Cisco RF Gateway 1 Software Release 6.02.01 Release Note

Overview

Introduction

Cisco RF Gateway 1 (RFGW-1) software Version 6.02.01 contains several improvements from Release 6.01.07. This release also includes new features.

Purpose

The purpose of this document is to notify users of the enhancements included in this release, and to identify known issues.

Audience

This document is intended for system engineers or managers responsible for operating and/or maintaining this product.

Related Publications

See 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 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, see the appropriate section of the equipment documentation.

For safe operation of this software, see 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
- Image Information....9
- Bug Toolkit....10
- Resolved Caveats....11
- Known Caveats....13
- Upgrade and Downgrade Information....15

New Features

Alarm Filtering

This feature enhances the alarms configuration in RFGW-1 to satisfy customer requests, and mainly addresses the following:

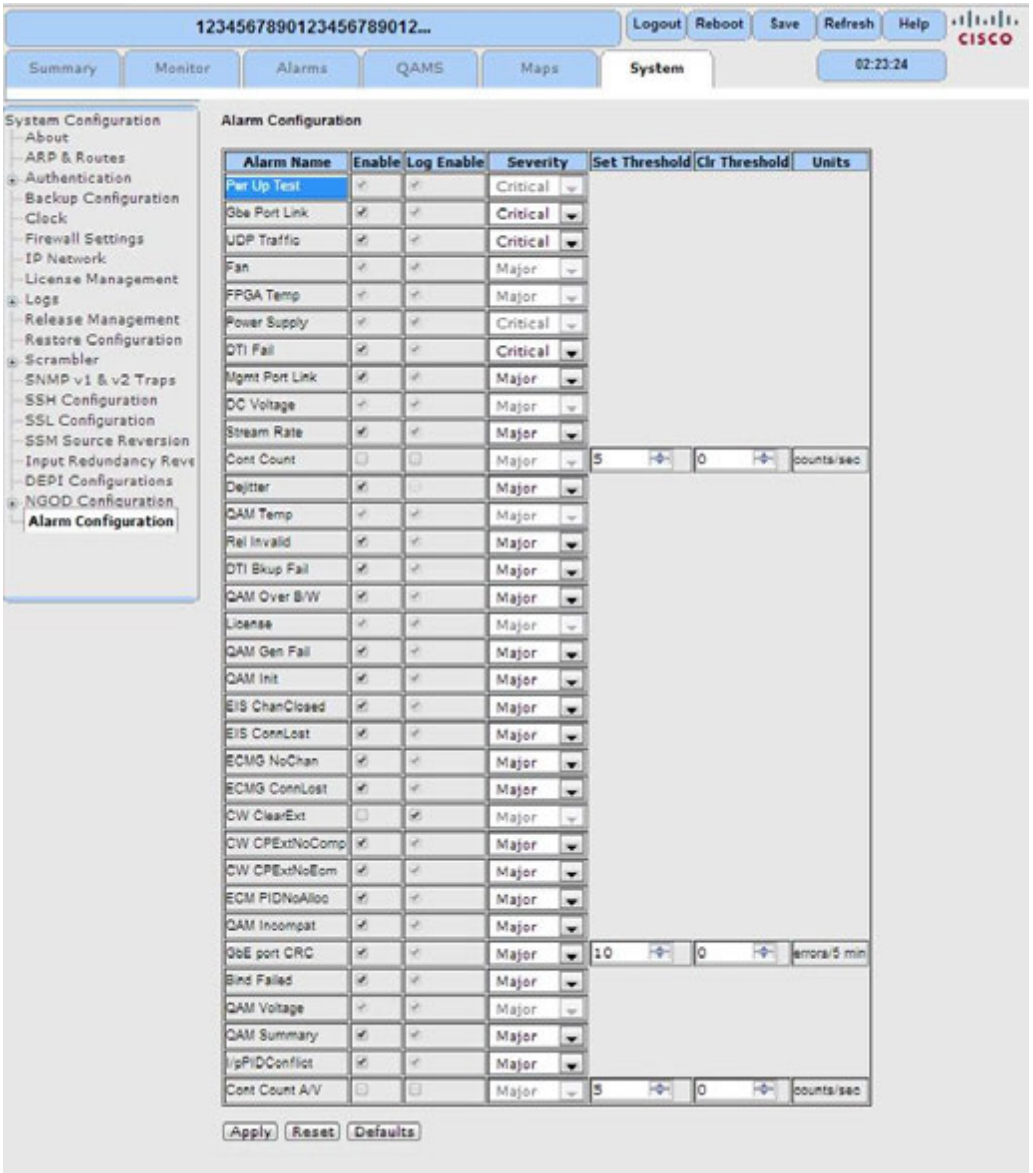
- Acknowledge an alarm condition and clear it with no further notification until the condition changes.
- Enable or disable certain alarms.
- Set the severity levels of the alarms.
- Control the thresholds of certain alarms.
- Filter the alarm log to omit logging CC errors for certain PIDs.

