the fourth octet for a Multicast IP address (e.g. 224.0.0.0). SNMP supports Multicast Destination IP addresses with a zero fourth octet as well.
- Stream content detection is improved as a result of the RF Gateway 1 performance monitoring speed enhancements allowing content detection in a timely manner.
- Startup logging is enhanced to display RF Gateway 1 application software version to assist with troubleshooting.
- Support for pre-encrypted Motorola DigiCipher streams and their corresponding C0 and C1 tables.
- A negligible dropped packet loss was observed in L2TPv3 mode (.002%). This is now corrected in Release 2.02.11 with enhancements to the MPEG framer of the RF Gateway 1. This negligible packet loss, in previous versions, could result in FTP failures for very large files. This has been resolved in V02.02.11.
- The RF Gateway 1 "Authentication" feature is now improved to warn an authenticated user before forcing another active user to be logged off. This allows gracefully maintaining single user operation of the RF Gateway 1 web user interface.

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 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.
- The Summary page displays the unit rear panel with Conditional Access (CA) port enabled/ disabled as green/grey. The CA port indication represents the on/off setting and does not represent actual link status.



- The database Restore feature in 2.02.11 requires disabling trap settings (in the restore from database file prior to release 2.01.09) before starting the restore procedure. This can be done before starting a restore configuration in 2.02.11. The procedure is needed to allow compatibility with the enhanced SNMP version 1 and 2 trap support in 2.02.11.
- SNMP community strings are provided in 2.02.11 to support SNMP v1 and v2 traps. Prior to release 2.01.09, there was a single community string applicable to all five trap receivers configurable for the operator. In release 2.02.11, in addition to supporting SNMPv1 and v2 traps, each of the five trap receivers have a separate configurable trap community string. This may cause a possible loss of SNMP trap community strings during an upgrade or downgrade procedure. An operator should carefully verify their trap community strings when upgrading to 2.02.11 or downgrading from 2.02.11, if they are being used.
- An upgrade to 2.02.11 from pre-2.01.09 automatically enables insertion of the Network PID into the PAT. If this is an issue in the user's system, it may be disabled on the System/System Configuration page.
- When using /31 IP addressing, although the RF Gateway 1 will allow setting of IP addresses and masks corresponding to this point-to-point protocol, it will not respond to ICMP ping requests.

Licensing

After an upgrade to 2.02.11, a system license is required for the following features. Refer to Licensing in the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.

- Data streams requiring use of the DOCSIS® Timing Interface
- DVB® 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 01.02.20 require a license file. This can be obtained from Cisco after an upgrade to 2.01.09. 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 continues to function until configuration changes are made. However, performing the upgrade may impact functionality of licensed features.

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*. It provides an FTP mechanism to transfer license files to the device. It is recommended that the operator monitor the file transfer status using feedback from the FTP server.

License Overview							
Type	Installed	Count	Usage	Expiration Date	Remaining Time	Expired	Key
DATA	Yes	1	0	00-000-0000	0	No	
DVB_SCRAMBLING	Yes	1	1	00-000-0000	0	No	

Upgrade Information

An RF Gateway 1 unit running release 1.02.20 can be upgraded directly to 2.02.11. 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. However, when upgrading to 2.02.11 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 2.02.11 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 above directly from 1.02.09 must not be attempted. This may cause the RF Gateway 1 to be non-operational.

Refer to Known Issues for SNMP related upgrade, downgrade and database restore considerations.

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.

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, 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 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 2.01.09. 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 shows the Cisco RF Gateway 1-0 Universal Edge QAM web interface. The browser address bar shows the URL <http://10.90.149.80/#>. The page title is "rfgw-1d". The navigation tabs include Summary, Monitor, Alarms, QAMS, Maps, and System. The System tab is selected, and the time is 15:57:02.

On the left, the System Configuration menu is visible, with "IP Network" selected. The main content area displays the IP Network configuration page, which includes the following sections:

- 10/100 Ports:** A table with columns for Management and Conditional Access. The IP Address is 10.90.149.80, and the Subnet Mask is 255.255.255.0.
- Port Pair Configuration:** A table with columns for Port Pair 1 and Port Pair 2. The Redundancy Mode is set to Auto, and the Revert To Primary is set to Enabled.
- GbE Input Ports:** A table with columns for Port 1, Port 2, Port 3, and Port 4. The Negotiation Mode is set to On for all four ports.

Red boxes highlight the following settings:

- The IP Address field (10.90.149.80) in the 10/100 Ports section.
- The Redundancy Mode (Auto) in the Port Pair Configuration section.
- The Revert To Primary (Enabled) in the Port Pair Configuration section.
- The Negotiation Mode (On) for all four ports in the GbE Input Ports section.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of cisco trademarks, go to this URL:

www.cisco.com/go/trademarks.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Product and service availability are subject to change without notice.

© 2009, 2012 Cisco and/or its affiliates. All rights reserved.

August 2012 Printed in USA

Part Number 7018981 Rev B