Configuring and Troubleshooting the Digital Emergency Alert System

For ISDS Networks

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 Acknowledgements

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

CableCARD is a trademark of Cable Television Labroratories, 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. (1110R)

Publication Disclaimer

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

Copyright

Contents

About This Guide

Introduction

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 IP Service Delivery System (ISDS) and the IPTV Services Delivery Platform (ISDP).

Purpose

After reading this guide, you will be able to configure, operate, maintain, and test EAS components on the ISDS and the RNCS. 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

You have the option of configuring your EAS as one of the following:

- A centralized configuration, where the central ISDS sends the EAMs to all the subscribers' set-tops.
- A distributed configuration, where the central ISDS and each Regional Network Control Server (RNCS) delivers the EAMs to the subscribers' set-tops.

Software Requirements

This document is valid for the ISDS 2.3 and later software releases.

Audience

This document was written for headend technicians. Field service engineers and Cisco Services engineers may also find the information in this document helpful.

Related Publications

You may find the following publications useful as resources when you implement the procedures in this document.

- *ISDP System Overview with Focus on the ISDP Server and ISDP Client* (part number 4017607)
- *Maintenance Recommendations for the ISDS System User Guide* (part number 4021188)
- *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377)

Document Version

This is the second release of this document.

1

Overview

Introduction

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

In This Chapter

Emergency Alert System Process

You must configure the ISDS correctly to receive and distribute EAMs. The configuration you use depends on the type of network you use:

- ***Configuration Process for a Centralized EAS Network*** (on page 2)
- ***Configuration Process for a Distributed EAS Network*** (on page 3)

Configuration Process for a Centralized EAS Network

The process for configuring the centralized EAS network (a network that does **not** use the RCS) is as follows:

1. Verify your third-party equipment configuration. See ***Verify Your EAS Equipment Configuration*** (on page 5).
2. Connect the EAC to your ISDS and/or network. See ***Configure the Network Connection*** (on page 17).
3. Make sure the correct environment variable is set up in the .profile file. See ***Verify and Configure the LOCAL_EAS_IP Environment Variable*** (on page 18).
4. Verify your EARS configuration. See ***Verifying EARS Configuration and Performance*** (on page 19).
5. Verify that the easftp directory exists on the ISDS. See ***Verifying the /export/home/easftp Directory*** (on page 19).
6. Determine the IP address of the ISDS. See ***Determining the Set-Top Facing IP Address of the ISDS*** (on page 20).
7. Verify that the VASP contains the MMM Server entry. See ***Configuring and Verifying the MMM Server Entry in the VASP List*** (on page 20).
8. Configure EAS messages, events, and tests. See ***Configure EAS Events, Messages, and Tests*** (on page 39).
9. Conduct in-house EAS tests. See ***Test the EAS from the ISDS*** (on page 54).

Configuration Process for a Distributed EAS Network

The process for configuring the distributed EAS network (a network that does use the RCS) is as follows:

1. Configure the central site.
2. Configure the remote site.

Process for the Central Site

1. Verify your third-party equipment configuration. See ***Verify Your EAS Equipment Configuration*** (on page 5).
2. Connect the EAC to your ISDS and/or network. See ***Configure the Network Connection*** (on page 17).
3. Make sure the correct environment variable is set up in the .profile file. See ***Verify and Configure the LOCAL_EAS_IP Environment Variable*** (on page 27).
4. Verify your EARS configuration. See ***Verifying EARS Configuration and Performance*** (on page 28).
5. Verify that the easftp directory exists on the ISDS. See ***Verifying the /export/home/easftp Directory*** (on page 28).
6. Determine the IP address of the ISDS. See ***Determining the Set-Top Facing IP Address of the ISDS*** (on page 28).
7. Verify that the VASP contains the MMM Server entry. See ***Configuring and Verifying the MMM Server Entry in the VASP List*** (on page 29).
8. Configure EAS messages, events, and tests. See ***Configure EAS Events, Messages, and Tests*** (on page 39).
9. Conduct in-house EAS tests. See ***Conduct EAS Tests*** (on page 53).

Process for the Remote Site

1. Verify your third-party equipment configuration. See ***Verify Your EAS Equipment Configuration*** (on page 5).
2. Connect the EAC to your ISDS and/or network. See ***Configure the Network Connection*** (on page 17).
3. Make sure the correct environment variable is set up in the .profile file. See ***Verify and Configure the LOCAL_EAS_IP Environment Variable*** (on page 33).
4. Verify that earsRemote is configured correctly. See ***Verifying earsRemote Configuration and Performance*** (on page 34).
5. Verify that the easftp directory exists on the ISDS. See ***Verifying the /export/home/easftp Directory*** (on page 35)
6. Determine the IP address of the remote ISDS. See ***Determining the IP Address of the Remote ISDS*** (on page 35).
7. Verify that the VASP contains the mmmRemote entry. See ***Verifying and Configuring the mmmRemote Server Entry in the VASP List*** (on page 36).

8. Configure EAS messages, events, and tests. See ***Configure EAS Events, Messages, and Tests*** (on page 39).
9. Conduct in-house EAS tests. See ***Conduct EAS Tests*** (on page 53).
10. Configure FIPS filtering (if applicable). See ***Configure FIPS Filtering (Optional)*** (on page 44)

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 ISDS. The following companies manufacture EAC solutions that are known to work with the ISDS:

- 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

Before you can configure the EAS on the ISDS, you must verify that your third-party EAS equipment is configured and performing correctly. This section provides parameters that allow the EAC to communicate with the ISDS. This section 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.

These instructions are valid for all network types and locations (non-RCS networks, central RCS sites, and remote RCS sites).

Note: In an RCS network, you need to verify your EAS equipment configuration at the central site **and** at each remote site.

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.

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

- ***Troubleshooting the MegaHertz System*** (on page 65)
- ***Troubleshooting MegaHertz System Performance*** (on page 66)

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 ISDS
TCP/IP Port	21
FTP Port	4098
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 ISDS. 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 ISDS*** (on page 54) 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.

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

- ***Troubleshooting the Trilithic System*** (on page 65)
- ***Troubleshooting Trilithic System Performance*** (on page 66)

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 ISDS
FTP Username	easftp
FTP Password	easftp
FTP Port	21
TCP/IP Port	4098
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 ISDS
Subnet Mask	Correct value for your installation
Default Gateway	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.

Verifying Trilithic EAC Performance

The EAC uses FTP to transfer WAV and TXT files to the ISDS. 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.

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 65)
- ***Troubleshooting Monroe System with Digital Envoy Performance*** (on page 67)

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)	21
FTP Server IP	IP address of the ISDS
FTP Username	easftp
FTP Password	easftp
FTP Port	4098
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 ISDS. 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 ISDS*** (on page 54) 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.

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

- ***Troubleshooting the Frontline System*** (on page 65)
- ***Troubleshooting Frontline System Performance*** (on page 68)

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 ISDS
TCP/IP Port	21
FTP 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 ISDS*** (on page 54) if necessary.

3

Configure the Centralized EAS

Introduction

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

In This Chapter

Overview

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

Important: This section provides configuration instructions for a centralized EAS. If you have a distributed EAS system, see ***Configure the Distributed EAS*** (on page 25).