  Note: When receiving a transport stream (TS) from a satellite, PIDs such as EMMs, AITs, and other data carousels are not of interest to the customer, and now may be filtered to reduce the size of the log buffer.

Alarm Configuration

A new Alarm Configuration page has been added to the WebUI to allow for editing of the alarm configuration.

This new page is accessible from the System tab, and appears as shown in the following example.



This page has the following fields:

- **Alarm Name –** Name of the Alarm for which the row settings apply.
- **Enable –** Enables the Alarm notification for a particular alarm type; this will enable the log by default.
- **Log Enable –** Enables the log for particular alarm; editable only when the Alarm is disabled.
- **Severity –** Enables the user to set the severity of alarms (Minor, Major, Critical, Warning).
- **Set Threshold/Clear Threshold/Units –** Helps to generate or clear alarms based on threshold values specified for some alarms.

This page also contains three buttons:

- **Apply –** Sets any changes made in the Alarm Configuration page (either Enable/Severity/Threshold).
- **Reset –** Cancels any changes made in the Alarm Configuration page but not yet applied.
- **Defaults –** Returns any applied changes in the Alarm Configuration page to their default values.

Note:

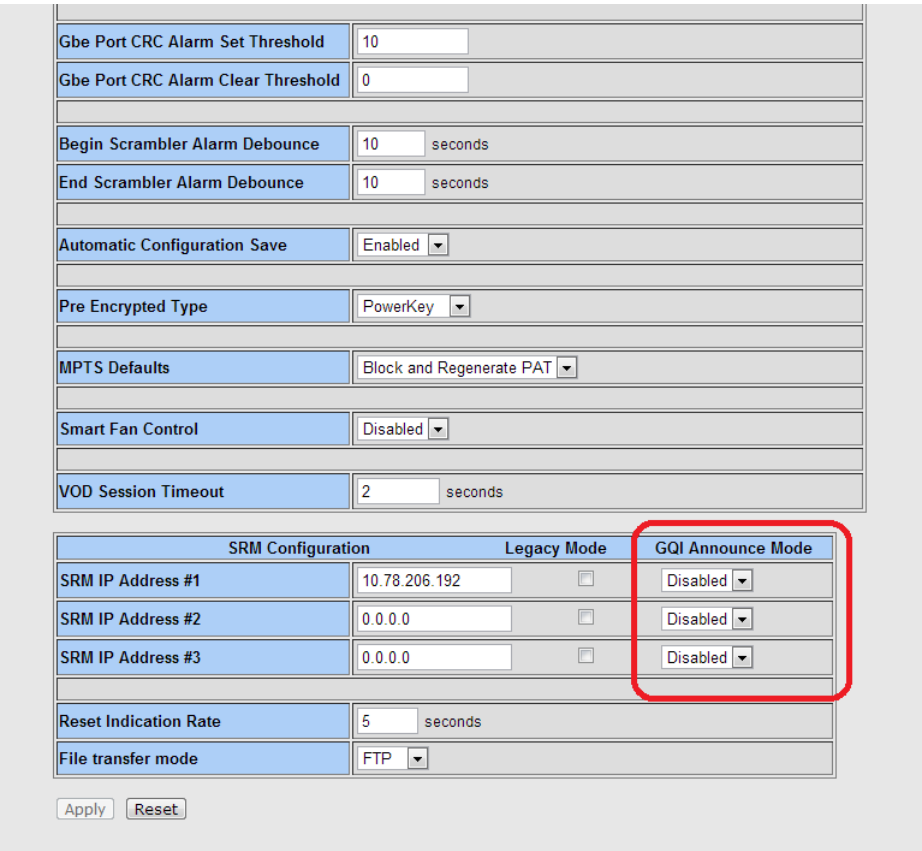
- Users are not permitted to edit certain critical alarm settings. Examples include hardware alarms such as Pwr Up Test, Fan, and so on. In these cases, the corresponding fields on the page are dimmed.
- This enhancement addresses the following CDETS bugs:
  - **CSCty20543 –** Feature request for alarm filtering
  - **CSCtx27655 –** RFGW-1: request for alarm log filtering for certain PIDs/errors
  - **CSCue65478 –** Feature request on implementing delete messages on status page GUI

