Cisco RF Gateway 1 Software Release Notes, Release 2.01.09

Overview

Introduction

Software Release 2.01.09 includes DVB Simulcrypt Scrambling capability for the RF Gateway 1 platform. It will support license upgradeable encryption and data features. A user authentication feature is also available for security of the RF Gateway 1 management interface and platform access.

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 2.01.09.

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

DVB Simulcrypt Scrambling

The expanded web interface capabilities include revised system pages with the following enhancements.

- System log configuration supports scrambling-specific log filtering.
- Scrambling configuration is supported via general, EIS-specific and ECMG-specific setup and control web pages.
- License Management has been extended to support the DVB_SCRAMBLING license option necessary to start the scrambling engine. The license key files will be loaded by on-site personnel during the upgrade support process. After the license is loaded on the RF Gateway 1, refresh the License Management page until the license is verified and enabled. Reboot the RF Gateway 1 to enable Scrambling.
- Log configuration has been extended to support Scrambling and provides several new module filters to fine tune logging messages. Due to the potential for high message traffic, it is recommended that Logging be set to **Terse** at the highest level. Several modules default to **Off** and should be left at that level (FTP License, Resource Allocator, Socket, Advanced Filters).
- Scrambler configuration has been added and consists of a page to apply some general system settings, and pages to configure the EIS and ECMG operation.

Authentication

The RF Gateway 1 supports Single and Multi-User (RADIUS) authentication for users. The default factory setting of RF Gateway 1 units shipped with 2.01.09 has authentication disabled. Users can enable and operate in two modes: local (single-user) or remote (multi-user or RADIUS).

Deploying multi-user or remote authentication requires the availability of a standard RADIUS server on the management network of the RF Gateway 1. Refer to Chapter 10, *Authentication* of the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112, for more information.

MIB Support

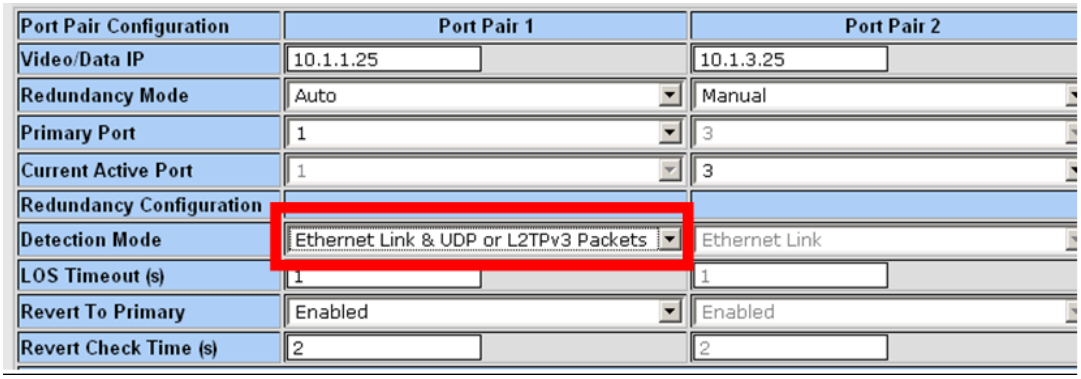
The following list summarizes 2.01.09 changes and enhancements to the RF Gateway 1 SNMP MIB.

- SNMP Version 1 and Version 2 traps are now supported.
- Trap community strings are supported.
- RF port center frequency is now reported in MHz (of type Octet String) instead of kHz.
- IF, IFx, DOCS-IF and Entity MIB support fixes.
- Maximum RF port output power level for quad mode is 54.0 dBmV.
- Minimum frequency range for 6,7,8 MHz port spacing is 48, 48.5 and 49 MHz.
- QAM channel current bandwidth is reported in bps (bits per seconds) instead of Kbps.
- Data map session ID minimum value is now 1 (instead of 0).
- GbE port detection mode now supports *Link* and *Link+UDP* only.
- Data map update set as false is now disallowed.
- Additional MIB objects are now available in 2.01.09 for management access. For example, dejitter buffer depth, CPU and memory usage, clock, active alarms, TriChannel mode, QAM card temp, GbE CRC rate, alarm SET/CLR thresholds, service group ID, QAM channel maximum bandwidth, ON ID, Data map measurement table, DTI client active port, state and timestamp and restore to factory.

Miscellaneous Enhancements

The following list identifies miscellaneous 2.01.09 enhancements.

- License Manager improvements include support for SNMP & GUI
- VxWorks patches for platform software.
- A feature to provide Ethernet Link and UDP or L2TPv3 packet redundancy detection is now available. The operator can select the following options: **Ethernet Link & UDP or L2TPv3 Packets** and **Ethernet Link**. The corresponding MIB object name remains "rfgw1GbePortPair1DetMode" or "rfgw1GbePortPair2DetMode". The RF Gateway 1 will still return "linkAndUDP" or "linkOnly" for each, respectively.

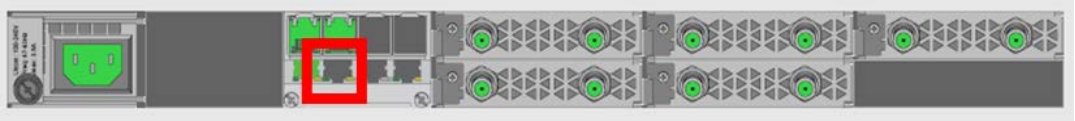


- System logging improvements for Licensing and Scrambler modules
- Web GUI enhancements

Known Issues

The following list identifies known limitations planned to be resolved as part of a GA release.

- The *Summary* page displays the unit rear panel with Conditional Access (CA) port always grey. Up link status indication by a color change to green as supported for GbE ports and the Management port is not currently available. This does not affect operation of the CA port. It also remains pingable on the network. The CA port is shown below.



