Cisco TV CDS 2.0 RTSP
Software Configuration Guide

March 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-15954-01
CONTENTS

Preface xi
Document Revision History xi
Audience xi
Objective xi
Document Organization xii
Document Conventions xiii
Related Documentation xiv
Obtaining Documentation and Submitting a Service Request xiv

CHAPTER 1
Product Overview 1-1
Overview 1-1
TV CDS Software 1-3
  TV Streamer CDA 1-4
  TV MediaX Suite CDA 1-4
Content Delivery System Architecture 1-4
  Vault 1-5
  Streamer 1-5
  Integrated Streamer-Vault 1-6
    Content Delivery System Manager 1-6
Resiliency and Redundancy 1-7
  Vault Disk Redundancy 1-7
  Vault Server Resiliency 1-8
  Streamer Disk Redundancy 1-8
  Streamer Server Resiliency 1-8
  Ethernet Link Resiliency 1-8
Scalability 1-9

CHAPTER 2
Network Design 2-1
Overview 2-1
  CDS with Vaults and Streamers 2-1
  CDS with ISVs 2-2
TV CDS Topologies 2-2
  Centralized Topology 2-2
  Decentralized Topology 2-3
Contents

Hybrid Topology  2-4
CDS Workflow  2-5
  Streamer Workflow  2-5
    Setup Server  2-6
    Control Server  2-6
    Play Server  2-6
BMS Considerations  2-6
  OpenStream ISA Integration  2-6
    Streaming Mode  2-7
nABLE Integration  2-7
Network Connections  2-8
  Ingest Interface  2-10
  Management Interface  2-10
  Cache Interfaces  2-10
  Cache/Stream Interfaces  2-10
    Streaming Interface  2-11

CHAPTER 3
Getting Started  3-1
  Initially Configuring the Devices  3-1
  Logging In to the TV CDSM  3-2
    Logging Out  3-3
  Initializing the CDS and Activating the Optional Features  3-3
  Navigating the CDSM  3-4
    Using Online Help  3-4
  Configuration Workflows  3-5
    TV MediaX Configuration Workflow  3-6

CHAPTER 4
Configuring the CDS  4-1
  System Level Configuration  4-1
    Configuring DNS Services  4-2
    Configuring the Hosts Service  4-3
    Configuring the Array Name  4-5
    Configuring QAM Gateways  4-6
      ARP  4-6
    Configuring the Headend Setup  4-8
    Configuring the Bandwidth Manager  4-9
    Configuring the Ingest Manager  4-10
    Configuring the Authentication Manager  4-14
Configuring Ingest Tuning 4-16
Configuring IP Nicknames 4-17
Configuring the Media Importer/Exporter 4-18
Configuring Call Signs 4-19
Configuring Input Channels 4-21
Configuring Transport Groups 4-23
Array Level Configuration 4-25
  Configuring the Array Level DNS Bindings 4-26
  Configuring Stream Groups 4-27
  Configuring the Control and Setup IPs 4-29
  Configuring the Media Scheduler 4-31
    User Preferences 4-32
    Scheduling Content for Ingest 4-33
    Package Metadata Editor 4-36
    Fixing Conflicts in the Media Scheduler 4-38
Server Level Configuration 4-39
  Configuring the Interfaces 4-39
  Configuring the Servers 4-41
  Configuring the Route Table 4-47
    Network Information 4-48
  Configuring the SNMP Agent 4-49
  Configuring the Server Level DNS Binding 4-51
  Configuring RTSP Setup 4-52
    RTSP Deployment 4-53
    Configuring FSI Setup 4-58

 CHAPTER 5 System Monitoring 5-1
  System Level Monitoring 5-1
    System Health 5-1
    System Snapshot 5-3
  Monitoring Content Objects 5-4
    Ingests 5-4
      List Content 5-7
    Packages 5-9
    Publish Failures 5-11
  Monitoring Stream Objects 5-13
    Stream Monitor 5-13
    Stream Failures 5-18
  Array Level Monitoring 5-21
Array Snapshot  5-21
Server Level  5-22
  Disk Monitor  5-22
  S.M.A.R.T  5-24
  NIC Monitor  5-25
  Cache/Fill Bandwidth  5-27
  Services Monitor  5-29
Recommended Monitoring Schedule  5-31
  Daily Tasks  5-31
  Weekly Tasks  5-31
    Monitoring Tasks for Streamers and Vaults  5-31
    Monitoring Tasks for Vaults  5-33
    Monitoring Tasks for Streamers  5-33
  Monthly Tasks  5-33
  Other Tasks  5-34

CHAPTER  6
System Reporting  6-1
  Stream Activity  6-1
    Streams by Array  6-1
    Streams by Time  6-6
    Stream Play History  6-8
    Cache/Fill Bandwidth  6-11
    Stream Failures  6-13
    Content Popularity  6-16
  Content Activity  6-17
    Content by Ingest Date  6-17
    Unpublished Package Report  6-19
  CDSM Audit Logs  6-21
  Archived Data  6-22
    CDSM Audit Log Archives  6-23
    Content Reports  6-24
    Stream Reports  6-24
    Stream Failure Reports  6-25
    Stream Activity Reports  6-26

CHAPTER  7
System Maintenance  7-1
  User Access  7-1
    Setting Up Users  7-2
    Editing User Settings  7-3
Deleting a User 7-4
Changing User Default Settings 7-4
Viewing User Settings 7-5
Server Maintenance 7-6
  Restarting a Server 7-6
  Shutting Down a Server 7-7
  Offloading a Server 7-9
    Server Offload—Disable 7-10
  Setting System Thresholds 7-10
Restarting the Services 7-11
Software Maintenance 7-13
  Updating the System Software 7-13
  Uploading an EPG File 7-14
Manuals 7-15

APPENDIX A
Troubleshooting A-1
  General Issues A-2
    File System A-2
      CDSM A-2
      Vault, Streamer, and ISV A-3
    Log Files A-3
      Linux Log Files A-3
      CServer Log Files A-4
      RTSP Log Files A-5
  Server Configuration Files A-6
    Description of the .arroyorc Settings A-6
    Description of the setupfile Settings A-7
  Identifying the Software Versions or Releases A-10
    Linux OS Version A-10
    CDS-Related Releases A-11
  Using ifstats to Monitor Traffic A-12
  Kernel Crash A-12
  Disk Drive Issues A-13
    CDSM GUI Disk Monitor Page Reports a Disk Warning A-14
  Memory Issues A-14
  Network A-15
    Interface Information A-16
  Startup Issues A-17
    BIOS Settings—Operating System Hangs or Goes into KDB Mode A-18
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Console Port Settings</td>
<td>A-18</td>
</tr>
<tr>
<td>Required Services Not Starting or Running Correctly</td>
<td>A-19</td>
</tr>
<tr>
<td>Management and Database Issues</td>
<td>A-19</td>
</tr>
<tr>
<td>System Health</td>
<td>A-20</td>
</tr>
<tr>
<td>Cannot Access the CDSM GUI</td>
<td>A-20</td>
</tr>
<tr>
<td>CDSM GUI Does Not Register the Vaults and Streamers</td>
<td>A-20</td>
</tr>
<tr>
<td>Database Monitoring</td>
<td>A-21</td>
</tr>
<tr>
<td>Ingest Issues</td>
<td>A-21</td>
</tr>
<tr>
<td>Ingest Interface</td>
<td>A-21</td>
</tr>
<tr>
<td>FSI Starts but Cannot Ingest Content</td>
<td>A-22</td>
</tr>
<tr>
<td>FSI Does Not Start</td>
<td>A-22</td>
</tr>
<tr>
<td>Content Not Ingesting</td>
<td>A-22</td>
</tr>
<tr>
<td>Asset Ingest Manager Restart Causes Endless Loop</td>
<td>A-23</td>
</tr>
<tr>
<td>Bad Content</td>
<td>A-24</td>
</tr>
<tr>
<td>Network</td>
<td>A-24</td>
</tr>
<tr>
<td>Content Processing Issues</td>
<td>A-25</td>
</tr>
<tr>
<td>Listing Content</td>
<td>A-25</td>
</tr>
<tr>
<td>Content Mirroring</td>
<td>A-25</td>
</tr>
<tr>
<td>Verifying GOIDs</td>
<td>A-26</td>
</tr>
<tr>
<td>Trick-Mode Issues</td>
<td>A-26</td>
</tr>
<tr>
<td>Cache-Fill Issues</td>
<td>A-27</td>
</tr>
<tr>
<td>Rules for ISV Interoperability with Vaults and Streamers</td>
<td>A-27</td>
</tr>
<tr>
<td>Network</td>
<td>A-27</td>
</tr>
<tr>
<td>Stream Stops Playing at the Same Place or Does Not Play at All</td>
<td>A-27</td>
</tr>
<tr>
<td>Streaming and Playout Issues</td>
<td>A-28</td>
</tr>
<tr>
<td>Listing of Streams</td>
<td>A-28</td>
</tr>
<tr>
<td>No Streaming</td>
<td>A-28</td>
</tr>
<tr>
<td>Stream Not Playing</td>
<td>A-29</td>
</tr>
<tr>
<td>Poor Video or Audio Quality</td>
<td>A-30</td>
</tr>
<tr>
<td>No Video Displayed</td>
<td>A-30</td>
</tr>
<tr>
<td>RTSP Cannot Start</td>
<td>A-31</td>
</tr>
<tr>
<td>Video Stops Playing</td>
<td>A-31</td>
</tr>
<tr>
<td>No Video Playing on the STB</td>
<td>A-31</td>
</tr>
<tr>
<td>CDS Is Streaming but No Video Is Playing on the STB</td>
<td>A-32</td>
</tr>
<tr>
<td>Session Messaging</td>
<td>A-33</td>
</tr>
<tr>
<td>Log File Search Tips</td>
<td>A-33</td>
</tr>
<tr>
<td>Codes</td>
<td>A-34</td>
</tr>
<tr>
<td>Database Issues</td>
<td>A-35</td>
</tr>
<tr>
<td>Database Replication</td>
<td>A-35</td>
</tr>
<tr>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>CDSM GUI Does Not Report All the Ingested Content</td>
<td>A-36</td>
</tr>
<tr>
<td>Errors in Log File</td>
<td>A-36</td>
</tr>
<tr>
<td>Many Log Files</td>
<td>A-36</td>
</tr>
<tr>
<td>Corruption Recovery</td>
<td>A-37</td>
</tr>
<tr>
<td>Advanced Features and Applications</td>
<td>A-38</td>
</tr>
<tr>
<td>Live Multicast Ingest</td>
<td>A-38</td>
</tr>
<tr>
<td>Ingest with Media Scheduler</td>
<td>A-38</td>
</tr>
<tr>
<td>Ingest without Media Scheduler</td>
<td>A-38</td>
</tr>
<tr>
<td>Ingest Troubleshooting</td>
<td>A-38</td>
</tr>
<tr>
<td>Frequently Asked Questions</td>
<td>A-39</td>
</tr>
<tr>
<td>Reliability and Availability</td>
<td>A-39</td>
</tr>
<tr>
<td>Serviceability and Manageability</td>
<td>A-39</td>
</tr>
<tr>
<td>Content</td>
<td>A-42</td>
</tr>
<tr>
<td>Other</td>
<td>A-43</td>
</tr>
<tr>
<td>CDS Content Quality Guidelines</td>
<td>A-44</td>
</tr>
<tr>
<td>Supported Elementary Stream Types</td>
<td>A-44</td>
</tr>
<tr>
<td>Scrambling</td>
<td>A-44</td>
</tr>
<tr>
<td>Transport Bit Rate</td>
<td>A-44</td>
</tr>
<tr>
<td>Stream Length</td>
<td>A-45</td>
</tr>
<tr>
<td>Format Restrictions</td>
<td>A-45</td>
</tr>
<tr>
<td>Preferred Formats</td>
<td>A-45</td>
</tr>
</tbody>
</table>

**APPENDIX B**

<table>
<thead>
<tr>
<th>SNMP MIB and Trap Information</th>
<th>B-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td></td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>B-1</td>
</tr>
<tr>
<td>SNMP Management Objects and Traps</td>
<td>B-2</td>
</tr>
<tr>
<td>RFC Compliance</td>
<td>B-7</td>
</tr>
</tbody>
</table>

**APPENDIX C**

<table>
<thead>
<tr>
<th>Engineering Access Level Pages</th>
<th>C-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDSM Diagnostics</td>
<td></td>
</tr>
<tr>
<td>CIDR Calculator</td>
<td>C-2</td>
</tr>
<tr>
<td>Stream Trick-Mode Debugger</td>
<td>C-2</td>
</tr>
<tr>
<td>Unix Timestamp Tool</td>
<td>C-2</td>
</tr>
<tr>
<td>Server Diagrams</td>
<td>C-2</td>
</tr>
<tr>
<td>CDSM Setup</td>
<td>C-2</td>
</tr>
<tr>
<td>Deployed CServer Version</td>
<td>C-2</td>
</tr>
<tr>
<td>Stream Failover Support</td>
<td>C-2</td>
</tr>
<tr>
<td>Stream Steering Mode</td>
<td>C-3</td>
</tr>
<tr>
<td>Deployment Network Config</td>
<td>C-3</td>
</tr>
</tbody>
</table>
Contents

Installation Type C-3
Media Scheduler C-3
Real-Time Capture Type C-3
Playout Scheduler C-3
Bandwidth Manager C-3
Ingest Manager C-4
RTSP Deployment Type C-4
Authentication Manager C-4
Service Group Steering C-4
CDSM NAV Setup C-4
CDSM Health Monitoring C-4

System Configs C-5
Group Map 0 C-5
Servers Group Map C-5
License Map C-5
Control IP Map C-5
Add New Server C-5

APPENDIX D

Software Licensing Information D-1

Notices D-1
OpenSSL/Open SSL Project D-1
License Issues D-1
Product Warranties D-3
Standard Warranty D-3
Returns D-3
Infringement D-4
No Other Warranties D-4
Cisco Software License D-4
GNU General Public License D-5
Preface

This preface describes the audience, use, and organization of the Cisco TV CDS 2.0 RTSP Software Configuration Guide. The preface also outlines the document conventions and support information.

This preface contains the following sections:

- Document Revision History, page xi
- Audience, page xi
- Objective, page xi
- Document Organization, page xii
- Document Conventions, page xiii
- Related Documentation, page xiv
- Obtaining Documentation and Submitting a Service Request, page xiv

Document Revision History

The Document Revision History table below records technical changes to this document.

<table>
<thead>
<tr>
<th>Document Revision</th>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>OL-15954-01</td>
<td>March 4, 2009</td>
<td>Initial release</td>
</tr>
</tbody>
</table>

Audience

This guide is for the networking professional managing the Cisco TV Content Delivery System, hereafter referred to as CDS. Before using this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of Ethernet, local area networking, and TV streaming.