GQI Announce

A GQI Announce feature has been added to inform the USRM when an input stream starts or stops.

To configure the GQI Announce feature:

1 Choose **System > System Configuration**.
The Device Information page is displayed, as shown in the following example.



2 Change **GQI Announce Mode** as needed to enable or disable the announce feature.

3 Click **Apply** and then click **Save**.

Note: This enhancement addresses the following CDETS bug:

- **CSCtx71661** – SW: Add GQI Announce Message Generation Support

Configurable VOD Session Timeout

When a user pauses a VOD session, the VOD Server continues to send the stream for that session with "stuffing" so that the RFGW-1 does not remove the PMT corresponding to the program from the TS. This keeps the session alive on the STB during the pause period.

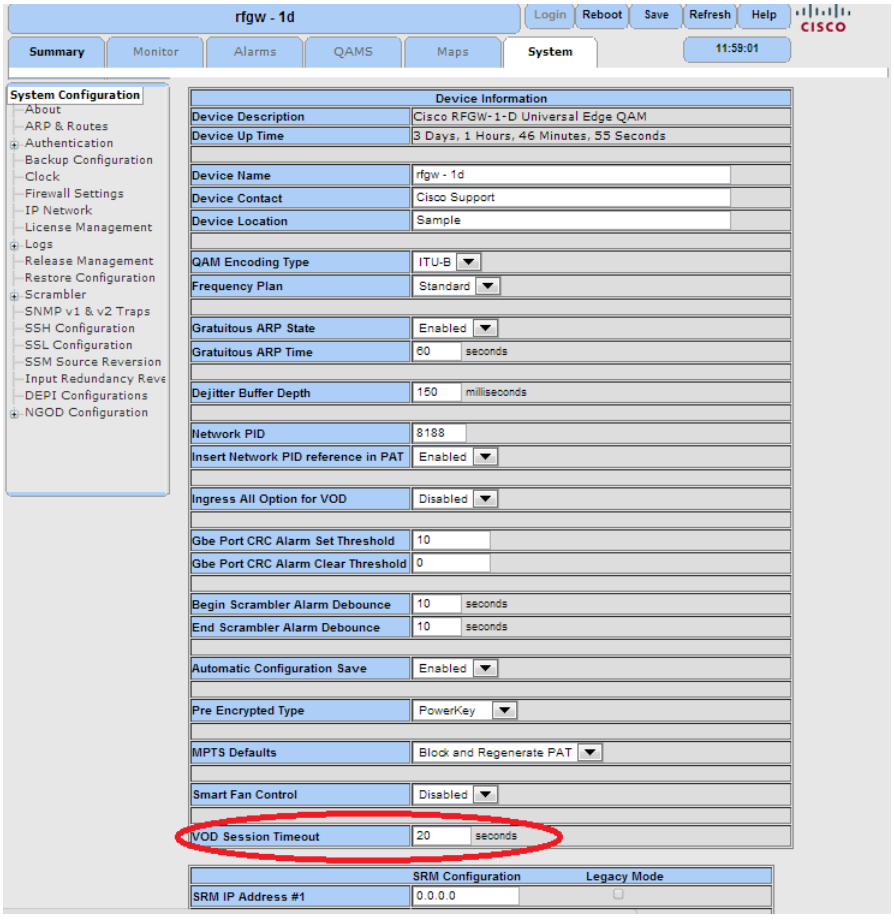
Newer versions of the VOD server stop streaming completely, and rely instead on the RFGW-1 to manage the pause timeout period. In existing RFGW-1 software versions, if the server stops streaming a session to the RFGW-1, the RFGW-1 cuts the PMT from the output immediately. In RFGW-1 software version 6.02.01, a Configurable VOD Session timeout feature is added which instructs the RFGW-1 to maintain the PMT for a session in the output for a specified time period (for example, 2 minutes) after it detects loss of input at the UDP port.

