CISCO

Configuring and Troubleshooting the Digital Emergency Alert System 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.

CableCARD, OCAP, OpenCable, and tru2way are trademarks of Cable Television Laboratories, Inc.

HDMI, the HDMI logo, and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing, Inc.

Other 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

© 2003-2004, 2006-2008, 2012 Cisco and/or its affiliates. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

About This Guide

Chapter 1 Overview

Emergency Alert System Process	2
Ensure Set-Tops Receive EAS Messages	4
Next Steps	5

Chapter 2 Verify Your EAS Equipment Configuration

Overview	8
Verify the MegaHertz System	9
Verify the Trilithic System	11
Verify the Monroe System with Digital Envoy	13
Verify the Frontline System	15

Chapter 3 Configure the Digital EAS

Overview	
Configure the Network Connection	
Configure the DNCS for EAS Messages	

Chapter 4 Enable FTP and Disable Password Expiration for EAS25

Enable FTP for the EAS	26
Check the Password Expiration Setting for easftp	27
Disable Password Expiration for easftp	28

Chapter 5 Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later 29

Configure the DNCS for EAS Messages	30
Configuring and Verifying the MMMRemote Server Entry in the VASP List	35
Configuring the EAS on the DNCS for System Release 5.0	39
Configure EAS to Properly Function with the CableCARD Module	46
Verifying and Modifying the MMM Out-of-Band Data Rate	49
EAS Suppression on Digital Channels	52
Setting Up and Configuring Weekly Tests	55
Setting Up and Configuring Monthly Tests	59
Conduct EAS Tests	63

V

1

7

17

Chapter 6 Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0

Configure the DNCS for EAS Messages	74
Configuring the EAS on the DNCS	
Configure EAS to Properly Function with the CableCARD Module	
Verifying and Modifying the MMM Out-of-Band Data Rate	
EAS Suppression on Digital Channels	
Setting Up and Configuring Weekly Tests	
Setting Up and Configuring Monthly Tests	
Conduct EAS Tests	110

Chapter 7 Troubleshooting

Troubleshoot Digital EAS Equipment	
Troubleshoot the DNCS Network	
Troubleshoot DNCS Configuration and Performance	
Troubleshoot Weekly and Monthly Tests	
Troubleshoot Set-Top Configuration and Performance	
Troubleshoot CableCARD Module Configuration	

Chapter 8 Customer Information

Appendix A FCC Test Requirements	147
----------------------------------	-----

11.61 Tests of EAS Procedures

Appendix B Disable the ORBIX Daemon on the Application Server151

Disabling the ORBIX Daemon on the Application Server15	52
--	----

Appendix C Configure FIPS Filtering

About FIPS Codes	
Recommendations for FIPS Filtering	
FIPS Code Example	
Configure FIPS Filtering for SR 5.0 and Later	
Configure FIPS Filtering for System Releases Prior to SR 5.0	

Index

155

73

121

145

About This Guide

Introduction

The Federal Communications Commission (FCC), the National Weather Service, and local authorities send emergency alert messages (EAMs) to service providers who broadcast these messages to television subscribers. These messages include regular tests of the Emergency Alert System (EAS), as well as messages that warn of dangerous conditions such as thunderstorms, floods, tornadoes, hurricanes, and earthquakes.

The FCC requires that service providers receive and send Emergency Alert Messages (EAMs). In addition, the FCC requires that service providers conduct weekly and monthly tests of the Emergency Alert System (EAS). By conducting weekly and monthly tests of the EAS, service providers ensure the reliability of their EAS equipment so that subscribers can receive national, state, and local warning messages about emergency situations.

This guide describes the digital EAS and the various EAS vendor components that interface with our Digital Network Control System (DNCS) and the Digital Broadband Delivery System (DBDS).

Purpose

After reading this guide, you will be able to configure, operate, maintain, and test EAS components on the DNCS and the DBDS. Properly configuring, maintaining, and testing your system lets you follow FCC regulations by receiving and then sending EAMs to subscribers through a correctly configured and fully automatic EAS process. If your system does not perform as expected, this guide also includes a troubleshooting section so you can quickly restore your system to full operation.

Scope

Beginning with DNCS System Release (SR) 2.5/3.5/4.0, you have the option of configuring your EAS as one of the following:

- A centralized configuration, where the central DNCS sends the EAMs to all the subscribers' set-tops.
- A distributed configuration, where the central DNCS sends the EAMs to Regional Network Control Servers (RNCS) in geographically dispersed sites. Each RNCS then delivers the EAMs to the subscribers' set-tops.

This document provides configuration instructions for a centralized EAS. If you have a distributed EAS system, refer to the *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342).

About This Guide

This document provides configuration instructions for EAS in a SARA environment. For instructions for configuration of EAS in an tru2way[™] (formerly OCAP[™]) environment, refer to the *Configure the DNCS for tru2way EAS Installation and Operation Guide* (part number 4019780).

Audience

This document is written for operators of digital television systems that use the SARA. System operators, field service engineers, and Cisco Services engineers may also find the information in this document helpful.

Document Layout

This document covers multiple DNCS System Releases (SRs). The following chapters have specific information for certain System Releases:

- Verify Your EAS Equipment Configuration (on page 7) For all System Releases
- *Configure the Digital EAS* (on page 17) For all System Releases
- *Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later* (on page 29) For System Release 5.0 and later
- Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0 (on page 73) - For System Releases prior to SR 5.0

Example: If your system uses SR 4.3, you would follow the procedures in the following chapters, in order:

- Verify Your EAS Equipment Configuration (on page 7)
- *Configure the Digital EAS* (on page 17)
- Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0 (on page 73)
- In addition, if you use the optional FIPS Filtering product, follow the procedures in *Appendix C - FIPS Filtering* (on page 155)

Document Version

This is the seventh release of this document. In addition to minor text and graphic changes, the following table provides the technical changes to this document.

Description	See Topic
Updated document for SR 5.0 and	• <i>Configure the Digital EAS</i> (on page 17)
separated the document into procedures for all SRs, procedures for SR 5.0 and later, and procedures for System Releases prior to SR 5.0.	Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later (on page 29)
	 Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0 (on page 73)
Added RWT and RMT troubleshooting, from FCC documentation	 Troubleshoot Weekly and Monthly Tests (on page 140)
Updated FCC EAS Requirements section based on updated FCC guidelines booklet	 Appendix A - FCC EAS Requirements (on page 147)
Enhanced the FIPS Filtering section and moved that information into a separate appendix.	 Appendix C - FIPS Filtering (on page 155)

1

Overview

Introduction

This chapter provides an explanation of the Digital Emergency Alert System (EAS) process.

In This Chapter

Emergency Alert System Process
Ensure Set-Tops Receive EAS Messages
Next Steps

Emergency Alert System Process

This process describes how the EAS works in a typical Digital Broadband Delivery System (DBDS) that **does not** use our Regional Control System solution. If your DBDS uses a Regional Control System, refer to *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342).

This process also describes how EAS works in a SARA environment. For the process for EAS in an tru2way[™] (formerly OCAP[™]) environment, refer to the *Configure the DNCS for tru2way EAS Installation and Operation Guide* (part number 4019780).

Note: Because many digital systems are very large, an EAM could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product (Federal Information Processing Standards [FIPS] filtering) that you can purchase separately to enable the DNCS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about FIPS filtering, contact the person who handles your account.

The Digital EAS Process

This section describes the process the Emergency Alert System uses to distribute a message from the FCC to the subscribers' homes.

- 1 The FCC or local authority broadcasts an Emergency Alert Message (EAM).
- **2** The RF radio receiver in your headend or at your hub site receives the signal, decodes the EAM, and sends it to the Emergency Alert Controller (EAC).
- **3** The EAC receives the text and audio information from the EAM. It formats the EAM and sends it to the DNCS.
- 4 On the DNCS, the Emergency Alert Receiver Server (EARS) process monitors a designated port to receive EAMs. When EARS receives an EAM, it looks for the audio file for the EAM in the /export/home/easftp directory and sends the EAM to the MMMServer.
- **5** The MMMServer converts the audio file in that directory to AIFF format and places it on the Broadcast File Server (BFS) in the MMMAud Server.
- **6** The MMMServer sends the EAM to one of the following, depending on the system in use, and as shown in the diagram below:
 - Cisco system: The EAM is sent to the PassThru process which delivers the EAM to all set-tops.
 - OpenCable (In Band): The EAM is sent to the siManager which sends the EAM to hosts without CableCARD modules.
 - OpenCable (Out Of Band): The EAM is sent to the QPSK Manager which sends the EAM to hosts with CableCARD modules.

Note: The in-band and out-of-band OpenCable processes are also shown in the following diagram.



- 7 The devices react to the EAM in one of the following manners, depending on the type of device and whether force tuning is used:
 - Set-tops (no force tune): Read the EAM and display a banner with the alert text. The set-top then reads the audio file (if present) and plays the audio associated with the alert.
 - Set-tops (with force tune): Tune to the designated channel that displays the alert text and (if present) audio associated with the alert.
 - CableCARD modules (no force tune): Displays a banner with the alert text.
 - CableCARD modules (with force tune): Tune to the designated channel that displays the alert text.

Ensure Set-Tops Receive EAS Messages

The PassThru process sends PassThru Digital Storage Media Command and Control (DSM_CC) messages. Some of these messages tell the set-top about an EAS alert.

To provide reliable performance, we recommend installing a patch to ensure that EAS messages are sent from the DNCS to the set-tops.

You can also install the patch yourself. If you do, please contact the person who handles your account so that we can track your installation progress.

Releases Affected

This patch affects all currently supported systems running DNCS System Release (SR) 2.2/3.2, SR 2.5/3.5, and SR 4.0, as well as older, unsupported releases.

Which Patch Do I Need?

We recommend that you load the appropriate patch at your earliest convenience. Use the following table to identify which version of the patch you need to install.

System Release	DNCS Application Patch
2.2/3.2	3.0.1.16p13.2EP16
2.5/3.5	3.5.25p4EP2
4.0	4.0.0.27p3EP1
2.7/3.7/4.2	No patch required
2.7.7/3.7.1/4.2.1	No patch required
2.8/3.8/4.3	No patch required
SR 5.0	No patch required

Important: Each DNCS application patch file listed above is included in any Service Pack (SP) released *after* the patch file is created. If you install the appropriate patch file and then install an SP that does not include the fix to the PassThru condition, you will need to re-install the patch file. Before installing a new SP, review the Release Notes that accompany the SP to verify that the appropriate DNCS patch for this issue is included.

Obtaining the Patch

To receive the patch, call Cisco Services.

Next Steps

This document covers multiple DNCS System Releases (SRs). Each chapter has specific information for certain System Releases. It is important to follow the proper steps for the System Release installed at your facility.

If your system uses System Release 5.0 or later, follow the procedures in the following chapters.

- 1 Verify Your EAS Equipment Configuration (on page 7)
- 2 *Configure the Digital EAS* (on page 17)
- 3 Enable FTP and Disable Password Expiration for EAS (on page 25)
- 4 *Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later* (on page 29)
- 5 FIPS Filtering (on page 155) (optional)

If your system uses a System Release prior to SR 5.0, follow the procedures in the following chapters.

- 1 Verify Your EAS Equipment Configuration (on page 7)
- 2 *Configure the Digital EAS* (on page 17)
- 3 Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0 (on page 73)
- 4 Disable ORBIX Daemon (on page 151) (if necessary)
- 5 FIPS Filtering (on page 155) (optional)

2

Verify Your EAS Equipment Configuration

Introduction

The Emergency Alert Controller (EAC) resides at your site and serves as an interface between your EAS receiver and the DNCS. The following companies manufacture EAC solutions that are known to work with the DNCS:

- Sage Alerting Systems, Inc. (MegaHertz)
- Trilithic, Inc. (Trilithic)
- Frontline Communications (Frontline)
- Monroe Electronics (Digital Envoy)

Note: The Monroe Electronics EAS uses an encoder/decoder manufactured by the HollyAnne Corporation.

This chapter contains procedures to verify the configuration of your EAC equipment.

In This Chapter

Overview	8
Verify the MegaHertz System	9
Verify the Trilithic System	11
Verify the Monroe System with Digital Envoy	13
Verify the Frontline System	15

Overview

Before you can configure the EAS on the DNCS, you must verify that your thirdparty EAS equipment is configured and performing correctly. This chapter provides parameters that allow the EAC to communicate with the DNCS. This chapter also provides procedures to verify the performance of your specific third-party EAC and EAS, so that you can achieve optimum system performance when receiving and sending Emergency Alert Messages (EAMs).

Important: Some configuration and troubleshooting information is provided for third-party equipment (such as MegaHertz, Trilithic, Monroe, and Frontline). However, you should always refer to the documentation that comes with that equipment when you configure or troubleshoot that equipment. The scope of this information is to make sure that equipment can communicate with our equipment, not to be a comprehensive configuration and troubleshooting guide for third-party equipment.

This document provides configuration instructions for a centralized EAS. If you have a distributed EAS system, refer to the *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342).

If you have a system using tru2way (formerly OCAP) instead of SARA, refer to *Configure the DNCS for tru2way EAS Installation and Operation Guide* (part number 4019780).

Verify the MegaHertz System

This section provides procedures for verifying the proper configuration and performance of the EAC if you are using a MegaHertz EAS.

Important:

- For detailed installation procedures, refer to the documentation that came with your EAC system.
- Cisco set-tops are designed to receive digital audio at sampling rates of either 8 or 16 kHz. Please ensure that you configure the sampling rate of the EAC correctly if you are transmitting digital EAS audio.

Note: You can find troubleshooting information on this EAC system in the following topics in this document:

- **Troubleshooting the MegaHertz System** (on page 123)
- **Troubleshooting MegaHertz System Performance** (on page 124)

MegaHertz EAC Configuration

Use the values in the following table to set the parameters of your MegaHertz EAC.

Parameter	Value
IP Address	IP address of the DNCS
TCP/IP Port	4098
FTP Port	21
FTP Username	easftp
FTP Password	easftp

Important: There may be additional parameters you need to set on your EAC to complete the configuration process. Refer to the EAC documentation for specific troubleshooting and configuration information.

Verifying MegaHertz EAC Performance

The EAC uses FTP to transfer WAV and TXT files to the DNCS. The system logs these transferred messages in the C:\MCMSA folder as **log.txt**.

Note: You can only check the log file if your system has previously sent EAMs.

Follow these steps to view the log.txt file.

- 1 On the EAC PC, use Microsoft Windows Explorer to locate the C:\MCMSA\log.txt directory and file.
- 2 Double-click the **log.txt** file to open it in Microsoft Notepad.

Note: If you cannot locate the log.txt file, use the **Find** feature of your system to locate the file.

- **3** Does the list of messages recorded in the log.txt file reflect the results of any recent weekly and monthly tests?
 - If yes, close Microsoft Notepad and Microsoft Windows Explorer, you have completed this procedure.
 - If **no**, call MegaHertz Corporation for further assistance.

Note: Go to *Test the EAS from the DNCS* (on page 63) if necessary.

Verify the Trilithic System

This section provides procedures for verifying proper configuration and performance of the EAC if you are using a Trilithic EAS.

Important:

- For detailed installation procedures, refer to the documentation that came with your EAC system.
- Cisco set-tops are designed to receive digital audio at sampling rates of either 8 or 16 kHz. Please ensure that you configure the sampling rate of the EAC correctly if you are transmitting digital EAS audio.

Note: You can find troubleshooting information on this EAC system in the following topics in this document:

- **Troubleshooting the Trilithic System** (on page 123)
- **Troubleshooting Trilithic System Performance** (on page 124)

Trilithic EAC Configuration

Use the values in the following table to set the parameters of your Trilithic EAC.

Parameter	Value
Devices	Contains the IP address of the DNCS
FTP Username	easftp
FTP Password	easftp
FTP Port	21
TCP/IP Port	4098
Enable Digital EAS Support	enabled
Use EAS Duration	selected
Time Zone	Correct value for your location
Originator	EAS Broadcast Station or Cable System selected
EASyNIC Ethernet Port	enabled
IP Address	IP address of the DNCS

Chapter 2 Verify Your EAS Equipment Configuration

Parameter	Value
Subnet Mask	Correct value for your installation
Default Gateway	Correct value for your installation
	0.1.1.1

Digital Audio Sample 8 kHz Rate

Important: There may be additional parameters you need to set on your EAC to complete the configuration process. Refer to the EAC documentation for specific troubleshooting and configuration information.

Verifying Trilithic EAC Performance

The EAC uses FTP to transfer WAV and TXT files to the DNCS. You can view these log files from the EASyPLUS screen.

Note: You can only check the log file if your system has previously sent EAMs.

Follow these steps to view the log files.

Note: This procedure was performed using Trilithic EASyPLUS software version 6.07.

- 1 On the EAC PC, in the Trilithic screen, click the **Logs** tab.
- 2 Select **Download EASy+ Log**. Verify that the log file has a current time and date stamp, and that the information in the log file accurately reflects recent EAS activity.

Note: For support for your Trilithic EAC, contact Trilithic, Inc.

Verify the Monroe System with Digital Envoy

This section provides procedures for verifying proper configuration and performance of the EAC if you are using the Monroe Digital Envoy EAC in your EAS.

Important:

- For detailed installation procedures, refer to the documentation that came with your EAC system.
- Cisco set-tops are designed to receive digital audio at sampling rates of either 8 or 16 kHz. Please ensure that you configure the sampling rate of the EAC correctly if you are transmitting digital EAS audio.

Note: You can find troubleshooting information on this EAC system in the following topics in this document:

- **Troubleshooting the Monroe System with Digital Envoy** (on page 123)
- **Troubleshooting Monroe System with Digital Envoy Performance** (on page 125)

Digital Envoy EAC Configuration

Use the values in the following table to set the parameters of your Digital Envoy EAC.

Parameter	Value
Server Port (TCP/IP Port)	4098
FTP Server IP	IP address of the DNCS
FTP Username	easftp
FTP Password	easftp
FTP Port	21
Com Port Number	Correct value for your installation
Debug ON/OFF	True

Important: There may be additional parameters you need to set on your EAC to complete the configuration process. Refer to the EAC documentation for specific troubleshooting and configuration information.

Verifying Digital Envoy EAC Performance

The EAC uses FTP to transfer WAV and TXT files to the DNCS. The system logs these transferred messages in the C:\java\altronix folder in the log.log file. You can click the JAVA bar to view the transfer in progress.

Note: You can only check the log file if your system has previously sent EAMs.

Follow these steps to view the log.log file.

- 1 On the EAC PC, use Microsoft Windows Explorer to locate the C:\java\altronix folder.
- 2 Click the **log.log** file to open it in Microsoft Notepad.

Note: If you cannot locate the log.log file, use the **Find** feature of your system to locate the file.

- **3** Does the log.log file have a current time and date stamp, and does the information in the log.log file accurately reflect recent EAS activity?
 - If yes, close Microsoft Notepad, and then close Microsoft Windows Explorer; you are finished with this procedure.
 - If no, call Monroe Electronics for further assistance.

Note: Go to *Test the EAS from the DNCS* (on page 63) if necessary.

Verify the Frontline System

This section provides procedures for verifying the proper configuration and performance of the EAC if you are using a Frontline EAS.

Important:

- For detailed installation procedures, refer to the documentation that came with your EAC system.
- Cisco set-tops are designed to receive digital audio at sampling rates of either 8 or 16 kHz. Please ensure that you configure the sampling rate of the EAC correctly if you are transmitting digital EAS audio.

Note: You can find troubleshooting information on this EAC system in the following topics in this document:

- **Troubleshooting the Frontline System** (on page 123)
- **Troubleshooting Frontline System Performance** (on page 126)

Verifying Frontline EAC Configuration

Use the values in the following table to set the parameters of your Frontline EAC.

Parameter	Value
Comm	Correct value for your installation
IP Address	IP address of the DNCS
FTP Port	21
TCP/IP Port	4098
FTP Username	easftp
FTP Password	easftp
Local	Correct value for your installation

Important: There may be additional parameters you need to set on your EAC to complete the configuration process. Refer to the EAC documentation for specific troubleshooting and configuration information.

Frontline EAC Performance

Note: You can only check the log file if your system has previously sent EAMs.

Follow these steps to verify the Frontline EAC configuration and performance using the Frontline Emergency Alert Controller (EAC) Application.

Note: This procedure was performed using the Frontline Emergency Alert Controller (EAC) Application version 1.2.

- 1 In the Frontline Emergency-Alert-Controller (EAC) Application window, click the **Log Status Viewing** icon. The Log window opens.
- 2 Verify that the date and time of the log is the current date and time.
- 3 Verify that the **The Application has been started** message appears.
- 4 Click **OK** to close the Log Status Viewing window.
- 5 Click the **Audio Playback Verification** icon. The Wave File Properties window opens.
- 6 Do the WAV files have a recent time and date stamp?
 - If **yes**, click **Exit** to close the Wave File Properties window.
 - If **no**, call Cisco Services for further assistance.
- 7 Click the **View Header/Text Message** icon. The Text and Header Message Viewing window opens.
- 8 Do the TXT files have a recent time and date stamp?
 - If **yes**, click **Exit** to close the Text and Header Message Viewing window.
 - If **no**, call Frontline Communications (Vela Broadcast) for further assistance.
- **9** Click **Cancel** to return to the Frontline Emergency-Alert-Controller (EAC) Application window.

Note: Go to *Test the EAS from the DNCS* (on page 63) if necessary.

3

Configure the Digital EAS

Introduction

This chapter provides procedures to configure your DNCS to use the EAS, so that you can achieve optimum system performance when receiving and sending EAMs.

Note: The procedures in this chapter are relevant to all DNCS System Releases.

In This Chapter

Overview	18
Configure the Network Connection	19
Configure the DNCS for EAS Messages	20

Overview

To provide optimum system performance, you must configure your EAS correctly.

This document provides configuration instructions for a centralized EAS. If you have a distributed EAS system, refer to the *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342).

This document also provides configuration instructions for EAS in a SARA environment. For instructions for configuration of EAS in an tru2way[™] (formerly OCAP[™]) environment, refer to the *Configure the DNCS for tru2way EAS Installation and Operation Guide* (part number 4019780).

If your system does not function as expected, refer to *Troubleshooting* (on page 121) for troubleshooting procedures for the EAS.

Important: If your system is running DNCS System Release (SR) 2.2/3.2, SR 2.5/3.5, or SR 4.0 (or earlier), you should verify that you have installed the patch as described in *Ensure Set-Tops Receive EAS Messages* (on page 4) before you begin configuring your EAS.

Configure the Network Connection

This section provides information that lets you verify that your EAC is correctly connected to the network.

Connecting to the Ethernet Hub

Connect an Ethernet cable from the EAC to the Ethernet hub of the DNCS.

Important: The Ethernet connection requires an 8-conductor category 5 cable (CAT-5) connected to the RJ-45 port of the EAC.

WARNING:

Be careful not to tangle or strain interconnecting cables or the cables might become unusable. Check all cable connections regularly to make sure that all connections are secure and that the cables are not frayed, tangled, or strained.

The following diagram shows a configuration that minimizes the number of potential failure points.



Configure the DNCS for EAS Messages

This section contains instructions for the following procedures that you must complete to configure the DNCS for receiving and forwarding EAS messages.

- **1** Verifying and configuring (if necessary) the LOCAL_EAS_IP variable in the .profile file.
- 2 Configuring the hosts file.
- **3** Configuring the hosts.equiv file.
- 4 Testing the hosts and hosts.equiv files.
- **5** Configuring the EARServer.
- 6 Verifying the presence of the /export/home/easftp directory.
- 7 Determining the IP address of the DNCS.

Verify and Configure the LOCAL_EAS_IP Environment Variable

Verifying the EAS Variable in the .profile File

You must set the LOCAL_EAS_IP variable in the .profile file to make the EAS work properly. This procedure describes how to set this variable.

- 1 Open an xterm window on the DNCS.
- 2 Type env | grep -i local and press Enter. The system displays the value of environmental variables that contain the word *local*.

Note: The grep command ignores capitalization.

- **3** Do the results show that the LOCAL_EAS_IP variable has been set to the IP address of the DNCS management IP address?
 - If yes, you are finished with this procedure.
 - If no, or if the IP address is incorrect, go to Adding an EAS Variable to the .profile File, next in this document.

Adding an EAS Variable to the .profile File

- 1 Before you begin, you need the public IP address of the DNCS. Check your network map or with your system administrator for the public IP address of the DNCS.
- 2 Open an xterm window on the DNCS.
- **3** Type cd /export/home/dncs and press Enter. The /export/home/dncs directory becomes the working directory.
- 4 Edit the .profile file to append the following line to the file: export LOCAL_EAS_IP=[management IP address of the DNCS] Note: Do not include the brackets [] in the IP address.
- 5 Save the file and close the editor.

- 6 Type . . / .profile so the DNCS uses the updated .profile file. **Note:** Be sure to type a space between the first two periods.
- 7 Stop and restart (bounce) the EARs process on the DNCS.

Configuring the hosts File

Follow these steps to configure the hosts file on the DNCS.

- 1 Open an xterm window on the DNCS.
- 2 Type su and press Enter. The system prompts you for a password. Note: This login is for the system super user.
- 3 Type the password and then press **Enter**. The prompt changes to the pound sign (#).

Note: If necessary, see your system administrator to obtain the password.

- 4 Type cd /etc and press Enter. The /etc directory becomes the working directory.
- 5 Open the **hosts** file in a UNIX text editor. This file is a list of Internet hosts (servers) and IP addresses.
- 6 In the first section of the Internet host table, add the following line to the list: [ip addr] eac

Note: In this procedure **[ip addr]** is the IP address of the EAC. Do not enter the brackets (**[]**) in the host table.

- 7 Save the file.
- 8 Close your su session by typing exit and pressing Enter.
- 9 Go to Configuring the hosts.equiv File, next in this document.

Configuring the hosts.equiv File

- 1 Open the **hosts.equiv** file in a UNIX text editor.
- 2 If not already present, add the line eac easftp to the end of the file and press Enter.
- 3 Save the file.
- 4 Go to **Testing the hosts and hosts.equiv Configuration**, next in this document.

Testing the hosts and hosts.equiv Configuration

After configuring the hosts file and the hosts.equiv file, you should test the configuration. Follow these steps to test the configuration.

- 1 On the EAC PC, open a DOS-prompt window.
- 2 To verify the configuration, type ftp [DNCS IP Address] and press Enter.

Note: In this command, [DNCS IP Address] is the IP address of the DNCS Ethernet interface. Do not type the brackets ([]).

Example: Type ftp 172.16.11.1 and press **Enter**.

- If you can connect to the DNCS, a message appears stating that the system is connected to the IP Address. Then an FTP prompt appears. Continue with step 3.
- If you cannot connect to the DNCS, correct the configuration of the hosts file in *Configuring the hosts File* (on page 21). Then run this test again.
- 3 Type easftp and press Enter. The system prompts you for a password.
- 4 Type easftp again, and press Enter.
- 5 Did the message "User easftp logged in" appear?
 - If yes, type bye and press Enter, or type ^D to return to the prompt. You are finished with this procedure.
 - If **no**, contact Cisco Services for assistance.