If your system does not function as expected, refer to ***Troubleshooting*** (on page 63) for troubleshooting procedures for the 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

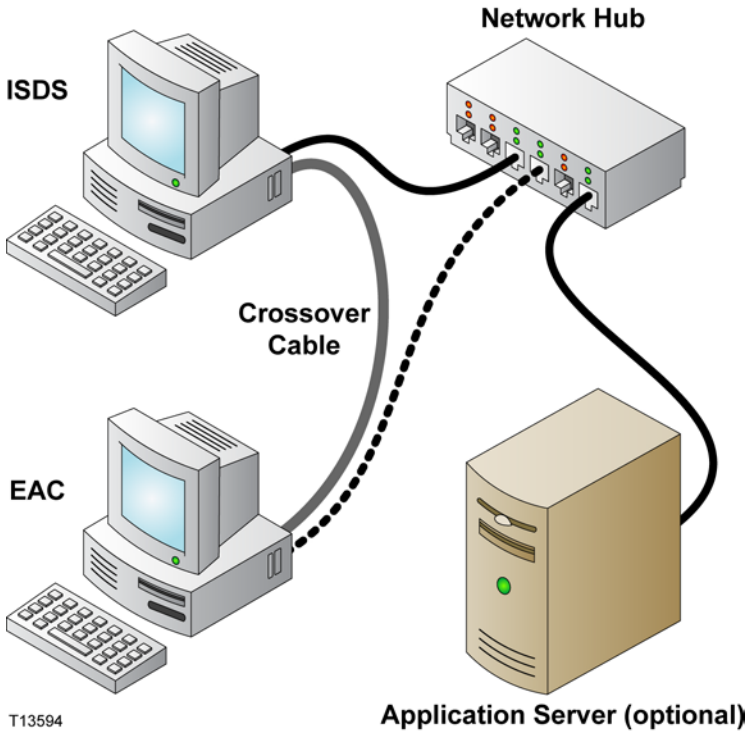
Connect a crossover Ethernet cable from the EAC to the ISDS. Alternately, you can connect a standard Ethernet cable from the EAC to the network hub.

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 ISDS for EAS Messages

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

1. Verifying and configuring (if necessary) the LOCAL_EAS_IP variable in the .profile file.
2. Configuring the EARServer.
3. Verifying the presence of the /export/home/easftp directory.
4. Determining the IP address of the ISDS.
5. Verifying and configuring (if necessary) the MMM Server configuration.

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 ISDS.
2. Type **env | grep -i local** and press **Enter**. The system displays the value of environmental variables that contain the word local.
3. Do the results show that the LOCAL_EAS_IP variable has been set to the IP address of the ISDS 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 ISDS. Check your network map or with your system administrator for the public IP address of the ISDS.
2. Open an xterm window on the ISDS.
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=[public IP address of the ISDS]

   Note: Do not include the brackets **[ ]** in the IP address.
5. Save the file and close the editor.
6. Type **. ./.profile** so the ISDS uses the updated .profile file.
7. Stop and restart (bounce) the EARs process on the ISDS.or the public IP address of the ISDS.

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 ISDS.
2. Type **cd /dvs/dncs/tmp** and press **Enter**. The /dvs/dncs/tmp directory becomes the working directory.
3. Type **ls –l 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 ISDS.

1. Open an xterm window on the ISDS.
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 ISDS

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

1. Log on to the ISDS as dncs user.
2. Open an xterm window on the ISDS.
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 ISDS 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:

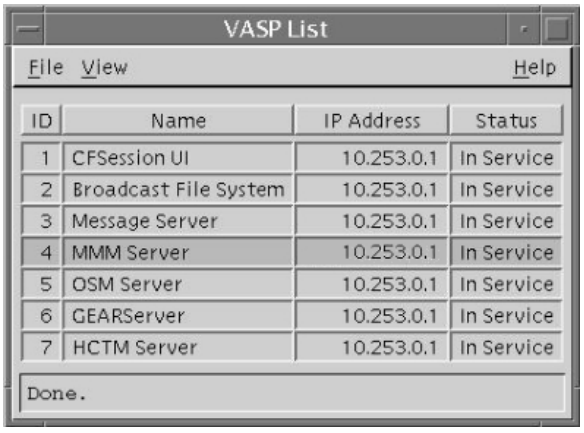
   _____
6. Type **exit** and press **Enter** to close the xterm window.

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

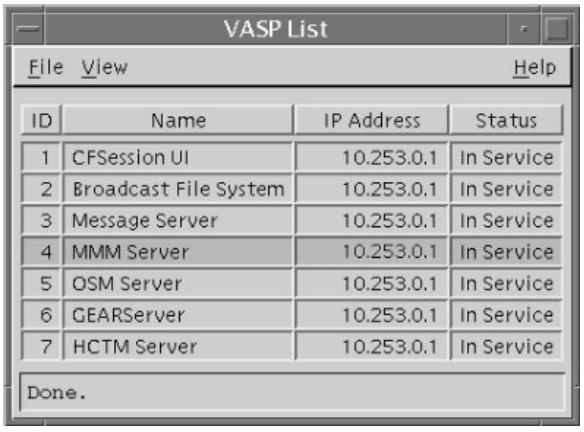
1. From the Administrative Console, click the **Network Element Provisioning** tab.
2. Click **VASP**. The VASP List window opens.



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 21)
   - If **no**, go to ***Configuring the MMM Server Entry in the VASP List*** (on page 22)

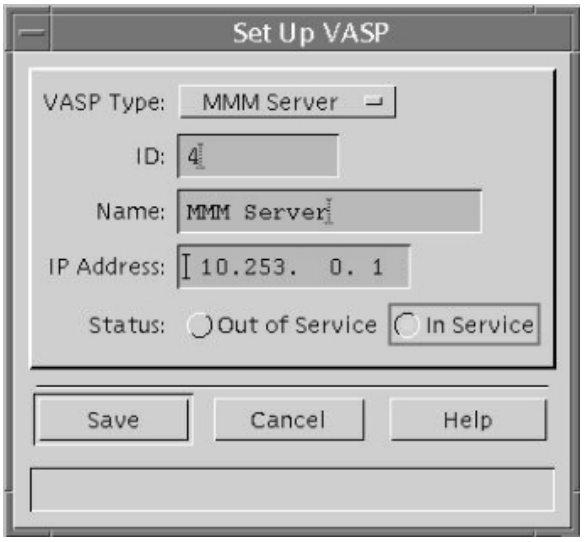
Verifying the MMM Server Entry in the VASP List

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



2 Click the row containing **MMM Server**.

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 ISDS*** (on page 20)?
- Is **Status** set to **In Service**?

5 Did you answer **yes** to every question in step 6?

- 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 22) and fix the incorrect entry.