The Configurable VOD Session Timeout feature allows for configuring the timeout parameter. The timeout starts at detection of loss of input for the corresponding UDP port. At the end of the timeout period, the RFGW-1 terminates the session.

To configure the VOD session timeout:

1 Choose **System > System Configuration**.

The Device Information page is displayed, as shown in the following example.



2 Edit the value (in seconds) in the **VOD Session Timeout** field as needed.
3 Click **Apply** and then click **Save**.

Note: This enhancement addresses the following CDETS bug:

- **CSCue59392 –** Configurable timeout parameter session hold time

Support Static UDP Port for NGOD

The RFGW-1 uses D6 to announce static UDP ports that are configured in the stream map. Stream map entries must be active to be announced. The D6 only announces static UDP ports if the QAM Channel mode is either NGOD or VIDEO.

- Only the first 2048 active stream map rows are announced using D6. For example, if there are more than 3000 stream map rows having streams in both active and inactive states, D6 only announces the first 2048 active stream map entries for static UPD ports.
- There are two modes of operation, **D6+ Static UDP** and **D6+R6**. The RFGW-1 uses a standard algorithm: PMT PID = (program_number + 1) * 32.
- The QAM channel can be used for D6+R6, in which case the QAM Channel mode should be NGOD.
- The QAM channel can also be used with D6+Static UDP port, in which case the QAM channel mode should be VIDEO.
- This feature also adds support for ITU–A mode bandwidth.

Note: This enhancement addresses the following CDETS bug:

- **CSCul06906 –** RFGW-1: Support Static UDP port for NGOD

Image Information

The following table lists the files included in this release and their file sizes.

File Name	Size (in Bytes)
app_06.02.01.gz	4834600
becks_06.01.19_fw.gz	2645862
bootrom_V5_02.05.00.bin	2097152
coors_05.00.27_fw.gz	2845585
dual_moretti_07.01.04_06.01.05_fw.gz	5440797
duvel_06.01.13_fw.gz	2681608
rfgw1_rel_06_02_01.xml	1689
miller_lite_05.01.20_fw.gz	56807
superfly_04.04.06_fw.gz	1421717
CISCO-RFGW-1-MIB.my	228683
V06.02.01.zip (Compressed file containing all of the files above minus the MIB files)	17481728

Note:

- The image files should be downloaded using the FTP Server in BINARY mode only.
- V06.02.01.zip is the compressed file of all the image components excluding the MIB files. If using this compressed file, you must decompress it before uploading into RFGW-1.
- The calculated MD5 checksum for V06.02.01.zip is b992d21cc17a7f1cdbb8989608a7eea5.

Bug Toolkit

Follow these instructions to log on to the Bug Toolkit. After you have logged on, you can search for all bugs in this release, search for a specific bug or search, for bugs using specific criteria.

1. Go to **http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl**.
2. When prompted, log on with your username and password. The Bug Toolkit page opens.

   Note: If you have not set up an account on Cisco.com, click **Register Now** and follow the on-screen instructions to register.

Search for a Specific Bug

1. In the **Search for Bug ID** field, enter the ID of the bug you want to view and click **Go**.
2. The Bug Toolkit displays information about the bug in the **Search Bugs** tab.

Search for All Bugs in This Release

1. To search for all the bugs in this release, enter the following search criteria in the **Search Bugs** tab:
   - Select Product Category: Select **Video**.
   - Select Products: Select **Cisco RF Gateway Series**.
   - Software Version: Select **6.2** to view the list of bugs in this release.
2. Click **Search**. The Bug Toolkit displays the list of bugs for this release.