Verifying EARS Configuration and Performance

Follow these steps to verify the EARS log exists, and to verify the configuration and performance of the EARS process.

- 1 Open an xterm window on the DNCS.
- 2 Type cd /dvs/dncs/tmp and press Enter. The /dvs/dncs/tmp directory becomes the working directory.
- **3** Type 1s -1 EARS.* and press Enter.

Note: The "l" in ls is a lowercase letter L.

Important: If an EARS file does not exist, call Cisco Services.

- 4 Verify that the EARS file(s) displays with the current date and time stamp.
- 5 To view the details of an individual EARS file, type view EARS.[xxx] and press Enter.

Note: In this command, [xxx] represents the extension of the file you want to view.

Verifying the /export/home/easftp Directory

Follow these steps to verify that the /export/home/easftp directory exists on the DNCS.

- 1 Open an xterm window on the DNCS.
- 2 Type cd /export/home/easftp and press Enter. The /export/home/easftp directory becomes the working directory.
- 3 Does an error message similar to **Directory not found** appear?
 - If no, the /export/home/easftp directory exists. You have completed this procedure.
 - If yes, go to step 4.
- 4 Type mkdir /export/home/easftp and press Enter to create the directory.
- 5 Type chown easftp dncs /export/home/easftp and press Enter to set the ownership of the directory.

Determining the Set-Top Facing IP Address of the DNCS

Follow these instructions to determine and record the IP address of the DNCS that communicates with the set-tops.

- 1 Log on to the DNCS as dncs user.
- 2 Open an xterm window on the DNCS.
- **3** Type cd /etc and press **Enter**. The /etc directory becomes the working directory.
- 4 Type grep dncsatm hosts and press Enter. A line with the DNCS ATM host and its IP addresses displays.

Example: The line looks similar to the following example:

10.253.0.1 dncsatm

- 5 Record the IP address associated with dncsatm in the space provided:
- 6 Type exit and press **Enter** to close the xterm window.

4

Enable FTP and Disable Password Expiration for EAS

Introduction

Security changes in recent versions of the DNCS software can disable FTP, and allow the easftp user account password to expire. Either of these situations can prevent the EAS system from functioning correctly.

This section contains the procedures for enabling FTP in your system and for disabling the password expiration for the eastfp user account.

This chapter is for systems that use SR 5.0 and later. If your system uses a system release earlier than SR 5.0, skip this chapter.

In This Chapter

Enable FTP for the EAS	26
Check the Password Expiration Setting for easftp	27
Disable Password Expiration for easftp	28

Enable FTP for the EAS

The EAS equipment uses the easftp user to deliver EAS files to the DNCS. We have enhanced the sftp process for the easftp user in the following ways:

- The easitp user is now confined to the directories under /export/home/secure/easitp.
- The easftp user is placed in the custom root directory when they login via sftp (/export/home/secure/<username>/).
- To ensure a smooth transition to sftp for the easftp user, the /export/home/easftp/ directory is linked to /export/home/secure/easftp/export/home/easftp.

Important: EAS equipment vendors must understand that the path **/export/home/easftp** must be specified when putting or getting files using sftp or scp.

Follow these instructions to enable the FTP service only if required.

Enabling FTP for the EAS

Follow these instructions to enable FTP for EAS on the DNCS.

- 1 Open an xterm window on the DNCS.
- 2 Log into the DNCS as root user.
- 3 Type inetadm -e svc:/network/ftp:default and press Enter.
- **4** Type usermod -s /bin/sh easftp and press Enter. The default shell changes to /bin/sh (Bourne shell) for the easftp user.
- 5 Did the system display a message that indicated that the easftp user did not exist?
 - If **yes** (the easftp user does not exist), follow these instructions.
 - a Type useradd -m -c "EAS FTP Account" -d
 /export/home/easftp -u 800 -g dncs -s /bin/sh easftp and
 press Enter.
 - **b** Type chmod 775 /export/home/easftp and press Enter.
 - c Type passwd easftp and press Enter to set the password.
 - If **no** (the easftp user exists), continue with the next step.
- 6 Type grep easftp /etc/passwd and press Enter.
- 7 Confirm that the last item in the output string from the previous step is **/bin/sh**.
Check the Password Expiration Setting for easftp

Complete the following procedure to check the status of the easftp user password on the DNCS. It is imperative to ensure that the passwords of the critical users are **not** set to expire and are **not** locked.

Checking the Password Expiration Setting for easftp

- 1 Open an xterm window on the DNCS as the root user.
- 2 Type passwd -s easftp and press Enter. If the easftp account is not locked, the output will look similar to the following: easftp PS
- 3 Is the second parameter in the output LK, as shown in the following example? easftp LK PS
 - If yes, the password is locked. Type passwd -u easftp and then press Enter. This unlocks the password.
 - If **no**, go to the next step.
- 4 Type passwd -s easftp and then press Enter. If the easftp user has password aging disabled, the output should be similar to the following: easftp PS
- **5** Do you see a date and several numbers after "PS", similar to the following example?

easftp PS 01/01/09 0 91 14

- If **yes**, go to *Disable Password Expiration for easftp* (on page 28) and follow the procedure.
- If **no**, you are finished with this procedure.

Disable Password Expiration for easftp

Use this procedure to disable the password expiration period for the easftp user account.

Disabling Password Expiration for easftp

- 1 If necessary, open an xterm window and log into the DNCS as root user.
- 2 Type the following command and press Enter:

```
passwd -x -1 easftp
```

- **3** Type passwd -s easftp and then press Enter. If password expiration has been disabled for the easftp user, the output should be similar to the following: easftp PS
- 4 Is the output similar to the above example?
 - If **yes**, you are finished with this procedure.
 - If no, repeat this procedure. If the procedure continually fails, contact your network administrator.

5

Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later

Introduction

This chapter contains the procedures specific to configuring the DNCS for EAS. It also contains the procedures for conducting EAS tests.

Note: The procedures in this chapter are for System Release 5.0 and later. If you are using a System Release prior to SR 5.0, go to *Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR* 5.0 (on page 73).

In This Chapter

Configure the DNCS for EAS Messages	30
Configuring and Verifying the MMMRemote Server Entry in	
the VASP List	35
Configuring the EAS on the DNCS for System Release 5.0	39
Configure EAS to Properly Function with the CableCARD	
Module	46
Verifying and Modifying the MMM Out-of-Band Data Rate	49
EAS Suppression on Digital Channels	52
Setting Up and Configuring Weekly Tests	55
Setting Up and Configuring Monthly Tests	59
Conduct EAS Tests	63

Configure the DNCS for EAS Messages

This section contains information and procedures required to configure your DNCS for carrying EAS messages.

This section contains additional instructions that you must complete to configure the DNCS for receiving and forwarding EAS messages.

- **1** Enabling FTP for the EAS.
- 2 Configuring and Verifying the MMM Server configuration.

Configuring and Verifying the MMM Server Entry in the VASP List

The MMM Server relays the TXT file to the PassThru process and converts the WAV file to AIFF format. It then places the AIFF file on the bfsServer. The system logs the MMM Server activity in MMMServer.[xxx] files, which are located in the /dvs/dncs/tmp directory.

Viewing the VASP List

- 1 From the DNCS Administrative Console, click the **Network Element Provisioning** tab.
- 2 Click VASP. The VASP List window opens.

	(localhos	t:8045) - Mozilla	a Firefox						
<u>F</u> ile <u>E</u> di	t <u>V</u> iew	<u>G</u> o	<u>T</u> ools	<u>H</u> elp						0
<>	- 🛃 😣	\bigcirc								
DNCS/VAS	P List									cisco
Help						v	ASP List			
Exit					ID	Name	IP Address	<u>Status</u>		
					1	CFSession UI	10.253.0.1	In Service		
					2	Broadcast File System	10.253.0.1	In Service		
					3	Message Server	10.253.0.1	In Service		
					4	MMM Server	10.253.0.1	In Service		
					5	OSM Server	10.253.0.1	In Service		
					6	SAM Server	10.253.0.1	In Service		
					7	HCTM Server	10.253.0.1	In Service		
					8	SGM Server	10.253.0.1	In Service		
					112	Appserv IPG	10.253.0.10	In Service	v J	
			1	A	ld	Edit	Delete			
Done										

- 3 Is there an MMM Server entry in the VASP List?
 - If yes, go to *Verifying the MMM Server Entry in the VASP List* (on page 76)
 - If no, go to *Configuring the MMM Server Entry in the VASP List* (on page 75)

Configuring the MMM Server Entry in the VASP List

The MMM Server VASP setting must be configured correctly so that the EAS can function properly. This section provides a procedure to configure the MMM Server VASP settings if one does not already exist.

1 From the VASP List screen, record an unused ID number in the space provided.

Unused ID number: ____

Note: We suggest that you sort the list before you choose an unused ID number, in case your ID numbers are not in sequential order. To sort the list, click the **ID** heading twice to see all the IDs in sequential order.

2 Click Add. The New VASP window opens.

XVA	SP List (localhost	:8045) - Mozilla	Firefox								
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	Tools	<u>H</u> elp								$\langle \rangle$
-	- <	Z 🗵	\bigcirc										
DNC	<u>s/vasp</u>	<u>List</u> /Ne	w VAS	SP									cisco
Help								I	New	VAS	Р		
Exit													
					VASP Type: ID: Name: IP Address: Status:	Gener	al	1					
Don	e			(Save		Cancel						

- 3 In the VASP Type field, select MMM Server from the list.
- 4 In the **ID** field, type the unused ID you recorded in step 1.
- 5 In the Name field, type MMM Server.
- 6 In the **IP Address** field, type the IP address of the DNCS that you recorded in *Determining the Set-Top Facing IP Address of the DNCS* (on page 23).

7 In the **Status** field, select **In Service**.

🗙 VASP List (localhost:8045) - Moz	illa Firefox	_ _ X
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>T</u> ool	s <u>H</u> elp	0
- 🔶 - 🛃 😣 🟠		
DNCS/VASP List/New VASP		cisco
Help	New VASP	
Exit		
	VASP Type: MMM Server	
	ID: 4	
	Name: MMM Server	
	IP Address: 10.253.0.1	
	Status: In Service 💌	
	Save Cancel	
-		
Done		

8 Click Save.

Results:

- The system saves the MMM Server configuration in the VASP list.
- The New VASP window closes.
- The VASP List window updates with the added MMM Server.
- **9** On the VASP List window, use the breadcrumb links to return to the DNCS Administrative Console.

Verifying the MMM Server Entry in the VASP List

1 From the VASP List window, find the MMM Server entry.

<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	Tools	<u>H</u> elp						1
\	\$·	20									
DNC	SIVASP	List									cisco
Help							V	ASP List			
<u>xit</u>						10		15.4.11	.		
						Ш	Name	IP Address	Status		
						1	CFSession UI	10.253.0.1	In Service	h	
						2	Broadcast File System	10.253.0.1	In Service		
						3	Message Server	10.253.0.1	In Service		
					2	4	MMM Server	10.253.0.1	In Service		
						5	OSM Server	10.253.0.1	In Service		
						6	SAM Server	10.253.0.1	In Service		
						7	HCTM Server	10.253.0.1	In Service		
						8	SGM Server	10.253.0.1	In Service		
						112	Appserv IPG	10.253.0.10	In Service		
				1	Ad	d] Edit]	Delete			

- 2 Select the row containing MMM Server.
- 3 Click Edit. The Update VASP window opens.

🗙 VASP List (localhost: 8045) - Mozil	la Firefox 📃 🗖 🔀
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>T</u> ools	s <u>H</u> elp
🔷 • 🏟 - 餐 🛞 😭	
DNCS/VASP List/Update VASP	diala cisco
Help	Update VASP
Exit	
	VASP Type: MMM Server ID: 4 Name: MMM Server IP Address: 10.253.0.1 Status: In Service
Done	Save Cancel

- **4** Examine the Set Up VASP Window and answer the following questions:
 - Is **VASP Type** set to **MMM Server**?
 - Is **Name** recorded as **MMM Server**?
 - Is IP Address the same as the IP address you recorded in Determining the Set-Top Facing IP Address of the DNCS (on page 23)?
 - Is **Status** set to **In Service**?
- 5 Did you answer **yes** to every question in step 4?
 - If yes (you answered yes to *every* question), your MMM Server is configured correctly in the VASP list. Click Cancel to close the Set Up VASP Window.
 - If **no**, fix the incorrect entry and click **Save**.

Configuring and Verifying the MMMRemote Server Entry in the VASP List

The MMMRemote Server relays the EAS messages to the remote RNCS (LIONN) servers in your network.

Note: Follow these procedures ONLY if your system uses our RCS solution. If your system does NOT use the RCS solution, continue to *Configuring the EAS on the DNCS for System Releases Prior to SR 5.0* (see "*Configuring the EAS on the DNCS for System Release 5.0*" on page 39).

For further instructions on setting up the RNCS for EAS, see *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342).

Viewing the VASP List for the MMMRemote Server

1 From the DNCS Administrative Console, click the **Network Element Provisioning** tab.

X VAS	P List (localhos	1:8045) - Mozilla Toole	Firefox	1					
	<u>-</u> un			10015	Tieth						
DNC	SIVASE	List			_	_				_	ahah
Help							V	ASP List			cisco
<u>Exit</u>						<u>ID</u>	<u>Name</u>	IP Address	Status		
						1	CFSession UI	10.253.0.1	In Service	A	
						2	Broadcast File System	10.253.0.1	In Service		
						3	Message Server	10.253.0.1	In Service		
						4	MMM Server	10.253.0.1	In Service		
						5	OSM Server	10.253.0.1	In Service		
						6	SAM Server	10.253.0.1	In Service		
						7	HCTM Server	10.253.0.1	In Service		
						8	SGM Server	10.253.0.1	In Service		
						112	Appserv IPG	10.253.0.10	In Service	v	
				l	Ad	ld	Edit	Delete			
Dan											

2 Click **VASP**. The VASP List window opens.

- **3** Is there an MMMRemote Server entry in the VASP List for each remote RNCS (LIONN) server in your network?
 - If yes, go to *Verifying the MMM Server Entry in the VASP List* (on page 37)
 - If no, go to *Configuring the MMM Server Entry in the VASP List* (on page 36)

Configuring the MMM Server Entry in the VASP List

The MMMRemote Server VASP setting must be configured correctly so that the EAS can function properly. This section provides a procedure to configure the MMMRemote Server VASP settings if one does not already exist.

Important: An MMMRemote Server VASP entry must exist for each RNCS (LIONN) server in your network.

1 From the VASP List screen, record an unused ID number in the space provided.

```
Unused ID number: _____
```

Note: We suggest that you sort the list before you choose an unused ID number, in case your ID numbers are not in sequential order. To sort the list, click the **ID** heading twice to see all the IDs in sequential order.

2 Click Add. The New VASP window opens.

🔮 VASP List (localhost:80) - Mozilla Fin	fox	
File Edit View History Bookm	arks Tools Help http://localhost/dncs/vasp/vaspList.do	G 🗸 Google 🧠
DNCS Web Server Admin Co	nsole	
DNCS/VASP List/New V/	ASP	diada
Help ¥	New \	ASP
	VASP Type: General ID: Name: IP Address: Status: In Service Site ID: 1	
Done		

- 3 In the VASP Type field, select MMM Server from the list.
- 4 In the **ID** field, type the unused ID you recorded in step 1.
- 5 In the Name field, type MMMRemote Server [name of RNCS server]. Example: If your RNCS server is named LIONN1, type MMMRemote Server LIONN1.
- 6 In the IP Address field, type the IP address of the RNCS server.
- 7 In the **Status** field, select **In Service**.
- 8 Select the Site ID associated with the RNCS server from the drop-down list.

9 Click Save.

Results:

- The system saves the MMMRemote Server configuration in the VASP list.
- The New VASP window closes.
- The VASP List window updates with the added MMMRemote Server.
- 10 Repeat this procedure for each RNCS (LIONN) server in your network.
- **11** On the VASP List window, use the breadcrumb links to return to the DNCS Administrative Console.

Verifying the MMM Server Entry in the VASP List

1 From the VASP List window, select the row containing the first **MMMRemote Server** in the list.

Note: To sort the list, click the **Name** heading twice to see all the server names in alphabetical order.

the Edit View History Bookn	uns 10	ols Help	p				
🗧 🗣 🔹 📴 😨 🚺	http://le	calhost/	dncs/vasp/vaspList.do		12	Google	
DNCS Web Server 🔪 Admin Co	nsole						
DNCS/VASP List							cisc
leip 🔻 🔪				VASP	List		
		D	Name	IP Address	Status	Site ID	
		1	CFSession UI	10.253.0.1	In Service	1	
		2	Broadcast File System	10.253.0.1	In Service	1	
		3	Message Server	10.253.0.1	In Service	1	
		4	MMM Server	10.253.0.1	In Service	1	
		5	OSM Server	10.253.0.1	In Service	1	
		6	SAM Server	10.253.0.1	In Service	1	
		7	HCTM Server	10.253.0.1	In Service	1	
		8	SGM Server	10.253.0.1	In Service	1	
		35	tstApr22Vasp2	10.25.32.11	Out of Service	1	
		42	bogus	10.253.0.162	In Service	1	
		92	mmmRemoteLionn2	10.202.0.1	In Service	2	
		93	mmmRemoteLionn3	10.203.0.1	In Service	3	
		110	Appserv DHCT Config	10.253.0.10	In Service	1	
		111	Appserv PPV	10.253.0.10	In Service	1	
		440	AppcopulDC	10.052.0.10	In Conrico	4 -	

2 Click Edit. The Update VASP window opens.

🖗 🔿 🕫 🕲 😧 두	ttp://localhost/dncs/vasp/vaspList.do	▼ Google	ę
DNCS Web Server 🔪 Admin Cons	le		
ONCS/VASP List/Update V	ASP		cisco
leip v	ι	Jpdate VASP	
	VASP Type: MMM Server ID: 92 Name: mmmRemoteLionn2 IP Address: 10.202.0.1 Status: In Service Site ID: 2		
	Save Cancel		

- 3 Examine the Set Up VASP Window and answer the following questions:
 - Is VASP Type set to MMM Server?
 - Is Name recorded as MMMRemote Server [name of RNCS server]?
 - Is **IP Address** the IP address of the RNCS server?
 - Is Status set to In Service?
 - Is the Site ID the same as the Site ID of the associated RNCS server?
- 4 Did you answer **yes** to every question in step 4?
 - If yes (you answered yes to *every* question), your MMMRemote Server is configured correctly in the VASP list.
 - If **no**, fix the incorrect entry and click **Save**.
- 5 Repeat this procedure for each RNCS (LIONN) server in your network.
- 6 Go to Configuring the EAS on the DNCS for System Releases Prior to SR 5.0 (see "Configuring the EAS on the DNCS for System Release 5.0" on page 39).

Configuring the EAS on the DNCS for System Release 5.0

On the System Provisioning tab of the DNCS Administrative Console, there are four access keys in the EAS Message area that let you configure the EAS on the DNCS and send EAMs. These keys function as follows:

- **MMM Config** Initiate changes to the individual configurations that determine how EAS messages are displayed and broadcast.
- **EAS Config** Select the configuration for individual Emergency Events.
- **EAS Message** Initiate an Emergency Event message.

Note: See Conduct EAS Tests for additional information.

FIPS Code — Assign FIPS codes and force tune services to each OOB bridge.
 Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

Configure EAS Events

Use EAS Config to configure EAS individual event codes by selecting message content type and the configuration name.

Configuring EAS Events

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the System Provisioning tab.

3 Click **EAS Config**. The Set Up Emergency Alert System Configuration window opens.



Note: The Event Code column lists the different types of emergencies.

- **4** Select from the list of options in the **Message Content Type** column. The options include:
 - None
 - Audio Only (sound only)
 - Video Only (text only)
 - Audio & Video (sound and text)

Important: CableCARD modules only receive text (video) EAS messages. If your system includes hosts with CableCARD modules, make sure that your EAS messages also include text (video).

5 Select Default in the **Configuration Name** column for all the Event Codes (except for RWT and RMT).

Important: We recommend that you select the Default configuration for all events except for the RWT and the RMT.

6 Click Save.

Configure FIPS Filtering (Optional)

FIPS filtering, through its integration with the DNCS, filters and sends EAS messages only to targeted states, counties, or subdivisions.

Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

If your system uses FIPS Filtering, you should configure the FIPS codes now. See *FIPS Filtering* (on page 155) for those procedures.

When you are finished configuring the FIPS codes, proceed with *Configuring EAS Messages*, next in this document.

Configuring EAS Messages

The DNCS supports defining a unique response for each of the 54 EAM types identified by the FCC. The configuration for a particular EAM requires you to make two selections:

- Message Content Type Options include None, Audio Only, Video Only, and Audio and Video.
- Associated configuration Determines how often the message is displayed and how quickly the text scrolls (when text cannot be displayed on a single screen) along with other parameters, covered later in this section.

Within the Associated configuration, there are two very important parameters that you must understand to configure EAMs when you do **not** use force tuning:

- Delay Between Repeats Controls how often the EAM displays, in seconds.
 - Longer duration messages EAMs that are in effect for several hours (typically weather-related EAMs such as tornado and hurricane warnings) should receive a delay of 15 minutes or so.
 - Shorter duration messages EAMs that last only an hour to a few hours (such as Amber alerts) should receive a shorter delay of 5 minutes or so.
- Motion Delay Controls how long the text of the EAM stays on the screen. If the EAM text is longer than the space dedicated to the EAM, this parameter controls how long the first section of the EAM displays before the second section of the EAM displays.

Best practice is to set the default configuration to match the behaviors you want to use for all real EAMs. Thus, you would have a minimum of four separate configurations:

- RWT
- RMT
- Weather-related alerts (hurricane, severe storm, tornado, etc.)
- Shorter-duration alerts (Amber alerts, etc.)

A dedicated configuration for the RWT and RMT minimizes the number of times the alert displays on the screen. Separate configurations for the longer-duration weather alerts and for the shorter-duration other alerts also minimizes the impact on the subscriber experience, since subscribers must either acknowledge the alert or turn the set-top off to clear the alert.

On the System Provisioning tab of the DNCS Administrative Console, there are four access keys in the EAS Message area that let you configure the EAS on the DNCS and send EAMs:

- **MMM Config** Initiate changes to the individual configurations that determine how EAS messages are displayed and broadcast.
- **EAS Config** Select the configuration for individual emergency events.
- **EAS Message** Initiate an emergency event message.

Note: See Conduct EAS Tests for additional information.

FIPS Code – Assign FIPS codes and force tune services. See *Appendix C - FIPS Filtering* (on page 155) for more information.

Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

Accessing the Set Up MMM Configuration Window

Follow these steps to access the Set Up MMM Configuration window.

The MMM Server VASP setting must be configured correctly so that the EAS can function properly. This section provides a procedure to configure the MMM Server VASP settings if one does not already exist.

- 1 On the DNCS Admin console, click the **DNCS** tab.
- 2 Click the System Provisioning tab.
- 3 Click MMM Config. The MMM Configuration List window opens.



4 Select the configuration name that you want to configure, then click **Edit**. The Set Up MMM Configuration window opens.

imes Set Up MMM Configuration (local	host:8045) - Mozilla Firefox	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>T</u> ool	s <u>H</u> elp	
🔷 • 🧼 - 🛃 😣 🟠		
DNCS/MMM Configuration List	Set Up MMM Configuration	cisco
Help	Set Up MMM Configuration	
EXIC	Name: Cfg02 Description:	-
	Force Tune Type Force Tune: O None C Default Service Default Service: A&E I	
	Message Time Delay Between Repeats: 300 seconds Audio File Timeout: 0 seconds	
	Display Type Display Motion: Delayed Scroll Motion Delay : 2 seconds	
	Save Cancel	
Done		

Configuring the Force Tune Type

Follow these steps to set up the Force Tune Type.

Important: Most systems configure their force tune type to use an analog channel as the force-tune channel for EAS messages. If you have subscribers who use digital-only set-top boxes, or who use the IEEE 1394 interface on their set-tops, and you use forced tuning, the channel that you force tune to <u>must</u> be a digital channel that can display information about local and national emergencies. For example, if you use an analog community access channel as the force-tune channel, you will need to digitize this channel with an encoder.

- **1** On the Set Up MMM Configuration window, enter a **Description** for this configuration.
- 2 Does the configuration require force tuning?
 - If **yes**, go to step 3.
 - If no, click None in the Force Tune field. Go to Configuring the Message Time, next in this document.
- **3** If the configuration requires force tuning, complete the following steps in the Force Tune Type fields:
 - a Click Default Service.
 - **b** In the **Default Service** field, select the SAM Service short description of the force tune service from the menu.

Note: An EAM configured with a forced tuning redirects the subscriber's TV to the selected service that provides the emergency alert information.

Configuring the Message Time

Message Time establishes the delay between repeats of the EAS message in seconds. Follow these steps to set up the **Message Time**.

- 1 In the **Delay Between Repeats** field, type a delay time for the EAS message, depending on the type of message you are configuring:
 - For standard EAS messages, type a delay that is *at least 6 seconds* for all configurations.
 - For required weekly test (RWT) and required monthly test (RMT) messages, type a delay greater than the default duration for each message so that subscribers only see the alert once during the RWT and RMT. Refer to Configure Weekly Tests and Configure Monthly Tests for more information about configuring RWT and RMT messages.
- 2 The **Audio File Timeout** field limits the time an audio file is used in systems using OpenCable audio support.

Configuring the Display Type

Display Type controls the type of display motion and how long the emergency message appears on the screen in seconds. Follow these steps to set up the **Display Type**.

- 1 On the Set Up MMM Configuration window, type the number of seconds the message will appear on the screen into the **Motion Delay** field.
- 2 To complete the configuration of the EAS message, click **Save**.

Configure EAS to Properly Function with the CableCARD Module

When setting up the CableCARD Module on the DNCS, the following events *can* occur:

- Priority value defaults to zero Because a zero priority value is an EAS test setting, some CableCARD hosts may not support the value, resulting in the inability to display EAS messages.
- EAS Alert Remaining Time for unique EAS event codes automatically defaults to zero seconds If this occurs, EAS messages are displayed on CableCARD-compliant hosts, but the messages do not stop unless an End of Message (EOM) message is sent. We recommend that you set this field to **30** (seconds).

Important: CableCARD modules only receive text (video) EAS messages. If your system includes hosts with CableCARD modules, make sure that your EAS messages also include text (video).

Configuring EAS to Properly Function with the CableCARD Module

To check these values and modify them, if necessary, follow these steps.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the System Provisioning tab.
- 3 Click EAS Config to view the Set Up EAS Configuration window.

