Maintaining and Troubleshooting QAM Devices in the DBDS

Operation and Maintenance Guide

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

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. (1009R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide

Introduction

As a leading provider of cable services, you want to ensure that your subscribers have a compelling experience—one that will prompt them to come back for more. For this reason, maintaining the Quadrature Amplitude Modulation (QAM) devices in your Digital Broadband Delivery System (DBDS) is more important than ever. This guide helps you perform the maintenance tasks and troubleshooting that keep the QAM devices on your DBDS in top condition.

Note: In this guide, the following products are referred to as "QAM devices."

- Conditional Access QAM Modulators (CAQAMs or QAMs)
- Multiple QAM Modulators (MQAMs)
- Gigabit QAM Modulators (GQAMs)
- Dual SFP Gigabit QAM Modulators (Dual SFP GQAMs)
- Gigabit Overlay QAM Modulators (GoQAMs)

Purpose

After reading this guide, you should be able to perform routine maintenance tasks on your QAM devices and identify operational issues before they become major problems. If problems occur, proceed to the troubleshooting tips provided in this guide.

Scope

The purpose of this guide is to provide guidelines and procedures for maintaining correct and efficient operation of your QAM devices. This guide includes normal maintenance tasks and troubleshooting procedures for the QAM devices.

Audience

This document was written for Digital Network Control System (DNCS) operators. Cisco® field service engineers and Cisco Services engineers may also find the information in this document helpful. Since many of the guidelines and checks in this document require the use of UNIX, readers should also be proficient in UNIX.

Document Version

This is the third formal release of this document. In addition to minor text and graphic changes, a procedure for ***Properly Deleting or Removing QAM Devices From Service*** (on page 16) was added to this document.

1

Daily Maintenance Checks

Introduction

QAM devices are integral components of Cisco's DBDS. QAM devices have input interfaces to process several data formats at various rates and then output multiple data formats such as:

- Video
- Audio
- Internet Protocol (IP)

QAM devices maintain high spectral efficiency by integrating powerful adaptive equalizers, interleavers, and error correction. They carry system information, conditional access information, Broadband File Server (BFS) files, and compressed and encoded MPEG transport streams of interleaved voice, video, and data in the RF spectrum to set-tops.

To keep your QAM devices in good working condition, you should perform daily maintenance and routine checks. This chapter provides guidelines and suggestions for the following daily maintenance checks that will help ensure the proper operation of your QAM devices.

- Run the Doctor Report
- Scan digital channels

Purchase a video-on-demand (VOD) or anything-on-demand (xOD) event

- Check third-party applications
- Check Interactive Program Guide (IPG) data
- Purchase a pay-per-view (PPV) event

Use the DNCS Online Help

This guide provides high level maintenance and troubleshooting tips and procedures. The DNCS contains an extensive Online Help system that covers maintenance and troubleshooting procedures. We recommend that you refer to the DNCS Online Help for your system for detailed procedures related to the topics covered in this guide.

For example, you can refer to the **Maintaining Your DBDS** topic in the *DNCS Online Help* for a detailed list of maintenance and troubleshooting procedures.

Assumption

This chapter is written with the assumption that you have already properly unpacked, installed, and configured your QAM devices at your headend or hub. For detailed information regarding unpacking, installing, and configuring your QAM devices, refer to the installation and operation guide for each individual QAM device.

In This Chapter

Run the Doctor Report

Test the Connection to the DNCS (-q Option of the Doctor Report)

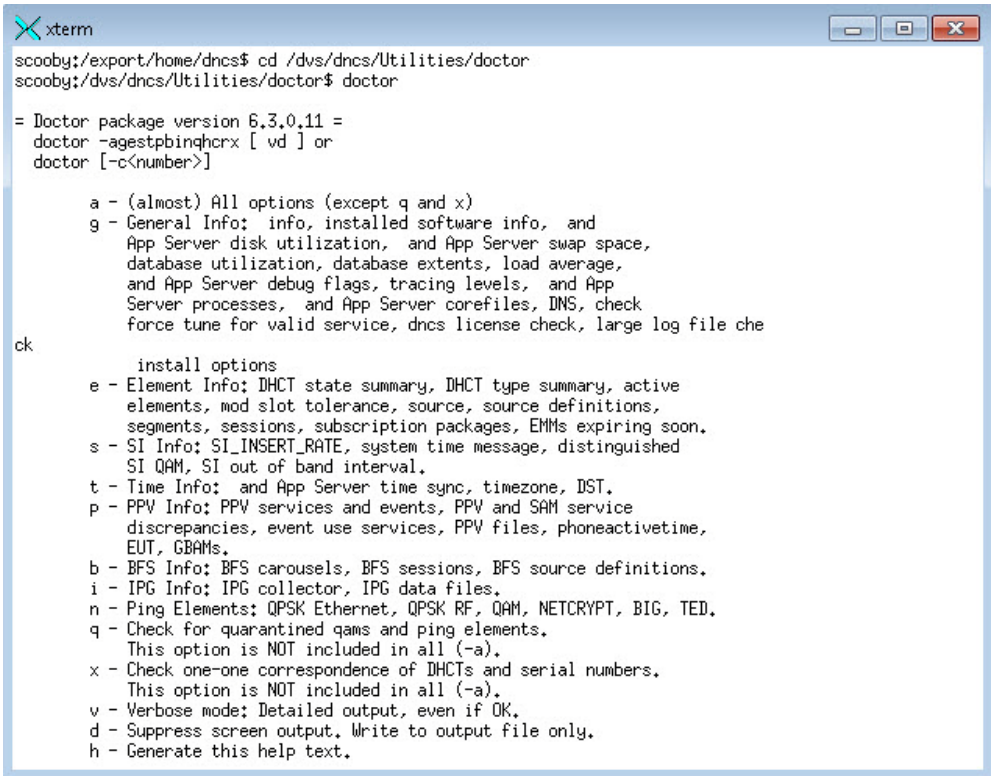
The Doctor Report includes the *–q* option. Through the *–q* option, system operators can ping the QAM, MQAM, GQAM, and GoQAM modulators and test the remote procedure call (RPC) connection between the modulators and the DNCS. Furthermore, the *–q* option generates a report that lists all the modulators, specifies whether the modulators are in a quarantined condition, and notes the date and time stamp of the quarantine, if applicable.

Running the Doctor Report

Use the following procedure to run the Doctor Report on the DNCS.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**. The /dvs/dncs/Utilities/doctor directory becomes the working directory.
3. Type **doctor** and then press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report.

   Note: Each parameter causes the Doctor Report to generate output with specific configuration information.



4 To generate a complete Doctor Report, type **doctor -av** and then press **Enter**.

Results:

- The system generates the Doctor Report listing all system configuration information and directs the output of the report to the screen.
- The system also saves the output of the Doctor Report to a file in the current directory on the DNCS.

Example: The system saves the report with a name similar to **report.061026_0921.doc**.

Notes:

- Depending upon the size of your system, it may take a few minutes for the report to generate.
- The final line of the report lists the file to which the output was saved.
- The report is a plain text file. You can view the report in a text editor of your choice.

Understanding the Doctor Report

The final line of the report generated to the screen lists the file to which the output was saved. The report is a plain text file. You can view the report in a text editor of your choice. Some of the data is only for informational purposes. Other data is preceded by the words **OK, Error**, or **Warning**.

Data in the report preceded by the word **OK** indicates that the data meets Cisco's recommendations regarding the field to which the data applies. Data in the report preceded by the word **Error** may indicate that some system process or function is not operating as it should. System operators should investigate and correct a situation producing an error in a data field. Data preceding by the word **Warning** indicates that a potentially serious condition, such as a disk partition nearing capacity, or that certain data does not meet Cisco's recommendations, has been detected.

Important: Anytime an unexpected or new error appears in the Doctor Report output or if defined thresholds are about to be reached, contact Cisco Services for assistance.

Check Encryption of Digital Channels

To make sure that all digital channels are encrypted and that no digital channels are broadcast in the clear, use a TV with a QAM tuner or a digital set-top to scroll through your digital channels.

TVs with QAM Tuners Require Special Attention

When upgrading QAM devices to new releases of software, you must check to make sure that your digital channels remain encrypted. As a part of the upgrade, you must reset the QAM devices in order for the devices to download the new software from the DNCS. When the software download is complete, the DNCS then recreates any broadcast sessions that were active on the QAM devices. The DNCS also activates encryption for any secure services that were running on the QAM devices.