Objective

This guide provides the information you need to configure and monitor the Cisco TV CDS.
This guide provides procedures for using the commands that have been created or changed for use with the Cisco TV CDS. It does not provide detailed information about these commands.

This guide does not describe system messages you might encounter or how to install your CDS. For information on installing the hardware, see the Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide, the Cisco Content Delivery Engine 110 Hardware Installation Guide, or the Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide. See the “Related Documentation” section on page xiv for links to documentation online.

For documentation updates, see the release notes for this release.

Document Organization

This document contains the following chapters and appendices:

<table>
<thead>
<tr>
<th>Chapters or Appendices</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Product Overview”</td>
<td>Provides an overview of the Content Delivery System.</td>
</tr>
<tr>
<td>Chapter 2, “Network Design”</td>
<td>Describes the possible network topologies for the Content Delivery System.</td>
</tr>
<tr>
<td>Chapter 3, “Getting Started”</td>
<td>Describes accessing and navigating the Content Delivery System Manager (CDSM).</td>
</tr>
<tr>
<td>Chapter 4, “Configuring the CDS”</td>
<td>Describes how to configure the CDS using the CDSM web-based user interface.</td>
</tr>
<tr>
<td>Chapter 5, “System Monitoring”</td>
<td>Explains how to monitor the CDS components using the CDSM.</td>
</tr>
<tr>
<td>Chapter 6, “System Reporting”</td>
<td>Explains the different reports available through the CDSM.</td>
</tr>
<tr>
<td>Chapter 7, “System Maintenance”</td>
<td>Explains how to install software updates, restart services, add administrator users, and shut down and reboot the servers.</td>
</tr>
<tr>
<td>Appendix A, “Troubleshooting”</td>
<td>Presents troubleshooting procedures for the CDS, including the symptoms, probable causes, and recommended actions for a variety of problems.</td>
</tr>
<tr>
<td>Appendix B, “SNMP MIB and Trap Information”</td>
<td>Provides information on SNMP and the Cisco TV CDS proprietary SNMP informational events and traps.</td>
</tr>
<tr>
<td>Appendix C, “Engineering Access Level Pages”</td>
<td>Describes the CDSM pages visible with the Engineering access level.</td>
</tr>
<tr>
<td>Appendix D, “Software Licensing Information”</td>
<td>Explains the software licensing agreement between Cisco and the purchaser of the Content Delivery System.</td>
</tr>
</tbody>
</table>
Document Conventions

This guide uses the following conventions for command syntax descriptions and textual emphasis:

<table>
<thead>
<tr>
<th>Conventions</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface font</strong></td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>italic font</em></td>
<td>Arguments for which you supply values are in <em>italics</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>screen font</strong></td>
<td>Terminal sessions and information the system displays are in <strong>screen font</strong>.</td>
</tr>
<tr>
<td><strong>boldface screen font</strong></td>
<td>Information you must enter is in <strong>boldface screen font</strong>.</td>
</tr>
<tr>
<td><em>italic screen font</em></td>
<td>Arguments for which you supply values are in <em>italic screen font</em>.</td>
</tr>
<tr>
<td>^</td>
<td>The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets in contexts where italics are not available.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point ( ! ) or a pound sign ( # ) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

⚠️ **Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

✍ **Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this publication.

🔍 **Tip**

Means the following information might help you solve a problem.
Related Documentation

These documents provide complete information about the CDS and are available from Cisco.com:

- Release Notes for the Cisco TV CDS 2.0
- Cisco TV CDS 2.0 ISA Software Configuration Guide
- Cisco TV CDS 2.0 API Guide
- Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide
- Cisco Content Delivery Engine 110 Hardware Installation Guide
- Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide
- Cisco Content Delivery System 2.x Documentation Roadmap
- Regulatory Compliance and Safety Information for Cisco Content Delivery Engines

You can access the software documents at the following URL:

You can access the hardware documents at the following URL:

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Product Overview

This chapter provides a brief introduction to the Cisco TV Content Delivery System Release 2.0 for a Real Time Streaming Protocol (RTSP) environment. For information on an Interactive Services Architecture (ISA) environment, see the Cisco TV CDS 2.0 ISA Software Configuration Guide. See the “Related Documentation” section on page xiv for links to documentation online. This chapter covers the following major topics:

- Overview, page 1-1
- Content Delivery System Architecture, page 1-4

Overview

The Cisco TV Content Delivery System (CDS) is a distributed network of Content Delivery Engines (CDEs) running Content Delivery Applications (CDAs) that collaborate with each other to deliver personalized entertainment and interactive media to subscribers.

The Cisco TV CDS has a variety of mechanisms to accelerate the distribution and delivery of content. The CDS interoperates with electronic program guides (EPGs), set-top boxes (STBs), and backoffice applications, offering an end-to-end solution for video delivery systems.

The Cisco TV CDS functionality can be separated into four areas:

- Ingest
- Storage
- Streaming
- Management

Each CDE in the CDS contributes to one or more of these functions as determined by the CDAs running on it. Table 1-1 describes the relationship between the CDA names and the names the TV Content Delivery System Manager (CDSM) uses.

<table>
<thead>
<tr>
<th>CDA Name</th>
<th>Functionalities</th>
<th>CDSM Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vault</td>
<td>Ingest and storage</td>
<td>Vault</td>
</tr>
<tr>
<td>TV Streamer</td>
<td>Content caching, personalization, and streaming to STBs</td>
<td>Streamer</td>
</tr>
</tbody>
</table>
Figure 1-1 illustrates how a TV CDS network can be deployed. A business management system (BMS), commonly called a backoffice, enables service providers to deploy on-demand services using VOD servers, networks, billing systems and other system components. The asset management system (AMS) manages the content on headend and node servers, while the BMS handles functions related to pitching and catching. Sometimes there is some overlap of functionality between the BMS and the AMS.

The Cisco TV CDS solution has three major elements:

- A Vault array consisting of one or more Vault servers. The Vault array is responsible for ingest and reliable storage of video on demand (VOD) content. The number of Vault servers in the Vault array is driven by the amount of content that the system offers and the degree of redundancy.

- One or more Streamer arrays each consisting of one or more Streamer servers. The Streamer array is responsible for the personalization and streaming of content in response to user requests. The number of Streamer servers and Streamer arrays is determined by the number of streams deployed and by the topology that best suits your individual network and redundancy requirements.

- A CDSM server. The Content Delivery System Manager is used to manage the Vault and Streamer servers, collect event logs, and provide reporting tools.

Note
In smaller systems, the Integrated Streamer-Vault (ISV) server can be used, where the Vault and Streamer functionalities exist in one ISV server.
TV CDS Software

The Cisco TV CDS kernel software, known as the CServer, creates a logical network that pools, load balances, and coordinates the physical resources of the CDEs, so that the whole network operates and is managed as if it is a single resource.

The CServer facilitates the rapid movement of content between Vaults and Streamers while keeping required bandwidth to a minimum. To accomplish this, the Cisco TV CDS software uses a proprietary protocol, the Cache Control Protocol (CCP), across the Gigabit Ethernet networks. All content is held reliably on the Vault servers and a large amount, but not all, of the content is also contained on the Streamer servers. Cisco CCP, a multilayered caching architecture, along with associated software algorithms ensures that content segments are delivered only to the Streamers where there is demand for that content. The TV CDS software monitors the frequency of subscriber demand and places content appropriately in either the serving Streamer’s dynamic random access memory (DRAM) or disk cache.

Content is delivered across the network in response to cache-fill calls from the Streamers in an opportunistic manner, depending on the availability of bandwidth; delivery can be faster than real-time delivery where bandwidth allows. The TV CDS software that ensures content on the Streamer servers is always the most popular content; that is, the content requested by the largest number of subscribers. User requests are generally served from the Streamer’s cache. Requests for content that are not already in the Streamer’s local cache are pulled from the Vault, cached on the Streamer, and streamed to the subscriber. Wherever the content is stored relative to the point of playout, all content appears as if it is local to the Streamer and the streaming of any content is nearly instantaneous.

Each Streamer array runs a load distribution protocol among its members to ensure that new streams are distributed to the “best” Streamer in the array. The “best” Streamer is the Streamer that has the requested content in the highest-performing cache resource (DRAM or disk) or that has the most unused capacity. In this way, new Streamers are brought into operation hitlessly—because once a new server is in service, fresh streams are automatically allocated to it. Furthermore, the cache capacity of the array is the sum of the caches of all Streamers in the array, which provides the most optimal system operation and the highest cache-hit rate.

The CServer is responsible for the following:
- Storing content
- Streaming content
- Managing bandwidth usage for ingests
- Managing bandwidth usage for streaming
- Mirroring content among Vault servers
- Making decisions on content retention on Streamer servers

On top of the CServer, and taking advantage of the services it offers, a variety of applications deliver individual personalized entertainment services. Cisco currently offers the following applications:
- TV Streamer delivering VOD and network personal video recorder (nPVR) services
- TV MediaX Suite for simplifying ingest and workflow scheduling tasks for asset-based and real-time content

In a full TV CDS network, the Vault, TV Streamer, and CDSM are required. The TV MediaX Suite is an optional CDA. In a smaller TV CDS network, the ISV can be used in place of the Vault and TV Streamer.
TV Streamer CDA

The TV Streamer CDA is used for VOD delivery systems. TV Streamers are responsible for personalizing content and playing that content out under subscriber control.

TV MediaX Suite CDA

The TV MediaX Suite CDA offers a set of tools that simplify content ingest workflow and scheduling tasks for both asset-based and real-time content. The TV MediaX Suite CDA consists of the following features:

- Publisher—Coordinates the ingest of pre-encrypted content.
- Scheduler—Schedules real-time content or imports the schedule from an EPG.

Content Delivery System Architecture

Vaults and Streamers have different but important functions that are required for the TV CDS software to run efficiently. The Integrated Streamer-Vault (ISV) server combines the functionality of both the Vault and Streamer for smaller networks. The Content Delivery System Manager provides a browser-based user interface for configuration, monitoring, maintenance, and reports of the TV Content Delivery System solution. Figure 1-2 shows the different elements of the TV Content Delivery System.

Figure 1-2  High-Level View of the Content Delivery System

Table 1-2 describes the system elements shown in Figure 1-2.
Table 1-2  
High-Level Description of the TV Content Delivery System

<table>
<thead>
<tr>
<th>Content Delivery System Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CServer</td>
<td>The CServer is the kernel software that handles bandwidth management, storage decisions, and Lightweight Stream Control (LSC) and stream processing on the TV Content Delivery System.</td>
</tr>
<tr>
<td>Database</td>
<td>The database stores information about the system including current states of all ingests and streams, configuration settings, and system statistics. Some database elements are global among all servers and some are local. For example, statistics are stored on the local server and the Content Delivery System Manager only. States about stream objects are replicated on all Streamer servers. The Content Delivery System Manager stores a superset of all database elements.</td>
</tr>
</tbody>
</table>
| Management                      | There are two types of management:  
• Content Delivery System Manager—Browser-based user interface.  
• SNMP agent—Network Management System (NMS) interface. |
| Storage                         | There are three levels of storage (or cache):  
• All content is stored on the Vault server, as well as mirrored to other Vaults.  
• Currently requested content, or popular content, is stored in the Streamer’s random access memory (RAM).  
• Recently requested content, or popular content, is stored on the Streamer’s hard drive. |
| Event Collection                | The Content Delivery System Manager collects logged events for reporting purposes as well as third-party applications |
| Reports                         | The Content Delivery System Manager provides a reporting tool to aid performance trending and analysis of streams, popular content, bandwidth usage, and more. |

Vault

The Vault server ingests content delivered over a standard interface (for example, using FTP to receive content from a catcher), performs whatever processing is required (for example, generating trick-play files), and stores the processed content reliability on disk. A Vault array consists of a scalable number of Vault servers that divide the responsibility for ingest and storage among the members of the array. Vault servers can be collocated or distributed to multiple locations across an IP or Ethernet network. Each Vault server can simultaneously ingest up to 200 channels of MPEG-2 transport stream (TS) content and store up to 6000 hours of MPEG-2 TS standard definition content with two mirrored copies of the content and one to two trick files.

Streamer

A Streamer server receives content from the Vault and delivers that content to subscribers. Streamers can be of different capacity, depending on the needs of the network, and have different applications, depending on the type of content being delivered. Currently, the highest-capacity Streamer can
simultaneously stream approximately 2500 streams of MPEG-2 TS standard definition VOD. Streamers can be collocated with Vaults or distributed to remote locations. The Streamer array is responsible for the personalization and streaming of content in response to user requests. The Streamer can have one or more of the following applications:

- TV Streamer
- TV MediaX Suite

Integrated Streamer-Vault

The Integrated Streamer-Vault (ISV) server offers the functionality of both a Vault and Streamer in one server in either a 2U or 4U CDE.

The ISV server ingests content delivered over a standard interface, performs whatever processing is required, and stores the processed content reliably on disk. An ISV array consists of a scalable number of ISV servers that divide the responsibility for ingest, storage, and streaming among the members of the array.

Content Delivery System Manager

The Content Delivery System Manager (CDSM) is a browser-based user interface accessible by means of a web browser program and designed to manage a TV CDS network. The CDSM provides centralized management functions for the TV CDS, including configuration, monitoring, troubleshooting, reporting, and maintenance. The CDSM has three configuration and monitoring levels: system, array, and server. System-wide configuration affects all servers in the TV CDS. The array-level configuration affects all the servers of the specified array, and the server-level configuration applies changes to a specific server.

The CDSM offers a drill-down approach to find the status of any stream or ingest point, or the physical status of any piece of hardware.

The CDSM reporting helps operators manage all aspects of the TV CDS. Information on stream traffic, content statistics, and server data are gathered from all servers in the network and correlated automatically, showing at a glance the status of the network and reporting on statistics such as content popularity, stream usage, and bandwidth usage for each service group.

Figure 1-3 shows the system monitoring page of the CDSM.
Resiliency and Redundancy

The TV Content Delivery System is designed with no single point of failure. The TV Content Delivery System incorporates redundancy at several levels within the architecture. These levels of redundancy eliminate any customer impact from potential failures of Vault disks, Vault servers, Streamer disks, Streamer servers, ISV servers, Ethernet connections, processors, and power supplies.

Each server constantly monitors the state of its peers. The TV CDS unique resource pooling and auto-failover techniques allow all servers in the network to actively contribute to satisfying storage and streaming demand at all times. If a server fails, the load is instantaneously redistributed among the surviving servers, ensuring continuity of service.

