Cisco RF Gateway 1 Software Release Notes, Release 2.02.21

Overview

Introduction

The Cisco RF Gateway Software Release 2.02.21 contains improvements in VOD stream startup timing and supports the IP-MIB. It now provides the GbE loop-through feature per port-pair with "configurable" redundancy parameters.

Purpose

The purpose of this document is to notify RF Gateway 1 users of the enhancements included in the current release, and informs users of any special upgrade procedures needed for using Release 2.02.21.

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

VOD Stream Startup

While interoperating with Panasonic's DCH-8000 STB (only), it was observed that VOD streams were often torn down immediately after starting. After testing, it was determined that this issue was directly related to stream startup time on the RF Gateway 1.

In software release 2.02.21, the RF Gateway 1 is enhanced to quickly detect new VOD streams arriving at the input. Streams are now detected and processed, on average, 500 ms quicker than before. This speed improvement solves the interoperability issue with the DCH-8000 and also improves overall VOD stream startup performance.

Miscellaneous Improvements

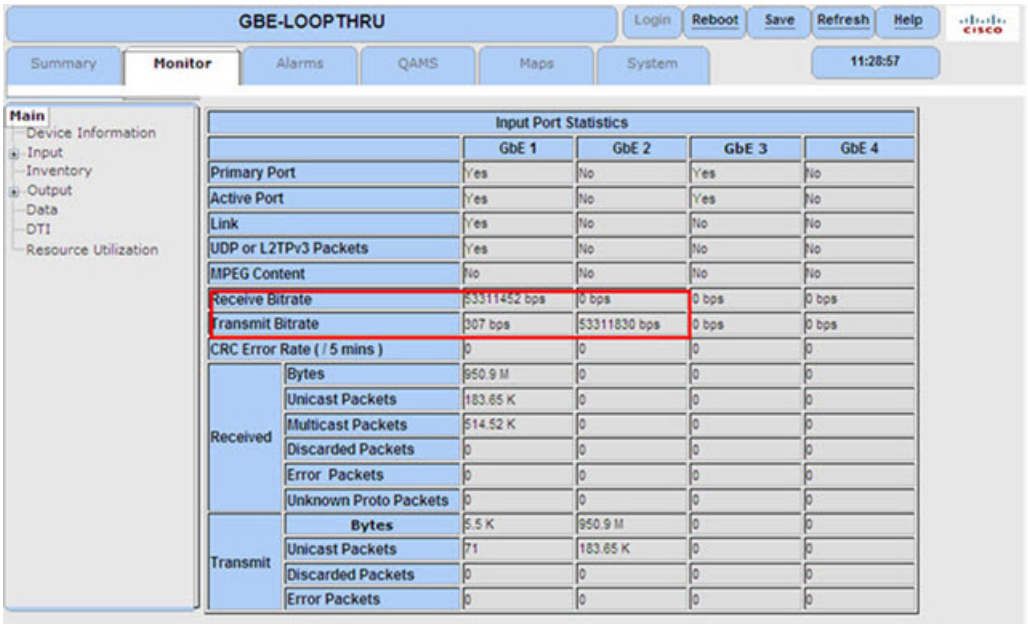
The following miscellaneous improvements have been made in release 2.02.21.

- GbE Loop Through - Software Release 2.02.19 included GbE loop-through capability while operating in Dual Port Pairs mode. The user can operate the RF Gateway 1 in two additional GbE data port modes. Refer to Chapter 3, *General Configuration and Monitoring* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112 for details. The user can navigate to the System/IP Network page to access the two new modes called Dual Port Pairs - Promiscuous Loop Through and Dual Port Pairs - Non Promiscuous Loop Through. While operating in Dual Port Pairs - Non Promiscuous Loop Through mode, packets destined for the active GbE port MAC address (for example, unicast traffic) are forwarded to the RF Gateway 1 packet processor for normal processing. All other multicast or broadcast traffic is sent to the backup port for loop-through. Conversely, while operating in Dual Port Pairs - Promiscuous Loop Through mode, all traffic (including unicast, multicast, or broadcast packets) are looped through to the backup port. In this mode, the traffic that needs to be processed by the RF Gateway 1 will still be processed.

Software Release 2.02.21 enhanced GbE Loop Through configurability allows Redundancy Mode configuration of the port pairs.

Negotiation Mode	On	On	On	On
Port Pair Configuration	Port Pair 1		Port Pair 2	
Video/Data IP	10.1.1.254		10.1.1.253	
Redundancy Mode	Auto		Manual	
Primary Port	2		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)	2		2	

While operating in GbE Loop Through modes, monitoring capabilities are provided to view Receive/Transmit bitrates indicating flow of traffic across GbE ports belonging to a Dual Port Pair. The user can navigate to the *Monitor/Main* page and view statistics as shown below.