6 Go to ***Configuring the EAS on the ISDS*** (on page 40).

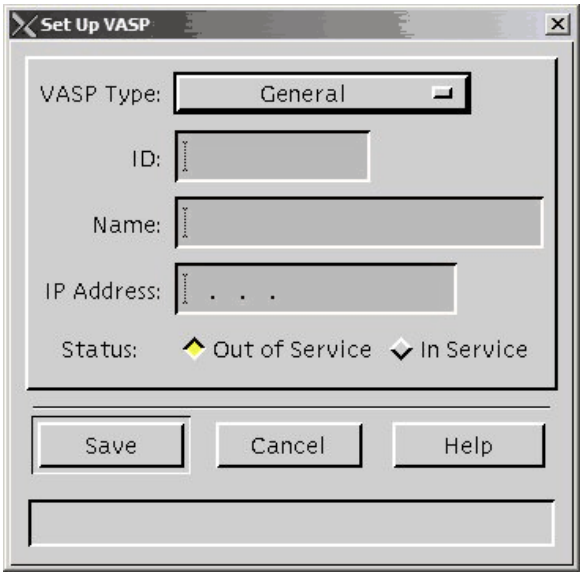
Configuring the MMM Server Entry in the VASP List

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: _____

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



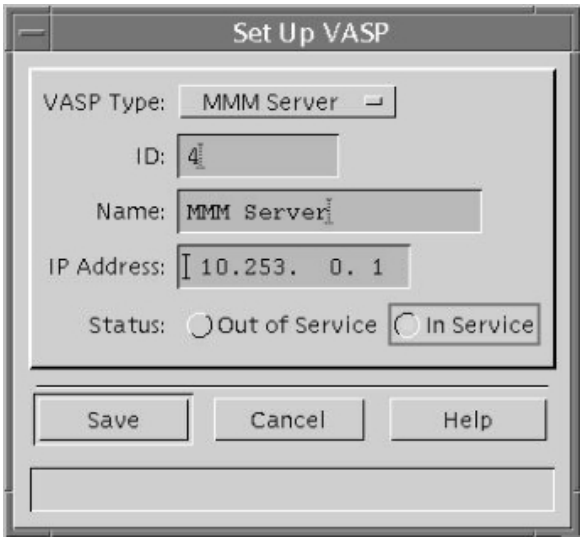
3 In the **VASP Type** field, select **MMM Server** from the list.

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 ISDS that you recorded in ***Determining the Set-Top Facing IP Address of the ISDS*** (on page 20).

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



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**.

10 Go to ***Configuring the EAS on the ISDS*** (on page 40).

4

Configure the Distributed EAS

Introduction

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

In This Chapter

Overview

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

Important: This section provides configuration instructions for a distributed EAS. If you have a centralized EAS system, see ***Configure the Centralized EAS*** (on page 15).

If your system does not function as expected, refer to ***Troubleshooting*** (on page 63) for troubleshooting procedures for the EAS.

Configure the Central RCS Site for EAS

Configure the ISDS for EAS Messages

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

1. Verifying and configuring (if necessary) the LOCAL_EAS_IP variable in the .profile file.
2. Configuring the EARServer.
3. Verifying the presence of the /export/home/easftp directory.
4. Determining the IP address of the ISDS.
5. Verifying and configuring (if necessary) the MMM Server configuration.

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 ISDS.
2. Type **env | grep -i local** and press **Enter**. The system displays the value of environmental variables that contain the word local.
3. Do the results show that the LOCAL_EAS_IP variable has been set to the IP address of the ISDS 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

Before you begin, you need the public IP address of the ISDS. Check your network map or with your system administrator for the public IP address of the ISDS.

1. Open an xterm window on the ISDS.
2. Type **cd /export/home/dncs** and press **Enter**. The /export/home/dncs directory becomes the working directory.
3. Edit the **.profile** file to append the following line to the file:

   export LOCAL_EAS_IP=[public IP address of the ISDS]

   Note: Do not include the brackets **[ ]** in the IP address.
4. Save the file and close the editor.
5. Type **. ./.profile** so the ISDS uses the updated .profile file.
6. Stop and restart (bounce) the EARs process on the ISDS.

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 ISDS.
2. Type **cd /dvs/dncs/tmp** and press **Enter**. The /dvs/dncs/tmp directory becomes the working directory.
3. Type **ls –l 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 ISDS.

1. Open an xterm window on the ISDS.
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 ISDS

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

1. Log on to the ISDS as dncs user.
2. Open an xterm window on the ISDS.
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 ISDS 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.

7 Go to ***Configuring and Verifying the MMM Server Entry in the VASP List*** (on page 29)

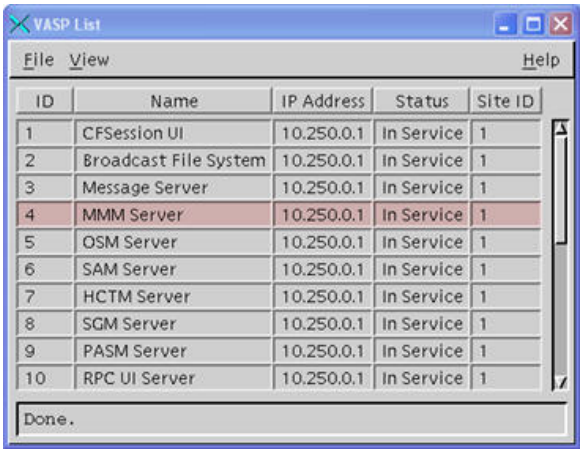
Configuring and Verifying the MMM Server Entry in the VASP List

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 Administrative Console, click the **Network Element Provisioning** tab.

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

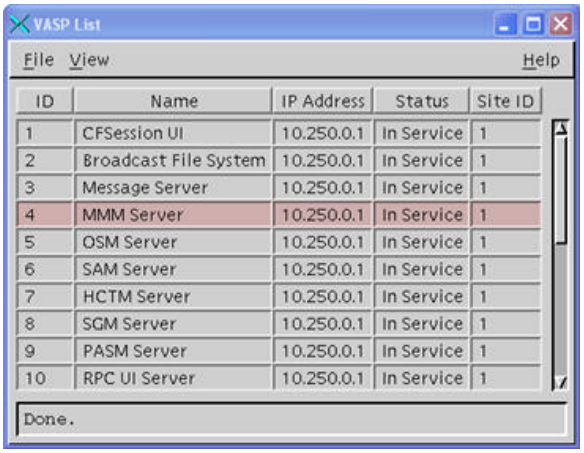


3 Is there an MMM Server entry in the VASP List?

- If **yes**, go to ***Verifying the MMM Server Entry in the VASP List*** (on page 30)
- If **no**, go to ***Configuring the MMM Server Entry in the VASP List*** (on page 31)

Verifying the MMM Server Entry in the VASP List

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



2 Click the row containing **MMM Server**.

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 ISDS*** (on page 28)?
- 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 31) and fix the incorrect entry.

6 Go to ***Configure the Remote RCS Site for EAS*** (on page 33).

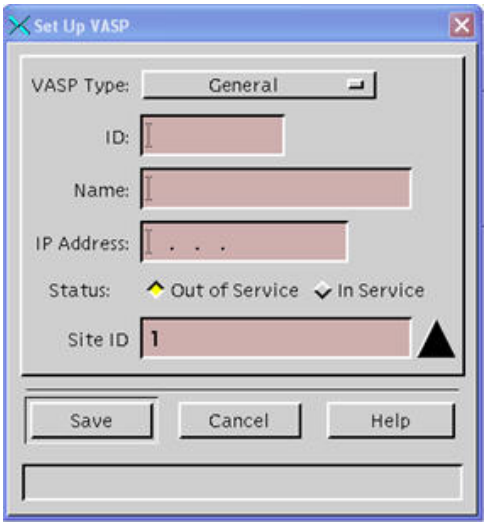
Configuring the MMM Server Entry in the VASP List

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: _____

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



3 In the **VASP Type** field, select **MMM Server** from the list.

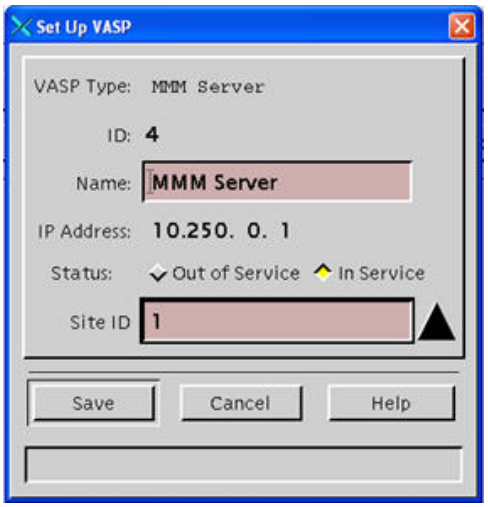
4 In the **ID** field, type the unused ID you recorded in step 1.