Vault Disk Redundancy

The Vault server protects content through full 1:N redundancy. If a disk fails, the data is available from a redundant server, spreading the load and optimizing the bandwidth. Additionally, the regeneration of the redundant content utilizes the bandwidth of the whole Vault array rather than just the disk bandwidth available inside a particular server, significantly reducing the rebuild window. The need to replace the failed drive is not time critical in the least, making quarterly replacement of any failed Vault drives feasible.

Mirroring

The primary method to protect the content against loss due to hardware failure is mirroring. Content is stored on a Vault and, based on the policy, it is mirrored to other locations in the Vault array. The number of mirrored copies is configurable. There are two types of mirroring:

- Remote mirroring
- Local mirroring
When remote mirroring is used, copies of the content are mirrored to drives on other Vaults, based on the number of Vault mirror copies configured.

When local mirroring is used, copies of the content are mirrored across all the available drives on the same Vault, so that the content can be recovered from another drive if one of the drives fails.

Local mirroring is not turned on by default, and is generally only used when there is a single Vault in a system.

**Vault Server Resiliency**

The Cisco TV CDS can handle the loss of an entire Vault server without impacting the subscriber. The communication with the backoffice suite is performed by a Vault server, designated as the Vault master. If the Vault master fails, one of the remaining slave Vault servers in the Vault array transparently takes over as the master. The remaining Vaults detect the loss of a Vault server, run a check of all stored content, and regenerate redundant content that was affected by the lost Vault server. This regeneration runs in the background utilizing spare system bandwidth that is not consumed by subscriber load, resulting in the shortest possible regeneration window possible without compromising performance to the subscriber.

**Vault Master**

The Vault master, designated by a virtual IP address on its management interface, is used as the representative of the Vault array to the backoffice and handles the ingest of new content.

**Streamer Disk Redundancy**

The disks in the Streamer are not used for full content storage like most VOD implementations. Rather, the Streamer disks are part of the TV CDS multilevel caching architecture. If a disk is lost on a Streamer, the only impact is a marginal loss of caching capability for the system. Any content that was cached on that Streamer disk is retrieved again from the Vault. The RAM on the Streamer has enough content cached for streaming to the subscriber, so that this refetch of content from the Vault occurs without impacting the subscribers. For example, for a Streamer array of five Streamers with sixteen hard drives each, a lost drive only reduces the total caching capability by less than 1.25 percent. The need to replace the failed drive is not time critical in the least, making quarterly replacement of any failed Streamer drives feasible.

**Streamer Server Resiliency**

The Cisco TV CDS architecture allows for failed Streamer servers as well. If any Streamer server fails, the communication to the backoffice is transparently handed off to another Streamer. With the TV CDS software, if a Streamer server fails the other Streamers recognize that failure and continue streaming to that subscriber.

**Ethernet Link Resiliency**

All Ethernet links used within the Cisco TV CDS architecture incorporate link failure detection with automatic failover. This includes interconnection between the Vault array and the Streamer array for cache-fill, and the Ethernet links that carry the subscriber streams to the transport networks.
Scalability

The Cisco TV CDS has separated streaming and storage, which enables a cable operator to add storage without affecting streaming counts and conversely to add streaming without affecting storage. This flexibility allows cable operators to grow according to the needs of customers and to scale the system on an as-needed basis. For example, if more storage is required, the cable operator adds a Vault server without taking the system offline, and in Layer 2 networks the new device is automatically discovered within the architecture and the new resources are automatically utilized by the system. If additional streaming is required, the content provider either purchases more streaming licenses within the current servers, or a Streamer server is added to the system without taking the system offline.
Network Design

This chapter describes the different network topologies for the Cisco TV CDS, the different network connections of the CDS servers, the CDS workflow, and network configuration considerations. The topics covered in this chapter include:

- Overview, page 2-1
- TV CDS Topologies, page 2-2
- CDS Workflow, page 2-5
- BMS Considerations, page 2-6
- Network Connections, page 2-8

Overview

The TV CDS enables cable operators and multiple service operators (MSOs) to offer VOD and MediaX services to consumer customers over their existing hybrid fiber coaxial (HFC) network, with existing next-generation digital STBs. The TV CDS solution uses a Gigabit Ethernet (GE) transport network from the headend to the distribution hub, where the HFC network terminates.

TV CDS grows seamlessly from a single server implementation to multiple servers. As growth continues, TV CDS allows operators to install distributed servers to address concentrations of subscribers while leaving content ingest and management centralized.

Streamer arrays can be distributed close to the subscriber and linked back to the central Vault locations by way of the Cisco Cache Control Protocol (CCP). CCP automatically ensures that any new content that is required by a customer edge device is transferred within a maximum of a 250-millisecond delay to the appropriate edge location, so all content appears local to each edge site, even though most content is stored at the central Vault location.

The TV CDS offers different configurations with regards to network topology, business management systems (BMSs), and streaming modes.

CDS with Vaults and Streamers

In a TV CDS with Streamers and Vaults, MPEG-2 transport stream (TS) video is stored on the Vault servers with the associated trick mode files. Content is transported from the Vault servers to the Streamer servers as needed, by using CCP over Gigabit Ethernet networks. Content is sent unicast from the
Streamers and delivered to the quadrature amplitude modulation (QAM) devices over Gigabit Ethernet or asynchronous serial interface (ASI), and then modulated onto the HFC plant to the subscriber’s set-top box (STB) for viewing.

CDS with ISVs

For the smallest networks, Cisco packages its solution in a single server, the Integrated Streamer-Vault (ISV), offering solutions for VOD services with large content libraries but small stream counts.

In a TV CDS with ISVs, MPEG-2 TS video is stored on the ISV servers with the associated trick mode files. Content is sent unicast from the ISV servers and delivered to the QAM devices over a Gigabit Ethernet network, and then modulated onto the HFC plant to the subscriber’s STB for viewing.

TV CDS Topologies

The TV CDS, using Vaults and Streamers, supports centralized, decentralized, and hybrid Gigabit Ethernet network designs. Because the use of Vaults and Streamers separates storage from streaming, streaming requirements can be satisfied on an “as needed” basis and the streaming can be centralized or distributed among multiple locations. The TV CDS topology can change with the evolving needs of the system operator. If the need to decentralize becomes evident, you can move the Streamers or Vaults to remote hubs without service disruption.

Caution

All Cisco servers are connected through a switch. Because all Vault and Streamer servers in the same array exchange heartbeat messages through the cache interfaces, it is important to ensure there is enough bandwidth among switches involved in delivering cache traffic, as well as to support the same aggregated amount of traffic on all cache interfaces.

Note

When using ISVs, with the Vault and Streamer functions contained in one server, the only topology possible is centralized.

Centralized Topology

In a centralized topology, both Vault and Streamer servers are located in either a single video headend or a remote hub. This is the right solution for certain situations, for instance very small starting systems or where a large amount of bandwidth is available. A centralized topology has advantages in reducing operational cost by placing equipment in one physical location. Figure 2-1 illustrates the centralized topology for Vaults and Streamers.
Chapter 2  Network Design

TV CDS Topologies

Figure 2-1  Centralized Topology with Vaults and Streamers

Figure 2-2 illustrates the centralized topology for ISVs.

Figure 2-2  Centralized Topology with ISVs

Decentralized Topology

The decentralized topology is a hub-and-spoke topology between the headend site and multiple hub sites, where the Vault servers are located at the headend and the Streamer servers are in the hub sites. The decentralized topology works well for distributing Streamer arrays close to subscribers. A decentralized topology has advantages in reducing the amount of long-haul fiber transport bandwidth needed—typically by a factor of ten or better. Figure 2-3 illustrates the decentralized topology.
Hybrid Topology

In a hybrid topology, the Vault servers and backup Streamer servers are located at the headend, with the active Streamers at a remote hub site. If the remote hub site goes down, the Streamers at the headend take over. A hybrid topology blends the advantages of centralized and decentralized topologies based on needs of the system implemented. Figure 2-4 illustrates the hybrid topology.
CDS Workflow

Content is ingested and stored on the Vault array. The Vault array consists of two or more Vault servers that are collocated or distributed to multiple locations across an Ethernet network. Content ingest is initiated by the backoffice based on a subscriber request, and based on schedule or Barker channel content. Manual ingest, which is operator initiated, is also offered as an optional feature.

Once the content is ingested into the Vault, any necessary trick mode files are created. The content and trick mode files are then mirrored within the same Vault or across the Vault array. The replication of content allows for data recovery should the system undergo a failure.

Content is delivered from the Vault array to the Streamer array in response to cache-fill calls from the Streamers in order to fulfill subscriber requests for VOD content. Content is also distributed across the network in response to scheduled or Barker stream content fulfillment.

Within the Streamer array are one or more Stream Groups. The following section describes how the Stream Groups deliver streams to the subscriber STBs.

Note: All servers can be on different subnetworks. However, given current backoffice restrictions, the externalized IP address is constrained to migrate among servers on the same subnetwork. This means the content store server in an Interactive Services Architecture (ISA) environment can migrate only among Vaults that are on the same subnet, and the Setup and Control servers can migrate only among Streamers on the same subnet.

Streamer Workflow

A Stream Group is a configurable group of Streamers that are designated to serve specified QAM devices, and subsequently, specific service groups. From a session setup and control perspective, there are three logical types of servers in a Stream Group:

- Setup server
- Control server
- Play server

The Setup and Control servers have both a primary and a backup server. The primary server services all messages, while the backup server simply maintains states. If a primary server is unreachable, the backup server takes over control and creates another backup server. Thus, there is always a primary and backup pair of servers for setup and control. The Play server does not have a backup server. However, the Control server selects a new Play server in the event of a failure of the existing Play server.

Note: The ability to have both a primary and backup server depends on the number of Streamers in the Stream Group.

The Setup and Control server IP addresses are configurable. For an ISA environment, the Setup IP address is the same as the Stream Master IP address. The Stream Service selects a Streamer in the Stream Group to be the Setup server, and another Streamer (sometimes the same Streamer) to be the Control server.
## Setup Server

A Streamer designated as the Setup server interfaces with the backoffice and forwards the setup messages to the appropriate Stream Group that is assigned to the destination service group. One Streamer in the Stream Group that is collocated with the backoffice server is assigned as the primary Setup server. The Setup server receives the setup request from the backoffice and maps the service group. The Setup server returns the IP address of the Control server, and the STB issues subsequent control messages to the IP address of the Control server.

## Control Server

The Control server assigns requests to specific Streamers and dynamically migrates streams between Streamers based upon changes in stream states (for example, content splice boundaries, maintenance trickle down, or server failures). One server in the Stream Group is assigned as the primary Control server. The Control server runs the Lightweight Stream Control Protocol (LSCP) proxy in an Interactive Services Architecture (ISA) environment and the Real-Time Streaming Protocol (RTSP) proxy in an RTSP environment.

For each and every setup message received from the backoffice, a CCP message is generated and sent to the Control server. In the initial setup request, the Control server receives the setup parameters but does not choose a Play server. Once a control message is received from the STB, the Control server gets performance information (for example, server load) from the potential Play servers within the Stream Group and sends a CCP message to the best candidate. Subsequent control messages, whether from the STB or from the Setup server, are forwarded to the chosen Play server.

## Play Server

The Playserver is the Streamer that is assigned to play the stream. This Streamer acquires the content, whether in RAM, a local disk, or a Vault, and ensures guaranteed service delivery of the stream. Every Streamer in a Stream Group is a possible candidate to be the Play server.

## BMS Considerations

The TV CDS integrates with Interactive Services Architecture (ISA) used in business management systems (BMSs) such as Tandberg OpenStream and the RTSP used in BMSs such as ARRIS nABLE, as well as in environments that are a combination of both ISA and RTSP. The BMS determines the roles and responsibilities of the TV CDS.

## OpenStream ISA Integration

The OpenStream BMS is built on Common Object Request Broker Architecture (CORBA) and provides naming and notification services. The Naming Service allows the TV CDS to locate objects in the system such as content, equipment, assets, and so on. The Notification Service allows the TV CDS to listen for important events in the system as well as send events to the OpenStream BMS and other components in the system.

Figure 2-5 illustrates how the TV CDS integrates with the OpenStream BMS.
Streaming Mode

OpenStream uses a session-based approach to handle resource requirements and allocation. In the course of setting up a session, a QAM device is specified that has available capacity and connectivity to the Cisco Streamer and the STB requesting the service. Typically, the Session and Resource Manager (SRM) is responsible for the allocation of network resources. OpenStream uses the Digital Storage Media-Command and Control (DSM-CC) session management protocol to request resources from the SRM.

When using Gigabit Ethernet for streaming, OpenStream communicates with the SRM to negotiate network resources and allocation for sessions.

When using Asynchronous Serial Interface (ASI) for streaming, the Cisco Streamer performs the role of the SRM by managing and allocating the access network resources and providing this information to the OpenStream BMS.

nABLE Integration

The nABLE BMS uses a combination of eXtensible Markup Language (XML) over Hypertext Transfer Protocol (HTTP) and Real-Time Streaming Protocol (RTSP) for communication between nABLE Headquarters (HQ) and Real-time (RT) components and the CDS. The HQ communicates file-related requests by using XML/HTTP to the Vault server, as well as server status information requests to both the Streamer and Vault servers. The RT communicates with the Streamer server by way of RTSP to establish session setups for multiple, interchangeable VOD flows (RTSP or DSM-CC).

Currently, configuring the CDS for integration with the nABLE BMS is performed by Cisco field engineers. For more information on integration of the CDS with the nABLE BMS, contact the Cisco technical support department.

Figure 2-6 illustrates how the CDS integrates with the nABLE BMS.
Network Connections

The network connections for a TV CDS with Vaults and Streamers differ from the network connections for a TV CDS with ISVs. Table 2-1 lists the different interfaces for each CDS server. The interfaces are described in the following sections. Figure 2-7 illustrates a TV CDS with Vaults and Streamers. Figure 2-8 illustrates a TV CDS with ISVs.

**Table 2-1 CDS Interfaces**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vault</th>
<th>Streamer</th>
<th>ISV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Ingest</td>
<td>1</td>
<td>—</td>
<td>1</td>
</tr>
<tr>
<td>Cache</td>
<td>1 to 8</td>
<td>1 to 13</td>
<td>—</td>
</tr>
<tr>
<td>Stream</td>
<td>—</td>
<td>1 to 13</td>
<td>1 to 8</td>
</tr>
</tbody>
</table>

Figure 2-7 shows the different logical networks of a CDS consisting of Vaults and Streamers. The ingest network receives content from the content source by way of an FTP staging server or FTP catcher where it is ingested by the Vaults. The management network consists of communication between the CDSM and the BMS, as well as communication to the Vaults, Streamers QAM devices, and STBs. The cache network consists of Vaults and Streamers.
Figure 2-7  Vault and Streamer Network Connections

Figure 2-8 shows the different logical networks of a CDS consisting of ISVs. The ingest network receives content from the content source by way of an FTP staging server or FTP catcher where it is ingested by the ISVs. The management network consists of communication between the CDSM and BMS, as well as communication to the ISVs, QAM devices, and STBs.