Resolved Caveats

Summary of Defects

This release mainly addresses the following caveats:

- When operating in DEPI, it was noted that the RFGW-1 ipcom_tickd task crashed during rapid PRE switchover from CMTS. Additionally, some malformed l2tp packets were detected after rapid PRE switchover and are handled by RFGW-1. These issues are fixed in this release.
- Some UI issues that were noted, such as incorrect tool tip display and problems related to Authentication, have been addressed in this release.
- When there was a PMT PID conflict, it sometimes led to a PID index leak. This release fixes this issue.
- When encrypted VOD sessions (very short sessions) were churned at a very high rate with DNCS Draco (6.0.x), the RFGW-1 stopped responding to new sessions after a few hours of operation. The issue was identified in internal PKey lib, and is fixed in this release.
- At times during a software upgrade, one of the GE ports locked up and the RFGW-1 recognized no unicast traffic. This issue was seen when continuously reverting between versions 3.2.6 and 6.1.xx, and once over a 3-6 hour test period, during continuous reboot of 6.1.xx using a script.

Specific Issues

In addition to the CDETS bugs listed under ***New Features*** (on page 3), this release resolves the following issues.

ID	Description
CSCua78157	Radius password authentication issue after changing Secret Key.
CSCub67221	Authentication UI: Change Password link not working. The "Change Password" link at the lower left corner of the RFGW1-D Login popup doesn't work. To change the password, log in as an administrator.
CSCuc19076	Insert & remove SFP raises unclearable alarm issue and rfgw1DtiPortMode should be on manual per default of suppressing the alarms are addressed as part of Alarm filtering feature.
CSCuc99824 CSCuc99831	DEPI GUI - DEPI sessions not filtered based on tunnel ID and Channel mode is not disabled in Leaf pages.
CSCud55526	If IP address field in syslog configuration page is changed to empty, it is not allowing the user to proceed further. It asks the user to enter valid IP address. It throws the error if syslog is disabled also.

ID	Description
CSCud55687 CSCud55690	Wrong tool tip inside input redundancy reversion UI. Wrong tool tip inside SSM Source reversion UI.
CSCuf49260	(See CSCuc19076)
CSCuj80060	RFGW-1 : PMT Pid Conflict causes PID index leak.
CSCul40430	Device Name field of RFGW1 should allow 64 char at least.
CSCul48964 CSCul49773	RFGW-1: DEPI: RFGW-1: Task "Ipcom_tickd" crashed during rapid PRE switchover from CMTS. Also identified some malformed packets which were not handled during these PRE switchovers.
CSCul80918	Field issue at NET SERVICOS, where one of the GE ports locked up and there was no traffic (unicast) being recognized by the RFGW. The summary page was showing bit rate. The issue was seen when continuous revert between 3.2.6 and 6.1.xx or continuous reboot of 6.1.xx using a script and the issue happened once during this 3-6 hour test.
CSCum49489	RFGW-1 continuous reboot with 3000 or more stream map configuration. This issue was found during integration testing of new features in this build.

Note: The following information applies to customers who have already upgraded to 6.01.02.

- The Broadcast Scrambling UI Flag was introduced in Release 6.01.02 for controlling the GQI functionality of the RFGW-1. This flag was available on the System Page of the RFGW-1 web UI. This flag was removed to support the version compactness of GQI functionality from Release 6.01.04 onward.
- The Dual Encryption Flag was introduced in 6.01.02 for controlling the total number of QAM channels. The flag was available on the System Page of the RFGW-1 in Version 6.01.02. This flag was removed from Release 6.01.04 onward.
- The default behavior for controlling the Audio and Video streaming during the encryption process, and in case of encryption failure, is *Clear*. If the previous release is 5.1.xx, and only then, the default value is *Black*.

Known Caveats

The following table lists the caveats found during system verification testing. These issues will be fixed in subsequent releases.

Note: These issues can be viewed using the Bug Toolkit. For more information, see ***Bug Toolkit*** (on page 10).