5 In the **Name** field, type **MMM Server**.

6 In the **IP Address** field, type the IP address of the ISDS that you recorded in *Determining the Set-Top Facing IP Address of the ISDS* (on page 20).

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

8 In the **Site ID** field, select a site.



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 On the VASP List window, click **File > Close**.

11 Go to ***Configure the Remote RCS Site for EAS*** (on page 33).

Configure the Remote RCS Site for EAS

Configure the Remote Site for EAS Messages

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

1. Verifying and configuring (if necessary) the LOCAL_EAS_IP variable in the .profile file.
2. Configuring the earsRemote configuration.
3. Verifying the presence of the /export/home/easftp directory.
4. Determining the IP address of the remote site.
5. Verifying and configuring (if necessary) the mmmRemote entry in the VASP list.

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 ISDS.
2. Type **siteCmd [name of remote site] env | grep -i local** and press **Enter**. The system displays the value of environmental variables on the remote site that contain the word **local**.
3. Do the results show that the LOCAL_EAS_IP variable has been set to the IP address of the remote ISDS 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

Before you begin, you need the public IP address of the ISDS. Check your network map or with your system administrator for the public IP address of the ISDS.

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root.
3. Type **ssh [IP address of remote site]** and press **Enter**.

   Note: Do not type the brackets **[ ]** in the command.

   Result: The SSH connection opens between the ISDS and the remote site.
4. Type the remote site **password** and press **Enter**.
5. Once you are logged into the remote site, type **cd /export/home/dncs** and press **Enter**. The /export/home/dncs directory becomes the working directory.

6 Edit the .profile file to append the following line to the file:

export LOCAL_EAS_IP=[public IP address of the RNCS]

Note: Do not include the brackets **[ ]** in the IP address.

7 Save the file and close the editor.

8 Type **. ./.profile** and press **Enter** so the ISDS uses the updated .profile file.

9 In the xterm window on the ISDS, log in as the dncs user.

10 Type **siteControl [IP addresss or name of the remote site]** and press **Enter**. This opens the lionnControl window.

Note: Do not type the brackets **[ ]** in the command.

11 Type **2** (Start/Shut Down Single Element) and press **Enter**.

12 Type **6** (MMM/EAS Remote) and press **Enter**.

13 Type **E** (Display Element Entries) and press **Enter**.

14 Type **2** (earsRemote) and press **Enter**.

15 Type **1** (Stop) and press **Enter**.

16 After a few moments, type **2** (Start) and press **Enter**.

Verifying earsRemote Configuration and Performance

The earsRemote process continuously monitors the system for messages that are sent by means of FTP from the EAC. The earsRemote process receives the WAV and the TXT files and logs the messages to an EARS file located in the /dvs/lionn/tmp/earsRemote directory on the RNCS.

Follow these steps to verify the configuration and performance of the earsRemote process.

1 Open an xterm window on the ISDS.

2 Type **siteCmd [name of remote site] ls -l /dvs/lionn/tmp** and press **Enter**. The contents of the remote site /dvs/lionn/tmp directory appear.

Note: Do not type the brackets **[ ]** in the command.

3 Type **siteCmd [name of remote site] ls -l /dvs/lionn/tmp/earsRemote.*** and press **Enter**. The earsRemote files display.

Important: If the earsRemote file does not exist, contact Cisco Services.

4 To view the details of an individual earsRemote file, type **siteCmd [name of remote site] view /dvs/lionn/tmp/earsRemote.[xxx]** and press **Enter**.

Note: In this command, **[xxx]** represents the extension of the earsRemote 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 RNCS.

1 Open an xterm window on the ISDS.

2 Type **siteCmd [name of remote site] ls -l /export/home/easftp** and press **Enter.** The /export/home/easftp directory becomes the working directory.

Note: Do not type the brackets **[ ]** in the command.

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 **siteCmd [name of remote site] mkdir /export/home/easftp** and press **Enter** to create the directory.

5 Type **siteCmd [name of remote site] chown easftp dncs /export/home/easftp** and press **Enter** to set the ownership of the directory.

Determining the IP Address of the Remote ISDS

Follow these instructions to determine and record the IP address of the remote ISDS.

1 Log on to the ISDS as dncs user.

2 Open an xterm window on the ISDS.

3 Type **siteCmd [name of remote site] more /etc/hosts** and press **Enter**.

Note: Do not type the brackets [ ] in the command.

Result: A message similar to the following appears:

```
Working directory is /dvs/lionn
Database is lionndb
Site ID=2 IPAddr=10.202.0.1
Internet host table
127.0.0.1       localhost
10.202.0.1      lionn2  loghost
10.253.0.1      dncsatm
```

4 Locate the line that contains lionn.

Example: `10.202.0.1  lionn2  loghost`

5 Record the IP address associated with lionn in the space provided:

_____

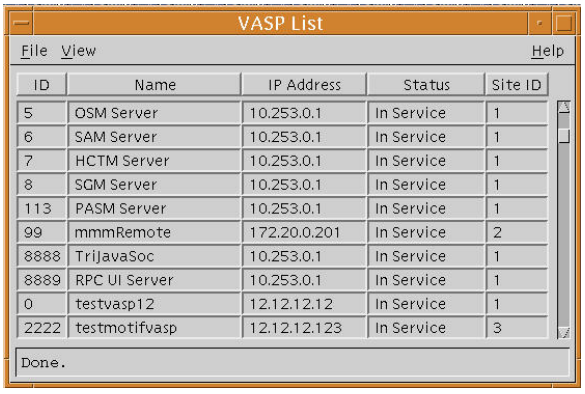
6 Type **exit** and press **Enter** to close the xterm window.

Verifying and Configuring the mmmRemote Server Entry in the VASP List

Viewing the VASP List

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

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



3 Is there an mmmRemote entry in the VASP List?

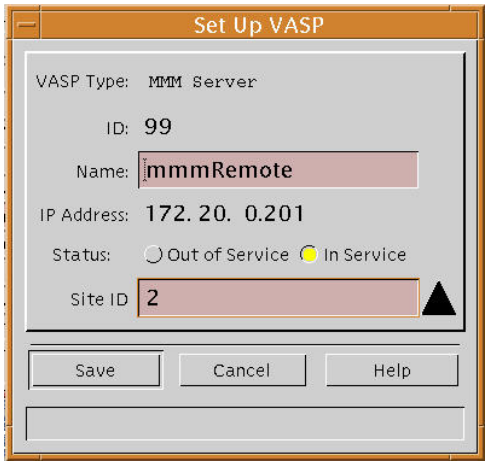
- If **yes**, go to ***Verifying the mmmRemote Entry in the VASP List*** (on page 36).
- If **no**, go to ***Configuring the mmmRemote Entry in the VASP List*** (on page 37)

Verifying the mmmRemote Entry in the VASP List

1 From the VASP List window, find the mmmRemote entry.

2 Click the row containing mmmRemote.

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 **IP Address** the same as the IP address you recorded in ***Determining the IP Address of the Remote ISDS*** (on page 35)?
- 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 entry is configured correctly in the VASP list. Click **Cancel** to close the Set Up VASP Window.
- If **no**, go to ***Configuring the mmmRemote Entry in the VASP List*** (on page 37) and fix the incorrect entry.