An increasing number of TVs are being manufactured and sold with QAM tuners that can access services that are not properly encrypted. Therefore, as a part of the upgrade process, we encourage you to verify that the DNCS re-establishes encryption for *all* secure services on the upgraded QAM devices. This extra step ensures that no QAM device that may be carrying content inappropriate for children can be viewed inadvertently when using a TV that is equipped with a QAM tuner.

Check Digital Services and Third-Party Applications

Purchase a VOD or xOD Event

Verify that you can purchase a VOD or xOD event, and then test the trick modes on the remote control for correct operation.

Check Third-Party Applications

Check your local third-party applications to verify that that are available and operating correctly. Some examples of third-party applications might include: GoToit, Compass, BlueStreak, StartOver, and others that may be unique to your system.

Note: Refer to *Avoiding Performance Impact When Monitoring DBDS Operations*, (part number 4014668) for detailed procedures.

Check Interactive Program Guide Data

Check your IPG and verify that you are receiving seven days of accurate IPG data and that the long descriptions and short descriptions are correct.

Purchase a PPV Event

Verify that you can purchase a PPV event.

Daily Checklist

The following checklist is provided as a tool to guide you through the daily checks you should make to ensure the proper operation and function of the QAM devices on your DBDS. You may copy this checklist for your daily use. Save a copy of each completed checklist for future reference.

Date:_____ **Check Time**:_____

Test	Tips	Passed?
Run the Doctor Report	Review the results of the doctor utility to make sure that there are no unexpected errors. If you find unexpected errors, you should correct them immediately.	☐ Yes ☐ No
Check encryption of digital channels	Verify that all digital channels are encrypted and that no digital channels are broadcast in the clear.	☐ Yes ☐ No
Purchase a VOD or xOD event	Verify that you can make the purchase, and then test the trick modes on the remote control for correct operation.	☐ Yes ☐ No
Check third-party applications	Verify that all third-party applications are available and function as expected.	☐ Yes ☐ No
Check IPG data	Verify that the IPG contains 7 days of data.	☐ Yes ☐ No
Purchase a PPV event	Verify that you can purchase a PPV event.	☐ Yes ☐ No

2

Customize Default Configurations

Introduction

In order to meet changing demands, improve performance, or upgrade your system, you may need to customize the default configuration for your QAM devices. This chapter provides the following procedures that will assist you in changing the default configurations for your QAM devices.

- Changing the input mode (SWIF/DHEI/ASI)
- Changing from 64 QAM to 256 QAM modulation
- Setting up QAM devices for passthrough mode

In This Chapter

Changing the Input Mode (SWIF/DHEI/ASI)

Complete these steps to change the input mode of a QAM device.

1. Open the GUI for the QAM and select the **Connectivity** tab.
2. Record the "Connect to:" entries for use later in this process.
3. Change the "Connect to:" entries to **any**, **none**, and **none**.
4. Click **Apply** on the QAM GUI.
5. Open the GUI for the IRT and change the output to **SWIF/ASI/DHEI**.
6. Click **Save** on the IRT GUI.
7. On the QAM GUI change the input to **SWIF/ASI/DHEI** and click **Apply**.
8. Select the **Connectivity** tab again.
9. Change the "Connect to:" entries back to the settings recorded in step 2.
10. Change the cables on the back of the QAM device.
11. Reboot the QAM device.

Changing From 64 QAM to 256 QAM Modulation

On the DNCS, use the appropriate configuration GUI for each QAM device to change the modulation from 64 QAM to 256 QAM.

Note: To avoid issues with the quality of your network feed, before you attempt to change the modulation for a QAM device to 256 QAM, verify that your RF network is performing at an optimal level.

Send High-Definition Signals in the Clear

Overview

The FCC mandates that any high-definition signal that is available over-the-air to a subscriber must be passed through to the subscriber without being encrypted. You achieve this by setting up a QAM device for passthrough mode. The procedures in this section provide the information you need to set up an MQAM to provide a passthrough signal to subscribers. For additional information see *Program and System Information Protocol Configuration for System Releases 2.5, 2.7, 3.5, 3.7, 4.0, 4.2, and CV 3.4 Technical Bulletin* (part number 4011319).

What You Need

The procedures in this section require that you first provide the following:

- An upgrade to the current software version for the QAM device.
- A PC or laptop to connect to the serial port of the QAM device with a terminal emulation software package using the following modem connection settings:
  - 9600 baud
  - 1 stop bit
  - No parity
  - 8 data bits
  - No flow control

Note: For MQAMs, use the hexadecimal number of any program ID (PID) that you do *not* want to automatically pass through the MQAM. See *Optional Commands for the Passthrough MQAM,* in this section, for more information.

Setting up MQAMs for Passthrough Mode

Typically, system operators use QAMs to provide this passthrough signal; however, system operators need the option of using MQAMs to provide the passthrough signal. The procedure in this section provides the information you need to set up an MQAM to provide a passthrough signal to subscribers.

Note: You can only provision ASI port 1 and RF output port 1 on an MQAM for passthrough functionality. When using passthrough functionality on an MQAM, you cannot use the other three ports on the MQAM.

1. Upgrade the MQAM to the current software version.
2. Reboot the MQAM.
3. Power on the PC, connect a PC to the serial port of the MQAM, and then open a terminal emulation program such as Procomm Plus or Hyperterm. You will receive an MQAM prompt similar to the following:

D9476 MQAM>

4 Turn on the passthrough functionality by typing the following command and pressing **Enter**:

pidmode 1 0x0 999

Note: This command allows port 1 on the MQAM to pass 999 PIDs starting with the number 0x0 without encryption. The MQAM stores the information in non-volatile random-access memory (NVRAM) so that the setting is preserved if the MQAM is rebooted.

5 Reboot the MQAM by typing the following command and pressing **Enter**:

boot

Result: Port 1 on the MQAM is now in passthrough mode and passes all PIDs without encryption.

6 Repeat steps 1 through 5 for any additional MQAMs.

Optional Commands for the Passthrough MQAM

If you want to encrypt a block of specific PIDs through the passthrough MQAM port, you can use optional parameters to specify exceptions to the passthrough mode. The PIDs must be in a consecutive numerical block and you must provide the hexadecimal numerical equivalent of the first PID in the block.

To set up a PID block range in the passthrough port that the MQAM will encrypt, type the following command at the MQAM prompt in your terminal emulation program and press **Enter**:

pidmode 1 [hexadecimal starting PID] [decimal number of PID range]

Example:

Typing **pidmode 1 0x1FF0 15** gives you the following results:

- The MQAM is setup for passthrough mode, passing through PIDs with values from 0x0 to 0x1FEF.
- The MQAM does not pass through 15 consecutive PIDs with values starting at 0x1FF0 (0x1FF0 to 0x1FFE). These PIDs can be used for DNCS-inserted packets.

Note: You can specify up to three blocks that identify exceptions to the passthrough mode. Be sure that you know the exact hexadecimal PID values for each block. The MQAM software will not allow you to overlap block values.

3

Check QAM Device Operations

Introduction

As a part of your QAM maintenance procedures, you should check the following system operations on a regular basis.

- Properly Delete or Remove QAM Devices From Service
- Service Groups
- Sessions
- Stat Mux Dejitter Groups on GQAMs
- Multicast Sessions

This chapter provides a high level overview of these system operations and provides a quick path for locating detailed procedures in the *DNCS Online Help* for your system.

In This Chapter

Properly Deleting or Removing QAM Devices From Service

When you delete a QAM device or remove a QAM device from service (set Administrative State to "Offline"), you must perform the procedures listed in this section in the order shown.

Important: For detailed procedures, refer to the *DNCS Online Help* for your system.

1. Use the session list filter to view only the sessions on the QAM device you plan to remove.

   Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Session List

2. After you display the appropriate sessions, tear down the sessions that are on the content QAM device you want to delete or remove from service.

   Important: Do *not* tear down sessions on BFS QAM devices.

   Note: Before you delete a QAM device, you must tear down all of the sessions associated with the QAM device. If you delete a QAM device without first tearing down its related sessions, system performance may be degraded. (Performance degrades because the DNCS uses its resources attempting to associate sessions with a QAM device that no longer exists.)

   Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display Sessions > [Select Session] > Tear Down

3. Do you want to delete the content QAM device?

   - If **yes**, go to step 4
   - If **no**, go to step 5.