File Edit View Go Tools	s <u>H</u> elp												
💭 - 🕪 - 🚰 🕓 🏠 NCS/Set Un EAS Configuration						de de							
SNCS/SECOP EAS Conliguration	<u>.</u>					cisco							
elp	Set Up EAS Configuration												
		Event Code	Event Description	Message Content Type	Configuration Name								
	0	ADR	Administrative Message	Audio & Video 💌	Default 💌								
	0	AVA	Avalanche Watch	Audio & Video 💌	Default 💌								
	0	AVW	Avalanche Warning	Audio & Video 💌	Default								
	C	BZW	Blizzard Warning	Audio & Video 💌	Default 💌								
	C	CAE	Child Abduction Emergency	Audio & Video 💌	Default								
	0	CDW	Civil Danger Warning	Audio & Video 💌	Default 💌								
	0	CEM	Civil Emergency Message	Audio & Video 💌	Default								
	0	CFA	Coastal Flood Watch	Audio & Video 💌	Default 💌								
	0	CFW	Coastal Flood Warning	Audio & Video 💌	Default								
	C	DMO	Practice/Demo Warning	Audio & Video 💌	Default								
	C	DSW	Dust Storm Warning	Audio & Video 💌	Default 💌								
	C	EAN	Emergency Action Notification	Audio & Video 💌	ForceTune 💌								
	_	<u> </u>											
	Sav	•	Edit Cancel										

4 Select the row containing the first unique configuration name that you are using, and click **Edit** to view the Set Up MMM Configuration window.

5 Verify that the **Priority** field contains a non-zero value.

Ket Up MMM Configuration (loca	ilhost: 8045) - Mozilla Firefox	
<u>File Edit View Go T</u> oc	bis <u>H</u> elp	
🏳 • ⊳ - 🛃 🛽 🏠		
NCS/Set Up EAS Configurati	on/Set Up MMM Configuration	ahal
	Sot Up MMM Configuration	cisco
vit	Set op Minim Configuration	
<u> </u>	Name: Default	
	Description:	
	Force Tune Type	
	Force Tune: C None C Default Service	
	Default Service: A&E 💌	
	Priority: 15	
	Message Time	
	Delay Between Repeats: 6 seconds	
	Open Cable Repeat Rate: 0 seconds	
	Audio File Timeout: 0 seconds	
	Alert Type	
	Alert Remaining Time: 120 seconds	
	Display Type	
	Display Motion: Delayed Scroll	
	Motion Delay : 2 seconds	
	Save Cancel	
Done		

- **6** Is the Priority value zero?
 - If **yes**, contact Cisco Services.
 - If **no**, go to the next step.
- 7 Verify that the Alert Remaining Time field is a non-zero value.

Note: The value in the Alert Remaining Time field defines the duration of EAS messages on OpenCable hosts (with and without CableCARD modules).

X Set Up MMM Configuration (loca	Ihost:8045) - Mozilla Firefox	
DNCS/Set Up EAS Configuration	on/Set Up MMM Configuration	cisco
Help	Set Up MMM Configuration	
	Name: Default Description:	
	Force Tune Type Force Tune: C None C Default Service Default Service: A&E Priority: 15	
	Message Time Delay Between Repeats: 6 Seconds Open Cable Repeat Rate: 0 Seconds Audio File Timeout: 0 seconds	
	Alert Type	
	Display Type Display Motion: Delayed Scroll Motion Delay: 2 seconds	
	Save Cancel	
Done		

- 8 Is the Alert Remaining Time set to zero?
 - If yes, contact Cisco Services.
 - If **no**, go to the next step.
- 9 Click Save.
- 10 Click Exit to close the Set Up MMM Configuration window.
- **11** Repeat this procedure from step 3 for each unique configuration you have in use.
- 12 From the Set Up EAS Configuration window, click Exit.
- **13** Test the EAS alert functionality to verify that it is working properly.

Note: We recommend that you test the EAS alert functionality each week. Refer to *Test the EAS from the DNCS* (on page 63) for more information.

Verifying and Modifying the MMM Out-of-Band Data Rate

This section contains the steps you need to follow to verify and modify the MMM OOB carousel data rate (if necessary).

Verifying and Modifying the MMM OOB Data Rate

Follow these steps to verify and modify the MMM OOB carousel data rate (if necessary).

- 1 From the DNCS Administrative Console, click the **Application Interface Modules** tab.
- 2 Click BFS Admin. The BFS Hosts window opens.

🔀 BFS He	osts (loca	alhost:	8045) - Mozilla	ı Firefox	
<u>F</u> ile <u>E</u>	dit <u>V</u> i	ew	<u>G</u> o	<u>T</u> ools	Help	
\$ - \$	> - 😼	8				
DNCS/B	SFS Adm	ninistr	ation	NBFS Ho	osts	cisco
Help					BFS Hosts	
<u>Exit</u>					BFS Hosts BFS Servers BFS Sources	
					Host Name AllSitesHost	
					Display	
Done						

3 Click the **BFS Sources** tab. A list of Sources and corresponding Source IDs displays in the BFS Administration window.

XBFS Sources (loc	alhost: 80	145) - Moz	illa Firefo	x					
$\frac{F_{\text{II}}}{4} + \frac{F_{\text{II}}}{4} + \frac{F_{\text{II}$	w <u>G</u> o 3 🔗		Help						
DNCS/BFS Admir	nistratio	n/BFS He	osts/BFS	Sources				ahaha	
Help BFS Sources									
Exit			BFS Host	s BFS Servers E	BFS Sources				
				Source Name	<u>Source ID</u>	<u>Data Rate</u>	<u>Block Size</u>		
				IPG7 IB	20	1000000	4000		
				In Band	2	1000000	4000		
				MMM OOB	21	100000	1024		
				Out of Band	1	50000	1024		
				POD_CHANNELS	11	30000	1024	71	
				PPV IB	8	1000000	4000		
				PPV IB2	22	1000000	4000		
		1	Add	Edit)elete			
Done									

4 Select **MMM OOB** and click **Edit**. The Edit BFS Source window opens displaying MMM OOB data.

×ars	Source	s (localh	ant: BO	45) Moz	illa Firefax											- 🗆 🗙
Elle	Edit	View	Go	Tools	Help											
<	·	50	6													
DNCS	BFS /	Adminis	tration	BFS H	sts/BFS Se	ources/Edit B	FS Source	•								cisco
Help									Edit B	S Sour	ce					
Exit																
					BFS Hosts	BFS Servers	BFS Source	es								
					Saurea	Name			DAMM OF	58	_					
					Source	ID:			21							
					Source	Type:			@ BFS	C BootL	oader					
					Transpo	rt Type:			(ASI	In-band ®	Out-	of-band				
					Data Ra	ite:			0.1		_	Mbps				
					Block S	ize:			1024	_	-	bytes				
					Indicati	on inteval:			200		-	msec				
					Data Pu	mp:			© run	@ stop						
						Available H					Select	ed Hort				
						Available In	4	-	alatta	AllSitesH	lost	eu nose	P			
							28	OR	emave				26			
					Availab	le Local BFS)Z		Output F	orts			IN.	Out	DUT TSID	
						in Local Di D	F					F		0		
							1					1				
				1	Save	Car	icel									
Dono			_								_			_		

- 5 Is the Data Rate set to 0.1 Mbps?
 - If yes, go to step 7.
 - If **no**, click in the Data Rate field and change the data rate to 0.1 Mbps.

Important: This setting might not match the existing published recommendations for BFS carousel data rates.

- 6 Click **Save** to save and apply the new setting. The system restarts the data carousel and applies the new data rate.
- 7 Send a test EAS message with audio.
- 8 Was the test successful?
 - If **yes**, go to step 14.
 - If no, increase the data rate in 0.01 Mbps increments and continue sending test EAS messages with audio until the test is successful. Then, go to step 9.
- **9** Run a Doctor report to evaluate your overall OOB data rate. Your overall (aggregate) OOB Carousel Datarate should be less than 35.00 Mbps (including the MMM OOB, which is not included as part of the aggregate OOB Carousel Datarate).
- **10** Is your overall (aggregate) OOB Carousel Datarate less than 35.00 Mbps (including the MMM OOB)?
 - If **yes**, go to step 14.
 - If **no**, go to step 11.
- 11 Click in the **Data Rate** field and change the data rate back to 0.1 Mbps.
- **12** Click **Save** to save and apply the new setting. The system restarts the data carousel and applies the new data rate.
- **13** Contact Cisco Services and report your Doctor report findings. Cisco Services will help you troubleshoot your overall OOB data rate, including the MMM OOB data rate.
- **14** When you are finished, use the breadcrumb links to return to the DNCS Administrative Console.

EAS Suppression on Digital Channels

WARNING:

Use this feature at your own risk. It is imperative that service providers use this feature carefully so as not to suppress EAS messages on services that do not already provide EAS information. We do not take responsibility for the incorrect use of this feature.

The EAS suppression feature allows service providers to suppress EAS information on digital channels that already provide EAS coverage to their viewers.

For example, the digital channel might carry a local over-the-air TV station that is rebroadcast through the service provider's system. The TV station provides EAS coverage through its own process.

Beginning with SARA 1.60 and SARA 1.90 (DVR), a new URL modifier (**;NOEAS**) was added that allows service providers to suppress EAS on digital channels.

Notes:

- EAS suppression is only available to systems that use SARA, our resident application.
- The URL modifier has no effect unless the set-top is tuned to a digital channel where the EAS message is received.

Configuring a Channel to Suppress EAS Messages

- **1** On the DNCS Administrative Console, click the **Application Interface Modules** tab.
- 2 Click SAM Service. The SAM Service List window opens.
- **3** Configure the SAM filter to view the service you want to edit and click **Show**. The SAM Service List updates to show the results of the SAM filter.

imes SAM Service List (localhost: 8045) - Mozi	lla Firefox				
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>T</u> ool	s <u>H</u> e	lp				
🧼 - 🍌 - 🛃 😣 🟠						
DNCS/SAM Service List						cisco
Help			SAMS	Service L	ist	
Filter	Total F	?ow(s):71 Rowsperp	age: 10 💌 🛯 🖣	Page 1 of	f8 ₽№ Search	<u> </u>
By Field:		Short Description	Service Name	Service ID	<u>URL Tag</u>	
Service Name 💌 By Value:		WAGA	WAGA	110	watchtv	
а		HBOE	HBOE CAO 500	233	watchtv	
Show		HBOE2	HBOE2 CAO 501	234	watchtv	
		HBOSE	HBOSE CAO 502	235	watchtv	
		HBOFE	HBOFE CAO 503	236	watchtv	
		HBOLE	HBOLE CAO 504	237	watchtv	
		CMAXE	CMAXE CAO 505	238	watchtv	
		MMAXE	MMAXE CAO 506	239	watchtv	
		VCDen	Virt Chan Denver	61	virtchan	
		PVRAC	PVRAC	20	pvrac;EID=3	
Server unreachable. Unable to load application URL.		Add	idit De	elete		
maning for user action.						

4 Select the digital service you want to edit and click **Edit**. The Edit SAM Service window for that service opens.

X SAM Service List (localhost: 8045)	- Mozilla Firefox	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>T</u> ools	<u>H</u> elp	
🤃 • 🔶 - 鱰 🗵 🟠		
DNCS/SAM Service List/Edit SA	N Service	cisco
Help	Edit SAM Service	
Exit		
	Service ID: 110 Service Name: WAGA	
	Short Description: WAGA Long Description: WAGA Analog Channel 5	
	Application URL: bfs://resapp/watchtv Select Logo: 0	
	Parameter:	
Done	Save Cancel	

- **5** Click in the Application URL line to place your cursor at the end of the URL statement.
- 6 Append the line to include ;NOEAS.

🔀 SAM Service List (localhost:8045) - Mozilla Firefox	
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>T</u> oo	s <u>H</u> elp	
🧇 • 🎲 - 🛃 😒 🟠		
DNCS/SAM Service List/Edit S	AM Service	cisco
Help	Edit SAM Service	
Exit		
	Service ID: 110 Service Name: WAGA	
	Short Description: WAGA Long Description: WAGA Analog Channel 5 Application URL: [Dfs://resapp/watchtv;NOEAS] Select Logo: 0	
	Parameter: C Number: 1005 C String:	
Done	Save Cancel	

7 Click **Save**. The Edit SAM Service window closes. The SAM Service shows the appended URL on the same line as the service you edited.

SAM Service List (localhost: 8045) File Edit View Go Tool)-Mozi s He	lla Firefox In							
	- 11-	·P				***			
DNCS/SAM Service List clist									
Help			SAM	Service L	ist				
Exit.	Total F	≀ow(s):71 Rowsperp	age: 10 🗾 🕅 🖣	Page 1 of	f8 💷 🕅 Search	<u> </u>			
By Field:		Short Description	Service Name	Service ID	<u>URL Tag</u>				
Service Name 💌 Bv Value:		WAGA	WAGA	110	watchtv;NOEAS				
a		HBOE	HBOE CAO 500	233	watchtv				
Show		HBOE2	HBOE2 CAO 501	234	watchtv				
		HBOSE	HBOSE CAO 502	235	watchtv				
		HBOFE	HBOFE CAO 503	236	watchtv				
		HBOLE	HBOLE CAO 504	237	watchtv				
		CMAXE	CMAXE CAO 505	238	watchtv				
		MMAXE	MMAXE CAO 506	239	watchtv				
		VCDen	Virt Chan Denver	61	virtchan				
		PVRAC	PVRAC	20	pvrac;EID=3				
SAM Service saved successfully.		Add	idit) De	lete					

8 When you are finished, use the breadcrumb links to return to the DNCS Administrative Console.

Setting Up and Configuring Weekly Tests

This section contains procedures for setting up and configuring required weekly tests for systems using System Release 5.0 and later.

Weekly tests consist of transmitting the EAS digital header codes and end of message (EOM) codes once per week. Weekly tests must be conducted by EAS participants on different days and at different times.

No weekly test is necessary during the week that a monthly test is conducted or when there is an EAS activation for a state or local emergency.

The FCC requires system operators to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

The procedures in this section provide you with instructions for configuring your DNCS to perform regular tests of your EAS.

Note: The DNCS and FCC use the following acronyms to refer to the mandated tests of the EAS:

- **RWT:** Required Weekly Test
- RMT: Required Monthly Test

Weekly tests consist of transmitting the EAS digital header codes and end of message (EOM) codes once per week. Weekly tests must be conducted by EAS participants on different days and at different times.

No weekly test is necessary during the week that a monthly test is conducted or when there is an EAS activation for a state or local emergency.

What You Need

To configure the DNCS for the required test, you need the **Default Duration** value from the user interface of your EAS Encoder/Decoder. Refer to the documentation that accompanied your EAS Encoder/Decoder for instructions on locating this value on your EAS Encoder/Decoder.

Note: The Default Duration refers to the duration of the outgoing alert messages.

Setting Up Weekly Tests

This section provides procedures for setting up the RWT on the DNCS.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the **System Provisioning** tab.
- 3 Click EAS Config. The Set Up EAS Configuration window opens.

🗙 Set	Up Eme	rgency A	lert Sy	/stem Co	nfiguratio	n (localhost:80	45) - Mozilla Firefox			
File	Edit	View	Go	Tools	Help					
<	- ≪ ²		<u>(</u>)							
DNC	Siserc	IP EAS C	onng	uration						cisco
Help							Set Up EAS	Configuration		
Exit						Event Code	Event Description	Message Content Type	Configuration Name	
					0	ADR	Administrative Message	Audio & Video 💌	Default	
					0	AVA	Avalanche Watch	Audio & Video 💌	Default 💌	
					0	AVW	Avalanche Warning	Audio & Video 💌	Default 💌	
					C BZW		Blizzard Warning	Audio & Video 💌	Default 💌	
					0	CAE	Child Abduction Emergency	Audio & Video 🔳	Default 💌	-
						CDW	Civil Danger Warning	Audio & Video 🔳	Default 💌	
					0	CEM	Civil Emergency Message	Audio & Video 💌	Default 💌	
					0	CFA	Coastal Flood Watch	Audio & Video 💌	Default 💌	
					0	CFW	Coastal Flood Warning	Audio & Video 🔳	Default 💌	
					0	DMO	Practice/Demo Warning	Audio & Video 🔳	Default 💌	
					0	DSW	Dust Storm Warning	Audio & Video 💌	Default	
					0	EAN	Emergency Action Notification	Audio & Video 💌	ForceTune 💌	
				1	Sav	•]	Edit Cancel	I		
Don	e									

- 4 Highlight the row that contains the **RWT** (Required Weekly Test).
- **5** Click the **Configuration Name** arrow for the RWT. A list of possible configuration names appears.

🔀 Set Up Emergency Alert System Config	guration (lo	calhost:804	15) - Mozilla Firefox			
<u>File Edit View Go Tools H</u>	lelp					$\langle \rangle$
🧼 · 🔶 · 🥰 🛽 🏠						
DNCS/Set Up EAS Configuration						alada cisco
Help			Set Up EAS	Configuration		
	Ev	rent Code	Event Description	Message Content Type	Configuration Name	
	0	NIC	National Information Center	Audio & Video 💌	Default 💌	
	C	NMN	Network Message Notification	Audio & Video 💌	Default	
	C	NPT	National Periodic Test	Audio & Video 💌	Default 💌	
	0	NUW	Nuclear Power Plant Warning	Audio & Video 💌	Default 💌	
	C	RHW	Radiological Hazard Warning	Audio & Video 💌	Default 💌	
	C	RMT	Required Monthly Test	Audio & Video 💌	Default 💌	
	¢	RWT	Required Weekly Test	Audio & Video 💌	Default	
	C	SMW	Special Marine Warning	Audio & Video 💌	Cfg01 Cfg02	
	0	SPS	Special Weather Statement	Audio & Video 💌	Cfg03 Cfg04 Cfg05	
	0	SPW	Shelter in Place Warning	Audio & Video 💌	Cfg06 Cfg07	
	C	SVA	Severe Thunderstorm Watch	Audio & Video 🖃	Cfg09 Cfg10	
	0	SVR	Severe Thunderstorm Warning	Audio & Video 💌	Cfg11 Cfg12 Cfg13	
	<u>_</u>	svs	Severe Weather Statement	▼ nehiV & nihuA	Cfg14	$\Box D$
Dana	Save		Edit Cancel		Cfg16 Cfg17 Cfg18	

6 Select the **Cfg00** configuration. The configuration appears in the Configuration Name column.

- 7 Click Save. The system saves the new RWT configuration.
- 8 Now, use the breadcrumb links to return to the DNCS Administrative Console

Configuring Weekly Tests

After you set up the RWT, you need to set up the MMM Server. The DNCS uses the MMM Server to conduct tests of the EAS. Follow these instructions to configure the MMM Server on the DNCS for the RWT of the EAS.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the **System Provisioning** tab.
- 3 Click MMM Config. The MMM Configuration List window opens.

imes MMM Configuration List (local	host:8045) - Mozilla Firefox			
<u>File Edit View Go To</u>	ools <u>H</u> elp			0 ⁰ 0 0 ₀ 0
🧼 • 🔶 • 🛃 😣 🟠				
DNCS/MMM Configuration L	ist			ahaha cisco
Help		ММ	M Configuration List	
Exit				1
			Configuration Name	
		0	Cfg00	
		0	CfgD1	
		0	Cfg02	
		0	Cfg03	
		0	Cfg04	
		0	Cfg05	
		0	Cfg06	
		0	Cfg07	
		0	Cfg08	
	Edit			
Done				
20110				

4 Select Cfg00 and click Edit. The Set Up MMM Configuration window opens.

<u>File Edit View Go Tools H</u>	lp
• • • • • • • • • • • • • • • • • • •	
DNCS/MMM Configuration List/Set U	o MMM Configuration cis
Help	Set Up MMM Configuration
Exit N	ime: Cfg00 scription: RWT
	rce Tune Type rce Tune: C None C Default Service fault Service: BLOOM ■ isority: 15 isoage Time itay Between Repeats: 300 seconds ren Cable Repeat Rate: 0 seconds idio File Timeout: 0 seconds idio File Timeout: 0 seconds ent Type ert Remaining Time: 120 seconds
	splay Type splay Motion: Delayed Scroll tition Delay : 6 seconds
	Save Cancel

- 5 In the **Description** field, type **RWT configuration**.
- 6 At your EAS encoder/decoder, locate the **Default Duration** value.

Note: If necessary, refer to the user guide that accompanied your EAS encoder/decoder.

7 In the **Delay Between Repeats** field, type a value (in seconds) that equals [(Default Duration/2) + 1 minute x 60]. Use whole integer division only (drop the decimal point before adding the +1 minute).

Important: We recommend setting the Delay Between Repeats field to **480** seconds for the RWT if the default duration for the RWT is 15 minutes.

Example: If the Default Duration for the RWT of your EAS encoder/decoder is 15 minutes, your Delay Between Repeats value must be $[(15/2 = 7) + 1 = 8 \times 60 = 480 \text{ seconds}].$

Note: Make sure that the Delay Between Repeats is always at least 6 seconds.

- 8 Click **Save**. The system saves your changes and the Set Up MMM Configuration window closes.
- **9** In the MMM Configuration List window, use the breadcrumb links to return to the DNCS Administrative Console.

Setting Up and Configuring Monthly Tests

This section contains procedures for setting up and configuring required weekly tests for systems using System Release 5.0 and later.

The FCC requires system operators to conduct weekly and monthly tests of their Emergency Alert Systems (EAS). These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

The procedures in this section provide you with instructions for configuring your DNCS to conduct monthly tests of your EAS.

Note: The DNCS and FCC use the following acronyms to refer to the mandated tests of the EAS:

- RWT: Required Weekly Test
- RMT: Required Monthly Test

Monthly tests consist of the transmitting the following:

- EAS digital header codes
- The two-tone attention signal
- A brief test script and EOM code
- A visual display of header code data

Monthly tests must be retransmitted within 60 minutes of receipt:

- In odd months, monthly tests must be conducted between 8:30AM to local sunset
- In even months, monthly tests must be conducted between local sunset and 8:30AM

No monthly test is necessary during a month when there is an EAS activation that includes a two-tone alert signal and an audio message.

What You Need

To configure the DNCS for the required test, you need the **Default Duration** value from the user interface of your EAS Encoder/Decoder. Refer to the documentation that accompanied your EAS Encoder/Decoder for instructions on locating this value on your EAS Encoder/Decoder.

Note: The Default Duration refers to the duration of the outgoing alert messages.

Setting Up Monthly Tests

This section provides procedures for setting up the RMT on the DNCS.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the **System Provisioning** tab.
- 3 Click EAS Config. The Set Up EAS Configuration window opens.

K Set	Up Eme	rgency A	lert Sy	ystem Cor	nfiguratio	n (localhost:80·	45) - Mozilla Firefox					
File	Edit		<u>G</u> o	Tools	Help							
DNCS	S/Set L	p EAS (Cul Config	juration						ahah		
Configuration										cisco		
ielp xit						Set up EAS Configuration						
_						Event Code	Event Description	Message Content Type	Configuration Name			
					0	ADR	Administrative Message	Audio & Video 💌	Default	4		
					0	AVA	Avalanche Watch	Audio & Video 💌	Default 💌			
					0	AVW	Avalanche Warning	Audio & Video 💌	Default			
					0	BZW	Blizzard Warning	Audio & Video 💌	Default			
					0	CAE	Child Abduction Emergency	Audio & Video 💌	Default	_		
					0	CDW	Civil Danger Warning	Audio & Video 💌	Default			
					0	CEM	Civil Emergency Message	Audio & Video 💌	Default			
					0	CFA	Coastal Flood Watch	Audio & Video 💌	Default			
					0	CFW	Coastal Flood Warning	Audio & Video 💌	Default 💌			
					0	DMO	Practice/Demo Warning	Audio & Video 💌	Default 💌			
					0	DSW	Dust Storm Warning	Audio & Video 💌	Default			
					0	EAN	Emergency Action Notification	Audio & Video 💌	ForceTune 💌			
					-				· · · · · · · · · · · · · · · · · · ·			
					Sav	•	Edit Cancel					
Done	•											

- 4 Highlight the row that contains the **RMT** (Required Monthly Test).
- 5 Click the **Configuration Name** arrow for the RMT. A list of possible configuration names appears.

ile <u>E</u> dit ⊻iew <u>G</u> o <u>T</u> ools	Help								
þ - 🔶 - 🛃 😒 🏠									
NCS/Set Up EAS Configuration	1					cis			
p	Set Up EAS Configuration								
		Event Code	Configuration Name	٦					
	0	NIC	National Information Center	Audio & Video 💌	Default	4			
	C	NMN	Network Message Notification	Audio & Video 💌	Default				
	C	NPT	National Periodic Test	Audio & Video 💌	Default 💌				
	0	NUW	Nuclear Power Plant Warning	Audio & Video 💌	Default				
	C	RHW	Radiological Hazard Warning	Audio & Video 💌	Default				
	۲	RMT	Required Monthly Test	Audio & Video 💌	Default				
	C	RWT	Required Weekly Test	Audio & Video 💌	Cfg01 k				
	0	SMW	Special Marine Warning	Audio & Video 💌	Cfg03 Cfg04 Cfg05				
	C	SPS	Special Weather Statement	Audio & Video 💌	Cfg06 Cfg07				
	0	SPW	Shelter in Place Warning	Audio & Video 💌	Cfg09 Cfg10				
	C	SVA	Severe Thunderstorm Watch	Audio & Video 💌	Cfg11 Cfg12				
	0	SVR	Severe Thunderstorm Warning	Audio & Video 💌	Cfg14 Cfg15				
	C	SVS	Severe Weather Statement	Audio & Video 💌	Cfg16 Cfg17 Cfs18				
	0	TOA	Tornado Watch	Audio & Video 💌	Cfg19	۲			
	C	TOE	911 Telephone Outage Emergency	Audio & Video 💌	Default				
	0	TOR	Tornado Warning	Audio & Video 💌	Default],			

- 6 Select the **Cfg01** configuration. The configuration appears in the Configuration Name column.
- 7 Click **Save**. The system saves the new RMT configuration.
- 8 Now, use the breadcrumb links to return to the DNCS Administrative Console.

Configuring Monthly Tests

After you set up the RMT, you must set up the MMM Server. The DNCS uses the MMM Server to conduct tests of the EAS. Follow these instructions to configure the MMM Server on the DNCS for the RMT of the EAS.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the **System Provisioning** tab.
- 3 Click MMM Config. The MMM Configuration List window opens.