- The database *Restore* feature in 2.01.09 requires disabling trap settings (in the restore from database file) prior to starting the restore procedure. This can be done before starting a restore configuration in 2.01.09. The procedure is needed to allow compatibility with the enhanced SNMP version 1 and 2 trap support in 2.01.09**.**
- SNMP community strings are provided in 2.01.09 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 2.01.09, 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 2.01.09 or downgrading from 2.01.09, if they are being used.
- Authentication of passwords outside the 4-16 character range is not recommended. Also, use of non-alphanumeric (special) characters is not supported. The web management page does not enforce restrictions in release 2.01.09.
- In 2.01.09, valid users logged in are not automatically logged out after a predetermined idle interval. This allows an unattended session to remain active and presents a security concern.
- While performing SNMP walk operations on supported MIBs, it is observed that extraneous logging entries are recorded. This extraneous logging can be manually disabled using the *System/Logs/Configuration* tab to turn off SNMP logging.
- When a 2.01.09 RF Gateway 1 unit licensed for data or DVB is reverted to an earlier release or database configuration, it has been reported that license files can get deleted without user interaction. It is recommended that users keep appropriate license files available before beginning a release reversion or database restore procedure. Refer to ***Licensing*** (on page 9) for installing the

original license in the event of any changes observed to licensed features. In addition, there is no longer an alarm for a missing license in 2.01.09. The user must check the license management page of the GUI to ensure that the RF Gateway 1 is properly licensed.

- An upgrade to 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.

Licensing

After an upgrade to 2.01.09, a system license is required for the following features. Refer to Licensing in the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.

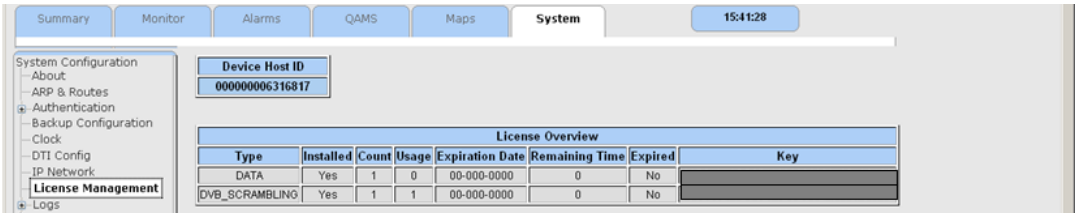
- Data streams requiring use of the DOCSIS Timing Interface
- DVB Encryption

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.



Upgrade Information

An RF Gateway 1 unit running release 1.02.20 can be upgraded directly to 2.01.09. 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 2.01.09 from 1.02.09, an intermediate step of using the bridge release 1.02.19 to arrive at 1.02.20 and finally 2.01.09 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 12).

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 (on page 7) 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 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 *System/IP Network* 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 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.

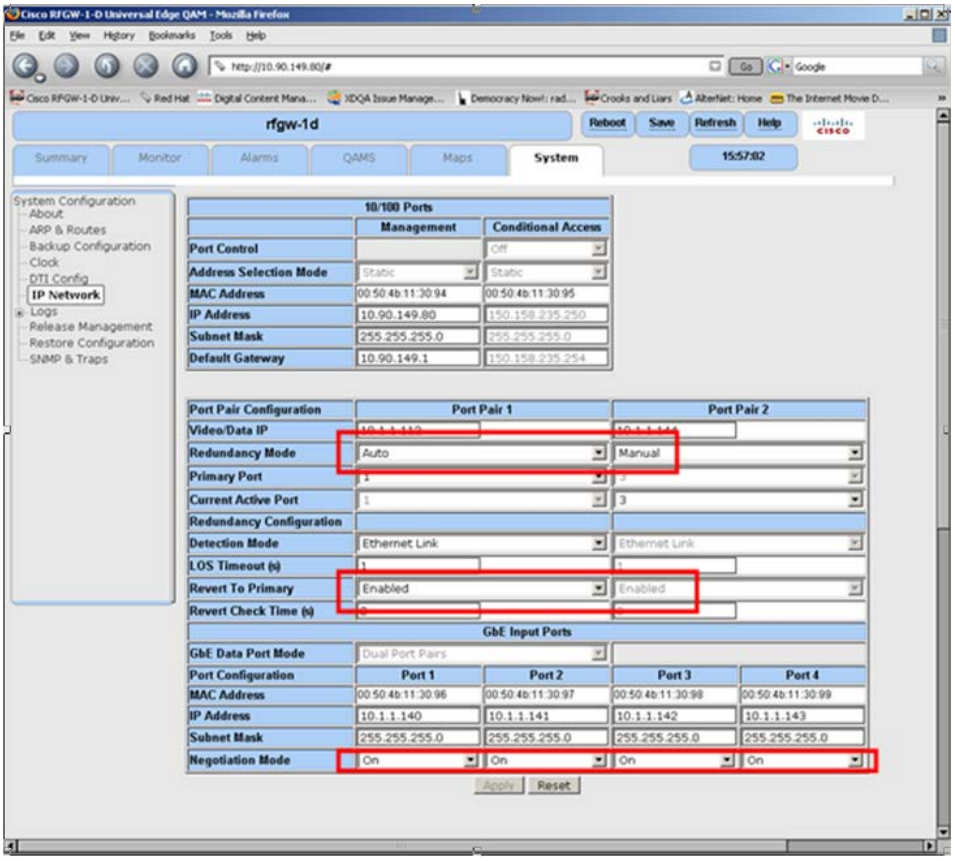
IP Port Configuration Parameter Settings

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.



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 7018300 Rev B