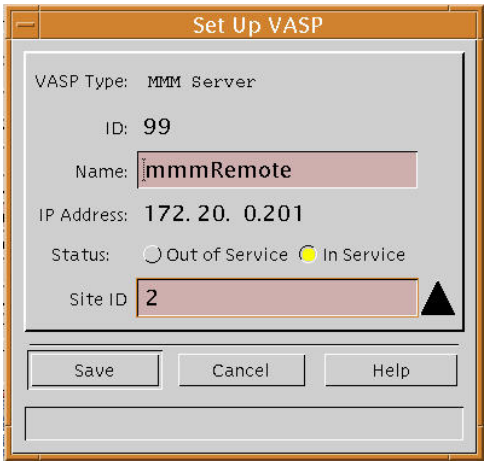
Configuring the mmmRemote Entry in the VASP List

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: _____

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 **mmmRemote**.

6 In the IP Address field, type the IP address of the ISDS that you recorded in ***Determining the IP Address of the Remote ISDS*** (on page 35).

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

8 Click **Save**.

Results:

- The system saves the mmmRemote configuration in the VASP list.
- The Set Up VASP window closes.
- The VASP List window updates with the added mmmRemote entry.

9 On the VASP List window, click **File > Close**.

5

Configure EAS Events, Messages, and Tests

Introduction

This chapter details the steps you need to follow to configure EAS events, messages, and tests. Included are the Required Weekly Test (RWT) and Required Monthly Test (RMT).

In This Chapter

Configuring the EAS on the ISDS

On the System Provisioning tab of the ISDS Administrative Console, there are four access keys in the EAS Message area that let you configure the EAS on the ISDS 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*** (on page 53) for additional information.
- **FIPS Code —** Assign FIPS codes and force tune services to each OOB bridge.

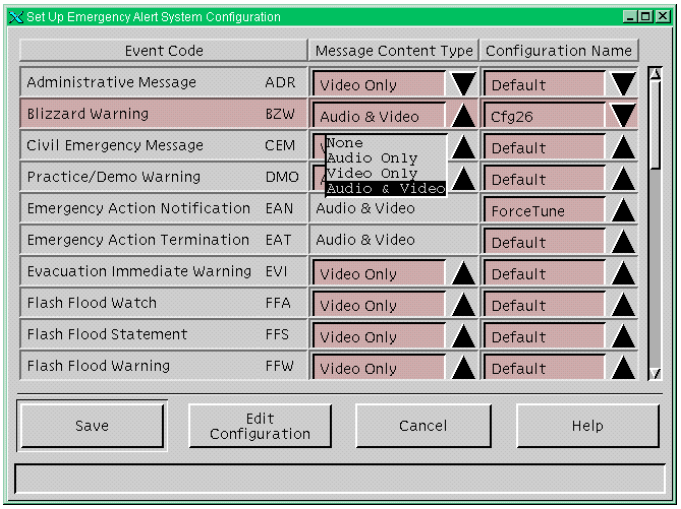
  Note: FIPS filtering is a separate software product. For more information on purchasing this software product, contact the person who handles your account.

Configure EAS Events

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

Configuring EAS Events

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



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
- Video Only
- Audio and 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.

Configuring EAS Messages

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

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, 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.

The ISDS 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 ISDS 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 setting are most appropriate for your operating environment.

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

Note: Each event only uses one of the MMM configuration settings.

- **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.

Configuring the Force Tune Type

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

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.

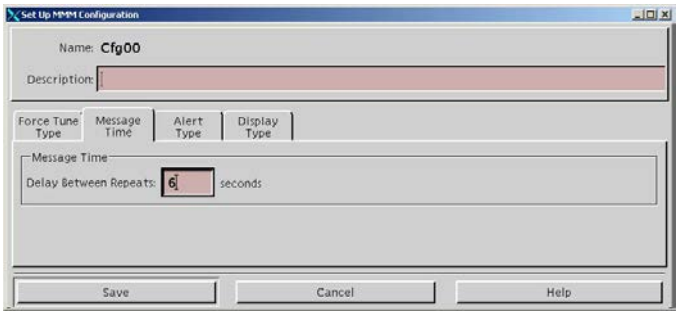
   Note: An EAM with configured with a forced tuning redirects the subscriber's TV to the selected service that provides the emergency alert information.
5. In the **Priority** field, type a priority for the message. The lower the number, the higher the priority.

   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.



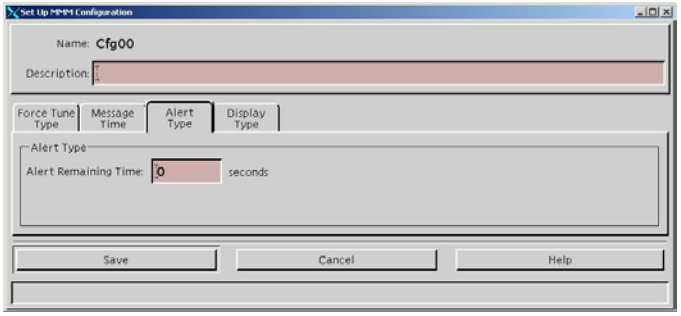
2 In the **Delay Between Repeats** field, type a delay time for the EAS message, depending on the type of message you are configuring:

- **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*** (on page 46) and ***Configure Monthly Tests*** (on page 49) 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.



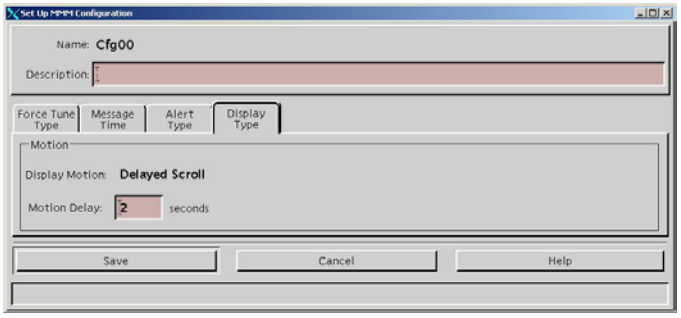
2 In the **Alert Remaining Time** field, type the number of seconds the messages will display on the screen. The Alert Remaining Time field has a maximum time limit of 120 seconds, which is also the default value.

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.



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 FIPS Filtering (Optional)

FIPS filtering, through its integration with the ISDS, 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.

Configuring FIPS Filtering

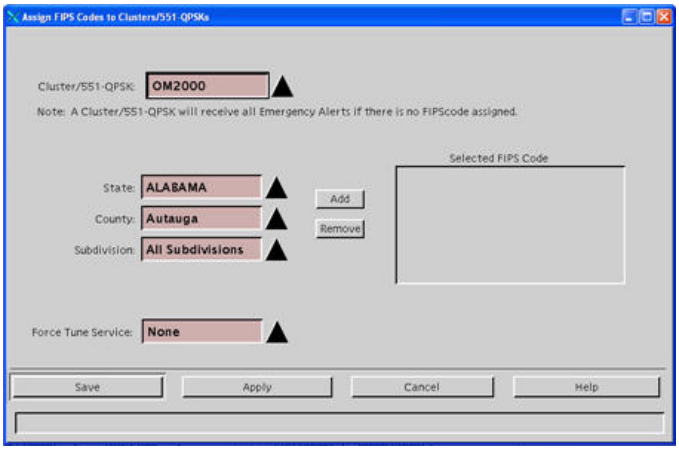
If you have purchased the EAS filtering software product, you need to define the EAS service area of each OOB bridge. If you do not assign FIPS codes to a bridge, that bridge receives all EAMs.