🗙 MMM Configu	ration L	.ist (lo	calhost:8	8045) - Mozilla Firefox				
<u>File E</u> dit <u>\</u>	⊻iew	<u>G</u> o	Tools	<u>H</u> elp				
🔶 • 🔶 • 🛃	7 🙁 🗧	<u> </u>						
DNCS/MMM C	Configu	iratio	n List					cisco
Help					ММ	M Configuration Lis	t	
Exit						Configuration Name		
					0	Cfg00	A	
					0	CfgD1		
					0	Cfg02		
					0	Cfg03		
					0	CfgD4		
					0	CfgD5		
					0	Cfg06		
					0	Cfg07		
					0	Cfg08	7	
			1	Edit				
Done								

4 Select Cfg01 and click Edit. The Set Up MMM Configuration window opens.

🗙 Set Up MMM Configuration (localhost:8045) - Mozilla Firefox						
<u>File Edit View Go T</u> ools	s <u>H</u> elp	0				
🗇 • 🧼 - 🎯 🛞 🟠						
DNCS/MMM Configuration List/	Set Up MMM Configuration	cisco				
Help	Set Up MMM Configuration					
Edt	Name: Cfg01 Description:					
Done	Save Cancel					

- 5 In the **Description** field, type **RMT configuration**.
- 6 At your EAS encoder/decoder, locate the **Default Duration** value.

Note: If necessary, refer to the user guide that accompanied your EAS encoder/decoder.

7 In the **Delay Between Repeats** field, type a value (in seconds) that equals [(Default Duration/2) + 1 minute x 60]. Use whole integer division only (drop the decimal point before adding the +1 minute).

Important: We recommend setting the Delay Between Repeats field to **1860** seconds for the RMT if the default duration for the RMT is 60 minutes.

Example: If the Default Duration for the RMT of your EAS encoder/decoder is 60 minutes, your Delay Between Repeats value must be $[(60/2 = 30) + 1 = 31 \times 60 = 1860 \text{ seconds}].$

Note: Make sure that the Delay Between Repeats is always at least 6 seconds.

- 8 Click **Save**. The system saves your changes and the Set Up MMM Configuration window closes.
- **9** In the MMM Configuration List window, use the breadcrumb links to return to the DNCS Administrative Console.
Conduct EAS Tests

Test the EAS from the DNCS

This section describes the procedure for using the DNCS EAS Message menu to test the EAS using the EAS Message menu. The Send Emergency Alert System Message screens allow you to create, modify, and send an emergency alert system message. This procedure is valuable in testing your EAS system.

Important: Sending EAS messages outside of the regularly scheduled EAS tests or by using the DNCS EAS Message menu does **not** meet the FCC requirements for conducting the RWT and the RMT. The RWT and RMT tests should be end-to-end tests, and as such should be initiated from the EAS receiver and monitored at the set-top.

Send EAS Test Messages

Follow the steps in these procedures to send EAS test messages on the DNCS.

Note: Actual Emergency Alert Messages originate from the FCC. Use the DNCS EAS Message menu for local testing purposes only.

Sending EAS Test Messages

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the System Provisioning tab.
- **3** Click the **EAS Message** tab. The Send Emergency Alert System Message window opens with the **EAS Message** tab in the forefront.

Send Emergency Alert System Mes	sage (localhost:8045) - Mozilla Firefox	
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>T</u> ools	: <u>H</u> elp	
🧼 • 🖒 • 🔁 😣 🟠		
DNCS/Send Emergency Alert Sy	stem Message	ahaha
Help	Send Emergency Alert System Message	
Exit	EAS Message Message Content Send Message	
	Event Code Event Code: Administrative Message (ADR) T Message Content Type: Audio & Video	
	Message Information Message Name: Duration: minutes	
Dana	Send Cancel	

4 Select the **Event Code** from the list.

Note: We recommend that you set the Event Code to **Administrative Message (ADR)**.

5 In the **Message Information** area, type a unique Message Name and Duration in the appropriate fields.

6 Click the **Message Content** tab. The Send Emergency Alert System Message window opens with the **Message Content** tab in the forefront.

			-				
<u>F</u> ile	<u>E</u> dit	View	<u>G</u> o	Tools	<u>H</u> elp		
	- <	20	€				
DNC	S/Send	Emerg	ency A	lert Sys	tem Message		cisco
Help					Send Er	nergency Alert System Message	
<u>Exit</u>					EAS Message Messag	e Content Send Message	
					Message Conten	t	
					Video Content Type:	None C Ascii	
					Video Content:		-
					Audio Content Type:	⊙ None ○ URL	
					Audio File:	/export/home/easftp/ -none-	
					Send]	Cancel	
					Jena j		

- 7 Choose one of the following options:
 - If you have only video (text) content, select ASCII and type the text in the Video Content.
 - If you have only audio (sound) content, select URL and click the Audio File arrow to select a file from the list.

Important: Be sure to select a WAV file from the list (a file with a *.wav* extension).

- If you have **audio and video** (sound and text) content, follow these steps:
 - a Choose ASCII and type the text in the Video Content text box.
 - **b** Choose **URL** and click the **Audio File** arrow to select a file from the list.

Chapter 5 Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later

8 Click the **Send Message** tab. The Send Emergency Alert System Message window updates with the **Send Message** tab to the forefront.

Send Emergency Alert System M	essage (localhost:8045) - Mozilla Firefox	
File Edit View Go Too	ls <u>H</u> elp	
DNCS/Send Emergency Alert	System Message	alada
Help	Send Emergency Alert System Message	
Eat.	EAS Message Message Content Seed Message	
	Send Message To	
	Selected FIPS Code	
	State: All States X Addo	2
	County: All Countres	40
	Subdivision: Per Subdivisions	IX
	DNCS DNCS DNCS	
	Source Site: Target Site:	
	Sand Conset	
	serie Lancer	
Done		

- **9** Did you purchase the EAS filtering product that provides FIPS filtering on your system?
 - If **no**, go to step 10.
 - If **yes**, go to step 11.
- 10 Your only option is to select All States. Select All States, then go to step 14.
- 11 Select the State to which you are sending the EAS message.
- **12** Select the **County** in the selected state to which you are sending the EAS message.
- **13** Select the **Subdivision** of the selected county to which you are sending the EAS message.
- 14 Click Add.
- 15 Is the content of the Selected FIPS Code window correct?
 - If yes, click Send.
 - If **no**, correct the information and then click **Send**.

Warning: The emergency information broadcasts to all DHCTs in the selected destinations. The message displays across the upper portion of the TV screen in a red banner with white text.

Notes:

- To remove any destination from the Selected FIPS Code window, highlight this destination and click Remove.
- Depending on the MMM configuration parameters, the emergency message repeats and lasts for the duration you specified in the Message Information area.
- 16 Go to Terminate EAS Messages, next in this document.

Terminate EAS Messages

Occasionally, you may want to suspend or terminate an EAM before it reaches its configured duration. When you terminate an EAM, you stop transmitting all EAMs that are currently active in your system. If you terminate an EAM on an OOB bridge, you stop transmitting all EAMs that are currently active on that OOB bridge.

This section provides instructions for terminating an EAM using the user interface of the DNCS.

Terminating EAS Messages

Follow this procedure to terminate an EAS message from the DNCS.

- 1 From the DNCS Administrative Console, click the DNCS tab.
- 2 Click the System Provisioning tab.
- **3** Click **EAS Message**. The Send Emergency Alert System Message window opens with the EAS Message tab to the forefront.

🗙 Sen	d Emerg	jency Ale	rt Sys	tem Mess	age (localhost:8045) - Mozilla Firefox	
File	Edit	View	Go	Tools	Help	
•	\$> · (3				
DNCS	/Send	Emerge	ency /	lert Sys	tem Message	cisco
Help					Send Emergency Alert System Message	
<u>Exit</u>					EAS Message Content Send Message	
					Event Code: Administrative Message (ADR) 💌 Message Content Type: Audio & Video	
					Message Information Message Name: Duration: minutes	
				l	Send Cancel	

- 4 In the Event Code area of the window, select one of the following options:
 - If you are using PowerKEY[®] CableCARD[™] modules on your system, go to step 5.

Note: The value in the Alert Remaining Time field defines the duration of EAS messages on OpenCable[™] hosts (with and without CableCARD modules).

If you are *not* using CableCARD modules on your system, go to step 15.

Chapter 5 Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later

- 5 Choose **End of Message (EOM)**. **End of Message (EOM)** appears in the Event Code field.
- 6 Type a unique message name in the **Message Name** field.
- 7 Click the **Send Message** tab.
- 8 Did you purchase the optional FIPS filtering software product for your system?
 - If **no**, go to step 9.
 - If **yes**, go to step 10.
- 9 Your only option is to select All States. Select All States, then go to step 14.
- 10 Select the State the EOM message is sent to.

Important: You can stop all active EAMs by sending an EOM to All States.

Note: There will be no interference with services if a DHCT that does not have any active EAMs receives an EOM.

- 11 Select the County the EOM message is sent to.
- **12** Select the **Subdivision** the EOM message is sent to.
- **13** Click **Add**. The system adds the appropriate FIPS code to the Selected FIPS Code list.
- 14 Is the content of the Selected FIPS Code window correct?
 - If yes, click Send. Go to step 25.
 - If **no**, correct the information and click **Send**. Go to step 25.

Important: If your system is currently broadcasting multiple EAMs, be sure you terminate the correct message.

Note: To remove any destination from the **Selected FIPS Code** window, highlight this destination and click **Remove**.

Result: The DNCS transmits instructions to CableCARD modules to stop displaying the EAM.

15 Choose **Emergency Action Termination (EAT)**. Emergency Action Termination appears in the Event Code field.

🗙 Sen	d Emer	gency Ale	ert Sys	tem Messa	ge (localhost:8045) - Mozilla Firefox	
<u>F</u> ile	<u>E</u> dit	⊻iew	<u>G</u> o	Tools	Help	0
4.	•	Z 🛛				
DNC	S/Send	Emerg	ency A	lert Syst	em Message	cisco
Help					Send Emergency Alert System Message	
<u>Exit</u>					EAS Message Message Content Send Message	
					Event Code	
					Event Code	
					Event Code: Emergency Action Termination (EAT)	
					Message Content Type: Audio & Video	
					Message Information	
					Message Name:	
					Duration: minutes	
					Send Cancel	
Don	e					

- **16** Type a unique message name in the **Message Name** field.
- 17 Click the **Send Message** tab.

<u>File Edit View Go Tools H</u> elp	
4 · 4 · 😼 🕄 😚	
DNCS/Send Emergency Alert System Message	diala
Send Emergency Alert System Message	
Exit EAS Message Message Content Seed Message	
Send Message To	
Selected FIPS Code	
State: All States Addt	2
County: All Counties	
Subdivision: All Subdivisions DRemove	z
DNCS DNCS Strong	
Source Site: Target Site:	
Send Cancel	
Done	

- 18 Did you purchase the optional FIPS filtering software product for your system?
 - If **no**, go to step 20.
 - If **yes**, go to step 21.
- 19 Your only option is to select All States. Select All States, then go to step 25.

Chapter 5 Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later

20 Select the State the EOM message is sent to.

Important: You can stop all active EAMs by sending an EOM to **All States**. **Note:** There will be no interference with services if a DHCT that does not have any active EAMs receives an EOM.

- 21 Select the County the EOM message is sent to.
- 22 Select the Subdivision the EOM message is sent to.
- 23 Click Add.
- 24 Is the content of the Selected FIPS Code window correct?
 - If yes, click Send.
 - If **no**, correct the information and click **Send**.

Important: If your system is currently broadcasting multiple EAMs, be sure you terminate the correct message.

Note: To remove any destination from the **Selected FIPS Code** window, highlight this destination and click **Remove**.

Result: The DNCS transmits instructions to DHCTs to stop displaying the EAM.

25 On the Send Emergency Alert System Message window, use the breadcrumb links to return to the DNCS Administrative Console.

Improve EAS Performance

You must identify the MMM out-of-band (MMM OOB) carousel data rate that works best for your system. This section provides a procedure for verifying and modifying the MMM OOB carousel data rate on the DNCS (if necessary) to improve EAS performance.

Important: The total overall out-of-band carousel data rate on your system must *not* exceed 0.35 Mbps.

Note: Refer to the *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377) for additional information on configuring the DNCS carousel data rates.

Verifying MMM Server Performance

Follow these steps to verify the configuration and performance of the MMM Server.

1 Send a test EAS message with audio to a selected destination.

Note: See *Send EAS Test Messages* (on page 64) for information on sending test messages.

- 2 Open an xterm window on the DNCS.
- **3** Type cd /dvs/dncs/tmp and press Enter. The /dvs/dncs/tmp directory becomes the working directory.
- 4 To locate the most recent MMMServer files, type ls -1 MMMServer.* and press Enter.

Note: The "l" in **ls** is a lowercase letter L.

Result: A list of **MMMServer** files appear.

- 5 To view the contents of one of these files, type view MMMServer.[xxx].
 Note: In this command, [xxx] represents the extension of the file you want to view.
- **6** Type cd /dvs/dvsFiles/MMM and press **Enter**. The /dvs/dvsFiles/MMM directory becomes the working directory.
- 7 Type ls -l *.aiff and press Enter.

Note: The "l" in -l is a lowercase letter L.

Result: A list of AIFF files in the /dvs/dvsFiles/MMM directory appears.

Important: Complete this procedure immediately after sending an EAS message with audio. The AIFF file will only exist in the directory when you send an EAS message with audio, and this message is still active. The system removes this file when the EAS message terminates.

- 8 Are there AIFF files in the /dvs/dvsFiles/MMM directory with a current time and date stamp?
 - If yes, you have completed this procedure.
 - If no, check the log for error messages. Contact Cisco Services for further assistance if necessary.

Note: For troubleshooting information on the MMM Server, go to *Troubleshoot the MMM Server* (on page 135).

Conduct Scheduled Weekly and Monthly Tests

This section provides a table of the requirements, methods, and procedures for conducting the RWT and the RMT on each EAS.

Important: You **must** configure your system so that the RMT *always* functions in automatic mode. The FCC conducts the RMTs.

Note: You can configure your system so that the RWT always functions in automatic mode or you can set up the RWT to run in manual mode. See *Test the EAS from the DNCS* (on page 63) for information on sending and terminating ad hoc EAS messages.

Chapter 5 Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later

Conducting Weekly and Monthly Tests

Use the following table to find your EAS equipment manufacturer, and follow the instructions provided for your system. Refer to the documentation for your specific EAC for additional information on conducting the RWT and the RMT.

Important: If your system does not function as expected, refer to *Troubleshooting* (on page 121) for troubleshooting procedures for the EAS.

System	RWT	RMT	
Megahertz	Automatic Mode:	Automatic Mode:	
	Automated process	Automated process	
	Manual Mode:	Manual Mode:	
	Press the Week soft key.	The FCC requires that the RMT	
	Enter your password .	function in automatic mode.	
	Press the Proceed soft key.		
Trilithic	Automatic Mode:	Automatic Mode:	
	Automated process	Automated process	
	Manual Mode:	Manual Mode:	
	Not available	The FCC requires that the RMT function in automatic mode.	
Monroe System	Automatic Mode:	Automatic Mode:	
with Digital Envoy	Automated process	Automated process	
Liivoy	Manual Mode:	Manual Mode:	
	 Press the MODE soft key. Various MIP-021 options appear on the LCD screen. 	The FCC requires that the RMT function in automatic mode.	
	 Press the NO soft key until the message SEND WEEKLY TEST appears. 		
	■ Press the YES soft key.		
Frontline	Automatic Mode:	Automatic Mode:	
	Automated process	Automated process	
	Manual Mode:	Manual Mode:	
	Press the key labeled Weekly Test on the EAS Encoder. The Send Hdr and the On Air Relay indicators illuminate to show that the test is in process.	The FCC requires that the RMT function in automatic mode.	

6

Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0

Introduction

This chapter contains the procedures specific to configuring the DNCS for EAS. It also contains the procedures for conducting EAS tests.

Note: The procedures in this chapter are for System Releases prior to SR 5.0. If you are using SR 5.0 or later, go to *Configure the DNCS for EAS and Conduct Tests for SR 5.0 and Later* (on page 29).

In This Chapter

Configure the DNCS for EAS Messages	
Configuring the EAS on the DNCS	88
Configure EAS to Properly Function with the CableCARD	
Module	94
Verifying and Modifying the MMM Out-of-Band Data Rate	97
EAS Suppression on Digital Channels	100
Setting Up and Configuring Weekly Tests	102
Setting Up and Configuring Monthly Tests	106
Conduct EAS Tests	110

Configure the DNCS for EAS Messages

This section contains information and procedures required to configure your DNCS for carrying EAS messages.

This section contains additional instructions that you must complete to configure the DNCS for receiving and forwarding EAS messages.

- 1 Configuring and Verifying the MMM Server configuration.
- **2** Verifying that the ORBIX daemon is disabled (for SRs 2.5/3.5/4.0 and previous only).
- **3** Verifying the naming service (for DNCS SRs 2.2 and 3.0 only).

Configuring and Verifying the MMM Server Entry in the VASP List

The MMM Server relays the TXT file to the PassThru process and converts the WAV file to AIFF format. It then places the AIFF file on the bfsServer. The system logs the MMM Server activity in MMMServer.[xxx] files, which are located in the /dvs/dncs/tmp directory.

Viewing the VASP List

- 1 From the DNCS Administrative Console, select one of the following tabs:
 - For DNCS SR 2.7/3.7/4.2 and later, click the **Network Element Provisioning** tab.
 - For DNCS SR 2.5/3.5/4.0 and earlier, click the **Element Provisioning** tab.
- 2 Click VASP. The VASP List window opens.

Note: The following example is from an SR 4.3 system. If you are using another System Release, your window might not look the same.

<u>File View</u>					
ID	Name	IP Address	Status		
1	CFSession UI	10.253.0.1	In Service		
2	Broadcast File System	10.253.0.1	In Service		
З	Message Server	10.253.0.1	In Service		
4	MMM Server	10.253.0.1	In Service		
5	OSM Server	10.253.0.1	In Service		
6	GEARServer	10.253.0.1	In Service		
7	HCTM Server	10.253.0.1	In Service		

- 3 Is there an MMM Server entry in the VASP List?
 - If yes, go to *Verifying the MMM Server Entry in the VASP List* (on page 76)
 - If no, go to *Configuring the MMM Server Entry in the VASP List* (on page 75)

Configuring the MMM Server Entry in the VASP List

The MMM Server VASP setting must be configured correctly so that the EAS can function properly. This section provides a procedure to configure the MMM Server VASP settings if one does not already exist.

Configuring the MMM Server Entry

1 From the VASP List screen, record an unused ID number in the space provided.

Unused ID number: _

Note: We suggest that you sort the list before you choose an unused ID number, in case your ID numbers are not in sequential order. To sort the list, click the **ID** heading twice to see all the IDs in sequential order.

🗙 Set Up VASP	X
VASP Type:	General 🗕
ID:	9
Name:	Y
IP Address:	¥
Status:	◆ Out of Service 🗼 In Service
Save	Cancel Help

2 Click File > New. The Set Up VASP window opens.

- 3 In the VASP Type field, select MMM Server from the list.
- 4 In the **ID** field, type the unused ID you recorded in step 1.
- 5 In the Name field, type MMM Server.
- 6 In the **IP Address** field, type the IP address of the DNCS that you recorded in *Determining the Set-Top Facing IP Address of the DNCS* (on page 23).

7 In the **Status** field, click **In Service**.

ACD TUDAL	MANA Control
ASP Type:	
ID:	4
Name:	MMM Server
IP Address:	I 10.253. 0. 1
Status:	Out of Service In Service
Save	Cancel Help

8 Click Save.

Results:

- The system saves the MMM Server configuration in the VASP list.
- The Set Up VASP window closes.
- The VASP List window updates with the added MMM Server.
- 9 On the VASP List window, click **File > Close**.

Verifying the MMM Server Entry in the VASP List

If the MMM Server already exists in the VASP list, you need to verify the information contained within the server settings.

Verifying the MMM Server Entry

1 From the VASP List window, find the MMM Server entry.

<u>F</u> ile <u>V</u> iew						
ID	Name	IP Address	Status			
1	CFSession UI	10.253.0.1	In Servic			
2	Broadcast File System	10.253.0.1	In Servic			
З	Message Server	10.253.0.1	In Servic			
4	MMM Server	10.253.0.1	In Servic			
5	OSM Server	10.253.0.1	In Servic			
6	GEARServer	10.253.0.1	In Servic			
7	HCTM Server	10.253.0.1	In Servic			

2 Click the row containing MMM Server.

- VASP Type: MMM Server -ID: 4 Name: MMM Server IP Address: [10.253. 0. 1 Status: Out of Service C In Service Save Cancel Help
- 3 Click File > Open. The Set Up VASP window opens.

- 4 Examine the Set Up VASP Window and answer the following questions:
 - Is VASP Type set to MMM Server?
 - Is Name recorded as MMM Server?
 - Is IP Address the same as the IP address you recorded in Determining the Set-Top Facing IP Address of the DNCS (on page 23)?
 - Is Status set to In Service?
- 5 Did you answer **yes** to every question in step 4?
 - If yes (you answered yes to *every* question), your MMM Server is configured correctly in the VASP list. Click Cancel to close the Set Up VASP Window.
 - If no, go to Configuring the MMM Server Entry in the VASP List (on page 75) and fix the incorrect entry.
- 6 Go to Configuring the EAS on the DNCS.

Configuring and Verifying the MMM Server Entry in the VASP List

The MMM Server relays the TXT file to the PassThru process and converts the WAV file to AIFF format. It then places the AIFF file on the bfsServer. The system logs the MMM Server activity in MMMServer.[xxx] files, which are located in the /dvs/dncs/tmp directory.

Viewing the VASP List

- 1 From the DNCS Administrative Console, select one of the following tabs:
 - For DNCS SR 2.7/3.7/4.2 and later, click the **Network Element Provisioning** tab.
 - For DNCS SR 2.5/3.5/4.0 and earlier, click the **Element Provisioning** tab.
- 2 Click VASP. The VASP List window opens.

Note: The following example is from an SR 4.3 system. If you are using another System Release, your window might not look the same.

<u>File View</u>				
ID	Name	IP Address	Status	
1	CFSession UI	10.253.0.1	In Service	
2	Broadcast File System	10.253.0.1	In Service	
З	Message Server	10.253.0.1	In Service	
4	MMM Server	10.253.0.1	In Service	
5	OSM Server	10.253.0.1	In Service	
6	GEARServer	10.253.0.1	In Service	
7	HCTM Server	10.253.0.1	In Service	

- 3 Is there an MMM Server entry in the VASP List?
 - If yes, go to *Verifying the MMM Server Entry in the VASP List* (on page 76)
 - If no, go to *Configuring the MMM Server Entry in the VASP List* (on page 75)

Configuring the MMM Server Entry in the VASP List

The MMM Server VASP setting must be configured correctly so that the EAS can function properly. This section provides a procedure to configure the MMM Server VASP settings if one does not already exist.

Configuring the MMM Server Entry

1 From the VASP List screen, record an unused ID number in the space provided.

Unused ID number: _

Note: We suggest that you sort the list before you choose an unused ID number, in case your ID numbers are not in sequential order. To sort the list, click the **ID** heading twice to see all the IDs in sequential order.

🗙 Set Up VASP	X
VASP Type:	General 🗕
ID:	9
Name:	Y
IP Address:	¥
Status:	◆ Out of Service 🗼 In Service
Save	Cancel Help

2 Click File > New. The Set Up VASP window opens.

- 3 In the VASP Type field, select MMM Server from the list.
- 4 In the **ID** field, type the unused ID you recorded in step 1.
- 5 In the Name field, type MMM Server.
- 6 In the **IP Address** field, type the IP address of the DNCS that you recorded in *Determining the Set-Top Facing IP Address of the DNCS* (on page 23).

7 In the **Status** field, click **In Service**.

ACD TUDAL	MANA Control
ASP Type:	
ID:	4
Name:	MMM Server
IP Address:	I 10.253. 0. 1
Status:	Out of Service In Service
Save	Cancel Help

8 Click Save.

Results:

- The system saves the MMM Server configuration in the VASP list.
- The Set Up VASP window closes.
- The VASP List window updates with the added MMM Server.
- 9 On the VASP List window, click **File > Close**.

Verifying the MMM Server Entry in the VASP List

If the MMM Server already exists in the VASP list, you need to verify the information contained within the server settings.

Verifying the MMM Server Entry

1 From the VASP List window, find the MMM Server entry.

<u>F</u> ile <u>V</u> iew <u>H</u> e			
ID	Name	IP Address	Status
1	CFSession UI	10.253.0.1	In Servic
2	Broadcast File System	10.253.0.1	In Servic
З	Message Server	10.253.0.1	In Servic
4	MMM Server	10.253.0.1	In Servic
5	OSM Server	10.253.0.1	In Servic
6	GEARServer	10.253.0.1	In Servic
7	HCTM Server	10.253.0.1	In Servic

2 Click the row containing MMM Server.

- VASP Type: MMM Server -ID: 4 Name: MMM Server IP Address: [10.253. 0. 1 Status: Out of Service C In Service Save Cancel Help
- 3 Click File > Open. The Set Up VASP window opens.

- 4 Examine the Set Up VASP Window and answer the following questions:
 - Is VASP Type set to MMM Server?
 - Is Name recorded as MMM Server?
 - Is IP Address the same as the IP address you recorded in Determining the Set-Top Facing IP Address of the DNCS (on page 23)?
 - Is Status set to In Service?
- 5 Did you answer **yes** to every question in step 4?
 - If yes (you answered yes to *every* question), your MMM Server is configured correctly in the VASP list. Click Cancel to close the Set Up VASP Window.
 - If no, go to Configuring the MMM Server Entry in the VASP List (on page 75) and fix the incorrect entry.
- 6 Go to Configuring the EAS on the DNCS.

Configuring and Verifying the MMMRemote Server Entry in the VASP List

The MMMRemote Server relays the EAS messages to the remote RNCS (LIONN) servers in your network.

Note: Follow these procedures ONLY if your system uses our RCS solution. If your system does NOT use the RCS solution, continue to *Verifying the ORBIX Daemon is Disabled* (on page 86).

For further instructions on setting up the RNCS for EAS, see *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342).

Viewing the VASP List

- 1 From the DNCS Administrative Console, select one of the following tabs:
 - For DNCS SR 2.7/3.7/4.2 and later, click the **Network Element Provisioning** tab.
 - For DNCS SR 2.5/3.5/4.0 and earlier, click the **Element Provisioning** tab.
- 2 Click **VASP**. The VASP List window opens.

Note: The following example is from an SR 4.3 system. If you are using another System Release, your window might not look the same.

<u>F</u> ile <u>V</u> iew <u>H</u> elp					
ID	Name	IP Address	Status		
1	CFSession UI	10.253.0.1	In Service		
2	Broadcast File System	10.253.0.1	In Service		
З	Message Server	10.253.0.1	In Service		
4	MMM Server	10.253.0.1	In Service		
5	OSM Server	10.253.0.1	In Service		
6	GEARServer	10.253.0.1	In Service		
7	HCTM Server	10.253.0.1	In Service		

- **3** Is there an **MMMRemote Server** entry in the VASP List for each remote RNCS (LIONN) server in your network?
 - If **yes**, go to Verifying the MMMRemote Server Entry in the VASP List
 - If **no**, go to Configuring the MMMRemote Server Entry in the VASP List

Configuring the MMMRemote Server Entry for System Releases Earlier than SR 5.0

1 From the VASP List screen, record an unused ID number in the space provided.

Unused ID number: _

Note: We suggest that you sort the list before you choose an unused ID number, in case your ID numbers are not in sequential order. To sort the list, click the **ID** heading twice to see all the IDs in sequential order.