4. After you tear down the appropriate sessions, you can delete the content QAM device from the DNCS database. Repeat steps 1 through 4 to delete additional content QAM devices. Then, go to step 6.

   Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [Select QAM device] > File > Delete

   Important: Do *not* attempt to delete a BFS QAM device. Contact us for assistance in deleting a BFS QAM device.

5. After you tear down the appropriate sessions, you can set the content QAM device to "Offline" and Save. Repeat steps 1 through 3 to set additional content QAM devices offline. Then, go to step 6.

Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > > QAM List [Select QAM device] > File > Open > Set Up [QAM device] > Basic Parameters tab > Set Administrative State to "Offline"

Important: Do *not* take a BFS QAM device offline. Contact us for assistance with taking a BFS QAM device offline.

6 You can now power down the QAM device and remove it from service.

Service Groups

Use the following quick path to access the Service Group GUI on the DNCS.

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group

A service group is a set of QAM, MQAM, or GQAM modulator channels that provide narrowcast (VOD) services to a unique group of set-tops. Service groups enable a set-top to identify to the VOD server the VOD QAM resources to which the set-top has access.

If you are going to provide VOD services, you must add a service group for each unique group of VOD QAM modulators. To provide low-demand (library) content, identify this service group as a parent service group and then add child service groups, which provide high-demand content, to the parent service group. If you do not want to manage content by distinguishing between content types, simply add a service group and do not identify it as a parent service group. (Standalone service groups contain no child service groups nor do they belong to parent service groups.)

Important: For additional details, refer to the *DNCS Online Help* for your system release.

Sessions

Use the following quick path to access the Sessions GUI on the DNCS.

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display (x) Sessions

Broadcast sessions are typically created when setting up services for subscribers. Broadcast sessions provide one or more of the following services:

- Services that are delivered to subscribers unscrambled or unencrypted; for example, programming available through the three major networks (ABC, CBS, and NBC) is usually broadcast in the clear
- Services that are encrypted or scrambled so that they are protected from being accessed (stolen) by people who have not paid for the service; usually offered at a price that is in addition to the price for clear services (for example, HBO, Showtime, and music channels)
- Services that carry PPV events that subscribers can choose to purchase in addition to their normal cable programming; has some of the same characteristics as both clear and secure services

Important: For additional details, refer to the *DNCS Online Help* for your system release.

Stat Mux Dejitter Groups on GQAMs

Use the following quick path to access the Stat Mux Dejitter Groups GUI on the DNCS.

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > GQAM > Advanced Parameters tab > Stat Mux Dejitter Groups: Set up

Statistical multiplexed dejitter groups (SMDGs) are used on GQAMs that receive input from a statistical multiplexor (stat mux). SMDGs identify each GQAM input and output that will carry the multiplexed source and also allow the modulator to appropriately process the multiplexed sources. After setting up SMDGs, you can set up sessions for groups to carry.

The SMDG provides the following functions:

- Processes the variable bit rate (VBR) stream as a group of programs
- Ensures optimum dejitter by using one buffer that is dedicated to only one transport stream
- Produces an output stream closer to the received jitter
- Processes the SMDG as a session, so it can be created and torn down as needed

Important:

- Setting up an SMDG enables the GQAM modulator to appropriately process multiplexed sources. Failing to set up SMDGs on GQAM modulators that receive multiplexed sources may result in tiling (macroblocking) of the video on DHCTs.
- If you are using a GQAM modulator that receives input from a statistical multiplexor (stat mux) to send multicast sessions to the network and you already added SMDGs to the DNCS and created a source for the session, follow the procedure to set up multicast sessions on the GQAM SMDGs. You can set up a maximum of 60 sessions on an SMDG.
- SMDG sessions must use the same input port and output port that the SMDG uses. Otherwise, the session may fail.

See *Dual SFP Gigabit QAM Modulator Installation and Operation Guide* (part number 4014102) for detailed configuration procedures.

Multicast Sessions

What are multicast sessions? What are the benefits? What am I looking for? What is a good one? What is a problem?

Use the following quick path to access the Multicast Sessions GUI on the DNCS.

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM > [Select Generic QAM] > Open > Multicast Sessions > New

This section describes how to use the Multicast Digital Session Definition window to set up multicast sessions on a GQAM modulator and on any SMDGs that have been set up for a GQAM modulator.

- GQAM modulator: If you are using a GQAM modulator to send multicast sessions to the network and you already added a GQAM modulator to the DNCS and created a source for the session, follow the procedure to set up multicast sessions on the GQAM modulator.
- GQAM SMDGs: If you are using a GQAM modulator that receives input from a statistical multiplexor (stat mux) to send multicast sessions to the network and you already added SMDGs to the DNCS and created a source for the session, follow the procedure to set up multicast sessions on the GQAM SMDGs. You can set up a maximum of 60 sessions on an SMDG. If you have not set up a SMDG, go to ***Stat Mux Dejitter Groups on GQAMs*** (on page 20).

  Important: SMDG sessions must use the same input port and output port that the SMDG uses. Otherwise, the session may fail.

Before you begin, you must have the following information. To obtain this information, consult your network map or your system administrator, unless noted otherwise in the following list. If you cannot locate your network map, contact Cisco Services for further assistance.

- Source ID as you defined it when you added the content source to the DNCS
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the content from the source (refer to your network map)
- MPEG program number (from your content service provider)
- IP addresses of source devices (up to 3 different source devices can be used)

- Input destination multicast ID address on the generic QAM modulator
- Destination UDP port on the generic QAM modulator

See the *DNCS Online Help* for additional detailed procedures.

4

General Troubleshooting

Introduction

This chapter describes some the most common hardware and network issues that may affect performance and cause errors with the QAM devices in your system. Common issues are described and diagnostic measures are presented to help you to determine why these system issues might be present.

Note: If the suggested actions to any system issue do not yield results or if you are unable to correct a problem that the diagnostics tool seems to demonstrate, contact Cisco Services.

In This Chapter

Macroblocking

If a QAM device is causing macroblocking, refer to the list of possible causes and then complete the check and correct procedure for each possible cause.

Possible Cause(s)	Check and Correct
The QAM device is running the wrong version of code.	1 Upgrade to the most recent version of code 2 Make sure you can load code. Go to ***Unable to Download Code*** (on page 28). 3 Make sure you can load the correct code. Go to ***Device Downloads the Wrong Code (Wrong config file)*** (on page 29).
The data rate as defined for the QAM device sessions is too low, which also means that the data rate of the ASI input to the QAM device is too high.	1 Reduce the amount of incoming data. 2 Reduce the amount of data added to the stream. 3 Increase the modulation mode. 4 Verify and correct session rate targets and threshold values.
Too many sessions are defined for the QAM device from the DNCS.	Reduce the total number of MPEG programs by moving or deleting sessions.
The satellite link contains data errors.	Contact your signal provider to verify if there are any problems with their satellite transmissions.
The modulation mode is incorrect.	Verify and correct the modulation mode.
A hardware problem occurred.	1 Run the Doctor Report on the DNCS, and examine the report for any network connectivity issues or indications of loss of services. See ***Running the Doctor Report*** (on page 3) for additional details. 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Possible Cause(s)	Check and Correct
Additional check and correct procedures	■ Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables. ■ Power down and then power up the QAM device using the on/off rocker-type switch on the back panel, or reset the QAM device from the DNCS. ■ Check the input devices. ■ The RF level settings on the QAM device are not calibrated to the correct frequency. ■ The EEPROM that stores the calibration data for the QAM device is not operational. ■ Mux device is creating an overload. ■ Stat mux dejitter groups are configured incorrectly.

Unable to Build Sessions

Try the following check and correct suggestions if a QAM device will not build sessions.

Possible Cause(s)	Check and Correct
QAM device will not build sessions.	■ Use the following craft port commands to troubleshoot the issue: • print_tab_sessions • print_session_status ■ Check the DNCS for duplicate sessions ■ Check the DNCS for conflicting sessions **Note:** Check the Session Source Definition List on the DNCS to see if the sessions are in conflict. Check for conflicts in relation to hubs, frequency, and/or modulation type. ■ Upgrade to the latest SW version for the QAM device ■ Check the GQAM GbE Link status **Note:** Use the procedure found in ***GQAM GbE Output Does Not Show a Link LED*** (on page 39) to check GQAM GbE link status.

- Check the config file to verify that the DNCS IP address is correct

  Example:

  Note: This applies to CAQAMs, MQAMs, and GQAMs.