Follow these steps to configure FIPS filtering.

1 On the ISDS Administrative Console, click the **ISDS** tab.

2 Click the **System Provisioning** tab.

3 In the EAS Message section, click **FIPS Code**. The Assign FIPS Codes to 55-1 QPSKs window opens.



4 Click the **Cluster/55-1 QPSK** arrow and select a bridge from the list.

5 Click the **State** arrow and select a state from the list.

6 Click the **County** arrow and select a county from the list.

7 Click the **Subdivisions** arrow and select a subdivision from the list or select **All Subdivisions**.

8 Click **Add**.

9 Repeat steps 4 through 8 until you have assigned all the required FIPS codes to this bridge.

10 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 ISDS 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 product_name_common).

11 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**.

12 Click **Save**. The system saves your settings and the Assign FIPS Codes to QPSK/CMTS Bridges window closes.

Configure Weekly Tests

The Federal Communication Commission (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 ISDS to conduct weekly tests of your EAS.

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

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

What You Need

To configure the ISDS 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.

Configuring Weekly Tests

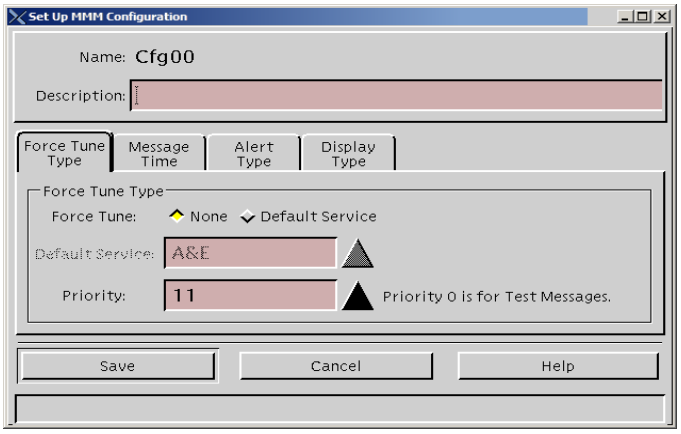
After you set up the RWT, you need to set up the MMM Server. The ISDS uses the MMM Server to conduct tests of the EAS. Follow these instructions to configure the MMM Server on the ISDS for the RWT of the EAS.

1 On the ISDS Administrative Console, click the **ISDS** tab.

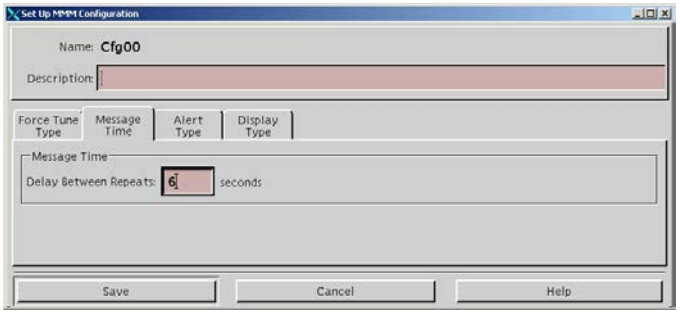
2 Click the **System Provisioning** tab.

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.



5 Click the **Message Time** tab.



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 x 60 = **480** 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 Weekly Tests

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

1 On the ISDS Administrative Console, click the **ISDS** tab.

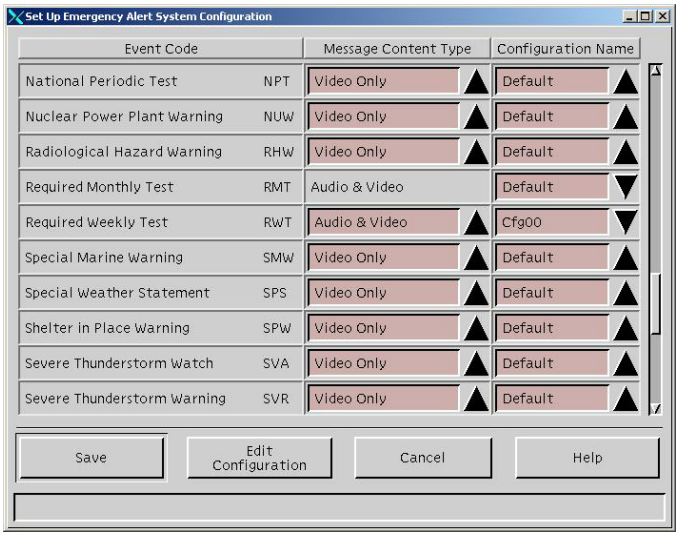
2 Click the **System Provisioning** tab.

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 configuration (Cfg00) you chose in step 3 of ***Configuring Weekly Tests*** (on page 47). The configuration you chose appears in the Configuration Name column.



7 Click **Save**. The system saves the new RWT configuration.

8 Click **Cancel**. The Set Up Emergency Alert System Configuration window closes.

Configure Monthly Tests

The Federal Communication Commission (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 ISDS to conduct monthly tests of your EAS.

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

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

What You Need

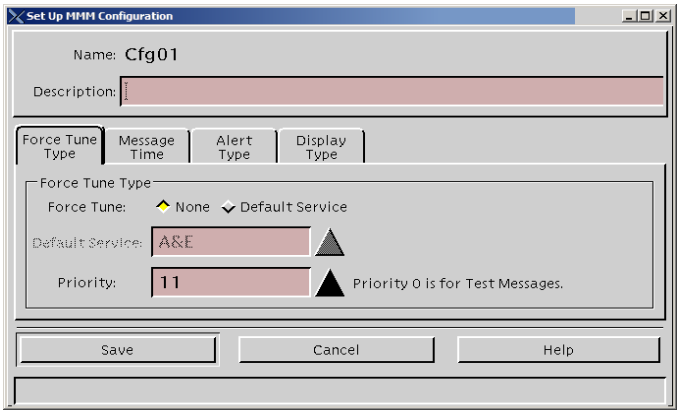
To configure the ISDS for the required test, you need the **Default Duration** value from the user interface of your EAS Encoder/Decoder. Refer to the documentation that accompanied your EAS Encoder/Decoder for instructions on locating this value on your EAS Encoder/Decoder.

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

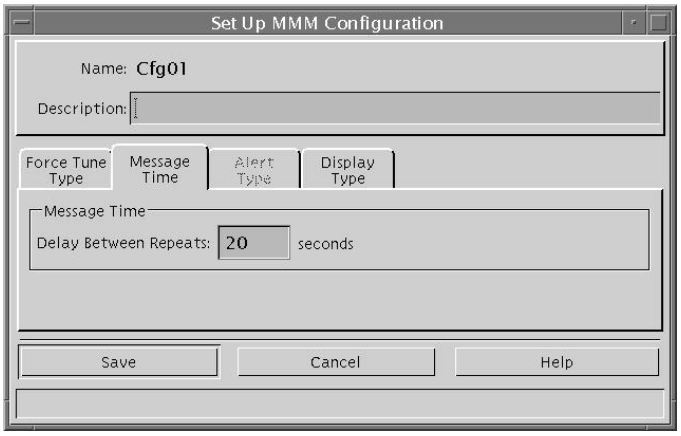
Configuring Monthly Tests

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

1. On the ISDS Administrative Console, click the **ISDS** 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.



5. Click the **Message Time** tab.



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 x 60 = **1860** 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 Monthly Tests

