Cisco RF Gateway 1 Software Release Notes, Release 2.06.03

Overview

Introduction

Software release 2.06.03 contains the following enhancements.

- SFTP
- GUI support for downloading an SSH key generated externally
- SNMPv3
- Support for programs with more than 32 PIDs
- 528 MHz spur suppression
- GbE loop-through
- GbE port redundancy operational improvements
- Support for an MPTS with multiple PMTs sharing the same PID

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.

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. *Please read the Securities Features Addendum thoroughly before upgrading.*

- *Cisco RF Gateway 1 Configuration Guide*, part number 4025112

- *Cisco RF Gateway 1 System Guide*, part number 4024958
- *Cisco RF Gateway 1 Software Version 2.6.x Security Features Addendum*, part number 4039214

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:

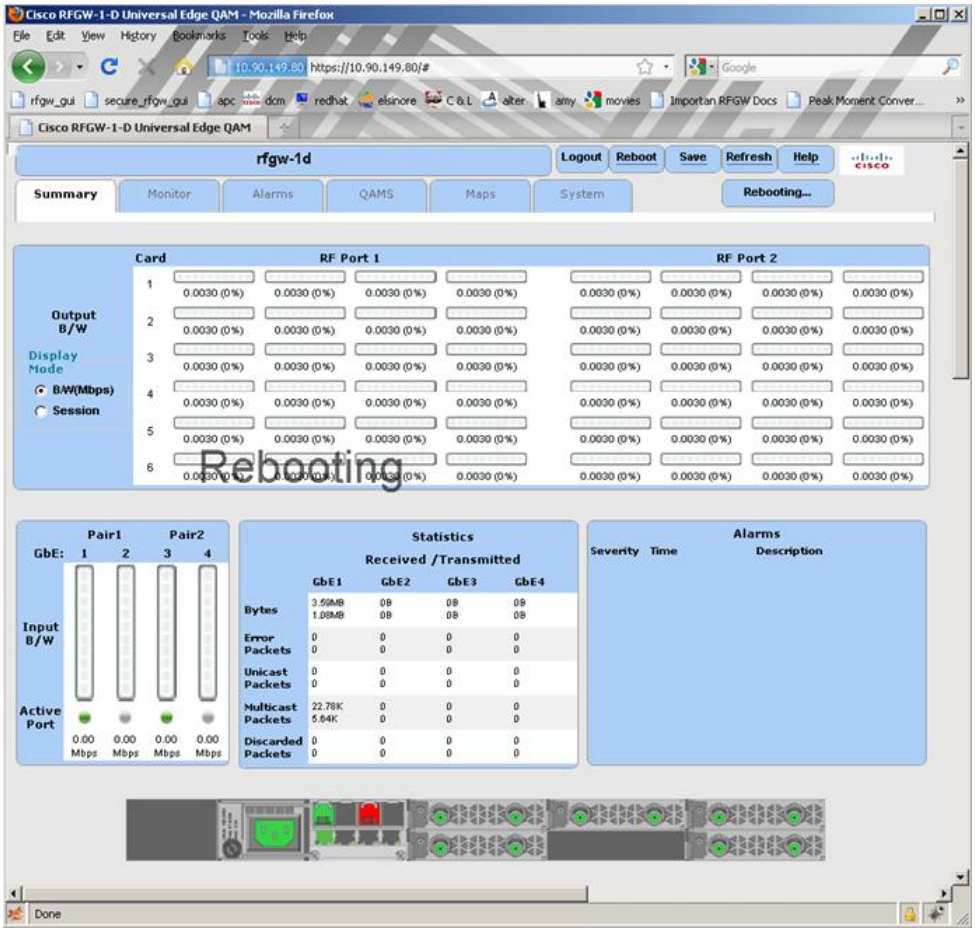
- Ensure that all optical connections are complete or terminated before using this equipment to remotely control a laser device. An optical or laser device can pose a hazard to remotely located personnel when operated without their knowledge.
- Allow only personnel trained in laser safety to operate 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

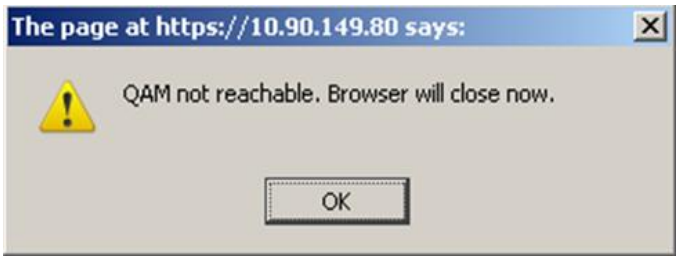
Known Issues

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

- The GUI times out after about 17 seconds of inactivity and does not automatically reconnect to the RF Gateway 1. For example, if the RF Gateway 1 is rebooted from the GUI, the following page is displayed.