  At the bottom of the config file, the following environment variables need to be set correctly:

  # RpcServerIpAddr should contain a string indicating the IP address

  # of the server responsible for replying to un-solicited RPCs

  # such as provision requests, issued from the GQAM.

  #(The format of the IP address should be four decimal numbers separated by dots.)

  # Example: RpcServerIpAddr = 100.101.102.103

  RpcServerIpAddr = 100.101.102.103

  # AlarmServerIpAddr should contain a string indicating the IP address

  # of the alarm server responsible for the QAM. #(The format of the IP address should be four decimal numbers separated by dots.)

  # Example: AlarmServerIpAddr = 100.101.102.103

- **AlarmServerIpAddr = 100.101.102.10**

Note: If, after you have tried all of the above suggestions, the QAM device still does not build sessions, contact Cisco Services for further assistance.

Unable to Download Code

Try the following check and correct suggestions if a QAM device will not download code.

Possible Cause	Check and Correct
The QAM device will not download code.	■ Check for network issues **Note:** See ***Network Issues*** (on page 32) for additional information. ■ Run the Doctor Report **Note:** See ***Running the Doctor Report*** (on page 3) for additional information. ■ Try to ping the device ■ Check the config file for the QAM device

Note: If, after you have tried all of the above suggestions, the QAM device still does not download code, contact Cisco Services for further assistance.

Device Downloads the Wrong Code (Wrong config file)

A QAM device may download the wrong code if the wrong config file is identified in the advanced parameters settings or if the wrong software is associated with the config file.

Note: See the most recent software upgrade documents for your current QAM device for detailed procedures.

If your QAM device downloaded the wrong configuration file, you should verify the number of configuration files in use and what software version is associated with each configuration file.

On occasion, for testing purposes, the configuration file for a test device or a set of test devices is changed to a non-standard value (for example qam111.config instead of qam.config). If your site has been involved in this type of testing (and you are now ready to use the released code again), you should update the configuration file setting for your test units to reflect the default values.

Note: The default configuration file for your QAM device is **/tftpboot/ [name of QAM device.config]**.

Failure to correct a unit from using a unique configuration will result in the unit remaining in the uniquely-specified configuration. Specifically, it will not load the new code and it will continue to load the code specified in the unique configuration file.

In extremely rare cases, the configuration file may have been specified in or may need to be specified in the /etc/bootptab file. In the event that a headend device fails to load the code you intended it to receive, you should check to see if a unique file was specified either through the DNCS GUI or in the /etc/bootptab file before contacting Cisco Services for assistance.

Checking for Multiple Config Files

1. From the DNCS Administrative Console, click **Utilities** and click **xterm**. The xterm window opens.
2. Type **dbaccess dncsdb <<%** and press **Enter**.
3. Type **unload to [name of QAM]data select qam_name, configfile from pdcaqam where modeltype=X**; and press **Enter**.

   Notes: In this command, depending on the type of QAM device, insert one of the following numbers in place of the "X" that follows "modeltype=":

   - For QAMs, the modeltype is **1**
   - For MQAMs, the modeltype is **2**

- For GQAMs, the modeltype is **3**
- For RF GoQAMs, the modeltype is **4**
- For IF GoQAMs, the modeltype is **5**

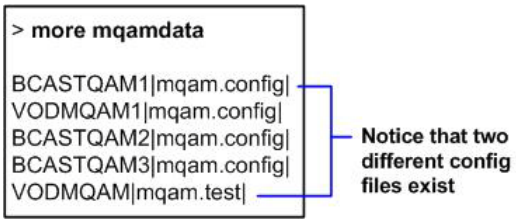
4 Type % and press **Enter**. A result similar to the following output, appears.

```
Database selected.

5 row(s) unloaded.

Database closed.
```

5 Type **more [name of QAM]data** and press **Enter**. A result, similar to the following output, appears.



6 Did more than one config file appear?

- If **yes**, keep the xterm window open and go to step 7.
- If **no**, go to ***Checking the Software Version Associated with the config File*** (on page 31).

7 Do you need to continue to run different versions of software on some QAMs in your network?

- If **yes**, refer to the instructions contained in the software installation instructions for your version of QAM code.
- If **no**, go to step 8.

8 Update the QAMs to use the same config file by performing the following steps:

a From the DNCS Administrative Console, click the **DNCS** tab, and then select one of the following tabs:

- For SR 2.7/3.7/4.2 and later, click **Network Element Provisioning.**
- For SR 2.5/3.5/4.0 and earlier, click **Element Provisioning**.

b Click **QAM**. The QAM List window opens.

c Select the QAM device, click **File** and select **Open**. The Set Up [Name of QAM] window opens.

d Click **Advanced Parameters** and modify the configuration file, as needed.

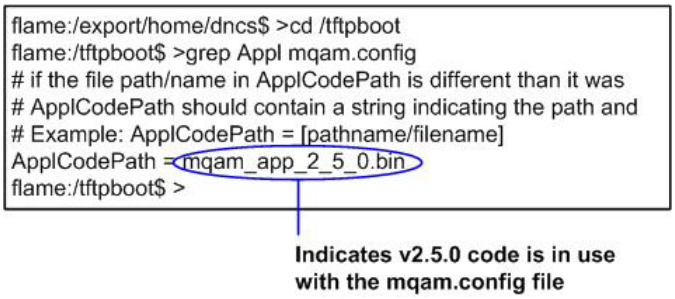
9 Go to ***Checking the Software Version Associated with the config File*** (on page 31).

Checking the Software Version Associated with the config File

1. From the xterm window, type **cd /tftpboot** and press **Enter**. The tftpboot directory becomes the working directory.
2. For each unique config file identified in ***Checking for Multiple Config Files*** (on page 29), type **grep Appl <config file name>** and press **Enter**.

   Example: grep Appl qam.config

   Result: A result, similar to the following output, appears.



3. Is the proper version of software installed?
   - If **yes**, type **exit** and press **Enter**.
   - If **no**, go to the release notes and installation instructions document for the version of software you want to install.

Network Issues

Perform the following tasks if you are experiencing network issues.

- Ensure that you have defined the default gateway correctly (it should be zero [0] or blank)
- Verify that the netmask is correct
- Verify that the MAC address is correct
- Tail the bootpd file and watch to make sure the devices are receiving all data correctly

5

Troubleshoot Front Panel Error Messages

Introduction

Various error messages appear on the front panel LED or in the error log files of each QAM device. This chapter provides information about these error messages along procedures for troubleshooting these messages.

In This Chapter

Runtime Errors on the Front Panel

Runtime errors can occasionally appear on the front panel of a QAM device. If these errors occur infrequently, they can generally be ignored. However, if runtime errors are frequently occurring on your system, reboot the QAM, monitor it for a month and, if the frequent errors reoccur, contact Cisco Services.

Verifying Runtime Errors

To make sure that a runtime error occurred on a QAM device, use the following procedure.

1. Connect to the craft port on the QAM device using a portable PC or laptop.
2. At the command prompt type **alarms** and press **Enter**. A list of the alarms on the QAM device appears on the screen.

   Example:

   D9476 QAM> alarms

   ID: 19 Runtime error

PPC860 Errors Following a Reboot

If a PPC860 error appears on the QAM front panel LED after rebooting the QAM, use the following procedure.

1. Examine the latest /dvs/dncs/tmp/bootpd.XXX log to determine if the QAM device is sending bootp requests to the DNCS.
2. Are bootp requests getting to the DNCS?
   - If **yes**, you have completed this procedure.
   - If **no,** there is a return path issue from the device back to the DNCS. Go to step 3.
3. Remove some of the devices in the chain and boot the QAM into the network closer to the DNCS.

Data Overflow Errors

Data overflow errors are displayed on front panel of the QAM device and indicate that the data rate for this session exceeds the threshold value. If a QAM device is generating data overflow errors, refer to the list of possible causes and then complete the check and correct procedure for each possible cause.