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

1 On the ISDS Administrative Console, click the **ISDS** tab.

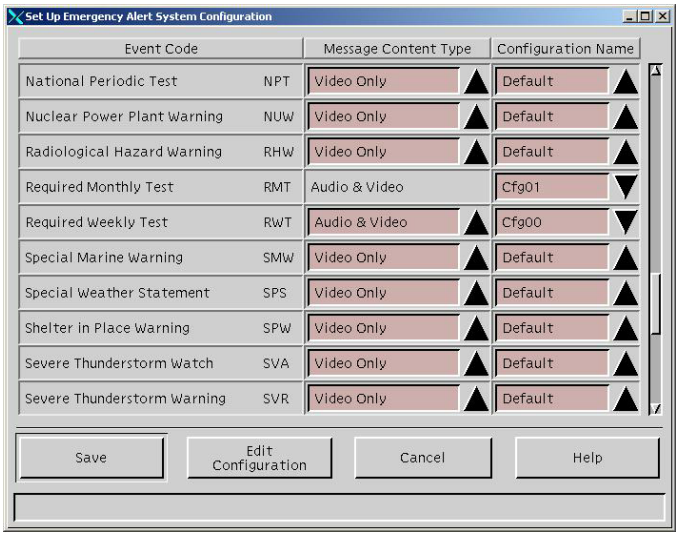
2 Click the **System Provisioning** tab.

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 configuration (Cfg01) you chose in step 3 of ***What You Need*** (on page 46). The configuration you chose appears in the Configuration Name column.



7 Click **Save**. The system saves the new RMT configuration.

8 Click **Cancel**. The Set Up Emergency Alert System Configuration window closes.

6

Conduct EAS Tests

Introduction

This chapter contains information about configuring and conducting weekly, monthly, and ad hoc tests of the EAS. The process is detailed in the following sections in this chapter:

- Test the EAS from the ISDS
- Conduct scheduled weekly and monthly tests

If your system does not function as expected, refer to ***Troubleshooting*** (on page 63) for troubleshooting procedures for the EAS.

In This Chapter

Test the EAS from the ISDS

This section describes the procedure for using the ISDS 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 ISDS 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.

Sending EAS Test Messages

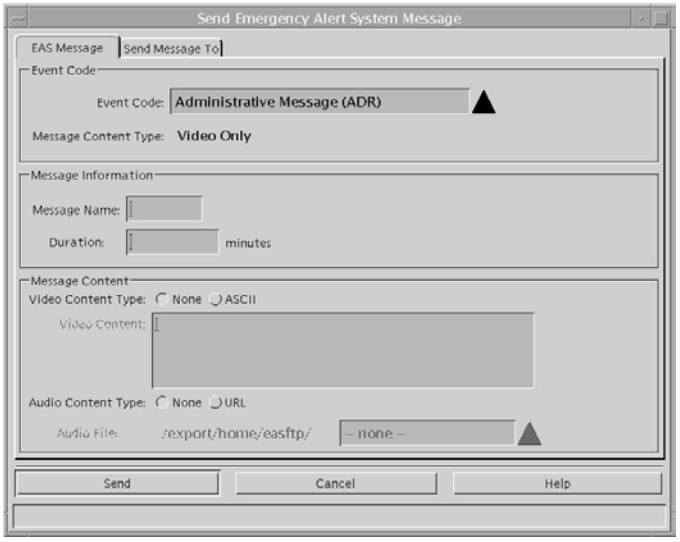
Follow these steps to send EAS test messages on the ISDS.

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

1 On the ISDS Administrative Console, click the **ISDS** 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.



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.

6 In the **Message Content** area, choose one of the following options:

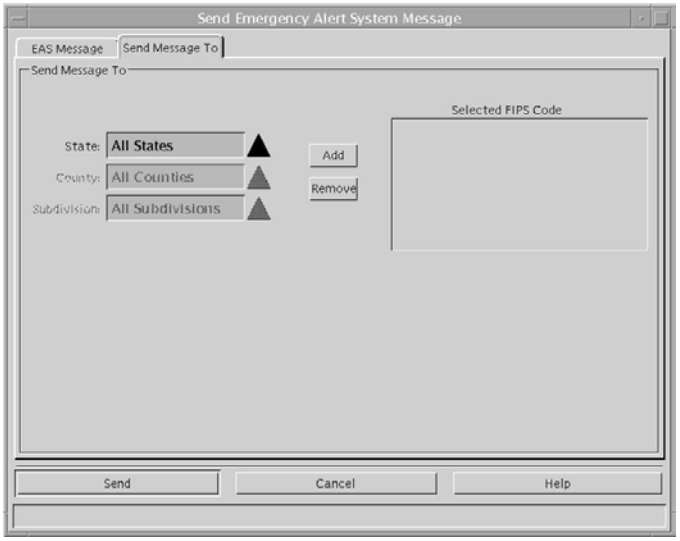
- If you have only *video* content, select **ASCII** and type the text in the **Video Content**.
- If you have only *audio* content, select **URL** and click the **Audio File** arrow to select a file from the list.

  Important: Be sure to select a WAV file from the list (a file with a *.wav* extension).
- If you have *audio and video* 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.



8 Did you purchase the EAS filtering product that provides FIPS filtering on 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 13.

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. 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.

15 Go to **Terminate EAS Messages**, next in this document.

Terminate EAS Messages

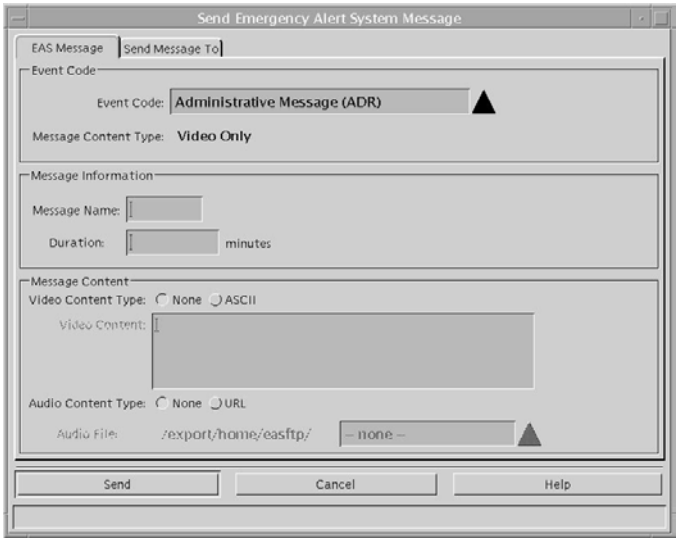
Occasionally, you may want to suspend or terminate an EAM before it reaches its configured duration. When you terminate an EAM, you stop transmitting all EAMs that are currently active in your system. If you terminate an EAM on an OOB bridge, you stop transmitting all EAMs that are currently active on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

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

Terminating EAS Messages

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

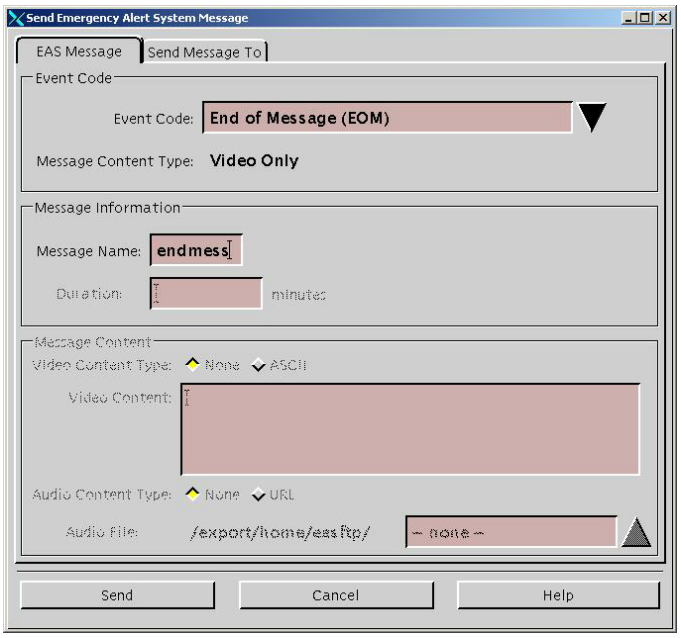
1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **EAS Message**. The Send Emergency Alert System Message window opens with the EAS Message tab to the forefront.