Figure 2-8  ISV Network Connections
Ingest Interface

The ingest interface takes in FTP traffic from the content provider at a maximum rate of one gigabit per second. After the Vault server receives URL information about the content from the BMS by using the management interface, the ingest interface either (1) receives FTP traffic by acting as an FTP client, or (2) receives live data upon receiving a request to act as the FTP server.

In order to segregate all ingest traffic through the switching fabric, we recommend the use of a port-based VLAN when using Layer 2 packet forwarding.

Management Interface

The management interface communicates with the network management system (NMS) by way of SNMP, the BMS by way of ISA commands and also RTSP, and with all Vault and Streamer servers in the same array. Information shared among servers in the same array includes the following:

- Host service information
- Domain Name System (DNS) service information
- QAM gateway information
- All ISA information

Management traffic is low volume; however, we recommend using a port-based VLAN to ensure delivery of critical management communications when using Layer 2 packet forwarding.

Cache Interfaces

The CCP uses the cache interfaces on the Vault and Streamer servers to transmit the following data among servers in the same array:

- Content sent to the Streamer servers
- Content mirrored among the Vault servers
- Messages containing information used for performance optimization exchanged among all the servers

Note

All Cisco servers are connected through a switch fabric. Because all Vault and Streamer servers in the same array exchange heartbeat messages through the cache interfaces, it is important to ensure there is enough bandwidth among switches involved in delivering cache traffic and to support the same aggregated amount of traffic on all cache interfaces.

We recommend the use of a port-based VLAN when using Layer 2 packet forwarding for cache traffic.

Cache/Stream Interfaces

The cache/stream interfaces on the Streamer server can be used for both cache and streaming traffic. The number of interfaces designated for each traffic type is configurable. If an interface is configured for both cache and streaming traffic, priority is given to the higher bandwidth stream traffic provided cache traffic is able to transmit on other interfaces.
We recommend the use of a port-based VLAN when using Layer 2 packet forwarding for cache and stream traffic.

**Streaming Interface**

The streaming interface delivers streaming traffic consisting of MPEG-2 TS transport streams to STBs by way of QAM devices.

If an interface is configured for both stream and cache traffic, and the jumbo frames feature is not enabled for stream traffic while jumbo frames is enabled for cache traffic, stream traffic uses 1500-byte packets while cache traffic uses jumbo frames.
Getting Started

This chapter provides information on configuring the TV CDS servers. The topics covered in this chapter include:

- Initially Configuring the Devices, page 3-1
- Logging In to the TV CDSM, page 3-2
- Initializing the CDS and Activating the Optional Features, page 3-3
- Navigating the CDSM, page 3-4
- Configuration Workflows, page 3-5

This chapter assumes the CDS servers are already installed and takes you through the next steps towards configuring and monitoring the CDS.

Initially Configuring the Devices

You must initially configure the Content Delivery Engines (CDEs) before they can participate in the CDS network. The CDE that runs the TV Content Delivery System Manager (CDSM) must be initialized first so that the CDEs running the Streamers and Vaults, or the ISVs can communicate with it. For more information about initially configuring the CDEs, see the Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide or the Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide. See the “Related Documentation” section on page xiv for links to the documentation at www.cisco.com.

Initial configuration of your CDEs includes a set of basic network configuration settings to provide connectivity to the CDSM. Once the CDEs are configured with these settings you can use the CDSM to configure and manage all the servers in the CDS.

After you have initially configured your CDEs, you must initially set up your CDS and activate any optional features. See the “Initializing the CDS and Activating the Optional Features” section on page 3-3 for more information.
Logging In to the TV CDSM

To log in to the TV CDSM, do the following:

**Step 1**  
Using your web browser, enter the IP address or hostname of your CDSM.  
For example, if the IP address of your CDSM is 192.168.0.236, you can access it by entering http://192.168.0.236 in the address or location text box of your browser program.

*Note* Consult your as-built documentation for the IP address of the CDSM.

The System Login page is displayed, as shown in Figure 3-1.

**Figure 3-1 System Login Page**

![System Login Page](image)

*Note* The CDSM supports Microsoft Internet Explorer version 6 or higher.

**Step 2**  
Enter your user name and password and click Log In.  
The built-in user name is admin and the initial password is admin.

*Note* We strongly recommend that you change the built-in user password as soon as possible. See the “Editing User Settings” section on page 7-3 for more information.

*Tip*  
To navigate within the CDSM, click one of the navigation bar options (for example, Maintain), then one of the tab options (for example, Users), and then one of the left-panel menu options (for example, Add Users). Navigational directions in procedures are written in the following way:  
Maintain > Users > Add Users
Logging Out

To log out of the CDSM from any page, click **Logout** at the upper-right part of the page. See Figure 3-2.

![Figure 3-2 Logging Out](image)

Initializing the CDS and Activating the Optional Features

Initial configuration of your CDS includes selecting the CServer version, the installation type, and other parameters that must be configured before you can continue the configuration process.

If the Media Scheduler or Ingest Manager are part of your deployment, you need to activate these features.

To initialize your CDS or activate the Media Scheduler and Ingest Manager, do the following:

**Step 1** Log in to the CDSM as **admin**, or use another user account that has master access.

**Step 2** Add a user with engineering access.
   a. Choose **Maintain > User > Add Users**. The Add Users page is displayed.
   b. In the **New User** and **Password** fields, enter the user name and password for this account.
   c. From the **Access** drop-down list, choose Engineering.
   d. Click **Add User**.

**Step 3** Log out of the CDSM, and log in as the user with the engineering access level that you specified in **Step 2**. The CDSM Setup page is displayed.

**Step 4** Select the options for your deployment and click **Submit**. For more information about the fields on this page, see the “CDSM Setup” section on page C-2.

**Step 5** Scroll down to the Media Scheduler section, and choose the **ON** radio button next to the **Media Scheduler** field.

**Step 6** In the **Activation Key** field, enter the software access key from your Right to Use Notification for the Content Delivery Application Media Scheduler (CDAMS) product.

**Step 7** In the **Importer/Transformer Type** field, choose either OCN or SA Tribune. The Importer/Transformer Type specifies the expected EPG format, the fields for the Input Channels page, and the expected ADI metadata.

**Step 8** Scroll down to the Ingest Manager section, and choose the **ON** radio button next to the Ingest Manager field.

**Step 9** In the **Activation Key** field, enter the software access key from your Right to Use Notification for the Content Delivery Application Ingest Manager (CDAIM) product.

**Step 10** Click **Submit**.
Navigating the CDSM

The CDSM pages consist of the elements illustrated in Figure 3-3.

Figure 3-3  CDSM User Interface

1. Left panel menu
2. Tabs
3. Tab options
4. Page title
5. Main panel
6. Tools (Home, Help, and, Logout)

The tabs are accessible from any page in the CDSM. The tab options are used to select the applicable level. In the Configure and Monitor pages, the tab option selected determines whether the configuration or monitoring applies to the system as a whole, the array level, or a specific server.

Using Online Help

Online help is available in the CDSM. You can use it by clicking on the Help button in the upper-right corner of any of the pages. Context-sensitive help is provided for the page you are viewing.

Step 11  Log out of the CDSM.
The CDSM offers several levels of help:

- Each page of the CDSM includes some basic Help, normally displayed in the main panel.
- The Help button displays context-sensitive help presented in a separate browser window. The content of this page is different depending on the page of the CDSM you are viewing when you click Help. Once inside the help system you can move around to view different topics by using a variety of navigation tools:
  - Back/forward page buttons
  - Links within the page contents
  - Table of Contents, accessed through the navigation panel at the left of the page.
  - Show the Table of Contents by clicking the Contents icon.
  - Print the page you are viewing by clicking the Print icon.
- From the Help window, you can display the full Cisco TV CDS 2.0 RTSP Software Configuration Guide by clicking the View PDF button.

## Configuration Workflows

Once you have completed the initial installation and configuration of the CDEs for the CDS and you have verified connectivity to the CDSM, you are ready to configure the CDS for content delivery.

Table 3-1 lists the basic tasks, in the recommended order, for configuring the CDS for content delivery with references to the associated sections in each chapter.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change admin</td>
<td>Change the administrator password for the CDSM.</td>
<td>“Editing User Settings,” page 7-3</td>
</tr>
<tr>
<td>password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface Setup</td>
<td>Configure the different interfaces on the CDS servers.</td>
<td>“Configuring the Interfaces,” page 4-39</td>
</tr>
<tr>
<td>Transport Groups</td>
<td>Transport Groups identify destination subnetworks for stream traffic.</td>
<td>“Configuring Transport Groups,” page 4-23</td>
</tr>
<tr>
<td>Server Setup</td>
<td>Configure the IP addresses and ports for the interfaces, as well as other</td>
<td>“Configuring the Servers,” page 4-41</td>
</tr>
<tr>
<td></td>
<td>settings such as quality of service (QoS).</td>
<td></td>
</tr>
<tr>
<td>Stream Groups</td>
<td>A Stream Group consists of one or more Streamers. Stream Groups relate to</td>
<td>“Configuring Stream Groups,” page 4-27</td>
</tr>
<tr>
<td></td>
<td>QAM gateways or destination subnetwork by the Stream Group preference.</td>
<td></td>
</tr>
<tr>
<td>Control and Setup</td>
<td>Configure the Control server and Setup server IP address for the Stream</td>
<td>“Configuring the Control and Setup IPs,” page 4-29</td>
</tr>
<tr>
<td>IPs</td>
<td>Groups.</td>
<td></td>
</tr>
<tr>
<td>QAM Gateways</td>
<td>Configure the QAM Gateways for the CDS.</td>
<td>“Configuring QAM Gateways,” page 4-6</td>
</tr>
</tbody>
</table>
Chapter 3      Getting Started

Configuration Workflows

The other configuration settings, DNS settings, and so on, can be configured in any order.

**TV MediaX Configuration Workflow**

Table 3-2 lists the basic tasks for configuring the TV MediaX Suite CDA with references to the associated sections in each chapter.

### Table 3-2  **TV MediaX Configuration Workflow**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the data feed import type used to populate the Media Scheduler, and the transformer type used to process the ADI metadata.</td>
<td>“Configuring Input Channels” section on page 4-21</td>
<td></td>
</tr>
<tr>
<td>Map each channel to a multicast group IP address and port, and specify the settings for every program in the channel.</td>
<td>“Configuring Input Channels” section on page 4-21</td>
<td></td>
</tr>
<tr>
<td>Upload an EPG file. During the upload process, the EPG file is parsed into database records that in turn populates the Media Scheduler.</td>
<td>“Uploading an EPG File” section on page 7-14</td>
<td></td>
</tr>
</tbody>
</table>
| Schedule the ingest of content. The Media Scheduler does three things:  
1. Values from the EPG file are combined with the values from the Input Channels page, and the ADI metadata XML file is created.  
2. The database records are marked according to the Media Scheduler settings (scheduled, unscheduled, marked for scheduling, and so on).  
3. The ADI metadata is published to the backoffice. | “Configuring the Media Scheduler” section on page 4-31 |
Configuring the CDS

This chapter provides information on configuring the CDS servers. The topics covered in this chapter include:

- **System Level Configuration**, page 4-1
- **Array Level Configuration**, page 4-25
- **Server Level Configuration**, page 4-39

### System Level Configuration

The System Level tab has the following configuration options:

- Configuring DNS Services
- Configuring the Hosts Service
- Configuring the Array Name
- Configuring QAM Gateways
- Configuring the Headend Setup
- Configuring the Bandwidth Manager
- Configuring the Ingest Manager
- Configuring the Authentication Manager
- Configuring Ingest Tuning
- Configuring IP Nicknames
- Configuring the Media Importer/Exporter
- Configuring Call Signs
- Configuring Input Channels
- Configuring Transport Groups

**Note**

The System Level configuration settings are distributed to all arrays and servers in the CDS.
Configuring DNS Services

The DNS page is used to configure the DNS services on the network.

⚠️ Caution
If you have individual DNS settings configured for an array or server and you change the System Level DNS settings, the individual DNS settings are overwritten. Therefore, first configure the System Level settings, then if necessary, Array Level settings, and finally Server Level settings.

To view the current DNS System Level settings, click Configure from any page in the CDSM.

To configure the DNS service settings, do the following:

**Step 1** Choose Configure > System Level > DNS. The DNS System Level page is displayed (Figure 4-1).

![Figure 4-1 DNS System Level Page](image)

**Step 2** Enter the DNS system level settings as appropriate. See Table 4-1 for descriptions of the fields.
Step 3

Click **Submit**.

To clear the fields and start over, click **Reset**.

To delete the DNS settings, check the **Delete** check box and click **Submit**.

---

### Configuring the Hosts Service

The Host Service page offers the option to enter a hostname and associated IP address as an alternative or backup to the DNS service. The system searches the host service table before the DNS services. The host service settings are considered an alternative or backup to the DNS service.

To view the current host service settings, Choose **Configure > Host Service**. The hostnames currently configured are listed at the bottom of the page.

To configure the host service settings, do the following:

**Step 1** Choose **Configure > Host Service**. The Host Service page is displayed (*Figure 4-2*).
Figure 4-2 Host Service Page

Step 2 Enter the host service settings as appropriate. See Table 4-2 for descriptions of the fields.

Table 4-2 Host Service Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>A hostname of no more than 64 characters. Assigning hostnames is optional. The hostname does not have to be a fully-qualified domain name.</td>
</tr>
<tr>
<td>Host IP Address</td>
<td>The IP address associated with the hostname.</td>
</tr>
</tbody>
</table>

Step 3 Click Submit. The new entry is added to the host table located at the bottom of the page.

To clear the fields and start over, click Reset.

Step 4 To add more hostnames to the host table, repeat Step 2 and Step 3.

To delete a host table entry, check the Delete check box associated with the entry and click Delete. To clear the Delete check boxes, click Reset.
Configuring the Array Name

The Array Name page is used to define Vault arrays, Streamer arrays, or ISV arrays. For more information about arrays, see the “Content Delivery System Architecture” section on page 1-4.

**Note**
Currently the CDSM allows only for the creation of one Vault array.

To view the current Array Name listings, Choose **Configure > Array Name**. The array names currently configured are listed.

To configure an array name setting, do the following:

**Step 1** Choose **Configure > Array Name**. The Array Name page is displayed (Figure 4-3).

**Figure 4-3 **Array Name Page

![Array Name Page](image)

**Step 2** Enter the array name that is used to identify the group of servers.
To reset the field, click **Reset**.

**Step 3** Click **Submit**.
Configuring QAM Gateways

The QAM Gateway page is used to identify the QAM Gateway devices and the association between the Streamers and QAM device. A QAM gateway is typically a Layer 3 device.