Possible Cause(s)	Check and Correct
The data rate as defined for the QAM device sessions is too low, which also means that the data rate of the ASI input to the QAM device is too high.	1 Reduce the amount of incoming data. 2 Reduce the amount of data added to the stream. 3 Increase the modulation mode. 4 Verify and correct session rate targets and threshold values.
Too many sessions are defined for the QAM device from the DNCS.	Reduce the total number of MPEG programs by deleting sessions.
The modulation mode is incorrect.	Verify and correct the modulation mode.
Upstream devices are sending too many MPEG packets to the QAM device.	Check the upstream devices that are sending MPEG packets to the input ports on the QAM device.
A hardware problem occurred.	1 Run the Doctor Report and examine the report for any network connectivity issues or indications of loss of services. See ***Running the Doctor Report*** (on page 3) for additional details. 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. 3 Replace the QAM device if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM device. 4 If the errors continue to occur, contact Cisco Services for further assistance.
Additional check and correct procedures	■ Verify and correct any session setup problems including the session rate target and threshold values ■ If the session setup is correct, data is becoming corrupted ■ Verify the sources feeding this QAM device

RPC Error Codes

Check for remote procedure call (RPC) errors in the qamManager error log. The qamManager.XXX logs are in located the /dvs/dncs/tmp directory on the DNCS.

The RPC error codes use the following format:

0xWWXXYYZZ

- WW = PRODUCT ID (90 = GQAM)
- XX = TYPE (01 = ALARMS and 02 = ERRORS)
- YY = Major category unique to TYPE
- ZZ = Minor category unique to TYPE and Major category

The following list is an example of the result codes for all RPC calls to the GQAM.

```
const GQAM_NO_ERROR = 0x90020000;
const GQAM_ERROR_RPC_OUT_OF_MEMORY = 0x90020001;
const GQAM_ERROR_RPC_HARDWARE_FAILURE = 0x90020002;
const GQAM_ERROR_RPC_SESSION_NOT_FOUND = 0x90020003;
const GQAM_ERROR_RPC_MISSING_MSK = 0x90020004;
const GQAM_ERROR_RPC_SESSION_ALREADY_EXISTS = 0x90020005;
const GQAM_ERROR_RPC_INSUFFICIENT_MEMORY = 0x90020006;
const GQAM_ERROR_RPC_INSUFFICIENT_CAPACITY = 0x90020007;
const GQAM_ERROR_RPC_PROVISION_FAILURE = 0x90020008;
const GQAM_ERROR_RPC_PROGRAM_NUMBER_CONFLICT = 0x90020009;
const GQAM_ERROR_RPC_BANDWIDTH_UNAVAILABLE = 0x9002000A;
const GQAM_ERROR_RPC_SAME_GIGAIP = 0x9002000B;
const GQAM_ERROR_RPC_GIGAIP_INVALID = 0x9002000C;
const GQAM_ERROR_RPC_GIGAIP_FAILURE = 0x9002000D;
const GQAM_ERROR_RPC_GROUP_SDB_SESSION_FAILURE = 0x9002000E;
const GQAM_ERROR_RPC_INSUFFICIENT_OUTPUT_CAPACITY = 0x9002000F;
const GQAM_ERROR_RPC_ROUTE_CONFLICT_OUTPUT = 0x90020010;
const GQAM_ERROR_RPC_ROUTE_CONFLICT_INPUT = 0x90020011;
const GQAM_ERROR_RPC_ROUTE_NOT_FOUND = 0x90020012;
const GQAM_ERROR_RPC_ROUTE_ALREADY_EXISTS = 0x90020013;
const GQAM_ERROR_RPC_INVALID_MULTICAST_ADDRESS = 0x90020014;
const GQAM_ERROR_RPC_INVALID_SOURCE_ADDRESS = 0x90020015;
const GQAM_ERROR_RPC_STAT_MUX_GROUP_DEJITTER_FAILURE =
0x90020016;
const GQAM_ERROR_RPC_GIGE_TYPE_CONFLICT = 0x90020017;
```

Overflow Buffer Condition

When this condition exists, one or more of the following issues may occur on your system:

- Black screens on TVs when tuned to encrypted channels
- Difficulty installing entitlement control messages (ECMs)
- Unable to add or delete sessions
- Unable to perform code version table (CVT) downloads

Use the following procedure to check for an overflow buffer condition.

1 Connect to the craft port on the back of the BFS QAM using a portable PC or laptop. At the command prompt type **dpart** and press **Enter**.

Example:

D9476 QAM>dpart

A display similar to the following appears on the screen.

Part ID	Size	Num of Free Blocks	Num allocated	Total
19	16	64	0	64
18	64	893	131	1024
17	128	188	68	256
16	256	0	1920	1920
15	512	72	0	72
14	1024	16	0	16
13	128	956	68	1024
12	64	188	68	256
11	128	1024	0	1024
10	32	1980	68	2048
9	8	256	0	256
8	32	256	0	256

2 Find the number of free blocks for Part ID 16. In the preceding example, Part ID 16 shows 0 (zero) free blocks.

3 If the number of free block for Part ID 16 is less than 100, the only recourse at this time is to reboot the BFS QAM. This will free up the number of free blocks on the QAM and allow the code to download to the set-top. Running the **dpart** command again will show that the number of free blocks is now greater than 100.

Important: For a long term solution, obtain and install QAM software version 2.4 or later on your system. This software version has the fix for this issue. Contact your Cisco Program Manager to request the current version of QAM code.

GQAM GbE Output Does Not Show a Link LED

Introduction

If the Link LED on the front panel of the GQAM modulator is not illuminated, use these procedures to troubleshoot the configuration.

Note: These procedures normally only need to be completed during installation. If you continue to have issues with the Link LED, contact Cisco Services.

The gigabit Ethernet port on a GQAM is designed to use interface modules. The interface modules allow the GQAMs to operate with copper or fiber connections. There are two types of interface modules for the GQAM:

- Gigabit Interface Converter (GBIC) module
- Dual Small Form-Factor Pluggable (SFP) module

The GQAMs use the interface modules to communicate with devices in the network. The interface module uses the auto negotiate setting to automatically determine the optimal link rate and duplex mode for the port to operate correctly. The auto negotiate setting must be configured on both the GQAM and the device it is connected to in the network. If only one device is configured for the auto negotiate setting, then there is no link between the devices and the port does not operate correctly. The operator can manually configure the auto negotiate setting on the GQAM or the connected device by using one of the following settings:

- 0 — Off
- 1 — On
- 2 — Query (Auto)

GQAMs are currently being shipped from the factory with the auto negotiate setting configured at 2 for all ports. This setting is commonly used for most interface modules. However, there are module manufacturers that require the auto negotiate setting to be either 0 or 1 to operate correctly. This section provides instructions to manually configure the auto negotiate setting.

Configure Auto Negotiate Setting

We recommend that you complete the following procedure to change the auto negotiate setting. As you begin this procedure, a computer or terminal server is required to be connected to the craft port of the GQAM.

Important: This procedure assumes that the GQAM is powered on. If you do not see a command prompt, press the **Enter** key until the prompt displays on the screen.

Port 1 - Single GBIC Port GQAMs

1. At the command prompt, type **gigaautoneg** and press **Enter**. This command provides the current mode of the GBIC module.
2. Type **gigaautoneg** <number> and press **Enter**. This command changes the auto negotiate setting.

   Important: Type either **1** or **0** for the <number> in the command.
3. Type **gigaautoneg** and press **Enter**.
4. Is the GQAM now operating in the correct mode, and does the GBIC module connect to an input device?
   - If **yes**, you have completed this procedure.
   - If **no**, contact Cisco Services.

Port 2 - Dual SFP GQAMs

1. At the command prompt, type **gigaautoneg-b** and press **Enter**. This command provides the current mode of the GBIC module.
2. Type **gigaautoneg** <number> and press **Enter**. This command changes the auto negotiate setting.

   Important: Type either **1** or **0** for the <number> in the command.
3. Type **gigaautoneg** and press **Enter**.
4. Is the GQAM now operating in the correct mode, and does the GBIC module connect to an input device?
   - If **yes**, you have completed this procedure.
   - If **no**, contact Cisco Services.

Troubleshooting the GBIC

There are three auto negotiate modes that the GQAM configures for a Gigabit Interface Converter (GBIC) module:

- 0 — Off
- 1 — On
- 2 — Query (Auto)

Generally, provisioning the GBIC module on the GbE interface works without difficulty. However, on rare occasions, if the GQAM is set to mode 0, then the GBIC module does not establish a connection with an input device. The operator does not see data passing without the connection to the device. If the following procedure is followed, then the GQAM resets to mode 2 and the GBIC module works correctly.

Important: If you are experiencing issues with the GBIC module on a GQAM, we recommend that you complete the following procedure using a computer or terminal server connected to the craft port of the GQAM.