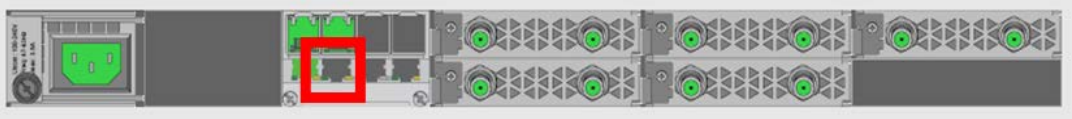
Input Port Statistics

		GbE 1	GbE 2	GbE 3	GbE 4
Primary Port		Yes	No	Yes	No
Active Port		Yes	No	Yes	No
Link		Yes	No	No	No
UDP or L2TPv3 Packets		Yes	No	No	No
MPEG Content		No	No	No	No
Receive Bitrate		53311452 bps	0 bps	0 bps	0 bps
Transmit Bitrate		307 bps	53311830 bps	0 bps	0 bps
CRC Error Rate (/ 5 mins)		0	0	0	0
Received	Bytes	950.9 M	0	0	0
	Unicast Packets	183.65 K	0	0	0
	Multicast Packets	514.52 K	0	0	0
	Discarded Packets	0	0	0	0
	Error Packets	0	0	0	0
	Unknown Proto Packets	0	0	0	0
Transmit	Bytes	5.5 K	950.9 M	0	0
	Unicast Packets	71	183.65 K	0	0
	Discarded Packets	0	0	0	0
	Error Packets	0	0	0	0

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 2.02.21 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 2.02.21.
- SNMP community strings are provided in 2.02.21 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 has 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 2.02.21 or downgrading from 2.02.21, if they are being used.
- An upgrade to 2.02.21 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.
- The system uptime counter rolls over to zero after approximately 49 days of continuous use. This behavior manifests on the web management GUI and via SNMP. The rollover does not cause any operational problems or side-effects on active services.

  Note: A power cycle or reboot of the RF Gateway 1 resets the system uptime counter as part of normal operation.

Licensing

After an upgrade to 2.02.21, a system license is required for the following features. Refer to Licensing in the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.

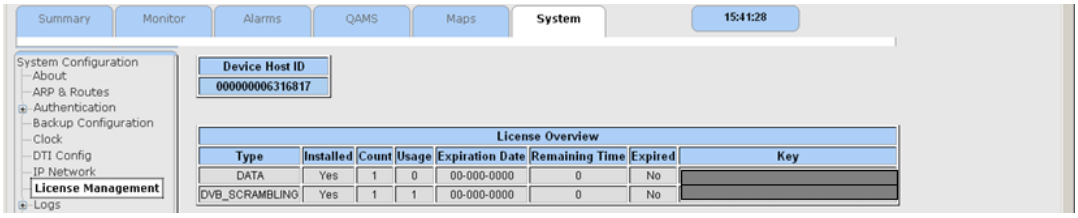
- Data streams requiring use of the DOCSIS® Timing Interface
- DVB® Encryption

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 2.02.21. 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.



Upgrade Information

An RF Gateway 1 unit running release 1.02.20 can be upgraded directly to 2.02.21. 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 2.02.21 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 2.02.21 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 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 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 2.02.21 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. See ***Recording IP Port Configuration Settings*** (on page 13).
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. 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 that 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 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.

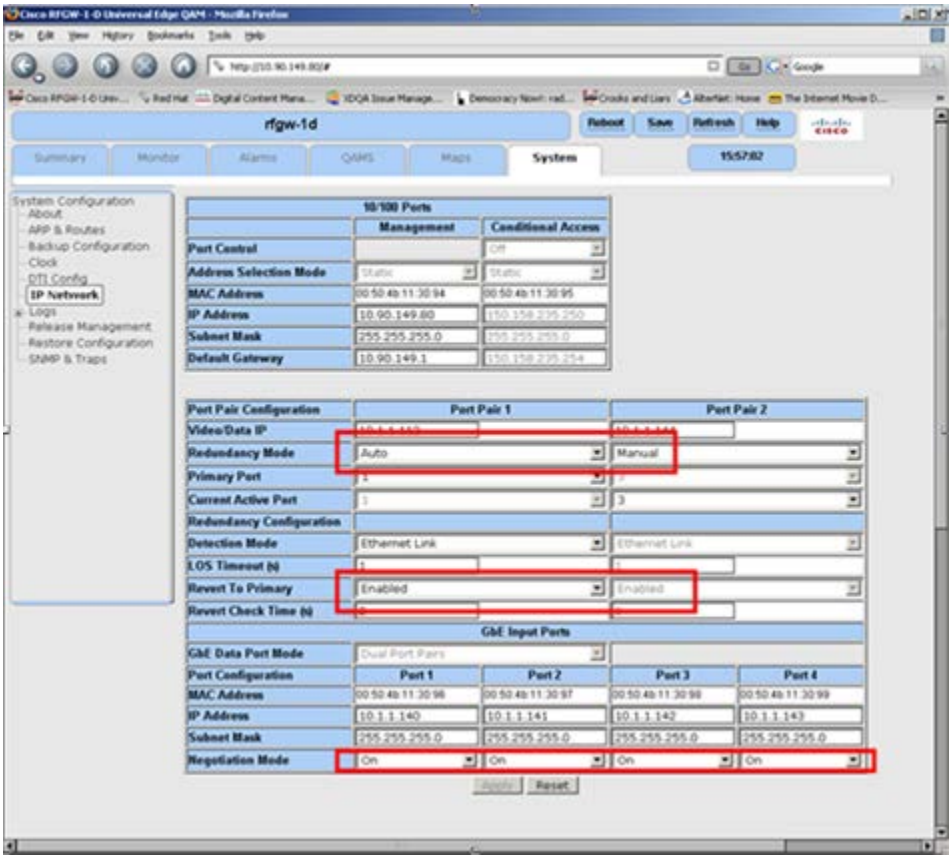
IP Port Configuration Parameter Settings

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 02.02.21 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. 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 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

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 62-7021059-01 Rev B