A QAM gateway is a device that sits between a Streamer and a QAM modulator. Depending on the design of your network, a QAM gateway is a Layer 3 routing device, Gigabit Quadrature Amplitude Modulation (GQAM), Narrowband Services Gateway (NSG), Path1, or similar device.

Single-site steering is supported in Release 2.0 for an RTSP environment. Single-site steering uses only one Stream Group to serve streams to a QAM device.

Note
Single-site steering assumes all Streamers in a Stream Group are located at the same geographical site.

With single-site steering, you are given the option to set a Stream Group to “high” or “none.” Only one Stream Group can be set to “high,” all others are set to “none.” In a CDS network with single-site steering, if one Streamer in the Stream Group that is serving streams to a QAM device fails, another Streamer in the same group takes over.

ARP

The Address Resolution Protocol (ARP) is the method for finding a host’s MAC address when only its IP address is known. The QAM Gateway page allows you to specify the MAC address of an IP gateway. There are three reasons you may want to do this:

1. To statically configure the MAC address of an IP gateway.
2. ARP is disabled on the QAM gateway.
3. To statically configure all devices on the network in order to have all packets go to a specific IP gateway.

For single-site steering, the QAM Gateway page allows you to specify the MAC address of the IP gateway when you enter the IP address of the QAM gateway. All streams from the Stream Group with a high preference route to the IP gateway specified.

Note
We recommend you leave all QAM MAC settings blank and allow ARP to determine the MAC address of the next Layer 3 device connected to the Streamer. To specify the next Layer 3 device, see the “Configuring the Route Table” section on page 4-47.

To view the current configuration for a QAM gateway, Choose Configure > QAM Gateway, choose the QAM IP address from the drop-down list, and click Next.

To configure a QAM gateway, do the following:

Step 1 Choose Configure > QAM Gateway. The QAM Gateway page is displayed (Figure 4-4).
Step 2 From the drop-down list, choose enter new and click Next.
Step 3  Enter the QAM gateway settings as appropriate. See Table 4-3 for descriptions of the fields.

### Table 4-3  QAM Gateway Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QAM IP</td>
<td>The IP address of the QAM gateway.</td>
</tr>
<tr>
<td>QAM MAC</td>
<td>The MAC address of the next Layer 3 device connected to the Streamer in the path to the QAM modulator. The MAC address can be entered with or without the colon separators. We recommend you leave the QAM MAC setting blank and allow ARP to determine the MAC address of the next Layer 3 device. To specify the next Layer 3 device, see the “Configuring the Route Table” section on page 4-47.</td>
</tr>
</tbody>
</table>
| Stream Group Preferences | Select the preference for each Stream Group. The preferences are:  
  - High—First preference of Streamer or Stream Group to stream to this QAM.  
  - None—Do not use this Streamer or Stream Group to stream to this QAM.  
For more information on creating Stream Groups, see the “Configuring Stream Groups” section on page 4-27. |

Step 4  Click Submit.
To reset the fields, click Reset.

To edit a QAM gateway, select the QAM IP address and click Next. Enter the new settings and click Submit.
To delete a QAM gateway, select the QAM IP address, click **Next**, and then click **Delete QAM**.

### Configuring the Headend Setup

**Note**
The Headend Setup page is an optional feature for the RTSP environment and is used for associating service groups with Stream Groups.

The Headend Setup page offers more granularity than the QAM Gateway page. The QAM Gateway page allows you to assign preference to which Stream Groups serve which QAM Gateways. The Headend Setup page allows you to assign preference to which Stream Groups serve which service group.

**Note**
You must first configure the Stream Groups before you can configure the headend setup for a specific service group. See the “Configuring Stream Groups” section on page 4-27.

**Note**
Any changes to the headend setup requires a reload of the service groups. See the “Restarting the Services” section on page 7-11 for more information.

To configure the headend setup, do the following:

**Step 1** Choose **Configure > Headend Setup**. The Headend Setup page is displayed (Figure 4-5).

**Figure 4-5  Headend Setup Page**

![Headend Setup Page](image)

**Step 2** From the **Select Service Group** drop-down list, choose **Add New**.

**Step 3** In the **New Service Group** field, enter the service group name.

**Step 4** Select the preference for each Stream Group. The preferences are:
• High—First preference of Streamer or Stream Group to stream to this service group.
• Medium—Second preference of Streamer or Stream Group to stream to this service group.
• Low—Lowest preference of Streamer or Stream Group to stream to this service group.
• None—Do not use this Streamer or Stream Group to stream to this service group.

For more information on creating Stream Groups, see the “Configuring Stream Groups” section on page 4-27.

Step 5 Click Submit.

To delete a service group, select it from the Select Service Group drop-down list and click Delete.

Configuring the Bandwidth Manager

The Bandwidth Manager runs on the master Streamer and keeps track of allocated streams and VOD network resources.

Note

The Bandwidth Manager is not listed on the System Level left-panel menu if this optional feature is not included in your deployment.

To configure the Bandwidth Manager, do the following:

Step 1 Choose Configure > Bandwidth Manager. The Bandwidth Manager page is displayed (Figure 4-6).

Figure 4-6 Bandwidth Manager Page

Step 2 Enter the Bandwidth Manager settings as appropriate. See Table 4-4 for descriptions of the fields.
Chapter 4      Configuring the CDS

System Level Configuration

Table 4-4        Bandwidth Manager Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Manager IP(^1)</td>
<td>The IP address of the network interface card (NIC) you want the Bandwidth Manager to bind to. Valid entry includes an asterisk (*) and 0.0.0.0, which signifies the Bandwidth Manager IP is set individually for each Streamer on the RTSP Setup page. See the “Configuring RTSP Setup” section on page 4-52 for more information.</td>
</tr>
<tr>
<td>Bandwidth Manager Port(^*)</td>
<td>The port number to listen on for incoming connections from the RTSP server. The default is 7791. The lowest port number you can allocate is 150. The highest port number is 60000.</td>
</tr>
<tr>
<td>Database Thread Pool</td>
<td>The number of threads in the database connection pool. The default is 10. The minimum number of database threads is 1; the maximum is 100.</td>
</tr>
<tr>
<td>Server Thread Pool</td>
<td>The number of threads in the Bandwidth Manager server pool that are used to process RTSP requests for the duration of the connection. The default is 5. The minimum number of server thread pools is 1; the maximum is 100.</td>
</tr>
<tr>
<td>Sync Thread Pool</td>
<td>The number of threads available to synchronize sessions with the RTSP during a synchronization operation. The default is 2. The minimum number of synchronization thread pools is 2; the maximum is 50.</td>
</tr>
<tr>
<td>Sync Alarm</td>
<td>How often the synchronization alarm is triggered. The default is 864,000 seconds (10 days). The minimum amount of time the synchronization alarm trigger can be set to is 2400 seconds (40 minutes). The maximum amount of time is 4,294,967,296 (over 136 years).</td>
</tr>
</tbody>
</table>

1. Changes to this field affect the same field on the RTSP Setup page.

Step 3    Click Submit.
To clear the settings, click Reset.

Step 4    Reload the Bandwidth Manager service.
  a. Choose Maintain > Services. The Services Restart page is displayed.
  b. From the drop-down list, choose the IP address or nickname of the server and click Display.
  c. Check the Reload Bandwidth Manager check box and click Submit.
     To clear the fields and start over, click Reset.

Configuring the Ingest Manager

The Ingest Manager takes care of provisioned content objects by collecting the metadata, sending messages to the appropriate subsystem to ingest the content, and sending messages to expire the content when the expiration period is past.

Note
The Ingest Manager is an optional feature. The Ingest Manager is not listed on the System Level left-panel menu if it is not included in your deployment.
To configure the Ingest Manager, do the following:

**Step 1** Choose **Configure > Ingest Manager**. The Ingest Manager page is displayed (Figure 4-7).

*Figure 4-7  Ingest Manager Page*
Step 2 Enter the Ingest Manager settings as appropriate. See Table 4-5 for descriptions of the fields.

**Table 4-5 Ingest Manager Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Ingest Manager Host</td>
<td>The Ingest Manager listener binds to this IP address. Enter an asterisk (*) if you want to listen to all IP addresses on the system.</td>
</tr>
<tr>
<td>Ingest Manager Port</td>
<td>The port number to use for listening for inbound connections.</td>
</tr>
<tr>
<td>Callback Port</td>
<td>The port number to use for File Services Interface (FSI) callbacks.</td>
</tr>
<tr>
<td>Additional Package Window</td>
<td>The additional time to wait once the package expiration window has been reached before destroying the content.</td>
</tr>
<tr>
<td>FTP Timeout</td>
<td>The maximum period (in seconds) the Ingest Manager waits before timing out an FTP session and terminating the process.</td>
</tr>
<tr>
<td>Use Asset ID</td>
<td>Choose <strong>Yes</strong> to use the Asset ID for the content name, otherwise choose <strong>No</strong>. The recommended setting is “no.” If set to “no,” the Ingest Manager uses the *.mpg as the content name when used in combination with the Media Scheduler.</td>
</tr>
<tr>
<td>Manage CORBA Services</td>
<td>Choose <strong>Yes</strong> to have the CDS manage the CORBA services, otherwise choose <strong>No</strong>.</td>
</tr>
<tr>
<td>Require Notify Service</td>
<td>Choose “<strong>Yes</strong>” to have the CDS require the use of the Notify Service, otherwise choose <strong>No</strong>.</td>
</tr>
<tr>
<td>Ingest Manager Debug</td>
<td>Choose <strong>Off</strong> to have the debug logging turned off. Choose <strong>Low</strong> to have minimal information and error logging. Choose <strong>Full</strong> for full debug logging information.</td>
</tr>
<tr>
<td>Meta Data Publish</td>
<td>Choose <strong>Enable</strong> from the drop-down list to publish the content metadata, otherwise choose <strong>Disable</strong>.</td>
</tr>
<tr>
<td>Meta Publish URL #1</td>
<td>The URL where the metadata is published, typically the backoffice.</td>
</tr>
<tr>
<td>Meta Publish URL #2</td>
<td>The URL of the backup server where the metadata is published.</td>
</tr>
<tr>
<td><strong>Ingest Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Ingest Interface</td>
<td>Choose all the ingest interfaces that apply: <strong>ISA, Cisco SOAP, Prodis SOAP</strong>; otherwise choose <strong>Disable</strong> to disable the Ingest Manager.</td>
</tr>
<tr>
<td>Name Service IP and Port</td>
<td>The IP address and port of the CORBA Naming Service used by the backoffice. ISA-only field.</td>
</tr>
<tr>
<td>Notify Service IP and Port</td>
<td>The IP address and port of the CORBA Notification Service used by the backoffice. ISA-only field.</td>
</tr>
<tr>
<td>Notify Service Factory</td>
<td>The name used to locate the Notify Service through corbaloc protocol. The default name used is NotifyEventChannelFactory. ISA only-field.</td>
</tr>
<tr>
<td>Event Channel ID</td>
<td>A simple name that identifies the root directory of the Event Channel where all event channels need to register. The default is EventChannels. ISA-only field.</td>
</tr>
<tr>
<td>Event Channel Kind</td>
<td>The directory extension of the Event Channel ID. The default is Context. ISA-only field.</td>
</tr>
<tr>
<td>Factories ID</td>
<td>A simple name that identifies the root directory of the factories where all factories need to register. The default is Factories. ISA-only field.</td>
</tr>
</tbody>
</table>
### Table 4-5  Ingest Manager Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factories Kind</td>
<td>The Factories ID extension. The default is Context. ISA-only field.</td>
</tr>
<tr>
<td>Package Channel ID</td>
<td>A simple name that identifies the Package Event Channel where all events concerning package objects are published. The default is PackageChannel. ISA-only field.</td>
</tr>
<tr>
<td>Package Channel Kind</td>
<td>The Event Channel Package ID extension. The default is Factory. ISA-only field.</td>
</tr>
<tr>
<td>Package Factory ID</td>
<td>A simple name that identifies the root directory of the factories where all factories need to register. The default is PackageFactory. ISA-only field.</td>
</tr>
<tr>
<td>Package Factory Kind</td>
<td>The Factories ID extension. The default is Factory. ISA-only field.</td>
</tr>
<tr>
<td>Package Factory Name</td>
<td>The name of the Package Factory that will be registered with the backoffice. The default is AVS_PackageFactory. ISA-only field.</td>
</tr>
<tr>
<td>Package Factory Server ID</td>
<td>The numeric value that identifies the Package Factory Server for all ingest. The default is 90. ISA-only field.</td>
</tr>
<tr>
<td>Cisco SOAP URL</td>
<td>The IP address, port, and directory on the Vault used to receive content using the Cisco SOAP (Simple Object Access Protocol). You can specify the IP address and port number, but the directory must be “CiscoAIM.” An example of the Cisco SOAP URL is <a href="http://10.22.216.251:8793/CiscoAIM">http://10.22.216.251:8793/CiscoAIM</a>.</td>
</tr>
<tr>
<td>Prodis SOAP URL</td>
<td>The IP address, port, and directory on the Vault used to receive content using the Prodis SOAP. You can specify the IP address and port number, but the directory must be “ProdisAIM.” An example of the Prodis SOAP URL is <a href="http://10.22.216.251:8793/ProdisAIM">http://10.22.216.251:8793/ProdisAIM</a>.</td>
</tr>
</tbody>
</table>

### Backoffice Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Retries</td>
<td>The maximum number of times to retry a failed communication with the backoffice. The range is 0–1000. The default is 10.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>The amount of time (in minutes) to wait before retrying a failed communication. The range is 0–10080. The default is 10.</td>
</tr>
<tr>
<td>Backoffice Timeout</td>
<td>The amount of time (in seconds) to wait for the backoffice to respond to a communication attempt. The range is 0–3600. The default is 300.</td>
</tr>
<tr>
<td>Backoffice</td>
<td>Choose ‘TotalManage’ to use the TotalManage backoffice support, otherwise choose ‘Disable’ to disable backoffice support.</td>
</tr>
<tr>
<td>Backoffice URL</td>
<td>The location of the TotalManage backoffice.</td>
</tr>
</tbody>
</table>

### Content Store Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Store</td>
<td>Choose the type of content store: ISA, FSI, or NGOD. To disable the content store, choose ‘Disable’.</td>
</tr>
<tr>
<td>Content Store URL</td>
<td>The URL where the content store is located.</td>
</tr>
</tbody>
</table>

### Encryption Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Choose ‘Verimatrix’, or ‘Widevine’ to use encryption. Select ‘Disable’ to disable encryption.</td>
</tr>
</tbody>
</table>
Chapter 4  Configuring the CDS

System Level Configuration

Table 4-5  Ingest Manager Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption URL</td>
<td>The location on the encryption server used to send MPEG files for encryption. An example of the Encryption URL is <a href="http://192.168.128.54:7898/files/encrypted">http://192.168.128.54:7898/files/encrypted</a>, where the IP address, port, and directory is specified.</td>
</tr>
<tr>
<td>Encryption FTP URL</td>
<td>The location on the encryption server used to retrieve encrypted MPEG files. An example of the Encryption FTP URL is ftp://192.168.128.54:7899/files/encrypted, where the IP address, port, and directory is specified.</td>
</tr>
</tbody>
</table>

Step 3  Click Submit.
To clear the settings, click Reset.