After 17 seconds, the following screen is displayed.



Click **OK**.

Result: The browser closes. You will need to reopen the browser after rebooting the RF Gateway 1.

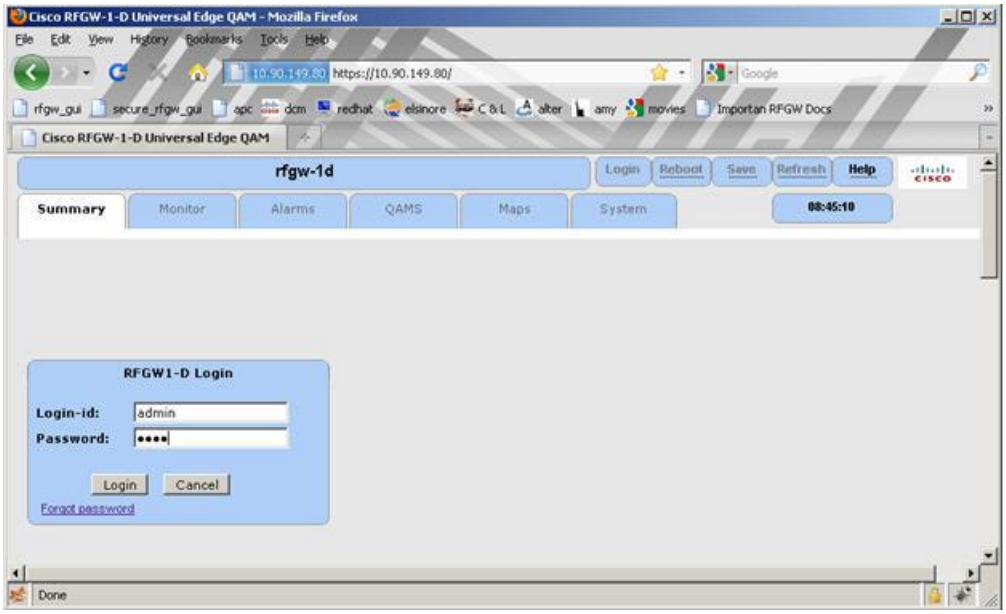
- If port 443 is hit with approximately twenty simultaneous telnet sessions, the RF Gateway 1 runs out of sockets. This may result in interruption of services such as SNMP, HTTP, HTTPS, and others.
- Use of any of the following six characters: ! $ ^ * ( ) in password strings may cause the GUI to display erratically.
- 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 2.00.14 and above. Use of Java 1.6.x is recommended.
- The *Summary* page displays the unit rear panel with the conditional access (CA) port enabled/disabled as green/gray. This represents the on/off setting and not the actual link status.
- The database restore feature requires disabling trap settings (in the "restore from database file" prior to release 2.1.9) before starting the restore procedure. This can be done before starting a restore configuration. This step is needed for compatibility with the enhanced SNMPv1 and 2 trap support in this release.
- SNMP community strings are provided to support SNMPv1 and 2 traps. Prior to release 2.1.9, a single community string was applicable for all five trap receivers configured for the operator. In release 2.2.11 and later, SNMPv1 and 2 traps are supported and 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 2.2.11 or later releases, or downgrading from 2.2.11 or later releases.
- An upgrade to this release from pre-release 2.1.9 automatically enables insertion of the Network PID into the PAT. If this is an issue in the user's system, it may be disabled using the *System/System Configuration* page.
- The system uptime counter rolls over to zero after about 49 days of continuous use. This behavior manifests on the web management GUI and via SNMP. The rollover does not cause 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.
- It is recommended that the telnet and ftp ports be blocked with the firewall in response to the CERT default hashing algorithm in standard authentication API (loginLib) alert. (CERT believes the WRS default hashing alogorithm used by ftp and telnet has too many collisions and is therefore insecure.)

Upgrade Information

After an upgrade to software version 2.06.03:

- All RF Gateway 1 settings will be the same after upgrading, ensuring that data and video continues to flow as before.
- All six authentication passwords, admin and rfgw1-5, will be initialized to 0000 after upgrading.
- During an upgrade to 2.6.x the configurations in the SNMP & Traps page will be copied over to the corresponding SNMPv3 tables. The SNMP & Traps page is not available in 2.6.x, and all configurations done using this page can be done from the SNMP manager, using the target, target params, and notification tables. When downgrading back to 2.5.x, the new configurations made in 2.6.x will not be available. Instead, the previous 2.5.x configurations will be restored.
- If authentication was not disabled before upgrading, you must login as "admin" with 0000 as the password after upgrading. See the following screen.



Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678.277.1000
www.cisco.com

Printed in United States of America
September 2010
Part Number 7021723 Rev A