1. At the command prompt, type **gigaautoneg** and press **Enter**. This command provides the current mode of the GBIC module.
2. Type **gigaautoneg 2** and press **Enter**. This command changes the mode to 2, the Query mode.
3. Type **gigaautoneg** and press **Enter**. This command verifies that the GQAM is now operating in a correct mode, and the GBIC module connects to an input device.

Note: For additional information, see one of the following operations alert bulletins:

- *Configuring the Auto Negotiate Setting on the GQAM (*part number 4020084)
- *Provisioning the GQAM GBIC Interface Module* (part number 4014669)
- *Ensuring Proper GQAM Operation and Provisioning of the GbE Port* (part number 4017870)

6

Troubleshoot Front Panel Alarms

Introduction

Various alarm messages appear on the front panel LED of each QAM device. The tables in this chapter list the most commonly occurring QAM device alarms. For detailed information about these alarm messages, refer to the Troubleshooting chapter of the installation and operation guide for each QAM device.

In This Chapter

GoQAM, GQAM, and MQAM Modulator Front Panel LCD Alarm Messages

This section applies only to GoQAMs, GQAMs, and MQAMs. For QAMs go to ***QAM Modulator Front Panel LCD Alarm Messages*** (on page 53).

The following tables list alarm messages displayed on the front panel LCD, the default level of severity, probable causes for the alarm, and suggestions for correcting the alarm condition. The probable causes and check and correct procedures are arranged in order from the least to the most complicated.

Using the Alarm Troubleshooting Tables

- The alarm types and LCD displays for each alarm are arranged in alphabetical order.
- Alarm messages that occur for the multiple RF outputs or the multiple ASI input ports are listed only once. The numbers in parentheses indicate the range of port numbers that might be affected by the alarm.

  Example: The "Input (1-5) errored MPEG packet" description corresponds to the input port that is affected.

ASI Alarms (MQAM only)

LCD Display	Severity	Probable Cause	Check and Correct
ASI (1-2) errored MPEG packets (MQAM only)	Minor	An error occurred in the header of MPEG packets as they arrived at the indicated Input port	Contact Cisco Services
ASI (1-2) FIFO overflow (MQAM only) See also ASI (1-2) packets were dumped	Minor	A first-in first-out (FIFO) overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the DNCS for the MQAM ■ The data rate as defined from the DNCS for the MQAM session is too low, which also means that the data rate of the ASI input to the MQAM is too high ■ Hardware problem ■ Incorrect modulation mode	1 Reduce the data rate of input to the MQAM by doing the following: • Reducing the amount of incoming data • Reducing the amount of data added to the stream • Increasing the MQAM modulation mode 2 Verify and correct session rate targets and threshold values 3 Contact Cisco Services

LCD Display	Severity	Probable Cause	Check and Correct
ASI (1-2) loss of signal (MQAM only)	Major	No ASI signal. This indicates one or more of the following conditions: ■ An upstream device that provides input to the MQAM has failed or is offline ■ A cable has been disconnected	1 Check for loose or broken DVB ASI cable connections to the MQAM 2 Check that the DVB ASI outputs of upstream devices are active 3 Run the Doctor Report to troubleshoot any network connectivity issues 4 Contact Cisco Services
ASI (1-2) Packets were dumped. (MQAM only) See also (ASI (1-2) FIFO Overflow.	Minor	A FIFO overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the DNCS for the MQAM ■ The data rate as defined from the DNCS for the MQAM session is too low, which also means that the data rate of the ASI input to the MQAM is too high ■ Hardware problem ■ Incorrect modulation mode	1 Reduce the data rate of input to the MQAM by doing the following: • Reducing the amount of incoming data • Reducing the amount of data added to the stream • Increasing the MQAM modulation mode 2 Run the Doctor Report to troubleshoot network connectivity issues 3 Contact Cisco Services

Craft Event Change

LCD Display	Severity	Probable Cause	Check and Correct
Craft event change	Status	QAM device settings were viewed or changed from the craft port	Verify that all services are still functioning correctly

Front Panel Event Change

LCD Display	Severity	Probable Cause	Check and Correct
Front panel event change	Status	QAM device settings were changed from the craft port	Verify that all services are still functioning correctly

Hardware Error

LCD Display	Severity	Probable Cause	Check and Correct
Hardware error	Major	General-purpose hardware error or failure	Contact Cisco Services

Input Alarms

LCD Display	Severity	Probable Cause	Check and Correct
Input (1-5) errored MPEG packets	Minor	Error occurred in the header of MPEG packets as they arrived at the indicated Input port	Contact Cisco Services
Input (1-5) FIFO overflow See also Input (1-5) packets were dumped	Minor	First-in first-out (FIFO) overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the DNCS for the QAM device ■ The data rate as defined from the DNCS for the QAM device session is too low, which also means that the data rate of the ASI input to the QAM device is too high ■ Hardware problem ■ Incorrect modulation mode	1 Reduce the data rate of input to the QAM device by doing the following: • Reducing amount of incoming data • Reducing amount of data added to the stream • Increasing the modulation mode 2 Verify and correct session rate targets and threshold values 3 Contact Cisco Services
Input (1-5) loss of input signal	Major	No signal. This indicates one or more of the following conditions: ■ An upstream device that provides input to the QAM device has failed or is offline ■ A cable has been disconnected	1 Check for loose or broken DVB ASI or GbE cable connections 2 Check that DVB ASI and GbE outputs of upstream devices are active 3 Run the Doctor Report to troubleshoot network connectivity issues 4 Contact Cisco Services
Input (1-5) MPEG continuity error	Minor	MPEG continuity error counter; one or more MPEG packets have been dropped	1 Check one or more upstream devices connected to the GbE ports or the DVB ASI input ports 2 Contact Cisco Services

LCD Display	Severity	Probable Cause	Check and Correct
Input (1-5) MPEG Transport Error	Minor	MPEG transport error indicator counter; error occurred in the header of the MPEG packet	1 Check one or more upstream devices connected to the GbE ports or the DVB ASI input ports 2 Run the Doctor Report to troubleshoot network connectivity issues 3 Contact Cisco Services
Input (1-5) packets were dumped See also Input (1-5) FIFO overflow.	Minor	FIFO overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the DNCS for the QAM device ■ The data rate as defined form the DNCS for the QAM device session is too low, which also means that the data rate of the ASI input to the QAM device is too high ■ Hardware problem ■ Incorrect modulation mode	1 Reduce the data rate of input to the QAM device by doing the following: • Reducing amount of incoming data • Reducing amount of data added to stream • Increasing modulation mode 2 Run the Doctor Report to troubleshoot connectivity issues 3 Contact Cisco Services

OUT Alarms

LCD Display	Severity	Probable Cause	Check and Correct
OUT (1-16) FIFO overflow	Minor	FIFO overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the DNCS for the QAM device ■ The data rate as defined from the DNCS for the QAM device session is too low, which also means that the data rate of the ASI input to the for the QAM device session is too high ■ Hardware problem ■ Incorrect modulation mode	1 Reduce the data rate of input to the QAM device by doing the following: • Reducing amount of incoming data • Reducing amount of data added to stream • Increasing modulation mode 2 Verify and correct session rate targets and threshold values 3 Contact Cisco Services

LCD Display	Severity	Probable Cause	Check and Correct
OUT (1-16) Packets dropped See also Input (1-5) FIFO overflow	Minor	Low priority packets are being dropped. The number of packets at the identified RF output carrier exceeds its capacity. This indicates one or more of the following conditions: ■ Too many sessions defined from the DNCS for the for the QAM device session ■ The data rate as defined from the DNCS for the for the QAM device session is too low, which also means that the data rate of the ASI input for the for the QAM device session is too high ■ Hardware problem ■ Incorrect modulation mode	1 Reduce the data rate of input to the QAM device by doing the following: • Reducing amount of incoming data • Reducing amount of data added to stream • Increasing modulation mode 2 Verify and correct session rate targets and threshold values 3 Reduce total number of MPEG programs by deleting sessions 4 Use a TV to verify program availability 5 Contact Cisco Services

Reset Detected

LCD Display	Severity	Probable Cause	Check and Correct
Reset Detected	Status	QAM device has been reset by either a power loss or a manual reset	Session and alarm provisioning are sent to the QAM device automatically from the DNCS. However, you should also check the following: 1 Verify that there are still no broadcast services on this QAM device 2 Verify that the reset did not adversely affect broadcast services 3 Run the Doctor Report to troubleshoot any network connectivity issues 4 Contact Cisco Services