Configuring the Authentication Manager

Note  The Authentication Manager is an optional feature. The Authentication Manager is not listed on the System Level left-panel menu if it is not included in your deployment.

The Authentication Manager communicates with the backoffice to validate a request received from a set-top box before setting up a session. Before requesting a session setup from the CDS, the set-top box requests an entitlement key from the backoffice. The set-top box then passes the entitlement key as one of the parameters in the request to the CDS. The CDS in turn passes the entitlement key to the backoffice in order to validate the request. If the backoffice responds that the entitlement key is not valid, the session is not set up and the CDS returns an error status to the set-top box.

To configure the Authentication Manager, do the following:

Step 1  Choose Configure > Authentication Manager. The Authentication Manager page is displayed (Figure 4-8).
Step 2  Enter the Authentication Manager settings as appropriate. See Table 4-6 for descriptions of the fields.

Table 4-6  Authentication Manager Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Manager IP*</td>
<td>The Authentication Manager resides on the master Streamer. Typically, the</td>
</tr>
<tr>
<td></td>
<td>Authentication Manager IP address is the same as the master Streamer.</td>
</tr>
<tr>
<td>Authentication Manager Port*</td>
<td>The Authentication Manager port number default is 7794. This port number</td>
</tr>
<tr>
<td></td>
<td>is determined by the properties specifications of the Authentication Manager.</td>
</tr>
<tr>
<td></td>
<td>If you need to change the port number, contact Cisco technical support.</td>
</tr>
<tr>
<td>EventIS Hostname</td>
<td>The hostname or IP address of the EventIS server.</td>
</tr>
<tr>
<td>EventIS Port</td>
<td>The port number on the EventIS server used to receive authentication</td>
</tr>
<tr>
<td></td>
<td>requests.</td>
</tr>
<tr>
<td>TRAXIS SOAP Interface</td>
<td>The IP address, port, and logical partition on the Streamer used to receive</td>
</tr>
<tr>
<td></td>
<td>messages about session teardowns from TRAXIS.</td>
</tr>
<tr>
<td>Server Thread Pool</td>
<td>The number of threads in the Authentication Manager server pool that are</td>
</tr>
<tr>
<td></td>
<td>used to process authentication requests for the duration of the connection.</td>
</tr>
<tr>
<td></td>
<td>The default is 5. The range is 1 to 100.</td>
</tr>
<tr>
<td>Debug Level</td>
<td>From the Debug Level drop-down list, choose Off to have the debug logging</td>
</tr>
<tr>
<td></td>
<td>turned off. Choose Low to have minimal information and error logging.</td>
</tr>
<tr>
<td></td>
<td>Choose Full for full debug logging information.</td>
</tr>
</tbody>
</table>

1. Changes to this field affect the same field on the RTSP Setup page.

Step 3  Click Submit.

To clear the settings, click Reset.
Configuring Ingest Tuning

The Ingest Tuning page allows you to set the speeds of the trick-mode files created for each ingested content.

To view the current ingest tuning settings Choose **Configure > Ingest Tuning**.

To configure the ingest tuning, do the following:

---

**Step 1**  Choose **Configure > Ingest Tuning**. The Ingest Tuning page is displayed (Figure 4-9).

**Figure 4-9  Ingest Tuning Page**

![Image of Ingest Tuning Page]

**Step 2**  Enter the ingest tuning settings as appropriate. See **Table 4-7** for descriptions of the fields.
Chapter 4  Configuring the CDS

System Level Configuration

Table 4-7  Ingest Tuning Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed 1</td>
<td>You can set eight different trick-mode speeds for each ingested content. A trick-mode file, either fast-forward or rewind (–X), is created for each selected speed.</td>
</tr>
<tr>
<td>Speed 2</td>
<td>Select the trick-mode speed from the drop-down list and click Submit. Available trick-mode speeds are 2, 4, 5, 6, 8, 10, 15, 30, 32, 60, and 127. To reset the values and start over, click Reset.</td>
</tr>
<tr>
<td>Speed 3</td>
<td></td>
</tr>
<tr>
<td>Speed 4</td>
<td></td>
</tr>
<tr>
<td>Speed 5</td>
<td></td>
</tr>
<tr>
<td>Speed 6</td>
<td></td>
</tr>
<tr>
<td>Speed 7</td>
<td></td>
</tr>
<tr>
<td>Speed 8</td>
<td></td>
</tr>
</tbody>
</table>

Step 3  Click Submit.
To clear the fields and start over, click Reset.

Configuring IP Nicknames

The IP nicknames are used as an alternative for the IP address in the CDSM drop-down lists.
To configure an IP nickname for a CDS server or QAM gateway, do the following:

Step 1  Choose Configure > IP Nickname. The IP Nicknames page is displayed (Figure 4-10).

Figure 4-10  IP Nicknames Page

Step 2  Select the IP address from the applicable drop-down list, either Cisco CDSM IP Addresses or Configured QAM Gateway IP Addresses, and click Display.

Step 3  In the IP Nickname field, enter a nickname. The name can be from 5 to 20 characters in length and can consist of uppercase and lowercase letters, numbers, and the underscore (_) or hyphen (-) symbols.

Step 4  Click Submit.
To reset the field, click **Reset**.

To edit or view a current IP nickname association, select an IP address or nickname from the drop-down list and click **Display**.

---

### Configuring the Media Importer/Exporter

**Note**

Media Importer/Exporter is part of the MediaX Suite, which is an optional feature. Depending on the transformer type that was selected at the time of initial configuration of your CDS, this page may only show Media Importer.

The Media Importer/Exporter page has two sections, Media Importer Settings and Media Exporter Settings. The Media Importer Settings allows you to specify the data feed import type used in populating the Media Scheduler with data from an EPG file. The Media Exporter Settings (only applicable to OCN transformer type) allow you to specify information for notifying a catalog server, or any other server, when a content program is about to start.

To configure the Media Importer/Exporter, do the following:

---

**Step 1**

Choose **Configure > System Level > Media Importer/Exporter** (or **Media Importer**). The Media Importer/Exporter page is displayed (Figure 4-11).

![Media Importer/Exporter Page](image)

**Figure 4-11  Media Importer/Exporter Page**

**Step 2**

Enter the settings as appropriate. See **Table 4-8** for descriptions of the fields.
Table 4-8  Media Importer/Exporter Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Media Importer Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Importer Type</td>
<td>To upload the EPG using the CDSM, set the Importer Type to host. For information on uploading an EGP file, see the “Uploading an EPG File” section on page 7-14.</td>
</tr>
<tr>
<td>Transformer Type</td>
<td>The Transformer Type is configured at the time of initial installation and specifies the EPG format of either OCN or SA Tribune. This is a read-only field.</td>
</tr>
<tr>
<td><strong>Media Exporter Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Pre-Notification</td>
<td>How much time (in seconds) prior to the start of a content program should the catalog server be notified to advertise the program to the set-top box.</td>
</tr>
<tr>
<td>Notify URL Prefix</td>
<td>Used to notify a catalog server that a real-time program is about to begin and to fetch the offering from the backoffice. An example of the prefix URL follows: <a href="http://10.74.124.131/Notification.asp">http://10.74.124.131/Notification.asp</a>.</td>
</tr>
</tbody>
</table>

1. Only for OCN transformer type.

**Step 3**

Click **Submit**.

To reset the field, click **Reset**.

---

### Configuring Call Signs

**Note**

The CallSign Setup is an optional feature. The CallSign Setup is not listed on the System Level left-panel menu if it is not included in your deployment.

The CallSign Setup page is used to configure the call signs of the program channels.

A call sign is a unique identifier for a program channel. The channels, identified by their call signs, are mapped to a multicast IP address and port that a content provider or satellite uses to send content by using the Single-Program Transport Stream (SPTS) IP interface.

To configure a CallSign, do the following:

**Step 1**

Choose **Configure > System Level > Callsign Setup**. The CallSign Setup page is displayed (Figure 4-12).
Enter the call sign settings as appropriate. See Table 4-9 for descriptions of the fields.

**Table 4-9 CallSign Setup Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallSign</td>
<td>A CallSign is a unique identifier for a program channel (content source).</td>
</tr>
<tr>
<td>Multicast IP</td>
<td>The multicast IP address of the device sending Single Program Transport Stream (SPTS).</td>
</tr>
<tr>
<td>Port</td>
<td>The port associated with the CallSign.</td>
</tr>
</tbody>
</table>

Click Submit.

To edit a CallSign setting, enter the CallSign, the new settings, and click Submit. The new settings overwrite the previous settings and are displayed in the Configured CallSigns section.

To delete a CallSign setting, check the Delete check box associated with the entry and click Delete.
Configuring Input Channels

Note

The Input Channels page is part of the MediaX Suite, which is an optional feature.

The Input Channels page allows you to define channels mapped to a multicast group IP address and port, where scheduled content is ingested. The Input Channels page also collects a number of values for metadata generation.

If you upload an EPG file, and you want to modify the metadata for all programs for a channel, then add the channel in the Input Channels page and enter the modifications in the fields provided. All scheduling information from the EPG file is listed on the Media Scheduler page. For more information, see the “Uploading an EPG File” section on page 7-14.

Caution

All channel default values specified on the Input Channels page will overwrite any metadata information for future ingested assets of the specified channel. The metadata for the assets already ingested are not affected.

To define a channel and set the metadata information, do the following:

Step 1

Choose Configure > System Level > Input Channels. The Input Channels page is displayed (Figure 4-13).

Figure 4-13 Input Channels Page
Step 2  From the **Select Channel** drop-down list, choose **Add New Channel**.

**Note**  The Channel Name is automatically generated by combining the Provider and Channel ID fields with a hyphen (-) between the values.

Step 3  In the **Multicast Group IP** field, enter the multicast IP address that the Vault must join (by using IGMP) to ingest content.

Step 4  In the **Port** field, enter the port number the Vault should listen to in order to ingest content.

**Note**  The combination of the IP address and port must be unique from all other channels.

Step 5  Enter the channel settings as appropriate. See Table 4-10 for descriptions of the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Code</td>
<td>Used to create the asset name and the category in the Asset Distribution Interface (ADI) metadata file. Maximum length is three characters.</td>
</tr>
<tr>
<td>Channel ID</td>
<td>Identifies the channel in the EPG file.</td>
</tr>
<tr>
<td>Category ID</td>
<td>Identifies the category corresponding to the channel (numeric only).</td>
</tr>
<tr>
<td>Catalog ID</td>
<td>The channel ID used in the catalog.</td>
</tr>
<tr>
<td>Product</td>
<td>Choose movie on demand (MOD), subscriber video on demand (SVOD), or Real-Time Innovations (RTI) as the product type for this channel.</td>
</tr>
<tr>
<td>Provider</td>
<td>The name of the provider.</td>
</tr>
<tr>
<td>Provider ID</td>
<td>A unique identifier for the provider of all assets in this channel. The Provider ID must be set to a registered Internet domain name that is restricted to at most 20 lowercase characters and belongs to the provider. For example, a valid Provider ID for CableLabs is “cablelabs-films.com.”</td>
</tr>
<tr>
<td>Preview Period</td>
<td>The amount of time (in seconds) the subscribers are allowed to preview assets on this channel before they are charged for viewing the asset.</td>
</tr>
<tr>
<td>Licensing Window Start</td>
<td>From the drop-down list, choose the number of days to add to the start date of the license window for all assets in this channel.</td>
</tr>
<tr>
<td>Licensing Window End</td>
<td>From the drop-down list, choose the number of days to add to the end date of the license window for all assets in this channel.</td>
</tr>
<tr>
<td>Encryption</td>
<td>If the assets on this channel are encrypted, choose <strong>Yes</strong> otherwise choose <strong>No</strong>.</td>
</tr>
<tr>
<td>Rating</td>
<td>The Motion Picture Association of America (MPAA) rating for all assets on this channel (G, PG, PG13, R, or NC-17).</td>
</tr>
<tr>
<td>Publish Time Adjustment</td>
<td>The amount of time to add to the start time for publishing each program on this channel to the backoffice. The Publish Time Adjustment must be longer than the value set for the Media Importer/Exporter Pre-Notification field.</td>
</tr>
<tr>
<td>Suggested Price</td>
<td>The suggested price for each asset on this channel. The format is xx.xx.</td>
</tr>
</tbody>
</table>
Configuring Transport Groups

Transport Groups identify destination subnetworks for stream traffic. Each Transport Group is associated with one or more Ethernet interfaces on an ISV or Streamer. If you do not associate the stream interfaces with any Transport Groups, then all stream interfaces are able to reach any transport network and the CServer determines which interface should perform the streaming based on cost and bandwidth usage.

One use of Transport Groups is to split the stream interfaces on two different Streamers, with half of each directed to two different switches servicing the same service group. In this way, if a Streamer’s service is interrupted, the active streams, as well as any new requests, are handled by the Streamer that is still providing service.

In the example illustrated in Figure 4-14, there are two Streamers with two stream interfaces going to each switch: one will stream to the switch that carries high-frequency streams, and the other will stream to the switch that carries low-frequency streams. Both switches connect to the same QAM devices servicing one service group.
Table 4-11 describes the four Transport Groups that would be created for the example shown in Figure 4-14. Once the Transport Groups are created, you need to assign them to the appropriate interfaces. See the “Configuring the Servers” section on page 4-41 for more information.

**Table 4-11 Transport Group to Stream Interface Association**

<table>
<thead>
<tr>
<th>Transport Group ID</th>
<th>Streamer–Stream Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>TG1</td>
<td>Streamer1–eth5 and eth4</td>
</tr>
<tr>
<td>TG2</td>
<td>Streamer1–eth3 and eth2</td>
</tr>
<tr>
<td>TG3</td>
<td>Streamer2–eth5 and eth4</td>
</tr>
<tr>
<td>TG4</td>
<td>Streamer2–eth3 and eth2</td>
</tr>
</tbody>
</table>

To configure a Transport Group, do the following:

**Step 1** Choose **Configure > Transport Group ID**. The Transport Group ID page is displayed (Figure 4-15).

**Step 2** In the **Transport Group ID** field, enter the Transport Group name and click **Submit**.

Allowable characters for the Transport Group ID are alphanumeric characters (0-9, a-z, A-Z), the dash (-), and the underscore (_). The range is 4 to 64.
Once the Transport Groups are created, you need to assign them to the appropriate interfaces. See the “Configuring the Servers” section on page 4-41 for more information.