2 Click File > New. The Set Up VASP window opens.

Set Up VASP		×
VASP Type:	General	-
ID:	Y	
Name:	*	
IP Address:	Ĭ • • •	
Status:	♦ Out of Service	🕹 In Service
Save	Cancel	Help

- 3 In the VASP Type field, select MMM Server from the list.
- 4 In the **ID** field, type the unused ID you recorded in step 1.
- 5 In the Name field, type MMMRemote Server [name of RNCS server].
 Example: If your RNCS server is named LIONN1, type MMMRemote Server LIONN1.
- 6 In the **IP Address** field, type the IP address of the RNCS server.
- 7 In the **Status** field, click **In Service**.

8 Select the Site ID associated with the RNCS server from the drop-down list.

🔀 Set Up VASP	Σζ.
VASP Type:	MMM Server 🖃
ID:	102
Name:	MRemote Server LIONN1
IP Address:	172.18.0.1
Status:	✓ Out of Service
Site ID	1
Save	Cancel Help

9 Click Save.

Results:

- The system saves the MMM Server configuration in the VASP list.
- The Set Up VASP window closes.
- The VASP List window updates with the added MMM Server.
- 10 Repeat this procedure for each RNCS (LIONN) server in your network.
- 11 On the VASP List window, click **File > Close**.

Verifying the MMMRemote Server Entry

1 From the VASP List window, click the row containing the first **MMMRemote Server** in the list.

Note: To sort the list, click the **Name** heading twice to see all the server names in alphabetical order.

VASP List				
<u>F</u> ile ⊻iew <u>H</u> elp				
ID	Name	IP Address	Status	Site ID
6	SAM Server	192.168.100.1	In Service	1
7	HCTM Server	192.168.100.1	In Service	1
8	SGM Server	192.168.100.1	In Service	1
9	PASM Server	192.168.100.1	In Service	1
112	Appserv IPG	10.90.176.147	In Service	1
102	MMM Remote Site ID 2	172.18.0.1	In Service	2
103	MMM Remote Site ID 3	172.18.0.9	In Service	3
104	MMM Remote Site ID 4	172.18.0.17	In Service	4
105	MMM Remote Site ID 5	172.18.0.25	In Service	5
111	Appserv PPV	10.90.176.147	In Service	1 7
Done.				

2 Click File > Open. The Set Up VASP window opens.

🔀 Set Up VASP	X	
VASP Type:	MMM Server	
ID:	102	
Name:	MMM Remote Site ID 2	
IP Address:	172.18.0.1	
Status:	🕹 Out of Service \land In Service	
Site ID	1	
Save	Cancel Help	

- 3 Examine the Set Up VASP Window and answer the following questions:
 - Is VASP Type set to MMM Server?
 - Is Name recorded as MMMRemote Server [name of RNCS server]?
 - Is **IP Address** the IP address of the RNCS server?
 - Is **Status** set to **In Service**?
 - Is the **Site ID** the same as the Site ID of the associated RNCS server?

- 4 Did you answer **yes** to every question in step 4?
 - If yes (you answered yes to *every* question), your MMMRemote Server is configured correctly in the VASP list. Click Cancel to close the Set Up VASP Window.
 - If **no**, fix the incorrect entry.
- 5 Repeat this procedure for each RNCS (LIONN) server in your network.
- **6** Go to Configuring the EAS on the DNCS.

Verifying the ORBIX Daemon is Disabled

Starting in DNCS SR 2.0, the functionality of the EAS moved from the Application Server to the DNCS. Because of this, you no longer need the ORBIX daemon on the Application Server.

Note: This procedure is only necessary if you are using an DNCS SR 2.2 or DNCS SR 3.2 system.

Follow these instructions to verify that the ORBIX daemon is disabled on the Application Server.

Note: You need to be logged in to the Application Server as **dncs user** to complete this procedure.

- 1 Open an xterm window on the Application Server.
- 2 Type appControl and press Enter. The Applications Control window opens.
- 3 Is the ORBIX daemon listed in the Applications Control window?
 - If **yes**, go to *Appendix B* (on page 151)
 - If no, close the Applications Control window, you are finished with this procedure

Verifying the Naming Service

Verifying the Naming Service for SR 2.2 or 3.2

Follow these steps to verify the naming service if you are using SR 2.2 or SR 3.2.

- 1 Open an xterm window on the DNCS.
- 2 Type ps -ef | grep ns and press Enter. A list of processes and directories appears. Look for /dvs/tools/iona/OrbixNames1.1c/bin/ns.

Important: There should only be one listing of /dvs/tools/iona/OrbixNames1.1c/bin/ns

- 3 Is /dvs/tools/iona/OrbixNames1.1c/bin/ns listed only once?
 - If yes, then the naming service is running and you have completed this procedure.
 - If **no**, follow these steps if the naming service is listed more than once.
 - **a** Use the **kill** command to stop all naming service processes.
 - b Type rm /dvs/tools/iona/OrbixNames1.1c/NamesRep/ * and press Enter.
 - c Stop and then restart the ORBIX Daemon.
 Note: For detailed instructions, go to *Troubleshooting the ORBIX Daemon* (on page 132).
 - **d** Stop and then restart the MMM Server, then go to step 4.
- **4** Repeat steps 1 through 3 to verify the naming service.

Note: If the naming service is still not running, call Cisco Services.

Configuring the EAS on the DNCS

On the System Provisioning tab of the DNCS Administrative Console, there are four access keys in the EAS Message area that let you configure the EAS on the DNCS and send EAMs. These keys function as follows:

- **MMM Config** Initiate changes to the individual configurations that determine how EAS messages are displayed and broadcast.
- **EAS Config** Select the configuration for individual Emergency Events.
- EAS Message Initiate an Emergency Event message.
 Note: See Conduct EAS Tests for additional information.
- **FIPS Code** Assign FIPS codes and force tune services to each OOB bridge.

Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

Configure EAS Events

Use EAS Config to configure EAS individual event codes by selecting message content type and the configuration name.

Configuring EAS Events

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the System Provisioning tab.
- **3** Click **EAS Config**. The Set Up Emergency Alert System Configuration window opens.

×	X Set Up Emergency Alert System Configuration					
	Event Code		Message Content Type	Configuration Name		
	Administrative Message	ADR	Video Only	Default 🗸		
	Blizzard Warning	BZW	Audio & Video	Cfg26		
	Civil Emergency Message	CEM	None	Default		
	Practice/Demo Warning	DMO	Video Only	Default		
	Emergency Action Notification	EAN	Audio & Video	ForceTune		
	Emergency Action Termination	EAT	Audio & Video	Default		
	Evacuation Immediate Warning	EVI	Video Only	Default		
	Flash Flood Watch	FFA	Video Only	Default		
	Flash Flood Statement	FFS	Video Only	Default		
	Flash Flood Warning	FFW	Video Only	Default		
[[Edit Cancel Help Save Configuration Cancel Help					

4 Highlight the event in the **Event Code** column.

Note: The Event Code column lists the different types of emergencies.

- 5 Click the corresponding arrow from the **Message Content Type** column and select from the list of options. The options include:
 - None
 - Audio Only (sound only)
 - Video Only (text only)
 - Audio and Video (sound and text)

Important: CableCARD modules only receive text (video) EAS messages. If your system includes hosts with CableCARD modules, make sure that your EAS messages also include text (video).

6 Click the corresponding arrow from the **Configuration Name** column and set all the Event Codes to the **Default** setting (except for RWT and RMT).

Important: We recommend that you select the Default configuration for all events except for the RWT and the RMT.

7 Click **Save** to save your settings and close the Set Up Emergency Alert System Configuration window.

Configure FIPS Filtering (Optional)

FIPS filtering, through its integration with the DNCS, filters and sends EAS messages only to targeted states, counties, or subdivisions.

Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

If your system uses FIPS Filtering, you should configure the FIPS codes now. See *FIPS Filtering* (on page 155) for those procedures.

When you are finished configuring the FIPS codes, proceed with *Configuring EAS Messages*, next in this document.

Configuring EAS Messages

The FCC has defined 54 EAM message types, which are listed on the FCC website.

The configuration of an EAM specifies how the set-top presents the alert. By default, all EAMs use the same configuration, which means that they are presented by the set-top in the same way. On a set-top (that uses an output other than the IEEE 1394 interface), the default configuration displays a red banner at the top of the screen and the text for the message is shown in white. If the message is sent with audio content, it is played instead of the normal program audio while the message is active. CableCARD hosts only display text.

Important: If the set-top is connected to the TV with only the IEEE 1394 interface, the TV will only receive the EAS audio. The set-top must be connected to the TV with an additional digital video connection (HDMITM, DVI, or PrPbY) to receive the EAS video (text).

The DNCS lets you configure an alternate behavior for each EAM by modifying one of the existing MMM configurations and by associating an EAM configuration with the new configuration. For example, if you want a Child Abduction Warning (e.g., an Amber Alert) to force tune the set-tops to a local news service, you would use the force-tune configuration for that EAM.

Although the DNCS provides the capability to have a unique configuration for each type of EAM, most operators only use a few configurations (one for messages that will use the banner, a second for force tuning, one for required weekly tests and finally one for required monthly tests). You should check current FCC and local requirements to determine what settings are most appropriate for your operating environment.

The following options can be configured as part of an EAS Configuration.

- Force Tune Type Defines where the set-top is supposed to tune when an EAM that uses this configuration is received.
- **Message Time** Defines the delay in seconds between repeats of the message. For example, if this is set to **6** then the message will repeat 6 seconds after the end of the last time the message was broadcast.
- Alert Type Defines how long the message stays on the screen (in seconds).
- **Display Type** Defines the type of display motion and how long the emergency message appears on the screen (in seconds).

Accessing the Set Up MMM Configuration Window

Follow these steps to access the Set Up MMM Configuration window.

The MMM Server VASP setting must be configured correctly so that the EAS can function properly. This section provides a procedure to configure the MMM Server VASP settings if one does not already exist.

- 1 On the DNCS Admin console, click the DNCS tab.
- 2 Click the System Provisioning tab.
- 3 Click MMM Config. The MMM Configuration List window opens.

🗙 MMM Configuration List	<u>- 0 ×</u>
<u>F</u> ile <u>V</u> iew	<u>H</u> elp
Configuration Name	
Cfg00	<u> </u>
Cfg01	
Cfg02	
Cfg03	
Cfg04	
Cfg05	
Cfg06	
Cfg07	
Cfg08	
Cfg09	

4 Click to highlight the configuration name that you want to configure, then select **File > Open**. The Set Up MMM Configuration window opens.

Configuring the Force Tune Type

Follow these steps to set up the **Force Tune Type**.

Important: Most systems configure their force tune type to use an analog channel as the force-tune channel for EAS messages. If you have subscribers who use digital-only set-top boxes, or who use the IEEE 1394 interface on their set-tops, and you use forced tuning, the channel that you force tune to <u>must</u> be a digital channel that can display information about local and national emergencies. For example, if you use an analog community access channel as the force-tune channel, you will need to digitize this channel with an encoder.

- 1 On the Set Up MMM Configuration window, select the Force Tune Type tab.
- 2 Enter a **Description** for this configuration.
- 3 Does the configuration require force tuning?
 - If yes, go to step 4.
 - If **no**, click **None** in the **Force Tune** field. Go to step 5.

- **4** If the configuration requires force tuning, complete the following steps in the Force Tune Type fields:
 - a Click **Default Service**.
 - **b** In the **Default Service** field, select the SAM Service short description of the force tune service from the menu.

Note: An EAM with configured with a forced tuning redirects the subscriber's TV to the selected service that provides the emergency alert information.

5 In the **Priority** field, type a priority for the message. The lower the number, the higher the priority.

Note: Priority 0 (zero) is reserved for test messages.

Configuring the Message Time

Message Time establishes the delay between repeats of the EAS message in seconds. Follow these steps to set up the **Message Time**.

1 On the Set Up MMM Configuration window, select the **Message Time** tab.

Set Up MMM Configuration	×
Name: Cfg00 Description:	
Force Tune Message Alert Display Type Time Type Type Message Time Delay Between Repeats: 6	
Save Cancel	Help

- 2 In the **Delay Between Repeats** field, type a delay time for the EAS message, depending on the type of message you are configuring:
 - For standard EAS messages, type a delay that is *at least 6 seconds* for all configurations.
 - For required weekly test (RWT) and required monthly test (RMT) messages, type a delay greater than the default duration for each message so that subscribers only see the alert once during the RWT and RMT. Refer to Configure Weekly Tests and Configure Monthly Tests for more information about configuring RWT and RMT messages.

Configuring the Alert Type

Follow these steps to set up the **Alert Type**.

1 On the Set Up MMM Configuration window, select the Alert Type tab.

Set Up MMM Configuration			<u></u>
Name: Cfg00			
Description:			
Force Tune Message Aler Type Time Type	Display		
Alert Type	seconds		
Save		Cancel	Help

2 In the **Alert Remaining Time** field, type the number of seconds the messages will display on the screen. The Alert Remaining Time field has a maximum time limit of 120 seconds, which is also the default value.

Note: The value in the Alert Remaining Time field defines the duration of EAS messages on OpenCable hosts (with and without CableCARD modules). We recommend you set this field to 30 (seconds).

Configuring the Display Type

Display Type controls the type of display motion and how long the emergency message appears on the screen in seconds. Follow these steps to set up the **Display Type**.

1 On the Set Up MMM Configuration window, select the **Display Type** tab.

Name: Cfg00		
Force Tune Message Alert D. Type Time Type D. Motion Display Motion: Delayed Scroll	splay ype	
Motion Delay: 2 seconds		
Save	Cancel	Help

- 2 Type the number of seconds the message will appear on the screen into the **Motion Delay** field.
- 3 To complete the configuration of the EAS message, click **Save**.

Configure EAS to Properly Function with the CableCARD Module

When setting up the CableCARD Module on the DNCS, the following events *can* occur:

- Priority value defaults to zero Because a zero priority value is an EAS test setting, some CableCARD hosts may not support the value, resulting in the inability to display EAS messages.
- EAS Alert Remaining Time for unique EAS event codes automatically defaults to zero seconds If this occurs, EAS messages are displayed on CableCARD-compliant hosts, but the messages do not stop unless an End of Message (EOM) message is sent. We recommend that you set this field to **30** (seconds).

Important: CableCARD modules only receive text (video) EAS messages. If your system includes hosts with CableCARD modules, make sure that your EAS messages also include text (video).

Configuring EAS to Properly Function with the CableCARD Module for System Releases Prior to SR 5.0

To check these values and modify them, if necessary, follow these steps.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the System Provisioning tab.
- **3** Click **EAS Config** to view the Set Up Emergency Alert System Configuration window.

Event Code		Message Content Type	Configuration Name
Administrative Message	ADR	Audio & Video	Default
Avalanche Watch	AVA	Audio & Video	Default
Avalanche Warning	AVW	Audio & Video	Default
Blizzard Warning	8ZW	Audio & Video	Default
Child Abduction Emergency	CAE	Audio & Video	Default
Civil Danger Warning	CDW	Audio & Video	Default
Civil Emergency Message	CEM	Audio & Video	Default
Coastal Flood Watch	CFA	Audio & Video	Default
Coastal Flood Warning	CFW	Audio & Video	Default
Practice/Demo Warning	DMO	Audio & Video	Default

4 Select the row containing the first unique configuration name that you are using, and click Edit Configuration to view the Set Up MMM Configuration window.Note: You can also double-click the event code to access this screen.

5 Verify that the **Priority** field contains a non-zero value.

Set Up MMM Configuration		_[0]
Name: Default		
Description:		
Force Tune Message Alert E Type Time Type E	Display Type	
Force Tune Type Force Tune: None Solution Default Service: A&E	iervice	
Priority: 3	Priority 0 is for Test Messages.	
Save	Cancel	Help

- **6** Is the Priority value zero?
 - If yes, click the Priority arrow and select a non-zero value (for example, 3). Then go to step 7.
 - If **no**, go to step 7.
- 7 Click the **Alert Type** tab to verify that the Alert Remaining Time field is a nonzero value.

Note: The value in the Alert Remaining Time field defines the duration of EAS messages on OpenCable hosts (with and without CableCARD modules).

Name: Default Description: Force Tune Message Alert Display Tune Tune	
Description:	
Force Tune Message Alert Display	
Type Time Type Type	
- Alert Type	
Alert Remaining Time: 30 seconds	
Saus I Cancel I	Help

- 8 Is the Alert Remaining Time set to zero?
 - If yes, enter a value (in seconds) greater than zero. Then go to step 9.
 Note: We recommend that you type 30 for this field.
 - If **no**, go to step 9.
- 9 Click **Save** and click **Close**.
- **10** Repeat steps 3 through 9 for each unique configuration you have in use.

- **11** From the Set Up Emergency Alert System Configuration window, click **Close**.
- 12 Test the EAS alert functionality to verify that it is working properly.Note: We recommend that you test the EAS alert functionality each week.Refer to *Test the EAS from the DNCS* (on page 63) for more information.

Verifying and Modifying the MMM Out-of-Band Data Rate

This section contains the steps you need to follow to verify and modify the MMM OOB carousel data rate (if necessary).

Verifying and Modifying the MMM Out-of-Band Data Rate for System Releases Prior to SR 5.0

1 From the DNCS Administrative Console, click the **Application Interface Modules** tab.

DNCS Administrative Console Host:	wembley			_ 🗆 ×
<u>F</u> ile				<u>H</u> elp
DNCS	Application Interface Modules	B Server	Network Managemen	t
Application Interface M	lodules			
BFS Admin	SAM Service	SAM Config	Non-Channel Services	
BFS Client	Channel Maps	Group Definitions	Client Filters	

- 2 Click BFS Admin. The BFS Administration window opens.
- **3** Click the **Sources** tab. A list of Sources and corresponding Source IDs displays in the BFS Administration window.

4 Double-click **MMM OOB**. The Set Up BFS Source window opens displaying MMM OOB data.

Set Up BFS Source		x
Source Name:	[МММ ООВ	
Source ID:	21	
Source Type	◆ BFS	
Transport Type:	↓ In-band	
Data Rate:	10 Mbps	
Block Size:	1024 bytes	
Indication Interval:	[200 msec	
Source:	♦ enable	
Available Host	s Selected Hosts	
ASI_BFS	Add >>	Z
Save	Cancel Help	

- 5 Is the Data Rate set to 0.10 Mbps?
 - If **yes**, go to step 7.
 - If **no**, click in the Data Rate field and change the data rate to 0.10 Mbps.

Important: This setting might not match the existing published recommendations for BFS carousel data rates.

- 6 Click **Save** to save and apply the new setting. The system restarts the data carousel and applies the new data rate.
- 7 Send a test EAS message with audio.
- 8 Was the test successful?
 - If **yes**, go to step 14.
 - If no, increase the data rate in 0.01 Mbps increments and continue sending test EAS messages with audio until the test is successful. Then, go to step 9.
- **9** Run a Doctor report to evaluate your overall OOB data rate. Your overall (aggregate) OOB Carousel Datarate should be less than 35.00 Mbps (including the MMM OOB, which is not included as part of the aggregate OOB Carousel Datarate).
- **10** Is your overall (aggregate) OOB Carousel Datarate less than 35.00 Mbps (including the MMM OOB)?
 - If **yes**, go to step 14.
 - If **no**, go to step 11.
Verifying and Modifying the MMM Out-of-Band Data Rate

- 11 Click in the Data Rate field and change the data rate back to 0.10 Mbps.
- **12** Click **Save** to save and apply the new setting. The system restarts the data carousel and applies the new data rate.
- **13** Contact Cisco Services and report your Doctor report findings. Cisco Services will help you troubleshoot your overall OOB data rate, including the MMM OOB data rate.
- 14 Close the Set Up BFS Source window.

EAS Suppression on Digital Channels

WARNING:

Use this feature at your own risk. It is imperative that service providers use this feature carefully so as not to suppress EAS messages on services that do not already provide EAS information. We do not take responsibility for the incorrect use of this feature.

The EAS suppression feature allows service providers to suppress EAS information on digital channels that already provide EAS coverage to their viewers.

For example, the digital channel might carry a local over-the-air TV station that is rebroadcast through the service provider's system. The TV station provides EAS coverage through its own process.

Beginning with SARA 1.60 and SARA 1.90 (DVR), a new URL modifier (**;NOEAS**) was added that allows service providers to suppress EAS on digital channels.

Notes:

- EAS suppression is only available to systems that use SARA, our resident application.
- The URL modifier has no effect unless the set-top is tuned to a digital channel where the EAS message is received.

Configuring a Channel to Suppress EAS Messages

- **1** On the DNCS Administrative Console, click the **Application Interface Modules** tab.
- 2 Click SAM Service. The SAM Service List window opens.
- **3** Double-click the digital service you want to edit. The Set Up SAM Service window for that service opens.

-		Set Up SAM Service	-
	Service ID:	501	
	Service Name:	WUVG	
	Short Description:	WUVG	
	Long Description:]wuvg	
	Application URL:	bfs://resapp/watchtv;NOEAS	Select
	Logo:	255	
	Parameter:	C Number: 1015) String:	
Ī	Save	Cancel Help	
Γ			

4 Click in the Application URL line to place your cursor at the end of the URL statement.

- SAM Service List <u>F</u>ile <u>V</u>iew <u>H</u>elp Short Description Service ID URL Tag Service Name WESTW WESTW HITS 734 13 805 watchtv WGN ANALOG 21 WGN 808 watchtv WMAXE WMAXE GB1 237 783 watchtv A011 PXA 782 WPXA WUVG WUVG 5(1 watchtv;NOEAS wwwww WIDTH TEST 570 ZDTV ZDTV HITS 752 802 watchtv bg bogus 624 virtchan hdtv dncs-hd 684 watchtv VCS_S vcs_source 678 watchtv
- 5 Append the line to include ;NOEAS.

6 Click **Save**. The Set Up SAM Service window closes. The SAM Service List shows the appended URL on the same line as the service you edited.

	SAN	1 Service Li	st	• [
<u>F</u> ile <u>V</u> iew				<u>H</u> elp
Short Description	Service Name	Service ID	URL Tag	1
WESTW	WESTW HITS 734	805	watchtv	[
WGN	WGN ANALOG 21	808	watchtv	
WMAXE	WMAXE GB1 237	783	watchtv	
WPXA	A011 PXA	782	watchto	
WUVG	WUVG	5 (1	watchtv;NOEAS	
WWWWW	WIDTH TEST	570	watchtu	
ZDTV	ZDTV HITS 752	802	watchtv	
bg	bogus	624	virtchan	
hdtv	dncs-hd	684	watchtv	
VCS_S	vcs_source	678	watchtv	

7 Click File > Close to close the SAM Service List.

Setting Up and Configuring Weekly Tests

This section contains procedures for setting up and configuring required weekly tests for systems using system releases prior to SR 5.0.

Weekly tests consist of transmitting the EAS digital header codes and end of message (EOM) codes once per week. Weekly tests must be conducted by EAS participants on different days and at different times.

No weekly test is necessary during the week that a monthly test is conducted or when there is an EAS activation for a state or local emergency.

The FCC requires system operators to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

The procedures in this section provide you with instructions for configuring your DNCS to perform regular tests of your EAS.

Note: The DNCS and FCC use the following acronyms to refer to the mandated tests of the EAS:

- **RWT:** Required Weekly Test
- RMT: Required Monthly Test

Weekly tests consist of transmitting the EAS digital header codes and end of message (EOM) codes once per week. Weekly tests must be conducted by EAS participants on different days and at different times.

No weekly test is necessary during the week that a monthly test is conducted or when there is an EAS activation for a state or local emergency.

What You Need

To configure the DNCS for the required test, you need the **Default Duration** value from the user interface of your EAS Encoder/Decoder. Refer to the documentation that accompanied your EAS Encoder/Decoder for instructions on locating this value on your EAS Encoder/Decoder.

Note: The Default Duration refers to the duration of the outgoing alert messages.

Setting Up Weekly Tests

This section provides procedures for setting up the RWT on the DNCS.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the **System Provisioning** tab.
- **3** Click **EAS Config**. The Set Up Emergency Alert System Configuration window opens.
- 4 Highlight the row that contains the **Required Weekly Test**.
- **5** Click the **Configuration Name** arrow. A list of possible configuration names appears.
- 6 Select the **Cfg00** configuration. The configuration appears in the Configuration Name column.

Event Code		Message Content Type	Configuration Name
National Periodic Test	NPT	Video Only	Default
Nuclear Power Plant Warning	NUW	Video Only	Default
Radiological Hazard Warning	RHW	Video Only	Default
Required Monthly Test	RMT	Audio & Video	Default
Required Weekly Test	RWT	Audio & Video	Cfg00
Special Marine Warning	SMW	Video Only	Default
Special Weather Statement	SPS	Video Only	Default
Shelter in Place Warning	SPW	Video Only	Default
Severe Thunderstorm Watch	SVA	Video Only	Default
Severe Thunderstorm Warning	SVR	Video Only	Default

- 7 Click **Save**. The system saves the new RWT configuration.
- 8 Click Cancel. The Set Up Emergency Alert System Configuration window closes.

Configuring Weekly Tests

After you set up the RWT, you need to set up the MMM Server. The DNCS uses the MMM Server to conduct tests of the EAS. Follow these instructions to configure the MMM Server on the DNCS for the RWT of the EAS.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the System Provisioning tab.
- 3 Click **MMM Config**. The MMM Configuration List window opens.
- **4** Double-click configuration **Cfg00** to use for the RWT. The Set Up MMM Configuration window opens with the Force Tune Type tab in the forefront.

Set Up MMM Configuration	IX
Name: Cfg00	
Description:	
Force Tune Message Alert Display Type Time Type Type	
Force Tune Type	
Force Tune: 🔷 None 💊 Default Service	
Default Service: A&E	
Priority: 11 Priority 0 is for Test Messages.	
Save Cancel Help	

5 Click the **Message Time** tab.

X Set Up MMM Configuration	_ 🗆 ×
Name: Cfg00 Description:	
Force Tune Message Alert Display Type Type Type Type Message Time Delay Between Repeats: 6	
Save Cancel	Help

- 6 In the Description field, type **RWT configuration**.
- 7 At your EAS encoder/decoder, locate the **Default Duration** value.

Note: If necessary, refer to the user guide that accompanied your EAS encoder/decoder.

8 In the **Delay Between Repeats** field, type a value (in seconds) that equals [(Default Duration/2) + 1 minute x 60]. Use whole integer division only (drop the decimal point before adding the +1 minute).