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.

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 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**.
- If **no**, correct the information and click **Send**.

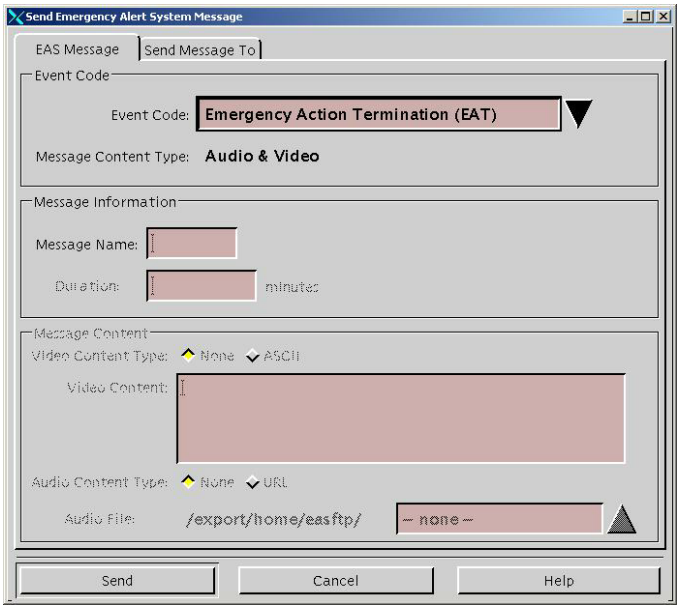
Important: If your system is currently broadcasting multiple EAMs, be sure you terminate the correct message.

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

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

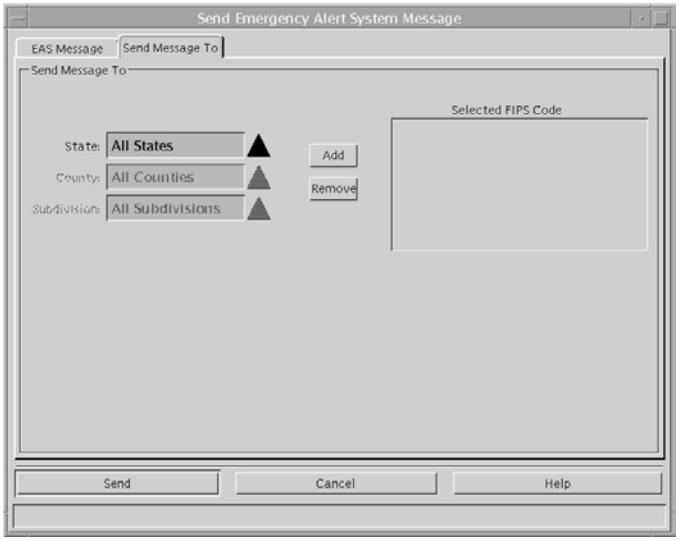
15 Click **EAS Message**. The Send Emergency Alert System Message window opens with the EAS Message tab to the forefront.

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



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

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



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 ISDS transmits instructions to DHCTs to stop displaying the EAM.

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

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 ISDS*** (on page 54) 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 63) for troubleshooting procedures for the EAS.

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

System	RWT	RMT
Monroe System with Digital Envoy	**Automatic Mode:** Automated process **Manual Mode:** ■ Press the **MODE** soft key. Various MIP-021 options appear on the LCD screen. ■ Press the **NO** soft key until the message **SEND WEEKLY TEST** appears. ■ Press the **YES** soft key.	**Automatic Mode:** Automated process **Manual Mode:** The FCC requires that the RMT function in automatic mode.
Frontline	**Automatic Mode:** Automated process **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.	**Automatic Mode:** Automated process **Manual Mode:** 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

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 ISDS. The following companies manufacture EAC solutions that are known to work with the ISDS:

- 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 5), 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 7) 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 9) 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 11) 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 13) and refer to your EAC system documentation for more information.

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 5), 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 ISDS to verify communication from the EAC to the ISDS.
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 ISDS. 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 ISDS to verify communication from the EAC to the ISDS.
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 ISDS.
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 ISDS to verify communication from the EAC to the ISDS.
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 ISDS and login to verify EAC communications with the ISDS.

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

Troubleshoot the ISDS Network

Troubleshoot the ISDS Ethernet Hub

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

Troubleshooting the ISDS Ethernet Hub

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

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

Troubleshoot the BFS

During normal operations, the BFS displays green status lights on the ISDS 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 ISDS to the set-tops.

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

Troubleshoot ISDS Configuration and Performance

This section provides procedures for troubleshooting ISDS configuration and performance.

Troubleshooting the ISDS MMM/EAS, Resident App Servers

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

1. Open an xterm window on the ISDS.
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 ISDS element groups.

   Note: You might need to expand the window to view the entire list of ISDS 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 ISDS.
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 **ls –l 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	Check and Correct
The following message appears at the bottom of the Send EAS Message screen on the ISDS: **MMMServer failure**	**1** Open an xterm window on the ISDS. **2** 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 ***Stop and Restart the MMM Server*** (on page 73).
The following message appears at the bottom of the Send EAS Message screen on the ISDS: **Send Message failed. Error occurred in accessing the database; Server will restart in a few minutes.**	Call Cisco Services for assistance.

Troubleshooting EAS after SR Upgrades

After performing an SR (System Release) upgrade, verify that your EAS equipment is still properly configured in the ISDS. Complete all the procedures in ***Test the EAS from the ISDS*** (on page 54).

After completing the procedures, verify that you can generate an EAS message for the EAC. Refer to ***Verify Your EAS Equipment Configuration*** (on page 5) and the manufacturer's documentation for more information.

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 ISDS.
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 73).

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 ISDS.
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 ISDS Administrative Console Status window, click **Control** in the **ISDS** 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 ISDS 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 ISDS Control window should still be open.

1. On the ISDS Administrative Console Status window, click **Control** in the **ISDS** section. The ISDS 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 ISDS 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 ISDS is bounced before an audio file expires, a link to that audio file remains on the ISDS.

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 ISDS.
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.

Deleting Stranded Audio Links

1. From the ISDS 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 74).
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.

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 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.
- The ticker display is 83% opaque over video and 100% opaque over any graphics such as the IPG, General Settings, and music.
- 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 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 that the MMM Server is working by sending an EAS test message from the ISDS 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.
4. Verify that the out-of-band Broadcast File System (OOB BFS) is operational by sending an EAS test message with audio content only.
5. Verify that the EAS client on the set-top is operational by sending an EAS test message with both text and audio.

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.

Index

T

V

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

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

August 2012 Printed in USA

Part Number 4024428 Rev B