All current Transport Group IDs are listed under the Edit/Remove Existing Transport Group ID section of the page.

To delete a Transport Group, check the Remove check box associated with the Transport Group in the Edit/Remove Existing Transport Group ID section and click Submit.

To edit a Transport Group ID, enter the new name of the existing name in the Edit/Remove Existing Transport Group ID section and click Submit.

**Array Level Configuration**

The Array Level tab has the following configuration options:

- Configuring the Array Level DNS Bindings
- Configuring Stream Groups
- Configuring the Control and Setup IPs
- Configuring the Media Scheduler

The Array Level configuration settings are distributed to all servers in the specified array.
Configuring the Array Level DNS Bindings

The DNS binding settings are used to configure the DNS services for a specific group of servers.

Caution

If you have individual DNS settings configured for a server and you change the Array Level DNS binding settings, the individual DNS settings are overwritten. Therefore, first configure the higher level settings before configuring the individual Server Level settings.

To view the current DNS Bindings settings for an Array Level, Choose Configure > Array Level, select a group from the drop-down list and click Display.

To configure the DNS binding settings for an Array Level, do the following:

Step 1

Choose Configure > Array Level. The DNS Binding page is displayed (Figure 4-16).

Step 2

From the drop-down list, choose an array and click Display.

Step 3

Enter the DNS binding Array Level settings as appropriate. See Table 4-12 for descriptions of the fields.
Table 4-12  DNS Binding Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Suffix</td>
<td>Specify, if applicable, the internal domain that is used to fully qualify an unqualified hostname. For example, if you are using OpenStream as the BMS, specify a subdomain consistent with what your backoffice is using, for instance, bms.n2bb.com. Accordingly, unqualified hostnames used in CORBA transactions, such as contentstore, resolve correctly to contentstore.bms.n2bb.com.</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>The IP address of the primary DNS server.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>The IP address of the secondary DNS server.</td>
</tr>
</tbody>
</table>

Step 4  Click Submit.
To clear the fields and start over, click Reset.

To delete the DNS settings, check the Delete check box and click Submit.

Configuring Stream Groups

A Stream Group consists of one or more Streamers. Streamers within a Stream Group work as a team with regard to content caching, load distribution, and bandwidth usage. Stream Groups interact with other Stream Groups by passing streams among each other based on performance qualification and cost considerations. If a Stream Group must give up a stream to another group, Stream Group preferences set on the QAM Gateway page are followed. Stream Groups relate to QAM gateways or destination subnetwork by the Stream Group preference. For more information about Stream Group and QAM gateway associations, see the “Configuring QAM Gateways” section on page 4-6.

A Streamer can never be a member of more than one Stream Group.

When grouping Streamers you should take into account network cost to stream, bandwidth usage, and geographic locations of Streamers and QAM gateways. All Streamers in a group are considered to have the same cost to reach a destination.

To configure a Stream Group, do the following:

Step 1  Choose Configure > Array Level > Stream Groups. The Stream Groups page is displayed (Figure 4-17).
Step 2  From the **Select Stream Group to View/Edit** drop-down list, choose **add new stream group** and click **Display**.

Step 3  In the **New Stream Group Name** field, enter the name of the Stream Group and click **Submit**.

You can only use alphanumeric characters (0-9, a-z, A-Z), the dash (-), and the underscore (_) to create a Stream Group name.

Step 4  Add the Streamers to the Stream Group.

The unassigned Streamers are listed along with a drop-down list for each that offers the options described in Table 4-13.

<table>
<thead>
<tr>
<th>Unassigned Streamer Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Change</td>
<td>Do not make any changes to the Stream Group assignment.</td>
</tr>
<tr>
<td>Stream Group Name</td>
<td>Add this Streamer to this Stream Group.</td>
</tr>
<tr>
<td>None</td>
<td>Remove this Streamer from this Stream Group. Applicable only to Streamers assigned to the selected Stream Group.</td>
</tr>
</tbody>
</table>

Step 5  Click **Submit**.

To reset the field, click **Reset**.

To view the members of a Stream Group, select the Stream Group from the drop-down list and click **Display**.
To delete a Stream Group, first remove all Streamers from the group, then click **Delete Group**.

To edit the members of a Stream Group, do the following:

---

**Step 1**  Select the Stream Group from the drop-down list and click **Display**.

**Step 2**  Select the appropriate options.

Table 4-13 describes the different option for each member of a Stream Group.

**Step 3**  Click **Submit**.

To reset the field, click **Reset**.

---

### Configuring the Control and Setup IPs

A Streamer designated as the Setup server interfaces with the backoffice and forwards the setup messages to the appropriate Stream Group. There can only be one IP address designated as the Setup server for each Stream Group.

The Control server is used to communicate with Lightweight Stream Control Protocol (LSCP) clients. Each Control server handles up to 6000 LSCP clients. You can use the Stream Master IP (Setup IP) as one of your Control server IP addresses. You must configure a Control server for each group of up to 6000 LSCP clients. For instance, if you have 7000 LSCP clients, you need to configure two Control servers. The Control servers are associated with each Stream Group. For this release, there can only be one Control server for each Stream Group.

For more information about the Control and Setup servers, see the “Streamer Workflow” section on page 2-5.
To configure a Control/Setup IP, do the following:

**Step 1** Choose **Configure > Array Level > Control/Setup IP**. The Control/Setup IP page is displayed (Figure 4-18).

![Figure 4-18 Control/Setup IP Page](image)

**Step 2** For each Stream Group, enter the IP address and subnet mask of the Control IP, Setup IP, or Control/Setup IP.

**Step 3** From the **IP Type** drop-down list, choose an IP type. See Table 4-14 for descriptions of the types.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control IP</td>
<td>The IP address used only for LSCP client control.</td>
</tr>
<tr>
<td>Setup IP</td>
<td>The IP address of the Setup server.</td>
</tr>
<tr>
<td>Control/Setup IP</td>
<td>The Control/Setup IP address used for LSCP client control and as the Master Stream Service.</td>
</tr>
</tbody>
</table>

**Step 4** Click **Submit**.

To reset the field, click **Reset**.

**Note**

All currently configured Control/Setup IPs are listed in the Configured Control/Setup IPs section of the Control/Setup IP page.

To edit a Control/Setup IP, make any changes to the Control/Setup IP as necessary, and click **Submit**.
To delete a Control/Setup IP, check the Delete check box and click Submit.

**Configuring the Media Scheduler**

*Note* The Media Scheduler page is part of the optional MediaX feature.

The Media Scheduler page allows you to schedule content for ingest and generate content metadata. The channels available in the Media Scheduler page are determined by the channels included in the uploaded EPG file and those configured on the Input Channels page. See the “Uploading an EPG File” section on page 7-14 and the “Configuring Input Channels” section on page 4-21 for more information.

The ingest time is calculated by adding the ingest schedule start timeslot to the Publish Time Adjustment field from the Input Channels page.

*Note* In order to be able to schedule content, you must add the channels through the Input Channel page, and then either upload an EPG file to populate the cells in the Media Scheduler, or manually enter the metadata using the Media Scheduler’s Package Metadata window.

From the Media Scheduler page, you can perform the following tasks:

- Choose the channels to schedule content ingest.
- View the content metadata for each selected timeslot.
- Schedule content to be ingested for a particular channel, provided all required ADI metadata values are available.
- Add metadata values if they are not available, or modify the metadata values.
- Resolve any conflicts in the EPG data.

The following procedure walks you through all these tasks.
### User Preferences

To schedule content ingest and edit metadata information, do the following:

**Step 1** Choose **Configure > Array Level > Media Scheduler**. The User Preferences for the Media Scheduler page is displayed (Figure 4-19).

#### Figure 4-19 Media Scheduler Page—User Preferences

<table>
<thead>
<tr>
<th>Array Level</th>
<th>Configure</th>
<th>Monitor</th>
<th>Report</th>
<th>Maintain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System Level</td>
<td>Array Level</td>
<td>Server Level</td>
<td></td>
</tr>
</tbody>
</table>

**User Preferences**

Below are the preferences set for when to edit the preferences change the settings below and click Save.

- **Preference Editor:**
  - [ ] Hide On Return
  - [ ] Show On Return

- **Action on Recurring Schedules**
  (Only for user generated schedules)
  - [ ] Preserve Existing Schedules
  - [ ] Overwrite Existing Schedules

- **Package Name Preferences**
  You can choose between auto generating a package name using the start time stamp, or entering the package name manually, if the package name already exists.
  - [ ] Auto generate
  - [ ] Don't auto generate

**Channels To Schedule**

**Step 2** Choose either **Hide On Return** or **Show On Return** to display the user preferences each time you go to the Media Scheduler page.

**Note** You can change the user preferences at any time by clicking **Edit Settings** in the main Media Scheduler page or when the calendar is displayed. To have your settings recalled each time you log in to the CDSM, see the “Changing User Default Settings” section on page 7-4.

**Step 3** For **Action on Recurring Schedules**, choose either **Preserve Exiting Schedules** or **Overwrite Existing Schedules**. This option is only for user-generated schedules; this option is not for uploaded EPG data. For more information, see the “Package Metadata Editor” section on page 4-36.
Preserving Existing Schedules keeps any content that is currently scheduled for the day and channel you selected and fills only the empty timeslots. Overwrite Existing Schedules overwrites any content that is currently scheduled for the day and channel you selected.

**Step 4**
When you schedule an event that originated from an uploaded EPG file, the Media Scheduler creates a package name combining the channel name, title brief, and the word “package.” For Package Name Auto-Generation, if the package name already exists and you want a new package name auto-generated, choose **Enable** and the start time is added to the package name. If the package name already exists and you want to create the package name using the Metadata Editor, choose **Disable**.

**Step 5**
Check the check boxes for the channels you want to schedule.

**Note**
To create new channels, see the “Configuring Input Channels” section on page 4-21.

**Step 6**
Click **Save** to save the settings. The calendar is displayed (Figure 4-20).

---

### Scheduling Content for Ingest

To schedule content ingest and edit metadata information, do the following:

**Step 1**
Choose **Configure > Array Level > Media Scheduler**. If Hide On Return was selected in the User Preferences, the Media Scheduler calendar is displayed (Figure 4-20). If Show On Return was selected in the User Preferences, the User Preferences are displayed (Figure 4-19).

**Step 2**
From the calendar, click the day you want to schedule. If the month you are scheduling is not shown, use the left and right arrows on either side of the calendar to change the month.

**Note**
Today’s date is displayed with a box around it.

The schedule for the day you selected is displayed (Figure 4-21).
Depending on the status of the schedule, the schedule’s cells that contain data (programs) are displayed in different colors. When you first view the Media Scheduler page with uploaded EPG data, all the programs are in the “Not Scheduled” state. The Media Scheduler page displays a legend describing the different colors for the cells in the schedule.

Small timeslots are marked blue. To view the program information on small timeslots, click the timeslot. The page refreshes and the schedule for the small timeslot is displayed at the bottom of the page.

Tip

To view information about a program, move the mouse pointer over a cell. A pop-up displays the program information (Figure 4-22).
Step 3  
Click each cell for each program you want to schedule.

If all the required information for metadata creation is available for the channel and the timeslot, the color of the cell changes to green, indicating that the timeslot is “Marked for Scheduling.”

If all the required information for metadata creation is not available, a new window opens and the Package Metadata Editor is displayed. See the “Package Metadata Editor” section on page 4-36.

Tip  
Alternatively, you can click the channel column heading to schedule all unscheduled events for that channel. This method automatically submits the changes and refreshes the page with all the channel’s timeslots marked “Scheduled,” if all required metadata information is available.

Note  
You can only schedule current and future timeslots. However, you can view past timeslots.

Step 4  
Click Submit. The Media Scheduler page refreshes and all the “Marked for Scheduling” cells are changed to “Scheduled.”

Note  
Only current and future schedule entries can be edited.

To remove a scheduled ingest, click the scheduled timeslot. The timeslot changes from “Scheduled” to “Marked for Unscheduling.” Click Submit.

Tip  
You can mark timeslots for unscheduling and mark different timeslots for scheduling, and submit all the changes at one time.
## Package Metadata Editor

The Package Metadata Editor allows you to edit or view existing metadata, or to enter new metadata for any future unused timeslot.

To use the Package Metadata Editor, do the following:

### Step 1

To enter new metadata for any unused timeslot, click the unused timeslot. To edit existing metadata, double-click the scheduled timeslot. A new window opens and the Package Metadata Editor is displayed (Figure 4-23).

![Package Metadata Editor—User-Generated Timeslot](image)

Metadata that originates from an EPG file is created using a combination of channel values (set in the Input Channels page) and data uploaded from the EPG file. If all the data is available, the metadata is generated, the content is scheduled for ingest, and the start time is set for publishing the content.
**Step 2**  For metadata created from user-generated schedules, there is an option for recurring schedules (Figure 4-24).

*Figure 4-24  Recurring Schedule Options for User-Generated Schedules*

Check the **Recurring Schedules** check box to copy the metadata information to the timeslots specified in the Recurring Schedule fields. See **Table 4-15** for descriptions of the Recurring Schedule fields.

**Table 4-15  Recurring Schedule Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurrence Pattern</td>
<td>Daily</td>
<td>If Daily is selected, the metadata is copied to the same timeslot each day until the Recurrence End Time is reached.</td>
</tr>
<tr>
<td></td>
<td>Weekly</td>
<td>If Weekly is selected, the metadata is copied to the same timeslot on each day of the week selected (Sun, Mon, Tue, Wed, Thu, Fri, Sat) until the Recurrence End Time is reached.</td>
</tr>
<tr>
<td></td>
<td>Monthly</td>
<td>If Monthly is selected, the metadata is copied to the same timeslot on the week selected (1st, 2nd, 3rd, 4th, last) and day of the week selected (Sun, Mon, Tue, Wed, Thu, Fri, Sat) until the Recurrence End Time is reached.</td>
</tr>
<tr>
<td>Recurrence End Time</td>
<td>One year from start time</td>
<td>The Recurrence Pattern is repeated for one year from the metadata Start Time.</td>
</tr>
<tr>
<td></td>
<td>End After</td>
<td>The Recurrence Pattern is repeated the number of times you specify in the occurrences field.</td>
</tr>
<tr>
<td></td>
<td>End By</td>
<td>The Recurrence Pattern is repeated until the date you specified in the End By field is reached.</td>
</tr>
</tbody>
</table>

Depending on the setting in the User Preferences settings, any existing metadata is preserved or overwritten. See the “User Preferences” section on page 4-32 for more information.

**Step 3**  Fill in any missing information, or edit existing information, using the Package Metadata and click **Submit**.