Important: We recommend setting the Delay Between Repeats field to **480** seconds for the RWT if the default duration for the RWT is 15 minutes.

Example: If the Default Duration for the RWT of your EAS encoder/decoder is 15 minutes, your Delay Between Repeats value must be $[(15/2 = 7) + 1 = 8 \times 60 = 480 \text{ seconds}].$

Note: Make sure that the Delay Between Repeats is always at least 6 seconds.

- **9** Click **Save**. The system saves your changes and the Set Up MMM Configuration window closes.
- **10** In the MMM Configuration List window, select **File > Close**. The MMM Configuration List window closes.

Setting Up and Configuring Monthly Tests

This section contains procedures for setting up and configuring required monthly tests for systems using system releases prior to SR 5.0.

The FCC requires system operators to conduct weekly and monthly tests of their Emergency Alert Systems (EAS). These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

The procedures in this section provide you with instructions for configuring your DNCS to conduct monthly tests of your EAS.

Note: The DNCS and FCC use the following acronyms to refer to the mandated tests of the EAS:

- **RWT:** Required Weekly Test
- **RMT:** Required Monthly Test

Monthly tests consist of the transmitting the following:

- EAS digital header codes
- The two-tone attention signal
- A brief test script and EOM code
- A visual display of header code data

Monthly tests must be retransmitted within 60 minutes of receipt:

- In odd months, monthly tests must be conducted between 8:30AM to local sunset
- In even months, monthly tests must be conducted between local sunset and 8:30AM

No monthly test is necessary during a month when there is an EAS activation that includes a two-tone alert signal and an audio message.

What You Need

To configure the DNCS for the required test, you need the **Default Duration** value from the user interface of your EAS Encoder/Decoder. Refer to the documentation that accompanied your EAS Encoder/Decoder for instructions on locating this value on your EAS Encoder/Decoder.

Note: The Default Duration refers to the duration of the outgoing alert messages.

Setting Up Monthly Tests

This section provides procedures for setting up the RMT on the DNCS.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the **System Provisioning** tab.
- **3** Click **EAS Config**. The Set Up Emergency Alert System Configuration window opens.
- 4 Highlight the **Required Monthly Test** row.
- **5** Click the **Configuration Name** arrow. A list of possible configuration names appears.
- **6** Select the Cfg01 configuration. The configuration appears in the Configuration Name column.

Event Code		Message Content Type	Configuration Name
National Periodic Test	NPT	Video Only	Default
Nuclear Power Plant Warning	NUW	Video Only	Default
Radiological Hazard Warning	RHW	Video Only	Default
Required Monthly Test	RMT	Audio & Video	Cfg01
Required Weekly Test	RWT	Audio & Video	Cfg00
Special Marine Warning	SMW	Video Only	Default
Special Weather Statement	SPS	Video Only	Default
Shelter in Place Warning	SPW	Video Only	Default
Severe Thunderstorm Watch	SVA	Video Only	Default
Severe Thunderstorm Warning	SVR	Video Only	Default

- 7 Click Save. The system saves the new RMT configuration.
- 8 Click Cancel. The Set Up Emergency Alert System Configuration window closes.

Configuring Monthly Tests

After you set up the RMT, you must set up the MMM Server. The DNCS uses the MMM Server to conduct tests of the EAS. Follow these instructions to configure the MMM Server on the DNCS for the RMT of the EAS.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the System Provisioning tab.
- 3 Click **MMM Config**. The MMM Configuration List window opens.
- **4** Double-click configuration **Cfg01** to use for the RMT. The Set Up MMM Configuration window opens with the Force Tune Type tab in the forefront.

Set Up MMM Configuration	
Name: Cfg01	
Description:	
Force Tune Message Alert Display Type Time Type Type	
Force Tune Type	
Force Tune: 🔸 None 💠 Default Service	
Default Service: A&E	
Priority: 11 Priority 0 is for Test Messages.	
Save Cancel Help	

5 Click the **Message Time** tab.

Set Up MMM Configuration	
Name: Cfg01 Description:	
Force Tune Type Message Time Alert Type Display Type Message Time Delay Between Repeats: 20	
Save Cancel Help	

- 6 In the Description field, type **RMT configuration**.
- 7 At your EAS encoder/decoder, locate the **Default Duration** value.

Note: If necessary, refer to the user guide that accompanied your EAS encoder/decoder.

8 In the **Delay Between Repeats** field, type a value (in seconds) that equals [(Default Duration/2) + 1 minute x 60]. Use whole integer division only (drop the decimal point before adding the +1 minute).

Important: We recommend setting the Delay Between Repeats field to **1860** seconds for the RMT if the default duration for the RMT is 60 minutes.

Example: If the Default Duration for the RMT of your EAS encoder/decoder is 60 minutes, your Delay Between Repeats value must be $[(60/2 = 30) + 1 = 31 \times 60 = 1860 \text{ seconds}].$

Note: Make sure that the Delay Between Repeats is always at least 6 seconds.

- **9** Click **Save**. The system saves your changes and the Set Up MMM Configuration window closes.
- **10** In the MMM Configuration List window, select **File > Close**. The MMM Configuration List window closes.

Conduct EAS Tests

Test the EAS from the DNCS

This section describes the procedure for using the DNCS EAS Message menu to test the EAS using the EAS Message menu. The Send Emergency Alert System Message screens allow you to create, modify, and send an emergency alert system message. This procedure is valuable in testing your EAS system.

Important: Sending EAS messages outside of the regularly scheduled EAS tests or by using the DNCS EAS Message menu does **not** meet the FCC requirements for conducting the RWT and the RMT. The RWT and RMT tests should be end-to-end tests, and as such should be initiated from the EAS receiver and monitored at the set-top.

Send EAS Test Messages

Follow the steps in these procedures to send EAS test messages on the DNCS.

Note: Actual Emergency Alert Messages originate from the FCC. Use the DNCS EAS Message menu for local testing purposes only.

Sending EAS Test Messages

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the System Provisioning tab.
- **3** Click **EAS Message**. The Send Emergency Alert System Message window opens with the **EAS Message** tab in the forefront.

Send Emergency Alert System Message
EAS Message Send Message To
- Event Code
Event Code: Administrative Message (ADR)
Message Content Type: Video Only
Message Information
Message Name:
Duration: minutes
-Message Content
Video Content Type: () None () ASCII
Video Content:
Audio Content Type: O None O URL
Audio File: /export/home/easftp/ -none -
Send Cancel Help

4 In the **Event Code** area, click the Event Code arrow and select an event from the list.

Note: We recommend that you set the Event Code to Administrative Message (ADR).

5 In the **Message Information** area, type a unique Message Name and Duration in the appropriate fields.

Note: If you need to send additional messages, you must change the name of the message or the message will not be processed by the DNCS or by the set-tops.

- 6 In the **Message Content** area, choose one of the following options:
 - If you have only video (text) content, select ASCII and type the text in the Video Content.
 - If you have only **audio** (sound) content, select **URL** and click the **Audio File** arrow to select a file from the list.

Important: Be sure to select a WAV file from the list (a file with a *.wav* extension).

- If you have **audio and video** (sound and text) content, follow these steps:
 - a Choose ASCII and type the text in the Video Content text box.
 - **b** Choose **URL** and click the **Audio File** arrow to select a file from the list.
- 7 Click the **Send Message To** tab. The Send Emergency Alert System Message window updates with the **Send Message To** tab to the forefront.

	Send	Emergency	/ Alert Syste	em Messa	ge	
EAS Message	Send Message To					
Send Message	e To					1
State: County: Subdivision:	All States All Counties All Subdivisions		Add Remove		Selected FIPS Code	
	Send		Cancel		Help	

- 8 Did you purchase the EAS FIPS filtering product that provides FIPS filtering on your system?
 - If **yes**, go to step 10.
 - If **no**, go to step 9.
- 9 Your only option is to select All States. Select All States, then go to step 13.

Chapter 6 Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0

- 10 From the **State** list, select the state to which you are sending the EAS message.
- **11** From the **County** list, select the county in the selected state to which you are sending the EAS message.
- **12** From the **Subdivision** list, select the subdivision of the selected county to which you are sending the EAS message.
- 13 Click Add.
- 14 Is the content of the Selected FIPS Code window correct?
 - If yes, click Send.
 - If **no**, correct the information and then click **Send**.

Warning: The emergency information broadcasts to all DHCTs in the selected destinations.

Notes:

- To remove any destination from the **Selected FIPS Code** window, highlight this destination and click **Remove**.
- Depending on the MMM configuration parameters, the emergency message repeats and lasts for the duration you specified in the Message Information area.
- 15 Go to Terminate EAS Messages (on page 67).

Terminate EAS Messages

Occasionally, you may want to suspend or terminate an EAM before it reaches its configured duration. When you terminate an EAM, you stop transmitting all EAMs that are currently active in your system. If you terminate an EAM on an OOB bridge, you stop transmitting all EAMs that are currently active on that OOB bridge.

This section provides instructions for terminating an EAM using the user interface of the DNCS.

Terminating EAS Messages

Follow this procedure to terminate an EAS message from the DNCS.

- 1 From the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the System Provisioning tab.
- **3** Click **EAS Message**. The Send Emergency Alert System Message window opens with the EAS Message tab to the forefront.

- Send Emergency Alert System Message	J
EAS Message Send Message To	
Event Code-	l
Event Code: Administrative Message (ADR)	ľ
Message Content Type: Video Only	
Message Information	
Message Name: [
Duration: minutes	
Message Content	l
Video Content Type: (None) ASCII	l
Video Content: I	
	l
Audio Content Type: C None OURL	l
Audio File: /export/home/easftp/none	
Send Cancel Help	
	Ī

- **4** In the Event Code area of the window, click the Event Code arrow and choose one of the following options:
 - If you are using PowerKEY[®] CableCARD[™] modules on your system, go to step 5.

Note: The value in the Alert Remaining Time field defines the duration of EAS messages on OpenCable[™] hosts (with and without CableCARD modules).

• If you are *not* using CableCARD modules on your system, go to step 16.

Chapter 6 Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0

5 Choose End of Message (EOM). End of Message (EOM) appears in the Event Code field.

Send Emergency Alert Sy	stem Message	-0-
EAS Message Ser	nd Message To	
Event Code		
Event Co	ode: End of Message (EOM)	
Message Content T	vpe: Video Only	
Message Informatio	on	
Message Name: e	ndmes s	
Duration:	minutes	
-Message Content-		
Video Content Type	: 🔷 None 👽 ASCII	
Video Content		
Audio Content Type	: 🔨 None 🗇 URL	
Audio File:	/export/home/easftp/ - none -	
Send	Cancel	Help

- 6 Type a unique message name in the **Message Name** field.
- 7 Click the **Send Message To** tab. The Send Emergency Alert System Message window updates with the **Send Message To** tab to the forefront.
- 8 Did you purchase the optional FIPS filtering software product for your system?
 - If **no**, go to step 9.
 - If **yes**, go to step 10.
- 9 Your only option is to select All States. Select All States, then go to step 14.
- 10 Click the **State** arrow and select the state the EOM message is sent to.

Important: You can stop all active EAMs by sending an EOM to All States.

Note: There will be no interference with services if a DHCT that does not have any active EAMs receives an EOM.

- **11** Click the **County** arrow and select the county in the selected State the EOM message is sent to.
- **12** Click the **Subdivision** arrow and select the subdivision of the selected county the EOM message is sent to.
- 13 Click Add.

- 14 Is the content of the Selected FIPS Code window correct?
 - If yes, click Send. Go to step 26.
 - If **no**, correct the information and click **Send**. Go to step 26.

Important: If your system is currently broadcasting multiple EAMs, be sure you terminate the correct message.

Note: To remove any destination from the **Selected FIPS Code** window, highlight this destination and click **Remove**.

Result: The DNCS transmits instructions to CableCARD modules to stop displaying the EAM.

- **15** Click **EAS Message**. The Send Emergency Alert System Message window opens with the EAS Message tab to the forefront.
- **16** Choose **Emergency Action Termination (EAT)**. Emergency Action Termination appears in the Event Code field.

Send Emergency Alert Syste	em Message		<u>_0×</u>
EAS Message Send	Message To		
Event Code			
Event Coo	le: Emergency Action Ter	mination (EAT)	
Message Content Typ	e: Audio & Video		
Message Information			
Message Name:			
Duration:	minutes		
Message Content			
Video Content Type:	♦ Nonel ♦ ASCH		
Video Content:	Year		
Audio Content Type:	None Via		
Audio File:	/export/home/easftp/	- none -	
Send	Cancel		Help

17 Type a unique message name in the Message Name field.

Chapter 6 Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0

18 Click the **Send Message To** tab. The Send Emergency Alert System Message window updates with the **Send Message To** tab to the forefront.

-	-	Send	Emergenc	y Alert Syst	em Messag	ge	
ſ	EAS Message	Send Message To					
	-Send Message	e To					
						Selected FIPS Code	
	State:	All States		Add			
	County:	All Counties		Remove			
	Subdivision:	All Subdivisions					
Ī		Send		Cancel		Help	

- 19 Did you purchase the optional FIPS filtering software product for your system?
 - If **no**, go to step 20.
 - If **yes**, go to step 21.
- 20 Your only option is to select All States. Select All States, then go to step 25.
- 21 Click the State arrow and select the state the EOM message is sent to.

Important: You can stop all active EAMs by sending an EOM to **All States**. **Note:** There will be no interference with services if a DHCT that does not have any active EAMs receives an EOM.

- **22** Click the **County** arrow and select the county in the selected State the EOM message is sent to.
- **23** Click the **Subdivision** arrow and select the subdivision of the selected county the EOM message is sent to.
- 24 Click Add.
- 25 Is the content of the Selected FIPS Code window correct?
 - If yes, click Send.
 - If **no**, correct the information and click **Send**.

Important: If your system is currently broadcasting multiple EAMs, be sure you terminate the correct message.

Note: To remove any destination from the **Selected FIPS Code** window, highlight this destination and click **Remove**.

Result: The DNCS transmits instructions to DHCTs to stop displaying the EAM.

26 Click **Cancel** on the Send Emergency Alert System Message window. The window closes.

Improve EAS Performance

You must identify the MMM out-of-band (MMM OOB) carousel data rate that works best for your system. This section provides a procedure for verifying and modifying the MMM OOB carousel data rate on the DNCS (if necessary) to improve EAS performance.

Important: The total overall out-of-band carousel data rate on your system must *not* exceed 0.35 Mbps.

Note: Refer to the *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377) for additional information on configuring the DNCS carousel data rates.

Verifying MMM Server Performance

Follow these steps to verify the configuration and performance of the MMM Server.

1 Send a test EAS message with audio to a selected destination.

Note: See *Send EAS Test Messages* (on page 64) for information on sending test messages.

- 2 Open an xterm window on the DNCS.
- **3** Type cd /dvs/dncs/tmp and press Enter. The /dvs/dncs/tmp directory becomes the working directory.
- 4 To locate the most recent MMMServer files, type ls -1 MMMServer.* and press Enter.

Note: The "l" in ls is a lowercase letter L.

Result: A list of MMMServer files appear.

5 To view the contents of one of these files, type view MMMServer. [xxx].

Note: In this command, **[xxx]** represents the extension of the file you want to view.

- **6** Type cd /dvs/dvsFiles/MMM and press Enter. The /dvs/dvsFiles/MMM directory becomes the working directory.
- 7 Type ls -l *.aiff and press Enter.

Note: The "l" in -l is a lowercase letter L.

Result: A list of AIFF files in the /dvs/dvsFiles/MMM directory appears.

Important: Complete this procedure immediately after sending an EAS message with audio. The AIFF file will only exist in the directory when you send an EAS message with audio, and this message is still active. The system removes this file when the EAS message terminates.

Chapter 6 Configure the DNCS for EAS and Conduct Tests for System Releases Prior to SR 5.0

- 8 Are there AIFF files in the /dvs/dvsFiles/MMM directory with a current time and date stamp?
 - If **yes**, you have completed this procedure.
 - If no, check the log for error messages. Contact Cisco Services for further assistance if necessary.

Note: For troubleshooting information on the MMM Server, go to *Troubleshoot the MMM Server* (on page 135).

Conduct Scheduled Weekly and Monthly Tests

This section provides a table of the requirements, methods, and procedures for conducting the RWT and the RMT on each EAS.

Important: You **must** configure your system so that the RMT *always* functions in automatic mode. The FCC conducts the RMTs.

Note: You can configure your system so that the RWT always functions in automatic mode or you can set up the RWT to run in manual mode. See *Test the EAS from the DNCS* (on page 63) for information on sending and terminating ad hoc EAS messages.

Conducting Weekly and Monthly Tests

Use the following table to find your EAS equipment manufacturer, and follow the instructions provided for your system. Refer to the documentation for your specific EAC for additional information on conducting the RWT and the RMT.

Important: If your system does not function as expected, refer to *Troubleshooting* (on page 121) for troubleshooting procedures for the EAS.

System	RWT	RMT
Megahertz	Automatic Mode:	Automatic Mode:
	Automated process	Automated process
	Manual Mode:	Manual Mode:
	Press the Week soft key.	The FCC requires that the RMT
	Enter your password .	function in automatic mode.
	■ Press the Proceed soft key.	
Trilithic	Automatic Mode:	Automatic Mode:
	Automated process	Automated process
	Manual Mode:	Manual Mode:
	Not available	The FCC requires that the RMT function in automatic mode.

System	RWT	RMT
Monroe System	Automatic Mode:	Automatic Mode:
with Digital Envoy	Automated process	Automated process
Litvoy	Manual Mode:	Manual Mode:
	 Press the MODE soft key. Various MIP-021 options appear on the LCD screen. 	The FCC requires that the RMT function in automatic mode.
	 Press the NO soft key until the message SEND WEEKLY TEST appears. 	
	■ Press the YES soft key.	
Frontline	Automatic Mode:	Automatic Mode:
	Automated process	Automated process
	Manual Mode:	Manual Mode:
	Press the key labeled Weekly Test on the EAS Encoder. The Send Hdr and the On Air Relay indicators illuminate to show that the test is in process.	The FCC requires that the RMT function in automatic mode.

7

Troubleshooting

Introduction

This chapter provides troubleshooting information that will help you to verify the proper configuration and performance of the EAS, so that you can achieve optimum system performance in the receiving and sending of EAS messages.

In This Chapter

Troubleshoot Digital EAS Equipment	122
Troubleshoot the DNCS Network	127
Troubleshoot DNCS Configuration and Performance	129
Troubleshoot Weekly and Monthly Tests	140
Troubleshoot Set-Top Configuration and Performance	141
Troubleshoot CableCARD Module Configuration	144

Troubleshoot Digital EAS Equipment

If you have problems with your digital EAS equipment, please refer to the appropriate documentation provided with your equipment, or contact the manufacturer.

This document refers to the manufacturers and distributors of digital EAS equipment used by our customers. The Emergency Alert Controller (EAC) resides at your site and serves as an interface between your EAS receiver and the DNCS. The following companies manufacture EAC solutions that are known to work with the DNCS:

- Sage Alerting Systems, Inc. (MegaHertz)
- Trilithic, Inc. (Trilithic)
- Frontline Communications (Frontline)
- Monroe Electronics (Digital Envoy)

Note: The Monroe Electronics EAS uses an encoder/decoder manufactured by the HollyAnne Corporation.

Troubleshoot the Emergency Alert Controller

This section provides information to help you troubleshoot your Emergency Alert Controller (EAC) configuration.

Important: Some configuration and troubleshooting information is provided for third-party equipment (such as MegaHertz, Trilithic, Monroe, and Frontline). However, you should always refer to the documentation that comes with that equipment when you configure or troubleshoot that equipment. The scope of this information is to make sure that equipment can communicate with our equipment, not to be a comprehensive configuration and troubleshooting guide for third-party equipment.

Troubleshoot the EAC PC

Important: When troubleshooting your EAC, if any of the settings are incorrect, go to the section pertaining to your system in *Verify Your EAS Equipment Configuration* (on page 7), and follow the verification procedures listed there. If you need additional assistance, call Cisco Services.

Use the following information to troubleshoot your EAC configuration.

Troubleshooting the MegaHertz System

- Verify that all configuration settings are correct. See *Verify the MegaHertz System* (on page 9) and your EAC system documentation for more information.
- Analyze the log file located in C:\MCMSA\log.txt.

For more troubleshooting information, refer to the documentation that came with your EAC system.

Troubleshooting the Trilithic System

- Verify that all configuration settings are correct. See *Verify the Trilithic System* (on page 11) and your EAC system documentation for more information.
- Verify that all events are enabled.
- You can test FTP, socket, and digital messages using the Messages-Destinations menu.

For more troubleshooting information, refer to the documentation that came with your EAC system.

Troubleshooting the Monroe System with Digital Envoy

 Verify that all configuration settings are correct. See *Verify the Monroe System with Digital Envoy* (on page 13) and your EAC system documentation for more information.

Note: The Monroe Electronics EAS uses an encoder/decoder manufactured by HollyAnne Corporation.

For more troubleshooting information, refer to the documentation that came with your EAC system.

Troubleshooting the Frontline System

 Verify that all configuration settings are correct. See *Verify the Frontline System* (on page 15) and refer to your EAC system documentation for more information.

Chapter 7 Troubleshooting

Troubleshooting EAC Performance

Important: When troubleshooting your EAC, if any of the settings are incorrect, go to the section pertaining to your system in *Verify Your EAS Equipment Configuration* (on page 7), and follow the verification procedures listed there. If you need additional assistance, call Cisco Services.

Use the following information to troubleshoot your EAC performance. For more troubleshooting information, refer to the documentation that came with your EAC system.

Troubleshooting MegaHertz System Performance

Follow these steps to troubleshoot your MegaHertz EAC performance.

- 1 From a DOS prompt on the MegaHertz EAC, ping the Ethernet address of the DNCS to verify communication from the EAC to the DNCS.
- 2 Check the C:\MCMSA\log.txt file for TXT and WAV files.
- **3** If you receive the error message **VideoData System License Expired**, you must close all programs and properly shut down the EAC; then, power off and power on the EAC.

For more troubleshooting information, refer to the documentation that came with your EAC system.

Troubleshooting Trilithic System Performance

The EAC uses FTP to transfer WAV and TXT files to the DNCS. You can view these log files from the EASyPLUS screen.

Note: You can only check the log file if your system has previously sent EAMs.

Follow these steps to view the log files.

Note: This procedure was performed using Trilithic EASyPLUS software version 6.07.

- 1 On the EAC PC, in the Trilithic screen, click the Logs tab.
- **2** Select **Download EASy+ Log**. Verify that the log file has a current time and date stamp, and that the information in the log file accurately reflects recent EAS activity.
- 3 Note: For support for your Trilithic EAC, contact Trilithic, Inc.

For more troubleshooting information, refer to the documentation that came with your EAC system.

Troubleshooting Monroe System with Digital Envoy Performance

Follow these steps to troubleshoot EAC performance in the Monroe system when using the Digital Envoy EAC.

- 1 From a DOS prompt on the Digital Envoy EAC, ping the Ethernet address of the DNCS to verify communication from the EAC to the DNCS.
- 2 Monitor the dynamic logging of message processing and transmission using a DOS window by clicking **JAVA** on the lower toolbar.
- **3** Check the content of this window for the type of message transferred, the date and time stamp, and the response time of the DNCS.
- **4** Follow these steps to view the **log.log** file to verify that the messages recorded there have a current time and date stamp.
 - a Click Stop on the Digital Envoy GUI.
 - **b** Minimize the Digital Envoy GUI.
 - c Minimize the DOS window.
 - d Click the Windows Explorer icon.
 - e Find and select the C:\java\altronix\ directory.
 - **f** Find and double-click the **log.log** file located in the C:\java\altronix directory. The log.log file opens in Windows WordPad.
 - **g** View the list of messages that are recorded in the log.log file and verify that they have a current time and date stamp.

Important: If the messages do not have a current time and date stamp, call Cisco Services for further assistance.

- 5 Follow these steps to return to the Digital Envoy GUI.
 - **a** Close Windows WordPad.
 - **b** Close Windows Explorer.
 - c Click **Envoy**, and then click **Java** on the Windows taskbar. The Digital Envoy GUI maximizes.
 - d Click **Start** on the Digital Envoy GUI.

For more troubleshooting information, refer to the documentation that came with your EAC system.

Troubleshooting Frontline System Performance

Follow these steps to troubleshoot your Frontline EAC performance.

- 1 From a DOS prompt on the Frontline EAC, ping the Ethernet address of the DNCS to verify communication from the EAC to the DNCS.
- 2 From the Log Status Viewing GUI on the EAC, verify that the time and date stamp of the log are a current time and date. **The Application has been started** message appears on the same line as the current time and date.
- 3 FTP to the DNCS and login to verify EAC communications with the DNCS.

For more troubleshooting information, refer to the documentation that came with your EAC system.

Troubleshoot the DNCS Network

Troubleshoot the DNCS Ethernet Hub

The DNCS Ethernet hub is a network hub that enables communication between the EAC and the DNCS. A Network Analyzer is a diagnostic tool that you can use to troubleshoot communication between the EAC and the DNCS.

Troubleshooting the DNCS Ethernet Hub

Connect the Network Analyzer to the same Ethernet hub as the EAC and the DNCS to capture messages from the IP address of the EAC to the Ethernet IP address of the DNCS.

Use this data to analyze and troubleshoot the communication between the EAC and the DNCS, based on the parameters listed in your EAC documentation.

Troubleshoot the BFS

During normal operations, the BFS displays green status lights on the DNCS Control window. If you have red or yellow status lights or you see messages that indicate a problem, contact Cisco Services.

Troubleshoot Pass-Through

Pass-Through is the element group that contains the single element item PassThru.

PassThru is a single element item that passes messages through the DNCS to the set-tops.

During normal operations, PassThru displays green status lights on the DNCS Control window. If you have red or yellow status lights or you see messages that indicate a problem, contact Cisco Services.

	_
r	1
т	

Troubleshoot the QPSK Hub

The QPSK hub is a point in the network where you can capture and analyze messages from the PassThru process to the set-tops. The Network Analyzer is a diagnostic tool that you can use to troubleshoot communication between the DNCS and the set-tops.

Troubleshooting QPSK

Connect the Network Analyzer at this point in the network and capture messages from the PassThru process to the subnet masks of the set-tops receiving the EAS message.

Important: The PassThru process will report "11 05 00 02" at offset 0 x 2a (42) of the packet. If other values are reported, contact Cisco Services for further assistance.

Refer to the documentation for your version of QPSK for troubleshooting information.

Troubleshoot DNCS Configuration and Performance

This section provides procedures for troubleshooting DNCS configuration and performance.

Troubleshooting the DNCS MMM/EAS, Resident App Servers

Follow these steps to verify the DNCS MMM/EAS, Resident App Servers.