ID	Severity	Description
CSCua16290	4	For simulcrypt applications, not all possible PID mismatch errors between the DNCS and the DCM will be detected. One such undetected error is the case where the DNCS and DCM PIDs are mismatched.
CSCub72868	5	The QAM output oversubscription firmware cannot detect bandwidth excursions above 170%, resulting in missed oversubscription alarms and failures to display, in red, the bandwidth horizontal bar graph on the GUI summary page. Once the bandwidth returns to less than 125%, the issue will clear.
CSCuc30036	4	The display PIDs in hex function doesn't work consistently on the Scrambler/SCG Details page. Don't check the hex display function.
CSCuc32960	3	For continuous feed scrambling applications, if the DNCS qamManager process is stopped, the RFGW-1 is rebooted, and then after about 5 minutes the qamManager process is restarted, the CF sessions don't restart on the RFGW-1. A reboot of the RFGW-1 will clear the issue.
CSCuc35255	3	For applications with encrypted unicast continuous feed sessions, STB debug screens will periodically indicate stream errors even though the streams are error free.
CSCuc37103	3	For scrambling applications, scrambling alarms will be observed during bootup after rebooting the RFGW-1. The alarms are cleared shortly thereafter, and the video will be properly delivered to and decoded by the STBs.
CSCud50641	3	For TBV applications, MPTS data PIDs are sometimes erroneously replicated and routed to another channel in addition to the intended channel. This is a very rare occurrence and has been observed by a single customer at a single site. A reboot of the RFGW-1 will clear the issue.
CSCud55505 CSCud55526 CSCud55562	4	For applications using sysLog, due to an issue with the sysLog server IP Address logic, it is necessary to disable and the re-enable sysLog when the IP address is entered for the first time or whenever it is changed thereafter. Refer to System/Configuration/Logs/Syslog Configuration page on the GUI.

ID	Severity	Description
CSCud81461	5	The "Current Active Port" display on the IP Network page is not applicable and should be ignored in socket redundancy mode of operation. Please ignore it.
CSCud90203	3	For simulcrypt applications, if sessions are torn down, the RFGW-1 is rebooted, and then the sessions are rebuilt in a different order, an output PID mismatch issue will occur, usually on the audio PID. The issue can be cleared by rebooting RFGW-1 between one and two times.
CSCuf50763	3	Summary Page shows Invalid Status for the CA Port is a UI issue and the functionality is not broken. This issue is observed in RFGW 03.02.06 as well. The only difference between 03.02.06 and 06.01.xx build is that CA port is always set to “ON: i.e linkup” by default in 03.02.06 and in 06.01.xx it is “Off:Link down” by default.

Upgrade and Downgrade Information

An RF Gateway 1 unit running Release 1.02.20 or higher can be upgraded directly to 6.02.00. See **General Configuration and Monitoring (Release Management)** in the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01, for more information.

The RF Gateway 1 reboots automatically at the end of the upgrade process. However, when upgrading to 6.02.00 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 6.01.07. 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 directly from 1.02.09 to 1.02.20 or 6.XX.XX. This may cause the RF Gateway 1 to become non-operational.

WARNING:

Before upgrading from 2.2.X.X to 6.1.X.X, be sure to make a backup of your RFGW-1 configuration (Configuration_backup1).

Before downgrading from 6.1.X.X to 2.2.X.X, and if the Octal license is enabled:

1. **Save the configuration and make a backup (Configuration_backup2).**
2. **Remove the Octal license in the RFGW-1.**
3. **Revert to 2.2.X.X and restore the configuration taken while performing the upgrade to 6.1.X.X (that is, Configuration_backup1).**

When upgrading an RF Gateway 1 unit running release 5.1.x to release 6.02.00, you must update through the intermediate bridge release designated as 5.01.13. Upgrading without the bridge release may cause errors when the QAM manager process runs on the DNCS.

WARNING:

Do not upgrade from any engineering release. Revert back to the previous official release, save the configuration, and then perform an upgrade to the latest official release.

For example, if the active Release is 6.1.2_C1 (Engineering build), follow the procedure below:

Revert back to release 6.1.2, click Save to save the configuration, and then download and activate release 6.1.6.

Note:

If authentication is enabled:

- During upgrade from 2.2.X.X to 6.1.X.X, the username and password are set to their defaults. More details on the types of users and usernames are provided in the *Cisco RF Gateway 1 Configuration Guide*, part number 78-4025112-01, available in PDF format at **www.cisco.com**.
- During downgrade from 6.1.X.X to 2.2.X.X, the authentication mechanism is changed, so the user must re-authenticate using the 2.2.X.X schema. In 2.2.X.X, the default username is **rfgw1** and the default password is **0000**.

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.

January 2014 Part Number OL-31265-01