RF Alarms

LCD Display	Severity	Probable Cause	Check and Correct
RF (1-4) Comm Failure	Major	Digital I/O board is not communicating with the modulator RF board MCU at the specified RF OUT module (1-4). This problem could be caused by a loose or broken cable or by the modulator MCU not being programmed correctly	1 Reset the QAM device 2 Contact Cisco Services
RF (1-4) DC Lock detect error See also RF (1-4) UC Lock detect error	Major	■ Downconverter (DC) lock detect signal not functioning correctly. During Modulator MCU Power On Self Test (POST), the lock detect signal from the downconverter phase-locked loop (PLL) did not indicate an unlocked condition when one existed **Note:** Since the MCU cannot correctly detect locked or unlocked status, the RF Output field displays “MUTED” when this condition occurred ■ The output converter synthesizer lock detect circuitry has malfunctioned	Contact Cisco Services
RF (1-4) DC PLL unlocked	Major	Downconverter (DC) PLL synthesizer cannot lock. The output frequency may not be correct. The RF Output field displays “MUTED” when this condition exists	Contact Cisco Services
RF (1-4) EEPROM failure	Minor	Modulator EEPROM failure. The EEPROM on the modulator board is not present or is not operational. If this alarm is set, RF calibration data is not available and the “RF (1-4) Level not calibrated” alarm is also active	Contact Cisco Services

LCD Display	Severity	Probable Cause	Check and Correct
RF (1-4) Exceeded max temp	Minor	The internal temperature of the QAM device is more than 70ºC (158ºF)	1 Remove vent obstructions 2 Provide more cooling and ventilation 3 Check the exhaust fans 4 Contact Cisco Services **Important:** You should check the temperature on the QAM device daily or more frequently if possible.
RF (1-4) level not calibrated	Minor	One of the RF Level settings is not calibrated to the correct frequency or the EEPROM that stores the calibration data is not operational	Contact Cisco Services
RF (1-4) Power Supply failure	Minor	At least one internal power regulator failed. The RF Output field displays "MUTED" when this condition exists	Contact Cisco Services
RF (1-4) UC Lock detect error	Major	Upconverter (UC) PLL lock detect signal is functioning incorrectly. The RF Output field displays "MUTED" when this condition exists	Contact Cisco Services
RF (1-4) UC PLL unlocked	Major	Modulator UC PLL is unlocked. The output frequency may not be correct. The RF Output field displays "MUTED" when this condition exists	Contact Cisco Services

Runtime Error

LCD Display	Severity	Probable Cause	Check and Correct
Runtime error (Operating System)	Major	General purpose software error	1 Reset the QAM device by the power switch or, if possible, by DNCS Control 2 Contact Cisco Services

Session Alarms

LCD Display	Severity	Probable Cause	Check and Correct
"Session xxx ca error" (where xxx is a number from 0-991)	Minor	An error in the conditional access (CA) encryption for a session has been detected. This could mean that an unencrypted signal is being transmitted	1 Delete the failed session and then restart the session 2 Check and correct the package setup and encryption settings on the DNCS 3 Check the VOD sessions for bad interactive session key (ISM) messages 4 Check all hardware settings 5 Contact Cisco Services
"Session xxx data error" (where xxx is a number from 0-991)	Minor	The data flow for the session is lesser or greater than what has been defined by the DNCS for the session indicating one of the following underflow or overflow conditions: ■ **Cause Code 1 - Underflow** – This session data rate for the session drops to 0 (zero) or is less than expected **Important:** The session rate dropping to 0 (zero) triggers an underflow alarm, but is not the result of a loss of signal condition. When a loss of signal occurs, the underflow alarm is not reported. This prevents the system from being overwhelmed with a large number of session data alarms. Alarms that occur as a result of higher level alarms are not reported. ■ **Cause Code 2-Overflow** – The data rate for this session exceeds the provisioned data rate	1 Verify and correct any session setup problems including the session rate target value. If session data is correct, data may be corrupted because of hardware problems. **Note:** Select data rates that you believe the program should not exceed. 2 For the overflow condition, teardown, rebuild, and then restart the session using a higher bandwidth 3 Run the Doctor Report on the DNCS and examine the report for any network connectivity issues or indications of loss of services 4 Contact Cisco Services

LCD Display	Severity	Probable Cause	Check and Correct
		Cause Code 3 - PID enable error –- A PID that should be enabled is not enabled on the QAM device	1 If this alarm occurs with this Cause Code and then quickly clears, it is not a cause for concern 2 Check the content of the input stream using an MPEG analyzer
		Cause Code 6 - Continuity error – This alarm identifies the specific session on which the Input Port (1-5) continuity error alarm occurred	Contact Cisco Services
		Cause Code 7 - PLL unlocked – The phase lock loop is unlocked for the given session	Contact Cisco Services
		Cause Code 8 - Excess glue frame events – Glue frames prevent macroblocking. Excess glue frame events indicate that the associated output port is receiving too much data. When the MPEG engine in the QAM device nears full output capacity, it begins to selectively choose video PIDs on which it will issue a "freeze frame" code in the MPEG video stream for that program and will drop the video packets for that session momentarily. This will happen only for sessions in which blue framing was enabled when the sessions was created. If this alarm occurs frequently, it is a signal that the output QAM carrying that session contains too much data	Reallocate the session from the QAM that appears to contain too much data to another QAM on the same QAM device modulator or to another QAM device modulator
"Session xxx program error" where xxx is a number from 0 to 991	Minor	**Cause Code 1** – A cyclic redundancy check (CRC) error was detected on a PMT	Delete the session
		Cause Code 2 – A new program map table (PMT) was detected	This is for information only. No action is required
		Cause Code 3 – An attempt to create a session failed	Teardown and rebuild the session
		Program Specific Information (PSI) Table data for the session contains errors	■ Check the upstream MPEG input sources connected to the QAM device ■ Contact Cisco Services

QAM Modulator Front Panel LCD Alarm Messages

The following table lists alarm messages displayed on the front panel LCD of a QAM modulator, the default level of severity, a probable cause for the alarm, and suggestions for correcting the alarm condition. The LCD descriptions for each alarm are arranged in alphabetical order. The probable causes and check and correct procedures are arranged in order from the least to the most complicated.

LCD Display	Severity	Probable Cause	Check and Correct
24 volt supply low	Minor	The 24 V DC power supply is out of specification but has not failed	1 Check the power connections for loose connections or defective wires; then, tighten any loose connections, and replace any defective power connections 2 Check the voltage levels at the power outlet to verify that the levels are correct 3 Contact Cisco Services
Continuity Count Error	Minor	MPEG continuity error counter; one or more MPEG packets have been dropped	1 Check one or more upstream devices connected to the input ports 2 Contact Cisco Services
Craft event change	Minor	QAM device settings were viewed or changed from the craft port	Verify that all services are still functioning correctly
Errored MPEG Packets	Minor	Error occurred in the header of MPEG packets as they arrived at the indicated Input port	Contact Cisco Services
Exceeded Max Temp	Minor	The internal temperature of the QAM modulator exceeded 70ºC (158ºF)	1 Check and clear any obstructions from the vents 2 Check and repair or replace the heating/cooling equipment in the room 3 Check and repair or replace the fan

LCD Display	Severity	Probable Cause	Check and Correct
FIFO Overflow	Minor	First-in first-out (FIFO) overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the DNCS for the QAM device ■ The data rate as defined from the DNCS for the QAM device session is too low, which also means that the data rate of the ASI input to the QAM device is too high ■ Hardware problem ■ Incorrect modulation mode	1 Reduce the data rate of input to the QAM device by doing the following: • Reducing amount of incoming data • Reducing amount of data added to the stream • Increasing the modulation mode 2 Verify and correct session rate targets and threshold values 3 Contact Cisco Services
Front panel changed	Status	A user or a system operator changed provisioning parameters on the QAM modulator using the front panel keys	Verify that all services are still functioning correctly
Hardware error	Major	General-purpose hardware error or failure	Contact Cisco Services