- 1 Open an xterm window on the DNCS.
- 2 Type **dncsControl** and press **Enter**. The Dncs Control window opens.
- **3** Type **2** (for **Startup/Shutdown Single Element Group**), and press **Enter**. The Dncs Control Startup/Shutdown Element Group window opens listing DNCS element groups.

Note: You might need to expand the window to view the entire list of DNCS elements.

- 4 Find DNCS MMM/EAS, Resident App Servers on the list, type the corresponding number, and press Enter. The system prompts you to enter a target status for the element group.
- 5 Type the letter **e** (for **Display Element Entries**), and press **Enter**. The Element Group DNCS MMM/EAS, Resident App Servers list appears, and the ResAppServer, MMMServer, and EARS processes display a status of running.

Note: If the ResAppServer, MMMServer, and EARS processes do *not* display a status of running, contact Cisco Services.

- 6 To return to the xterm window, type **x** and press Enter.
- 7 Type **x** and press **Enter**, again.
- 8 Type **x** and press **Enter**, a third time. The Dncs Control window closes and the xterm window reopens.

Troubleshooting the EARServer

Follow these steps to troubleshoot the EARServer.

- 1 Open an xterm window on the DNCS.
- **2** Type **cd/dvs/dncs/tmp** and press **Enter**. The /dvs/dncs/tmp directory becomes the working directory.
- **3** To verify that **EARS** files exist in the directory, type **1s -1 EARS.*** and press **Enter**.

Note: The "l" in **ls** is a lowercase letter L.

Result: A list of **EARS** files appears. Check the time and date stamp for the most current time and date.

4 Type **view EARS.[xxx]** and press **Enter** to analyze an individual **EARS** file. Look for any current EAC messages or error messages.

Note: In this command, **[xxx]** represents the extension of the file you want to view.

Troubleshooting Error Messages

The following table provides procedures for troubleshooting EAS error messages.

Error Message	Ch	eck and Correct
The following message appears at the bottom of the Send EAS Message screen on the DNCS: MMMServer failure	1 2	Open an xterm window on the DNCS. Type cd/dvs/dncs/tmp and press Enter . The /dvs/dncs/tmp directory becomes the working directory.
	3	Save the latest EARS and MMMServer files, or copy these files to another directory, and then stop and restart the MMM Server.
		Important: If you choose to rename the files, do not use .000 in the file name extension.
		Note: For more information, go to <i>Stop and Restart the MMM Server</i> (on page 136).
The following message appears at the bottom of the Send EAS Message screen on the DNCS:	Ca	ll Cisco Services for assistance.
Send Message failed. Error occurred in accessing the database; Server will restart in a few minutes.		

Troubleshooting EAS with CableCARDs

When setting up the CableCARD Module on the DNCS, the following events *can* occur:

- Priority value defaults to zero Because a zero priority value is an EAS test setting, some CableCARD hosts may not support the value, resulting in the inability to display EAS messages.
- EAS Alert Remaining Time for unique EAS event codes automatically defaults to zero seconds If this occurs, EAS messages are displayed on CableCARD-compliant hosts, but the messages do not stop unless an End of Message (EOM) message is sent.

To check these values and modify them, if necessary, refer to *Configure EAS to Properly Function with the CableCARD Module* (on page 46).

Troubleshooting EAS after SR Upgrades

After performing an SR (System Release) upgrade, verify that your EAS equipment is still properly configured in the DNCS. Complete all the procedures in *Test the EAS from the DNCS* (on page 63).

After completing the procedures, verify that you can generate an EAS message for the EAC. Refer to *Verify Your EAS Equipment Configuration* (on page 7) and the manufacturer's documentation for more information.

Troubleshooting the Orbix.hosts File Configuration

Follow these steps to verify that the NS:dncsatm: line exists in the Orbix.hosts file.

- 1 Open an xterm window on the DNCS.
- 2 Type cd/dvs/tools/iona/OrbixMT_2.3c/cfg and press Enter. The /dvs/tools/iona/OrbixMT_2.3c/cfg directory becomes the working directory.
- 3 Type more Orbix.hosts and press Enter.
- 4 Does the line **NS:dncsatm:** appear?
 - If **yes**, you have completed this procedure.
 - If no, follow these steps if the NS:dncsatm: line is *not* listed in the Orbix.hosts file.
 - a In a Unix text editor, open the Orbix.hosts file.
 - **b** Scroll to the bottom of the file and type the following line: **NS:dncsatm:**
 - c Save the file.
 - **d** Repeat steps 1 and 2 to verify that **NS:dncsatm:** line now exists in the Orbix.hosts file.

Important: If NS:dncsatm: still does not appear, contact Cisco Services.

Troubleshooting the ORBIX Daemon

The ORBIX Daemon is a process on the DNCS that monitors requests between programs and between servers. If the DNCS stops receiving EAS messages from the EAC, the ORBIX Daemon might not be working correctly. To remedy this situation, you can stop and restart the daemon process. This section provides instructions for stopping and restarting ORBIX Daemon process.

Notes:

- Starting in SR 2.0, the Orbix daemon functionality of the EAS moved from the Application Server to the DNCS.
- The ORBIX Daemon is **not** used on the DNCS in system releases beginning with SR 2.7, 3.7, or 4.2.

Stopping the ORBIX Daemon Process

Follow these instructions to stop the ORBIX Daemon process.

- 1 Open an xterm window on the DNCS as **dncs** user.
- 2 Type dncsControl and press Enter. The Dncs Control window opens.

SNMP	ExAg	nt V1.1 (c) 1997. Licensed Ver	sion.
SysAp	ip Ag	nt: Main Menu	
]	1 2] Startup / Shutdown All Elem] Startup / Shutdown Single E	ent Groups Tement Group
[3] Define / Update Element Gro	up
[4] Define / Update Grouped Ele	ments
]	5] Update Agent Executive Para	meter.
]]]	LCX] List Connection Paramaters.] Connect To Different Agent.] Exit Menu Utility.	

- **3** Type **2** (Startup/Shutdown Single Element Group) and press **Enter**. The system displays a list of all servers and processes running on the DNCS.
- **4** Type the number associated with the **ORBIX Daemon** process, and press **Enter**. The system prompts you to enter a target status for the element group, or to type the letter **e** to display the individual element entries.
- **5** Type the letter **e** to Display Element Entries, and press **Enter**. The Element Group: DNCS SNMP & ORBIX Daemons list appears.

-	Dncs Control 🧧 🗖
Sta Ele Hos	artup / Shutdown Single Element Item ement Group: DNCS SNMP & ORBIX Daemons stname: dudley, UpTime: 0:06:31.00
[1	1]/dvs/dncs/bin/dncs-snmpd -s BIG 2>&1 Logger -g -n/dvs/dncs/tmp/dncs-s
rimp	Tgt Stt: running(2), Curr Stt: running(2), Wait: 0, Rest: 0
[2	2]/dvs/dncs/bin/dncs-snmpd -s CAQAM 2>&1 Logger -g -n/dvs/dncs/tmp/dncs
31	Tgt Stt: running(2), Curr Stt: running(2), Wait: 0, Rest: 0
[3	3]/dvs/dncs/bin/dncs-snmpd –s DAVIC_QPSK 2>&1 Logger –g –n/dvs/dncs/tmp
7 01	Tgt Stt: running(2), Curr Stt: running(2), Wait: 0, Rest: 0
[4	4]/dvs/dncs/bin/orbixd –u –c /dvs/dncs/tmp/orbixSync 2>&1 Logger –t –g
20117	Tgt Stt: running(2), Curr Stt: running(2), Wait: 0, Rest: 0
(Er	nter Number / X=Return To Menu / L=List Details / CR=Refresh)> 📕

- 6 Find the selection for orbixd in the list, type the corresponding number, and press **Enter**. The system prompts you to enter a target status for the element.
- 7 Type **1** (for stopped) and press **Enter**. The system displays a confirmation message.

Chapter 7 Troubleshooting

- 8 Type y (for yes) and press Enter. The Dncs Control window refreshes.Note: The Dncs Control window refreshes periodically, or you can press Enter at any time to force a refresh.
- 9 Wait until Curr Stt (for current state) indicates stopped.
- 10 Continue with Restarting the ORBIX Daemon Process, next in this document.

Restarting the ORBIX Daemon Process

Follow these instructions to restart the ORBIX Daemon process.

Note: If you have followed the instructions in this chapter in order, the Startup/Shutdown Single Element Item window should still be open.

- 1 Find the selection for orbixd in the Startup/Shutdown Single Element Item window list, type the corresponding number, and press **Enter**. The system prompts you to enter a target status for the element.
- **2** Type the letter **e** to Display Element Entries, and press **Enter**. The Element Group: DNCS SNMP & ORBIX Daemons list appears.
- **3** Find the selection for orbixd in the list, type the corresponding number, and press **Enter**. The system prompts you to enter a target status for the element.
- **4** Type **2** (for running) and press **Enter**. The system displays a confirmation message.
- 5 Type y (for yes) and press Enter. The Dncs Control window refreshes.Note: The Dncs Control window refreshes periodically, or you can press Enter to force a refresh.
- 6 Wait until Curr Stt (for current state) indicates running.
- 7 Type **x** and press **Enter**. The main menu of the Dncs Control window reappears.
- 8 Type **x** and press **Enter** to close the Dncs Control window.
- **9** Type **x** and press **Enter** again to return to the xterm window. The Dncs Control window closes and the xterm window reappears.
- **10** You must now stop and restart the MMM Server. Go to *Stop and Restart the MMM Server* (on page 136) for detailed instructions.
Troubleshoot the MMM Server

The MMM Server relays the TXT file to the PassThru process and converts the WAV file to AIFF format. It then places the AIFF file on the bfsServer. The system logs the MMM Server activity in MMMServer.[xxx] files, which are located in the /dvs/dncs/tmp directory.

Increase Debugging on the MMM Server

You can troubleshoot the MMM Server by increasing the debugging process.

CAUTION:

Do not let this increased debugging process run for more than a few hours. This process uses a large amount of disk space, so use this procedure only during troubleshooting.

Follow these steps to increase the debugging process on the MMM Server.

- 1 Open an xterm window on the DNCS.
- **2** Type **cd/export/home/dncs** and press **Enter**. The /export/home/dncs directory becomes the working directory.
- **3** Type **vi .profile** and press **Enter**. The system opens the .profile file in the vi editor.
- 4 Find the line containing **export EMCDEBUG=** in the file. **Example: export EMCDEBUG=SBbKKQ0-9**
- 5 Does the line contain an L?

Example: export EMCDEBUG=SBbKkQ0-9L

- If **yes**, close the file, you have completed this procedure.
- If no, append an uppercase letter "L" to the line and press Enter. The line should now read similar to the following:

export EMCDEBUG=SBbKkQ0-9L

- **6 Save** the configuration.
- 7 Stop and restart the MMM Server group to activate the new debugging settings. For more information, go to *Stop and Restart the MMM Server* (on page 136).

Troubleshooting the MMM Server Configuration

Follow these steps to troubleshoot the MMM Server.

Important: Complete this procedure immediately after sending an EAS message with audio. The AIFF file will only exist in the directory when you send an EAS message with audio, and this message is still active. The system removes this file when the EAS message terminates.

- 1 Open an xterm window on the DNCS.
- 2 Type **cd/dvs/dncs/tmp** and press **Enter**. The /dvs/dncs/tmp directory becomes the working directory.
- **3** To verify that **MMMServer** files exist in the directory, type **ls –l MMMServer.*** and press **Enter**.

Note: The "l" in **ls** is a lowercase letter L.

Result: A list of **MMMServer** files appears. Check the time and date stamps to verify that they are current.

4 Type **view MMMServer.[xxx]** and press **Enter** to analyze an individual **MMMServer** file. Look for EAC or error messages with the current time and date.

Note: In this command, **[xxx]** represents the extension of the file you want to view.

- 5 In the xterm window, type **cd/dvs/dvsFiles/MMM** and press **Enter**. The /dvs/dvsFiles/MMM directory becomes the working directory.
- 6 To verify that there are AIFF files in this directory, type **ls -l *.aiff** and press **Enter.** A list of AIFF files in the /dvs/dvsFiles/MMM directory appears.

Note: The "l" in ls is a lowercase letter L.

7 Check time and date of the AIFF file to verify that it has a current time and date.

Stop and Restart the MMM Server

If you have changed debugging settings, stopped and restarted ("bounced") the ORBIX daemon, or received an MMMServer failure error message, you need to stop and restart the MMM server.

Stopping the MMM Server

Follow these instructions to stop the MMM Server.

- 1 On the DNCS Administrative Console Status window, click **Control** in the **DNCS** section. The DNCS Control window displays.
- 2 Highlight the MMM Server process.
- **3** Click the **Process menu** and select **Stop Process**. A confirmation window appears.
- 4 Click **Yes**. When the DNCS stops the MMM Server process, it turns the green status indicator to red.
- 5 Go to **Restarting the MMM Server**, next in this document.

Restarting the MMM Server

Follow these instructions to restart the MMM Server.

Note: If you have followed the instructions in this section in order, the DNCS Control window should still be open.

- 1 On the DNCS Administrative Console Status window, click **Control** in the **DNCS** section. The DNCS Control window displays.
- 2 Highlight the MMM Server process.
- **3** Click the **Process menu** and select **Start Process**. A confirmation window appears.
- 4 Click **Yes**. The DNCS starts the MMM Server process and turns its red status indicator to green.

Stranded Audio Links

Audio files used with the EAS system are defined with an expiration time and date. Sometimes, when the MMM Server process of the DNCS is bounced before an audio file expires, a link to that audio file remains on the DNCS.

This audio link is referred to as being "stranded".

After an upgrade, you need to examine the dncsLog for the presence of stranded audio links, then delete those links if they exist.

Checking for Stranded Audio Links

- 1 Open an xterm window on the DNCS.
- 2 Type **cd/var/log** and press **Enter**. The /var/log directory becomes the working directory.
- **3** Type **grep -i aiff dncsLog** and press **Enter**. The system checks the dncsLog for the presence of aiff.

Note: The file extension of audio files the MMM Server uses is .aiff.

4 Did the grep operation from step 3 return a line similar to the following?

[Date Time] dncs bfsServer VGSDir::_checkLinkedFiles() Error, can't find file/MMMAud/a1847750.aiff, marking as inaccessible

- If yes, go to Deleting Stranded Audio Links, next in this document.
- If **no**, close the xterm window. You are finished with this procedure.

Chapter 7 Troubleshooting

Deleting Stranded Audio Links

- 1 From the DNCS Administrative Console, select the **Application Interface Modules** tab.
- 2 Click **BFS Client**. The Broadcast File Server List window opens.
- **3** Scroll down the window and double-click the **MMMAud** icon.

Note: The icon looks like a filing cabinet.

Result: The filing cabinet "opens" to display its files.

- **4** Highlight the file that corresponds to the stranded audio link you identified in *Checking for Stranded Audio Links* (on page 137).
- 5 Click **File > Delete**. A confirmation window displays.
- 6 Click Yes. The system deletes the file.

Notes:

- In some cases, you might have to repeat this procedure until the system finally deletes the file.
- If, after several attempts, the system does not delete the file, delete the entire MMMAud filing cabinet.
- 7 Close the Broadcast File Server List window.

Server Error when Registering with BFS

Beginning with DNCS SR 2.5/3.5, there can be times when the MMMServer fails to recover if, for some reason, the MMMAud BFS cabinet is removed, but the MMMCfg cabinet remains. When this happens, the DNCS writes an error message similar to the following in the dncsLog file:

...MMMBfs::_registerServer(): BFS Error registering with BFS

The initial symptom of this error shows up when you try to send an EAS message with both audio and video, and the DNCS GUI disappears from the screen.

If you see this behavior, follow the procedure in this section to remedy the error.

Note: This behavior was fixed by CR 52603 in DNCS SR 2.5/3.5 SP1.

Fixing the Server Error when Registering with BFS

To fix the server error when registering with BFS, you need to delete the MMMCfg cabinet from the BFS client. The MMMServer will re-register both the MMMAud and MMMCfg files after you refresh the BFS client.

- 1 From the DNCS Administrative Console, select the **Application Interface Modules** tab.
- 2 Click BFS Client. The Broadcast File Server List window opens.
- 3 Highlight the **MMMCfg** cabinet (the file looks like a filing cabinet).
- 4 Click File > Delete. A confirmation window opens.
- 5 Click Yes.
- 6 Click **View > Refresh**. The MMMServer re-registers both the MMMAud and MMMCfg files.

Troubleshoot Weekly and Monthly Tests

This section provides procedures for troubleshooting the receiving and transmission of weekly and monthly required tests.

Note: This information is culled from the FCC publication *Cable Emergency Alert System Procedures - 2007,* available at the FCC website (www.fcc.gov).

Failure to Receive an EAS Test

If you do not receive an RWT from your assigned monitoring sources, take the following actions:

- Determine why you did not receive a test:
 - Check your EAS equipment
 - Call your monitoring source(s)
- Take appropriate corrective action
- Document your findings in your EAS logs

Failure to Send an EAS Test

Failure to Send an RWT

If you are unable to send an RWT, take the following actions:

- Determine why no test was sent by checking your EAS equipment
- Take the appropriate corrective action
- Document your findings in your EAS record logs

Failure to Send an RMT

If you cannot sent an RMT received from your assigned monitoring sources, take the following actions:

- Determine why you did not receive a test:
 - Check your EAS equipment
 - Call your monitoring source(s)
- Take appropriate corrective action
- Document your findings in your EAS logs

Troubleshoot Set-Top Configuration and Performance

This section provides set-top configuration guidelines along with procedures for you to use to verify and troubleshoot set-top configuration and performance when verifying the correct operation of your EAS.

Important: Digital EAS activation occurs only if the set-top is powered on and is tuned to a digital channel. Digital EAS messages do not display on analog channels. You must provide separate EAS support for analog channels.

Verifying Set-Top Configuration

Use the following criteria when verifying set-top configuration:

- The configuration data is included in the MMM pass-through message.
- The text display and audio files are configurable and dependent on the EAS event type. An EAS event may contain text and/or audio contents. There could be no text or audio content at all, but only the configuration data; for example, in a Force Tune message.

Note: A Force Tune message is a message that forces all set-tops to automatically switch to another channel to receive an EAS message.

- Text data in HTML format, if any, is included in the EAS message.
- Audio data in AIFF format, if any, is found in the BFS file referenced by a URL in the EAS message.

Verifying Set-Top Performance

Use the following criteria when you verify set-top performance:

- The service for the digital channel does **not** contain the ;NOEAS URL modifier.
- The one-line EAS display starts in the upper left corner of the Society of Motion Picture and Television Engineering (SMPTE) safe title area of the screen.
- The EAS line of text, or ticker, scrolls from right to left at a rapid rate. The text appears for the amount of time that is set in the configuration data of the motion delay setting.
- If the Interactive Program Guide (IPG) is active, the captured video in the upper right corner of the screen freezes while the ticker displays.
- If the EAS is not Force Tuned, the ticker display remains while the resident application (ResApp) operates normally. The ticker appears over the General

Chapter 7 Troubleshooting

Settings menu, music channels, PIN entry screens, and other IPG screens.

- The EAS audio file always overrides analog and digital audio and internally generated sounds.
- The text display, or ticker, and audio playback repeat as long as necessary to fill the duration. If the delay time is greater than 5 seconds, the program audio is heard during the delay time between repeats.
- The EAS suspends operation when one of the following occurs:
 - The time reaches the origination time plus the duration received in the EAS request pass-through message.

Note: Origination time plus duration does not apply to Force Tuned messages.

- The set-top receives an EAS Termination (EAT) pass-through message.
- If the EAS message is active when a new EAS message is received, the entire new message including the audio file, if applicable, downloads and the old message suspends operation.
- If the EAS message causes Force Turning, other message types are ignored, except for the EAT message.

Troubleshooting Set-Top Configuration and Performance

A dedicated debug set-top is very useful for troubleshooting purposes, especially when EAS messages generate detailed debug logs.

Note: The switched power supply on the set-top is not powered on or off by the EAS.

Follow these procedures to troubleshoot the set-top configuration and performance.

- **1** Verify that the set-top is powered on and tuned to a digital channel when sending an EAS message.
- **2** Verify that the volume levels on both the set-top and the television set are accurate.
- 3 Verify the EAS status information on the SARA Information diagnostic screen.

Important:

- The SARA Information diagnostic screen displays information on the duration and origination time of the most recent EAS message. Use this information to verify correct reception and download of the latest EAS message.
- For additional information on set-top diagnostic screens, refer to *Understanding Diagnostic Screens for the Explorer DHCTs Application Guide* (part number 749244).
- 4 Verify that the MMM Server is working by sending an EAS test message from the DBDS GUI with text content only.

Important: All subscribers will receive the EAS test message unless you set up a test environment. We recommend that you set up test hubs (for example, using FIPS filtering) that are not on your production system. That way, subscribers will not receive the test messages.

- **5** Verify that the out-of-band Broadcast File System (OOB BFS) is operational by sending an EAS test message with audio content only.
- **6** Verify that the EAS Client on the set-top is operational by sending an EAS test message with both text and audio.

Troubleshoot CableCARD Module Configuration

To troubleshoot the EAS for CableCARD modules, verify the configuration as detailed in *Configure EAS to Properly Function with the CableCARD Module* (on page 46).

8

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.



Introduction

This appendix contains the text of the FCC requirements that requires service providers to conduct regular tests of their EAS equipment. This text is codified in the United States Code of Federal Regulations, Title 47: Telecommunication, Part 11 – Emergency Alert System (EAS), Section 11.61, Tests of EAS procedures.

Important:

- This text was current as of the date of publication of this document. For the most current requirements, contact the FCC.
- This section was culled from the FCC publication *Cable Emergency Alert System Procedures* 2007.
- You are required by the FCC to have a copy of FCC Parts 11 and 76 on your site. Refer to the FCC website (www.fcc.gov) for more information.

In This Appendix

11.61 Tests of EAS Procedures

Cable System Size	EAS Requirements	Small Cable System Requirements Under Option B		
Cable systems with fewer	Option A			
than 5,000 subscribers per headend must comply with either option A or option B	Provide National Level EAS Message on all programmed channels, including the required testing.			
	Option B	Video Interruptions	Must include a statement	
	Install EAS equipment that is capable of providing:		telling listeners on which channel the EAS video and audio message is displayed.	
	1 The Audio Alert Messages on all programmed channels.		Must flash a blank or black television screen simultaneously with, and of	
	2 Video Interrupt on all channels.		the same duration, as the EAS message.	
	3 Audio and Video EAS Messages on one programmed channel.			
Cable systems with 5,000 to 10,000 subscribers per headend	Install EAS equipment that is capable of providing Audio and Video EAS Messages on all programmed channels.			
Cable systems with 10,000 or more subscribers per headend	Install EAS equipment that is capable of providing Audio and Video EAS Messages on all programmed channels.			

EAS Designation

EAS instructions vary for each particular designation. Cable systems are designated as either participating or non-participating sources. Most cable systems have elected to participate in EAS and are designated as Participating National (PN) sources. However, cable systems that elect not to participate in the national level EAS must hold an FCC authorization letter. Nonparticipating systems are designated as Non-Participating National (NN) sources.

The EAS transmissions of national, state, and local emergencies by PN sources are intended for direct public reception. (47 C.F.R. Section 11.18(e)). All systems, including NN sources, are required to install and test EAS equipment. Upon activation of the national level EAS, NN sources are required to broadcast the EAS codes, Attention Signal, and the sign-off announcement in this handbook (*Cable Emergency Alert System Procedures - 2007*, an FCC publication), and then stop operating until the end of message code is received. (47 C.F.R. Section 11.18(f))

Monitoring Requirements

All EAS Participants must monitor two EAS sources. The monitoring assignments are specified in the EAS State Plans and are determined according to FCC monitoring priorities. If the required EAS sources cannot be received, alternate arrangements or a waiver may be obtained by written request to the FCC. In an emergency, a waiver may be issued over the telephone with a followup letter to confirm temporary or permanent reassignment. (47 C.F.R. Section 11.52)

EAS Equipment Readiness

EAS participants are required to test their ability to receive and distribute EAS messages and to keep records of all tests. EAS participants are responsible for ensuring that encoders, decoders, and signal generating equipment used as part of the EAS are installed so that the monitoring and transmitting functions are available during the times that the station is in operation. In addition, EAS participants must determine the cause of any failure to receive the required tests or activations specified in Section 11.61(a)(1) and (a)(2) and indicate in the station's EAS log why the tests were not received. These logs must be retained for three years at the EAS participant's headquarters.

In the event the EAS equipment becomes defective, a cable system may operate without the equipment pending its repair or replacement for a period not to exceed 60 days. If repair or replacement of defective equipment is not completed within 60 days, participants must submit an informal request for additional time to their assigned FCC field office. The request must include an explanation of what steps have been taken to repair the equipment. (47 C.F.R. Section 11.35(b) & (c)). Entries must be made in the participant's logs showing the date and time the equipment was removed and restored to service.

B

Disable the ORBIX Daemon on the Application Server

Introduction

Starting in DNCS SR 2.0, the functionality of the EAS moved from the Application Server to the DNCS. Because of this, you no longer need the ORBIX daemon on the Application Server.

Note: This procedure is only necessary if you are using an DNCS SR 2.2 or DNCS SR 3.2 system.

This appendix contains instructions to disable the ORBIX daemon on the Application Server.

In This Appendix

Disabling the ORBIX Daemon on the Application Server

Follow these instructions to disable the Orbix daemon on the Application Server.

Note: You need to be logged in to the Application Server as **dncs user** to complete this procedure.

- 1 Open an xterm window on the Application Server.
- 2 Type appControl and press Enter. The Applications Control window opens.
- **3** Type 2 (for Startup/Shutdown Single Element Group) and press **Enter**. The window updates to show all the server and process groups on the Application Server.
- **4** Type 1 (for Orbix Daemon) and press **Enter**. A message appears that asks you to enter the target status for the selected group.
- 5 Type 1 (for stopped) and press **Enter**. A confirmation window appears.
- **6** Type y (for yes) and press **Enter**. The window updates to display the status of the Application Server server and process groups.
- 7 Wait until the current status (Curr Stt) of ORBIX Daemon displays stopped.
- 8 Type x and press **Enter** to return to the main menu of the Applications Control window.

Note: You might have to press **x** more than once to return to the main menu.

- **9** From the main menu of the Applications Control window, type 4 (for Define/Update Grouped Elements) and press **Enter**. The window updates to display all element groups.
- **10** Type 1 (for ORBIX Daemon) and press **Enter**. The window displays a message that prompts you to select the number associated with an installed element.
- **11** Type 1 (for /dvs/appserv/bin/orbixd) and press **Enter**. A message appears that asks you to enter the full pathname to the Orbix element.
- **12** Press **Enter** to accept the default pathname value. A message appears that asks you to enter the command line parameters used by the Orbix element.
- **13** Press **Enter** to accept the default command line parameters. A message appears that asks you to set the wait delay for the Orbix element.
- **14** Press **Enter** to accept the default wait delay value. A message appears that asks you to set the wait action for the Orbix element.
- **15** Press **Enter** to accept the default wait action value. A message appears that asks you to set the maximum restarts value for the Orbix element.
- **16** Press **Enter** to accept the default maximum restarts value. A message appears that asks you to set the value for the stop signal for the Orbix element.

