Cisco RF Gateway 1 Software Release 5.01.15 Release Note

Overview

Introduction

RF Gateway 1 (RFGW-1) software Release 5.01.15 addresses a specific Auto Session Refresh failure condition. This condition occurs when PMT PIDs carry input program numbers different from those that are set up in the sessions.

Purpose

The purpose of this document is to notify RFGW-1 users of the enhancements included in the current release, and to inform users of any special upgrade procedures needed for using RFGW-1 software Release 5.01.15.

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 78-4025112-01
- *Cisco RF Gateway 1 System Guide*, part number 78-4024958-01

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

- New Features....3
- Known Caveats....4
- Upgrade Information....5
- Release 5.01.15 Update Summary....6

New Features

Important: Before proceeding, we strongly recommend that you read or review the notes on PID conflicts found in **Downloading System Release Images** in the Configuration chapter of the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01.

Auto Session Refresh - PID Conflict Enhancement

When the RFGW-1 detects an input PID conflict, in some cases, simply correcting the PID conflict is not enough to recover the session. There are some transient ES PID conflict scenarios from which the RFGW-1 does not recover. To handle these situations, an automatic session refresh is done on the MPTS stream. This ensures all the sessions on the MPTS stream are rebuilt properly without operator interference.

The Auto Session Refresh feature was introduced in RFGW-1 software Release 5.01.13. In Release 5.01.15, this feature is enhanced to provide auto recovery when transient PMT PIDs carry input program numbers different from those that are set up in the sessions.

Known Caveats

The following are known issues in this release.

- The RFGW-1 Web management interface is not fully tested with IE-8 and FireFox 3.5.x and later. The RFGW-1 Web interface is tested with IE-6 or Firefox 2.0.0.14 and later. Use of Java 1.6.x is also recommended.
- When using /31 IP addressing, although the RFGW-1 allows setting IP addresses and masks that correspond to this point-to-point protocol, it will not respond to ICMP ping request.

Upgrade Information

An RFGW-1 unit running Release 1.02.20 and later can be upgraded directly to 5.01.15. Refer to **Release Management** in the Configuration chapter of the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01 for more information.

The RFGW-1 reboots automatically at the end of the upgrade process. However, when upgrading to 5.01.15 from 1.02.09, an intermediate step is required: use bridge Release 1.02.19 to upgrade to final Release 1.02.20, and from there, to 5.01.15. The bridge release designated as 1.02.19 has been created to provide a secure and robust upgrade path. Bridge Release 1.02.19 and final Release 1.02.20 have identical user features and functionality.

WARNING:

Do not attempt to upgrade to 1.02.20 or 5.01.15 directly from 1.02.09, as this may cause the RFGW-1 to become non-operational.

Release 5.01.15 Update Summary

The following table describes the enhancements in software Release 5.01.15 in detail.

ID	Severity	Title	Description
CSCuh57320	Severe	Input PID conflict streams not recovered after streams are recovered	RFGW-1 initiates Session Refresh if PID conflict is cleared. This scheme was initially developed to address ES PID conflicts in RFGW-1 software Release 5.01.13. In Release 5.01.15, it is extended to cover cases in which PMT PIDs carry incorrect program numbers for a transient time period.

For Information

If You Have Questions

If you have technical questions, contact Cisco Services at the following URL:

http://www.cisco.com/web/services/

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **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.
© 2014 Cisco and/or its affiliates. All rights reserved.

February 2014 Part Number OL-31526-01