LCD Display	Severity	Probable Cause	Check and Correct
Interface error	Minor	The number of errored packets arriving at the QAM modulator MPEG input ports exceeds the allowed pre-defined threshold **Notes:** ■ This alarm appears and immediately clears when the QAM modulator is powered off and powered on from the back panel ■ This alarm appears when the digital video broadcasting asynchronous serial interface (DVB ASI) cable is loose, disconnected, or defective ■ This alarm appears and immediately clears when either the single wire interface (SWIF) cable or the emitter-coupled logic (ECL) cable is disconnected and then re-connected	1 No action is required when the alarm automatically clears 2 Check for loose DVB ASI connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables 3 Clean up the MPEG input signal to the QAM 4 Contact Cisco Services
Level not calibrated	Minor	The QAM modulator level is not calibrated to its frequency. The QAM modulator continues to operate, but the radio frequency (RF) level may vary beyond specified limits (as much as ±3 dB) when the output frequency changes	1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS 2 Contact Cisco Services
Lock detect logic failed	Major	The synthesizer lock-detect circuitry failed	1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS 2 Contact Cisco Services

LCD Display	Severity	Probable Cause	Check and Correct
Loss of input signal	Major	The carrier detect bit for the installed digital headend expansion interface (DHEI), the single wire interface (SWIF), or the digital video broadcasting asynchronous serial interface (DVB ASI) is not active. None of the bits indicating one of the three input ports (DHEI, SWIF, or DVB ASI) is active **Note:** This alarm also appears and immediately clears when the QAM modulator is powered off and then powered on from the back panel. No action is required in this instance.	1 Check for loose or broken cable connections to the QAM 2 Check that outputs of upstream devices are active 3 Run the Doctor Report to troubleshoot any network connectivity issues 4 Contact Cisco Services
Mod ASIC init failed	Major	The application-specific integrated circuit (ASIC) chip failed to initialize	1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS 2 Contact Cisco Services
NVM failed	Minor	The non-volatile RAM (NVRAM) self-test failed	1 Replace the QAM modulator if you have a spare, or contact your Cisco Program Manager to arrange for replacing or repairing the QAM modulator 2 Contact Cisco Services
Packets were dumped	Minor	FIFO overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the DNCS for the QAM device ■ The data rate as defined form the DNCS for the QAM device session is too low, which also means that the data rate of the ASI input to the QAM device is too high ■ Hardware problem ■ Incorrect modulation mode	1 Reduce the data rate of input to the QAM device by doing the following: • Reducing amount of incoming data • Reducing amount of data added to stream • Increasing modulation mode 2 Run the Doctor Report to troubleshoot connectivity issues 3 Contact Cisco Services

LCD Display	Severity	Probable Cause	Check and Correct
PLL unlocked	Major	The synthesizer phase-locked loop (PLL) cannot lock	1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS 2 Contact Cisco Services
Power supply failed	Minor	The power supply is out of specifications or is not operating correctly	1 Check power source, power wires, and the on/off switch on the back panel of the QAM modulator 2 Contact Cisco Services
Power-up/Reset	Minor or Status	QAM device has been reset by either a power loss or a manual reset	Session and alarm provisioning are sent to the QAM device automatically from the DNCS. However, you should also check the following: 1 Verify that there are still no broadcast services on this QAM device 2 Verify that the reset did not adversely affect broadcast services 3 Run the Doctor Report to troubleshoot any network connectivity issues 4 Contact Cisco Services
Runtime Error	Major	General purpose software error	1 Reset the QAM device by the power switch or, if possible, by DNCS Control 2 Contact Cisco Services
SMC communication failed	Major	The system is unable to communicate with the QAM modulator board when setting provisioning information or polling for status monitoring and control (SMC)	1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables 2 Contact Cisco Services

Boot Screen Error Conditions

This section contains examples of warning screens associated with booting error conditions associated with QAM devices. Some booting error conditions may require you to contact Cisco Services.

The following table lists booting error conditions sorted alphabetically by error type, and provides suggestions for correcting the error condition.

Error Condition	LCD Messages	Check and Correct

Application Code Download Failure Screens	■ Bad TFTP Checksum
	The following message appears if the QAM device is unable to download application code execution files from the TFTP server due to a bad checksum.
	`Bad TFTP App Checksum`
	`Restarting...`
	The QAM device automatically reboots.
	■ Unable to TFTP App Code (Boot Mode=2)
	The following message appears if the QAM device is unable to download application code execution files from the TFTP server during boot mode 2.
	`Unable to TFTP App Code`
	`Restarting...`
	The QAM device automatically reboots.
	■ Unable to TFTP App Code (Boot Mode=1)
	The following message appears if the QAM device is unable to download the application code execution files from the TFTP server during boot mode 1.
	`Unable to TFTP App Code`
	`Continuing Startup...`
	The QAM device then starts the application program.
		A corrupted application file may cause this condition.
		1 Reinstall the QAM device package on the DNCS if all QAM devices have this error condition.
		2 Check IP connectivity.
		3 Contact Cisco Services.

Error Condition	LCD Messages	Check and Correct
Boot Download Failure Screens	■ Unable to TFTP Boot Code (Boot Mode=1) The following message appears if the QAM device is unable to download the boot code execution file from the TFTP server during boot mode 1. Unable to TFTP Boot Code Continuing Startup... The QAM device then starts the application program. ■ Unable to TFTP Boot Code (Boot Mode=2) The following message appears if the QAM device is unable to download the boot code execution file from the TFTP server during boot mode 2. Unable to TFTP Boot Code Restarting... The QAM device then automatically reboots.	An incorrect DNCS configuration may also cause this condition. 1 Reinstall the QAM device package on the DNCS if all QAM devices have this error condition. 2 Check IP connectivity. 3 Contact Cisco Services.
Default Status Screen	If an RF carrier channel cannot be accessed or is missing, the following message appears: CH1 Info Not Available	A possible RF hardware problem occurred. Contact Cisco Services.
Incorrect Configuration File Screens	■ Invalid Config File (Boot Mode 1) The following message appears when in boot mode 1 and the configuration file type is incorrect for the QAM device. The first line of the configuration file contains GqamBootpFileType=1.0. Invalid File format Continuing Startup... The QAM device then starts the application program. ■ Invalid Config File (Boot Mode 2) The following message appears when in boot mode 2 and the configuration file type is incorrect for the QAM device. The first line of the configuration file contains GqamBootpFileType=2.0. Invalid File format Restarting... The QAM device then automatically reboots.	1 Correct the configuration file. 2 Contact Cisco Services.

Error Condition	LCD Messages	Check and Correct

RF Module Code Download Failure Screen	Unable to TFTP RF Code
	The following message appears if the QAM device is unable to download the RF module code execution files for boot mode 1 or boot mode 2 from the TFTP server.
	`Unable to TFTP RF Code`
	`Restarting...`
	The QAM device then automatically reboots.
		1 Check the configuration file.
		2 Check for an incorrect IP address, boot mode, or DNCS address.
		3 Reinstall the QAM device package on the DNCS if all QAM devices have this error condition.
		4 Check IP connectivity.
		5 Contact Cisco Services.

Unable to Boot Successfully	■ Unable to perform BootP (Boot Mode 1)
	The following message appears if the QAM device is in boot mode 1 while unable to perform a successful boot process (BootP).
	`Unable to perform BootP`
	`Continuing Startup...`
	The QAM device then starts the application program.
	■ Unable to perform Bootp (Boot Mode 2)
	The following message appears if the QAM device is in boot mode 2 while unable to obtain a successful BootP.
	`Unable to perform BootP`
	`Restarting...`
	The QAM device then automatically reboots.
		1 Verify that the Ethernet port is connected and that the MAC address for the unit matches the MAC address listing on the DNCS.
		2 Contact Cisco Services.

Error Condition	LCD Messages	Check and Correct

Unable to Download Configuration File from TFTP Server	■ Unable to TFTP Config File (Boot Mode 1)
	The following message appears when in boot mode 1 and the QAM device is unable to download the configuration file from the TFTP server.
	`Problem with Config File`
	`Continuing Startup...`
	The QAM device then starts the application program.
	■ Unable to TFTP Config File (Boot Mode 2)
	The following message appears when in boot mode 2 and the QAM device is unable to download the configuration file from the TFTP server.
	`Problem with Config File`
	`Restarting...`
	The QAM device then automatically reboots.
		An incorrect DNCS configuration may cause this error condition.
		1 Verify that the configuration file provisioned on the DNCS is present in the DNCS File system.
		2 Contact Cisco Services.

7

Customer 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.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

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

678 277-1120
800 722-2009
www.cisco.com

Part Number 4019476 Rev C
April 2012 Printed in USA