Disabling the ORBIX Daemon on the Application Server

- **17** Press **Enter** to accept the default stop signal value. A message appears that asks you to set the control status for the Orbix element.
- 18 Type 2 (for disabled) and press Enter. A confirmation message appears.
- **19** Type y (for yes) and press **Enter**. The message Element definition was modified appears.
- 20 Follow the on-screen instructions to exit from the appControl utility.

C Configure FIPS Filtering

Introduction

FIPS filtering, through its integration with the DNCS, filters and sends EAS messages only to targeted states, counties, or subdivisions.

Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

In This Appendix

About FIPS Codes	156
Recommendations for FIPS Filtering	157
FIPS Code Example	158
Configure FIPS Filtering for SR 5.0 and Later	160
Configure FIPS Filtering for System Releases Prior to SR 5.0	166

About FIPS Codes

Federal Information Processing Standards (FIPS) are developed by the United States government to identify states, counties, and subdivisions.

A FIPS code for a location is formatted as follows:



First digit

Determines the subdivision.

- 0 = all subdivisions
- A number indicates the area of the county (subdivision) impacted (1 through 9)

Second and third digits

Determines the state.

Examples:

- 04 = AZ
- 10 = DE
- 27 = MN
- 38 = ND

Fourth, fifth, and sixth digits

Determines the county within the state.

Examples: DE has three county designations:

- 001 = Kent
- 003 = New Castle
- 005 = Sussex
- 000 = All counties (state-wide alert)

An EAS message header can contain as many as 31 FIPS codes.

Recommendations for FIPS Filtering

We recommend that you follow these guidelines when using FIPS codes to filter EAS messages.

- 1 Make sure all FIPS codes that apply to your network are mapped to a cluster (hub).
- **2** Make sure all FIPS codes that you might receive alerts for which are NOT applicable to your network are either:
 - a Filtered out by your EAC equipment
 - **b** Mapped to a "dummy" cluster on the ISDS
- **3** If possible, avoid having clusters that cover multiple states. If multiple states must be associated with the cluster, alerts for any state covered by the cluster will be seen.

Example: Two states border each other - state A and state B. You have one cluster that covers a part of both states. If state A issues a statewide alert, the viewers in state B who are included in the cluster will receive the alert. Likewise, if state B issues a statewide alert, those viewers in state A who are included in the cluster will also receive the alert.

4 Try to avoid using the special configuration of NO-subdivisions, which only allows statewide and countywide messages to be seen. Messages that include a subdivision are ignored.

Caution: Messages received for unmapped regions will be seen by all regions.

FIPS Code Example

The following configuration example should clarify how the system works regarding FIPS codes and how they are passed to specific areas.

Configuration example for SR 5.0 and later:

🥑 Assign FIPS Codes to (QPSK/CMTS Bri	dges (localhost80) - Mozilla	Firefox			
Elle Edit View His	tory Bookm	arks Tools Help	/fipsCode.do		▼ C ▼ Goode	<u>्</u>
DNCS Web Server	Admin Cor	nsole				
DNCS/Assign Fl	IPS Code	s to QPSK/CMTS I	Bridges			diala
Help V		Assign FIPS Codes to QPSK/CMTS Bridges				
		QPSK/CMTS Bri Note A QPSK/CN	dge: <u>testHub</u> ITS Bridge will receive a	II Emergency Alerts If then	e is no FIPS Code assi elected FIPS Code	igned.
		State: County: Subdivision:	Apache • NORTHWES'•	Add⇒ AZ-Apache	NW(104001)	-
		Force Tune Serv	rice: Testi 🔻			
Done		Save _	Cancel			

Configuration example for SR 4.3 and earlier:

Assign FIPS Codes to Clusters Cluster: CLUSTE Note: A Cluster will State: County: Subdivision:	R1 receive all Emergency Alerts i ARIZONA Apache NORTHWEST	f there is no FIPS Add Remove	icode assigned. Selected FIP AZ-Apache-NW(1040)	S Code	
Force Tune Service:	None		Cancel	Help	

The following table describes possible FIPS codes in the EAS message header and how they will be processed by the DNCS.

From the *About FIPS Codes* (on page 156) section, we know that the state code is 04 (Arizona), the county code is 001 (Apache), and the subdivision code is 1 (Northwest).

Code	Description	Passed To
004000	Statewide alert	All set-tops in bridge/cluster
004001	County-wide alert	All set-tops in bridge/cluster
104001	Subdivision alert	All set-tops in bridge/cluster
Any other alert (010000, 004002, 104002, etc.)	Other states, counties, or subdivisions	No set-tops in bridge/cluster (even if the subdivision is in the same county)

Configure FIPS Filtering for SR 5.0 and Later

FIPS filtering, through its integration with the DNCS, filters and sends EAS messages only to targeted states, counties, or subdivisions.

Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

Configuration 1: All Subdivisions are Mapped to Hubs

In this configuration, each of the nine possible subdivisions are mapped to their own specific hub. Here, each subdivision receives the following EAMs:

- Subdivision-specific EAMs
- County EAMs
- State EAMs
- National EAMs

Configuring FIPS Filtering for Configuration 1

Follow these steps to configure FIPS filtering for configuration 1 as described above.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the System Provisioning tab.
- 3 In the EAS Message section, click **FIPS Code**. The Assign FIPS Codes to QPSK/CMTS Bridges window opens.

🐳 🌳 🛪 📴 🥨 🏠 📉 http://localhost/dncs/fips/fipsCode.do						
DNCS Web Sen	er 🔪 Admin Cons	ole				
DNCS/Assign	FIPS Codes	to QPSK/CMTS Bridges		cisco		
Help ¥		Assign FIPS Codes to QPSK/CMTS Bridges				
		OPSK/CMTS Bridge: OPSK1 Note A OPSK/CMTS Bridge will receive all Emergen	ncy Alerts if there is no FIPS Code assign	ned.		
		State: ALABAMA ▼ County: Autauga ▼ Subdivision: All Subdivisio ▼	AL-Autauga-NO(001001) AL-Autauga-NW(101001) AL-Autauga-NC(201001) AL-Autauga-NE(301001) AL-Autauga-VE(401001)	*		

- 4 Select a **QPSK/CMTS Bridge** from the drop-down menu.
- 5 Select a **State** from the drop-down menu.

- 6 Select a **County** from the drop-down menu.
- 7 Select one of the following options:
 - Select a Subdivision from the drop-down list.
 - Select **All Subdivisions** from the drop-down list.
- 8 Click Add. The FIPS code moves to the Selected FIPS Code list.
- **9** Repeat this procedure from step 4 until you have assigned all the required FIPS codes to this bridge.
- 10 Are you using Force Tune for the EAM?
 - If yes, go to the next step.
 - If **no**, go to step 12.
- **11** Click the **Force Tune** arrow and select a Force Tune Service from the list. Go to step 13.

Note: The Force Tune Service you enter here overrides the default Force Tune Service defined in MMM Config on the DNCS for the messages you send through this bridge.

- **12** Click the **Force Tune** arrow and select **None** from the list. In this case, the system only uses a Force Tune Service if it is defined in the MMM Config on the DNCS.
- 13 Click Apply.

Note: The window remains open after you click **Apply**. You can modify the current bridge, or select another bridge to assign FIPS codes and/or a Force Tune Service before you click **Save**.

14 Click Save. The system saves your settings and the Assign FIPS Codes to QPSK/CMTS Bridges window closes.

Configuration 2: Some Subdivisions are Mapped to Hubs

In this configuration, only some of the nine subdivisions are assigned (mapped) to hubs. For example, some of the subdivisions might not be in your service area.

Here, since not all subdivisions are assigned to hubs, each subdivision receives the following EAMs:

- Subdivision-specific EAMs (for the mapped subdivisions)
- All EAMs targeted to the unmapped hubs
- County EAMs
- State EAMs
- National EAMs

Subdivision	Assigned To	Receives These Messages
1	Hub #1	Only EAMs targeted to subdivision 1, AND any EAM targeted to an unmapped subdivision
2	Not Assigned	Any EAM targeted to any subdivision
3	Hub #2	Only EAMs targeted to subdivision 2, AND any EAM targeted to an unmapped subdivision
4	Not Assigned	Any EAM targeted to any subdivision
5	Hub #3	Only EAMs targeted to subdivision 3, AND any EAM targeted to an unmapped subdivision
6	Not Assigned	Any EAM targeted to any subdivision
7	Not Assigned	Any EAM targeted to any subdivision
8	Not Assigned	Any EAM targeted to any subdivision
9	Not Assigned	Any EAM targeted to any subdivision

For example, consider that your FIPS subdivision mapping is set to the following:

Only subdivisions 1, 3, and 5 receive subdivision-specific EAMs; however, they also receive the EAMs targeted to any of the unmapped subdivisions.

To prevent subdivisions from receiving EAMs targeted to unmapped subdivisions, assign the unmapped subdivisions to a 'dummy' hub. This traps the EAMs and prevents them from being passed to the subdivisions that do not need to receive the EAM.

Configuring FIPS Filtering for Configuration 2

Follow these steps to configure FIPS filtering for configuration 1 as described above. Your first step is to create the dummy hubs required for the unmapped subdivisions. Then you will configure the FIPS filtering for both mapped and unmapped subdivisions.

Creating a Dummy Hub

Follow these instructions to create the dummy hub for your unmapped subdivisions.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the Network Element Provisioning tab.
- 3 Click Hub. The Hub Summary window opens.
- 4 Click Add. A new line appears at the top of the .

- 5 Use the following list to set up the initial parameters for your dummy hub.
 - Hub Name The name you will use to identify this hub. You can use up to 15 alphanumeric characters.

Important: Be sure to use a name that will immediately identify the hub as a dummy hub for unmapped FIPS subdivisions.

• **Hub ID** - The number you will use to identify this hub.

Important:

- Be sure to use an ID number that will immediately identify the hub as a dummy hub for unmapped FIPS subdivisions.
- You will not be able to modify this field later.
- Headend Select the headend associated with this hub.
- **Time Zone -** Select the time zone where this hub is located.
- **DST Zone** Select the zone ID for this hub.
- 6 Click **Save**. The system saves the hub information in the DNCS database and the Hub Summary window updates to include the new hub.
- 7 Add the new hub to your network map.

Configuring FIPS Filtering with a Dummy Hub for Unmapped Subdivisions

Follow these steps to configure FIPS filtering using a dummy hub for your unmapped subdivisions.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the **System Provisioning** tab.
- 3 In the EAS Message section, click **FIPS Code**. The Assign FIPS Codes to QPSK/CMTS Bridges window opens.
- 4 Configure your mapped subdivisions by following these instructions.
 - a Select the QPSK/CMTS Bridge from the list.
 - **b** Select the **State** from the list.
 - c Select the **County** from the list.
 - d Select all of the **Subdivisions** that you want to map to this hub.
 - e Click Add.
 - **f** Click the **Force Tune** arrow and select a Force Tune Service from the list. **Notes:**
 - The Force Tune Service you enter here overrides the default Force Tune Service defined in MMM Config on the DNCS for the messages you send through this hub.
 - If you select **None** in the Force Tune Service field, the system uses the default Force Tune Service (if defined in MMM Config on the DNCS).
 - g Click Apply.

- **h** Repeat these steps until you have assigned all the mapped subdivisions to a hub.
- 5 Configure your unmapped subdivisions by following these instructions.
 - **a** Select the dummy hub **QPSK/CMTS Bridge** that you created in the previous procedure.
 - **b** Select the **State** from the list.
 - c Select the **County** from the list.
 - d Select all of the unmapped **Subdivisions** that you want to map to this hub.
 - e Click Add.
 - f Click the Force Tune arrow and select None.
 - g Click Apply.
- 6 Click **Save**. The system saves your settings and the Assign FIPS Codes to QPSK/CMTS Bridges window closes.

Configuration 3: No Subdivisions are Mapped to Hubs

In this configuration, the system is not required to pass alerts for subdivisions. Here, since no subdivisions are mapped to hubs, each subdivision receives the following EAMs:

- County EAMs
- State EAMs
- National EAMs

Configuring FIPS Filtering for Configuration 3

Follow these steps to configure FIPS filtering for systems that do not need to use subdivisions.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the **System Provisioning** tab.
- 3 In the EAS Message section, click **FIPS Code**. The Assign FIPS Codes to QPSK/CMTS Bridges window opens.
- 4 Select the **QPSK/CMTS Bridge** from the list.
- 5 Select the **State** from the list.
- 6 Select the **County** from the list.
- 7 Select either the Subdivisions or No Subdivision.
- 8 Click Add.

- 9 Click the **Force Tune** arrow and select a Force Tune Service from the list. **Notes:**
 - The Force Tune Service you enter here overrides the default Force Tune Service defined in MMM Config on the DNCS for the messages you send through this bridge.
 - If you select None in the Force Tune Service field, the system uses the default Force Tune Service (if defined in MMM Config on the DNCS).
- 10 Click Apply.

Note: The window remains open after you click **Apply**. You can modify the current bridge, or select another bridge to assign FIPS codes and/or a Force Tune Service before you click **Save**.

11 Click **Save**. The system saves your settings and the Assign FIPS Codes to QPSK/CMTS Bridges window closes.

Configure FIPS Filtering for System Releases Prior to SR 5.0

FIPS filtering, through its integration with the DNCS, filters and sends EAS messages only to targeted states, counties, or subdivisions.

Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

Configuration 1: All Subdivisions are Mapped to Hubs

In this configuration, each of the nine possible subdivisions are mapped to their own specific hub. Here, each subdivision receives the following EAMs:

- Subdivision-specific EAMs
- County EAMs
- State EAMs
- National EAMs

Configuring FIPS Filtering for Configuration 1

Follow these steps to configure FIPS filtering for configuration 1 as described above.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the System Provisioning tab.
- 3 In the EAS Message section, click **FIPS Code**. The Assign FIPS Codes to QPSK/CMTS Bridges window opens.

QPSK/CMTS Bridge:	DudleyMod1HE				
Note: A QPSK/CMT	S Bridge will receive	all Emerger	ncy Alerts if the	ere is no FIPScode assigned.	
				Selected FIPS	Code
State:	ALABAMA			AL-Autauga-NO(0010))1)
County:	Autauga		Add		
Subdivision:	All Subdivisions		Remove		
iorca Tuna Saruica	None				
orce rune service.	Intoine				

- 4 Select the QPSK/CMTS Bridge from the list.
- 5 Select the **State** arrow from the list.

- 6 Select the **County** from the list.
- 7 Select either the Subdivisions or select All Subdivisions.
- 8 Click Add.
- **9** Repeat this procedure from step 4 until you have assigned all the required FIPS codes to this bridge.
- 10 Are you using Force Tune for the EAM?
 - If yes, go to the next step.
 - If **no**, go to step 12.
- **11** Click the **Force Tune** arrow and select a Force Tune Service from the list. Go to step 13.

Note: The Force Tune Service you enter here overrides the default Force Tune Service defined in MMM Config on the DNCS for the messages you send through this bridge.

- **12** Click the **Force Tune** arrow and select **None** from the list. In this case, the system only uses a Force Tune Service if it is defined in the MMM Config on the DNCS.
- 13 Click Apply.

Note: The window remains open after you click **Apply**. You can modify the current bridge, or select another bridge to assign FIPS codes and/or a Force Tune Service before you click **Save**.

14 Click Save. The system saves your settings and the Assign FIPS Codes to QPSK/CMTS Bridges window closes.

Configuration 2: Some Subdivisions are Mapped to Hubs

In this configuration, only some of the nine subdivisions are assigned (mapped) to hubs. For example, some of the subdivisions might not be in your service area.

Here, since not all subdivisions are assigned to hubs, each subdivision receives the following EAMs:

- Subdivision-specific EAMs (for the mapped subdivisions)
- All EAMs targeted to the unmapped hubs
- County EAMs
- State EAMs
- National EAMs

Subdivision	Assigned To	Receives These Messages
1	Hub #1	Only EAMs targeted to subdivision 1, AND any EAM targeted to an unmapped subdivision
2	Not Assigned	Any EAM targeted to any subdivision
3	Hub #2	Only EAMs targeted to subdivision 2, AND any EAM targeted to an unmapped subdivision
4	Not Assigned	Any EAM targeted to any subdivision
5	Hub #3	Only EAMs targeted to subdivision 3, AND any EAM targeted to an unmapped subdivision
6	Not Assigned	Any EAM targeted to any subdivision
7	Not Assigned	Any EAM targeted to any subdivision
8	Not Assigned	Any EAM targeted to any subdivision
9	Not Assigned	Any EAM targeted to any subdivision

For example, consider that your FIPS subdivision mapping is set to the following:

Only subdivisions 1, 3, and 5 receive subdivision-specific EAMs; however, they also receive the EAMs targeted to any of the unmapped subdivisions.

To prevent subdivisions from receiving EAMs targeted to unmapped subdivisions, assign the unmapped subdivisions to a 'dummy' hub. This traps the EAMs and prevents them from being passed to the subdivisions that do not need to receive the EAM.

Configuring FIPS Filtering for Configuration 2

Follow these steps to configure FIPS filtering for configuration 1 as described above. Your first step is to create the dummy hubs required for the unmapped subdivisions. Then you will configure the FIPS filtering for both mapped and unmapped subdivisions.

Creating a Dummy Hub

Follow these instructions to create the dummy hub for your unmapped subdivisions.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the Network Element Provisioning tab.
- 3 Click Hub. The Hub List window opens.
- 4 Click **File > New**. The Set Up Hub window opens.

- 5 Use the following list to set up the initial parameters for your dummy hub.
 - Headend Name Select the headend associated with this hub.
 - **Hub Name** The name you will use to identify this hub. You can use up to 15 alphanumeric characters.

Important: Be sure to use a name that will immediately identify the hub as a dummy hub for unmapped FIPS subdivisions.

• Hub ID - The number you will use to identify this hub.

Important:

- Be sure to use an ID number that will immediately identify the hub as a dummy hub for unmapped FIPS subdivisions.
- You will not be able to modify this field later.
- **Timezone -** The time zone where this hub is located.
- **DST Zone ID** The zone ID for this hub.
- 6 Click **Save**. The system saves the hub information in the DNCS database and the Hub List window updates to include the new hub.
- 7 Add the new hub to your network map.

Configuring FIPS Filtering with a Dummy Hub for Unmapped Subdivisions

Follow these steps to configure FIPS filtering using a dummy hub for your unmapped subdivisions.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the **System Provisioning** tab.
- 3 In the EAS Message section, click **FIPS Code**. The Assign FIPS Codes to QPSK/CMTS Bridges window opens.
- 4 Configure your mapped subdivisions by following these instructions.
 - a Select the QPSK/CMTS Bridge from the list.
 - **b** Select the **State** from the list.
 - c Select the **County** from the list.
 - d Select all of the **Subdivisions** that you want to map to this hub.
 - e Click Add.
 - **f** Click the **Force Tune** arrow and select a Force Tune Service from the list. **Notes:**
 - The Force Tune Service you enter here overrides the default Force Tune Service defined in MMM Config on the DNCS for the messages you send through this hub.
 - If you select **None** in the Force Tune Service field, the system uses the default Force Tune Service (if defined in MMM Config on the DNCS).
 - g Click Apply.

- **h** Repeat these steps until you have assigned all the mapped subdivisions to a hub.
- 5 Configure your unmapped subdivisions by following these instructions.
 - **a** Select the dummy hub **QPSK/CMTS Bridge** that you created in the previous procedure.
 - **b** Select the **State** from the list.
 - c Select the **County** from the list.
 - d Select all of the unmapped **Subdivisions** that you want to map to this hub.
 - e Click Add.
 - f Click the Force Tune arrow and select None.
 - g Click Apply.
- 6 Click **Save**. The system saves your settings and the Assign FIPS Codes to QPSK/CMTS Bridges window closes.

Configuration 3: No Subdivisions are Mapped to Hubs

In this configuration, the system is not required to pass alerts for subdivisions. Here, since no subdivisions are mapped to hubs, each subdivision receives the following EAMs:

- County EAMs
- State EAMs
- National EAMs

Configuring FIPS Filtering for Configuration 3

Follow these steps to configure FIPS filtering for systems that do not need to use subdivisions.

- 1 On the DNCS Administrative Console, click the DNCS tab.
- 2 Click the **System Provisioning** tab.
- 3 In the EAS Message section, click **FIPS Code**. The Assign FIPS Codes to QPSK/CMTS Bridges window opens.
- 4 Select the **QPSK/CMTS Bridge** from the list.
- 5 Select the **State** from the list.
- 6 Select the **County** from the list.
- 7 Select No Subdivision.
- 8 Click Add.
- 9 Click the **Force Tune** arrow and select a Force Tune Service from the list. **Notes:**
 - The Force Tune Service you enter here overrides the default Force Tune Service defined in MMM Config on the DNCS for the messages you send through this bridge.
 - If you select None in the Force Tune Service field, the system uses the default Force Tune Service (if defined in MMM Config on the DNCS).
- 10 Click Apply.

Note: The window remains open after you click **Apply**. You can modify the current bridge, or select another bridge to assign FIPS codes and/or a Force Tune Service before you click **Save**.

11 Click **Save**. The system saves your settings and the Assign FIPS Codes to QPSK/CMTS Bridges window closes.

Index

A

alert type configuring • 93 described • 90 ATM address of DNCS, determining • 23

В

BFS server in EAS Process • 2 server error • 138 troubleshooting for EAS • 127, 138

С

CableCARD and EAS • 46, 94 configuring for EAS • 46, 94 errors • 46 troubleshooting EAS with • 131

D

debugging increasing on MMM server • 130 DHCT ensure DHCTs receive EAS messages • 4 in EAS Process • 2 troubleshooting for EAS • 141 verifying configuration for EAS • 141 verifying EAS performance • 141 digital channels, suppressing EAS on • 53, 100 Digital Envoy • 13 scope of information • 8 troubleshooting • 123, 125 verifying configuration • 13 verifying performance • 14 Digital Network Control System • See DNCS display type configuring • 45, 93 described • 90

DNCS • 19 configure EAS for use with CableCARD • 46, 94 configure EAS on • 88 configure for EAS messages • 30 determine ATM address of • 23 GUI disappears • 138 troubleshoot configuration and performance • 129 troubleshoot Ethernet hub • 127 troubleshooting MMM on • 136 verify for EAS messages • 18 verify hosts file configuration • 21 verify hub connection • 19

Ε

EAC • 8 in EAS process • 2 troubleshooting • 122 EAMs • 8 EARServer in EAS process • 2 troubleshooting • 130 verifying configuration • 22 verifying performance • 22 EAS • 8 and CableCARDs • 46 configure EAS messages • 18, 88 configure messages • 43, 91 EAS process • 2 performance, improving • 70 performance, troubleshooting • 129 suppression • 53, 100 testing • 63 troubleshooting • 122 EAS events • 39 configuring • 39, 88

Index

EAS messages configuring • 43, 91 how they get from FCC to set-top • 2 sending • 64, 110 terminating • 67, 113 EAS tests conduct • 63 conduct RWT and RMT • 71 configure • 55, 59, 102, 106 configure monthly tests • 59, 106 configure weekly tests • 55, 102 send test messages • 64, 110 teminate EAS messages • 67, 113 Emergency Alert Controller • See EAC Emergency Alert System • See EAS error messages • 130 Error registering with BFS • 138 MMMServer failure • 130 Send Message failed • 130 Ethernet hub connecting • 19 troubleshooting • 127 event codes • See EAS events events • See EAS events export/home/easftp directory verifying • 23

F

FCC in EAS process • 2 FIPS filtering described • 40 force tune type configuring • 44, 91 described • 90 Frontline System • 15 scope of information • 8 troubleshooting • 123, 126 verifying configuration and performance • 16

Η

HollyAnne Corporation • See Digital Envoy hosts file configuring • 21 testing configuration • 22 hosts.equiv file configuring • 21 testing configuration • 22 hub connection configuring • 19

L

 $LOCAL_EAS_IP \bullet 20$

Μ

MegaHertz • 9 scope of information • 8 troubleshooting • 123, 124 verifying configuration • 9 verifying performance • 10 message time configuring • 45, 92 described • 90 messages • 4. See error messages MMM Server configuration • 31, 75 error when registering with BFS • 138 in EAS process • 2 increase debugging on • 135 increasing out-of-band data rate • 49, 97 performance • 70 restarting • 137 stopping • 136 troubleshooting • 136 verifying configuration • 33, 76 verifying performance • 70 Monroe System • See Digital Envoy

Ν

Naming Service verifying • 87

0

OCAP • See tru2way ORBIX daemon process disabling on Application Server • 152 hosts file configuration • 132 restarting • 134 stopping • 133 out-of-band data rate, increasing • 49, 97

Ρ

PassThru

in EAS process • 2

Q

QPSK troubleshooting • 128

R

resident app servers troubleshooting • 129 RMT conducting • 71 configuring • 59, 106 setting up • 59, 106 terminating • 67, 113 troubleshooting • 140 What You Need • 55 RWT conducting • 71 configuring • 55, 102 setting up • 55, 102 terminating • 67, 113 troubleshooting • 140 What You Need • 55

S

server error when registering with BFS • 138 suppression, of EAS on digital channels • 53, 100

Т

test EAS • 63 hosts file configuration • 22 hosts.equiv file configuration • 22 Trilithic • 11 troubleshooting • 123, 124 verifying configuration • 11 verifying performance • 12 troubleshooting BFS server • 127 CableCARD EAS errors • 46 Digital Envoy system • 124 DNCS GUI disappears • 138 DNCS MMM • 129 EAC controller • 122 EARServer • 130 EAS performance • 124 EAS with CableCARDs • 131 error messages • 130 Ethernet hub • 127 Frontline system • 126 MegaHertz system • 124 MMM Server • 136, 138 Naming Service • 87 Orbix.hosts file configuration • 132 **QPSK** • 128 resident app servers • 129 RMT • 140 **RWT** • 140 server error when registering with BFS • 138 set-top EAS configuration and performance • 141 Trilithic system • 124 tru2way • v

יו|ייו|יי כוsco

Cisco Systems, Inc. 678 277-1120 5030 Sugarloaf Parkway, Box 465447 800 722-2009 Lawrenceville, GA 30042 www.cisco.com This document includes various trademarks of Cisco and/or its affiliates. Please see the Notices section of this document for a list of the Cisco trademarks used in this document. Product and service availability are subject to change without notice. © 2003-2004, 2006-2008, 2012 Cisco and/or its affiliates. All rights reserved. Part Number 4004455 Rev G March 2012 Printed in USA