For information on the fields displayed in the Package Metadata, see the *CableLabs Video-On-Demand Content Specification Version 1.1* (MP-SP-VOD-CONTENT1.1-I03-040107) document at www.cablelabs.com.
Fixing Conflicts in the Media Scheduler

Conflicts can occur as a result of the following scenario:

- Information was uploaded from an EPG file and the Media Scheduler is using this information. However, the schedule was modified.
- The schedule information is updated with new entries for the same time and channel, but each entry has different content information.

To view these conflicts and schedule the latest information, do the following:

**Step 1** Choose **Configure > Array Level > Media Scheduler**. The Media Scheduler page displays all the conflicts, including those events that have passed (Figure 4-25).

To go to the main Media Scheduler page, click **Go To Scheduler**.

**Figure 4-25 Media Scheduler Page—Conflicts**

<table>
<thead>
<tr>
<th>Record</th>
<th>Channel</th>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>01:00:00</td>
<td>01:30:00</td>
</tr>
<tr>
<td>2</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>01:30:00</td>
<td>02:00:00</td>
</tr>
<tr>
<td>3</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>02:00:00</td>
<td>02:30:00</td>
</tr>
<tr>
<td>4</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>02:30:00</td>
<td>03:00:00</td>
</tr>
<tr>
<td>5</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>03:00:00</td>
<td>03:30:00</td>
</tr>
<tr>
<td>6</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>03:30:00</td>
<td>04:00:00</td>
</tr>
<tr>
<td>7</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>04:00:00</td>
<td>04:30:00</td>
</tr>
<tr>
<td>8</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>04:30:00</td>
<td>05:00:00</td>
</tr>
<tr>
<td>9</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>05:00:00</td>
<td>05:30:00</td>
</tr>
<tr>
<td>10</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>05:30:00</td>
<td>06:00:00</td>
</tr>
<tr>
<td>11</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>06:00:00</td>
<td>06:30:00</td>
</tr>
<tr>
<td>12</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>06:30:00</td>
<td>07:00:00</td>
</tr>
<tr>
<td>13</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>07:00:00</td>
<td>07:30:00</td>
</tr>
<tr>
<td>14</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>07:30:00</td>
<td>08:00:00</td>
</tr>
<tr>
<td>15</td>
<td>CHAN1</td>
<td>June 3-2008</td>
<td>08:00:00</td>
<td>08:30:00</td>
</tr>
</tbody>
</table>

**Step 2** To fix a scheduling conflict, click the link for the record number. The Media Scheduler page refreshes and displays the channel of the selected conflict.

The timeslots that have conflicts are displayed with a brown color.

**Step 3** To clear a conflict, click the timeslot. The timeslot gets the latest information and is displayed with the color green, indicating “Marked for Scheduling” if all the metadata information is available.

If all the required information for metadata creation is not available, a new window opens and the Package Metadata Editor is displayed (Figure 4-23). Fill in the metadata as required and click **Submit**. The Package Metadata Editor window closes.

**Step 4** Once all the conflicts have been cleared on the Media Scheduler page, click **Submit** to schedule all “Marked for Scheduling” timeslots.
Server Level Configuration

Once a server has been initially configured (see the “Initially Configuring the Devices” section on page 3-1) the CDSM detects it and the server’s IP address or nickname is available for selection in the server drop-down lists.

The Server Level tab has the following configuration options:

- Configuring the Interfaces
- Configuring the Servers
- Configuring the Route Table
- Configuring the SNMP Agent
- Configuring the Server Level DNS Binding
- Configuring RTSP Setup
- Configuring FSI Setup

Configuring the Interfaces

The Interface Setup page is used to configure the different interfaces on the CDS servers. The functionality of the Ethernet interfaces on the CDS servers is configurable. However, there is an optimal configuration for each server. The interface functions are described in Table 4-16.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>The general interface is used to reserve an Ethernet interface to allow optimal configuration.</td>
</tr>
<tr>
<td>Management</td>
<td>The management interface is used to communicate with other network devices with regards to condition of the server, stream control, and ISA communications.</td>
</tr>
<tr>
<td>Ingest</td>
<td>The ingest interface is used to establish connectivity with a content provider system and to ingest content on to a Vault or an ISV.</td>
</tr>
<tr>
<td>Cache</td>
<td>The cache interface is used to transport content between Vaults and Streamers.</td>
</tr>
<tr>
<td>Stream/Cache</td>
<td>The stream/cache interface on the Streamer can be used for both cache and streaming traffic. If an interface is configured for both cache and streaming traffic on a Streamer, priority with be given to the higher-bandwidth stream traffic provided cache traffic is able to transmit on other interfaces.</td>
</tr>
<tr>
<td>Stream</td>
<td>The stream interface is used to transport streams to the QAM devices.</td>
</tr>
<tr>
<td>Stream Control</td>
<td>The stream control interface is used to transmit control messages between the STBs and the Streamers. Designating an interface as a stream control interface allows for the separation of stream control traffic from management traffic. For more information about stream control, see the “Configuring the Control and Setup IPs” section on page 4-29.</td>
</tr>
</tbody>
</table>

For all CDE servers, the optimal configuration is:

- eth0 as management
- eth1 as ingest on Vaults and ISVs
all other interfaces are available for cache, stream, or stream/cache as appropriate for the server

To configure the interface settings, do the following:

**Step 1** Choose **Configure > Server Level**. The Interface Setup page is displayed (Figure 4-26).

**Step 2** From the **Server IP** drop-down list, choose the server’s IP address or nickname and click **Display**.

**Figure 4-26 Interface Setup Page—Vault Page**

**Step 3** Select each interface setting as appropriate.

**Step 4** Click **Submit** to save the settings.

To clear the fields and start over, click **Reset**.
Configuring the Servers

Once a server has been initially configured, the CDSM detects it and the server’s IP address or nickname is available for selection in the server drop-down lists.

To configure the server settings, do the following:

---

**Step 1** Choose **Configure > Server Level > Server Setup**. The Server Setup page is displayed.

**Step 2** From the **Server IP** drop-down list, choose a server’s IP address or nickname and click **Display**.

**Step 3** The fields differ for a Vault, Streamer, and ISV server. Figure 4-27 shows the Server Setup for a Vault. Figure 4-28 shows the Server Setup for a Streamer. The ISV server setup page has a combination of the Vault and Streamer fields. See Table 4-17 for descriptions of the fields and to which server they apply.
Figure 4-27  Server Setup–Vault Server Page

<table>
<thead>
<tr>
<th>Server Level</th>
<th>Interface Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Server Setup</td>
</tr>
<tr>
<td></td>
<td>Replac Tapes</td>
</tr>
<tr>
<td></td>
<td>SNIF Agent</td>
</tr>
<tr>
<td></td>
<td>DNS Server</td>
</tr>
<tr>
<td></td>
<td>RTSP Setup</td>
</tr>
<tr>
<td></td>
<td>PST Setup</td>
</tr>
</tbody>
</table>

**Server Setup CONFIGURE**

Select the IP of the specific server that you wish to edit and click **Display**.

Current settings for (10.22.216.111). To make changes to these settings, edit the field you wish to change and click **Submit** below.

### 4U-SATA 2z Vault

**Server Name:**
- Hostname: rack11
- TTL: 16

**Default Stream/Cache Settings**
- Source IP: 195.168.207.65
- Cache Port: 0

**Jumbo Frames Support**
- Cache Jumbo Frames: **Enabled**

**Server Offload:**
- **Enabled**

**Vault Mirror Copies:**
- 0

**Vault Local Copies:**
- 1

**Cache IP Packets:**
- Differentiated Services Code Point: 0 (0-63)
- Explicit Congestion Notification: 0 (0-3)

**FTP Out Settings**
- FTP Out Interface: [Management]
- FTP Out Bandwidth: max 600Mbps
- FTP Out Sessions: 1-100

**Ethernet Interface Settings**

**eth0 (General)**
- IP: 192.168.111.111
- Subnet Mask: 255.255.255.0

**eth1 (Native)**
- IP: 192.168.110.111
- Subnet Mask: 255.255.255.0

**eth1 (Native)**
- IP: 192.168.110.111
- Subnet Mask: 255.255.255.0

**eth2 (Management)**
- IP: 10.22.230.111
- Subnet Mask: 255.255.255.1

**eth2 (Cache)**
- Subnet Mask: 255.255.255.1

Source IP: 19.22.26.111
Cache Port: 0
Server Setup—Streamer Server Page

Server Setup configure

Select the IP of the specific server that you wish to edit and click Display.

Current settings for 10.22.216.55. To make changes to these settings, edit the field you wish to change and click Submit below.

Server Name: 55
Group ID: SBS5

Hostname:
TTL:

Default Stream/Cache Settings

Source IP: 192.168.197.65
Starting Transport Port: 0
Ending Transport Port: 0
Cache Port: 0

Stream Group Info

Stream Group: StreamGroup1
Stream Group Id: 1

Jumbo Frames Support

Stream Jumbo Frames: Enabled
Cache Jumbo Frames: Disabled

Server Status

Server Offline: Enabled

Transport/Cache IP Packets

Transport
Differentiated Services Code Point: 46 (0-63)
Explicit Congestion Notification:
Cache
Differentiated Services Code Point: 33 (0-63)
Explicit Congestion Notification:

Ethernet Interface Settings
c0/0 (Management)
Management IP: 10.22.216.55
Gateway: 10.22.216.1
Subnet Mask: 255.255.255.0
c0/1 (Not Used)
To configure this interface click here.
c0/2 (Stream/Cache)

Source TPs: 192.168.465.18
Transport Port: 4660
Cache Port: 3110
Transport Group ID: none

Figure 4-28
## Table 4-17  Server Setup Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>A fully qualified hostname for this server. The name can be up to 64 characters. Assigning a hostname is optional. The hostname must be fully qualified, for example: vault.cisco.com. The DNS must be able to resolve the hostname to the IP address you select, with both forward and reverse lookups. If you enter a hostname that cannot be resolved, you may not be able to access the server.</td>
<td>All servers: Vault, Streamer, ISV</td>
</tr>
<tr>
<td>TTL</td>
<td>The IP time to live (TTL) for data packets. The IP time to live default is 16 hops. Valid entries range from 0 to 255.</td>
<td>All servers</td>
</tr>
<tr>
<td>Default Stream/Cache Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>The default source IP address for all stream and cache interfaces. If the source IP address is left blank, the default of 192.168.207.65 is used.</td>
<td>All servers</td>
</tr>
<tr>
<td>Starting Transport Port</td>
<td>The beginning default UDP port number used for stream and stream/cache interfaces. If the starting transport port is left blank, the default of 48879 is used.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Ending Transport Port</td>
<td>The ending default UDP port number used for stream and stream/cache interfaces. There is no default for the ending transport port number.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Cache Port</td>
<td>The default UDP port number used for cache traffic between servers. If the cache port is left blank, the default of 48879 is used.</td>
<td>All servers</td>
</tr>
<tr>
<td>Stream Group Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stream Group ID</td>
<td>These fields display the Stream Group and Stream Group ID the ISV or Streamer is a member of. The Stream Group and Stream Group ID are only informational. To configure Stream Groups, see the “Configuring Stream Groups” section on page 4-27.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Jumbo Frames Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stream Jumbo Frames</td>
<td>By default, jumbo frames are disabled on stream interfaces. In this case, stream traffic adheres to standard frames, which is a maximum frame size of 1500 bytes. If jumbo frames are enabled, you need to make sure that your switch is configured to support jumbo frames. The jumbo frame size must be set, at a minimum, to 8192 bytes.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Cache Jumbo Frames</td>
<td>By default, jumbo frames are disabled on cache interfaces. In this case, cache traffic adheres to standard frames, which is a maximum frame size of 1500 bytes. If jumbo frames are enabled, you need to make sure that your switch is configured to support jumbo frames in order to be able to communicate across the cache interfaces. The jumbo frame size must be set, at a minimum, to 8192 bytes.</td>
<td>All servers</td>
</tr>
<tr>
<td>Server Status</td>
<td>Server Offload shows the current offload status of the server. When Server Offload is enabled, the server is configured to reject new provisioning. Server offload is typically enabled when system maintenance needs to be performed, or when a server needs to be removed from service.</td>
<td>All servers</td>
</tr>
<tr>
<td>Vault Mirror Copies</td>
<td>Select the number of copies from the drop-down list that ensures there is at least one copy of the content at each site. For example, if there are two different sites, each with two Vaults, set the Vault Mirror Copies to 3.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td>Vault Local Copies</td>
<td>From the drop-down list, choose the number of copies of content that will be stored on this server.</td>
<td>Vault, ISV</td>
</tr>
</tbody>
</table>
Table 4-17  Server Setup Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transport/Cache IP Packets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Differentiated Services Code Point</td>
<td>Differentiated Services Code Point (DSCP) uses six bits of the DiffServ field, which was originally the ToS octet, to mark all outgoing packets with a specific DSCP value. Cache or transport traffic may require certain forwarding behavior, known as the per-hop behavior (PHB), which is specified in the DSCP. The network gives priority to marked traffic. Generally, the lower number has lower priority and the higher number has higher priority. The valid entries are 0–63. DSCP is set separately for cache and transport interfaces.</td>
<td>All servers</td>
</tr>
<tr>
<td>Explicit Congestion Notification</td>
<td>The Explicit Congestion Notification field consists of two bits that denote the end points of a transfer protocol as ECN-capable, or that ECN is not being used. The ECN Capable Transport (ECN) code points are 1, meaning ECT(1), and 2, meaning ECT(0). If you use ECN, it is recommended that you set the ECN field to 2. If you are not using ECN, set the field to 0, which means do not use ECN. Typically, setting the ECN field to 3 is performed by the router to indicate congestion is experienced. ECN is set separately for cache and transport interfaces.</td>
<td>All servers</td>
</tr>
<tr>
<td><strong>FTP Out Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP Out Interface</td>
<td>The FTP out interface determines whether the management interface or the ingest interface is used for FTP pulls and FTP pushes. It is also used for the ISA 1.5 FTP out feature.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td>FTP Out Bandwidth</td>
<td>Enter the maximum bandwidth (in Mbps) allowed for FTP functionality. Valid entries are 0 to 1000.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td>FTP Out Sessions</td>
<td>Enter the maximum number of FTP out sessions allowed from 1 to 10.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td><strong>Management Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management IP</td>
<td>The IP address of the management interface on this server.</td>
<td>All servers</td>
</tr>
<tr>
<td>Gateway</td>
<td>The IP address of the gateway to the network.</td>
<td>All servers</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask that defines the subnetwork for this server.</td>
<td>All servers</td>
</tr>
<tr>
<td>FTP Listener</td>
<td>Select either the Management Interface or the Ingest Interface as the FTP listener. The FTP listener selected determines which interface is used for FTP pulls or FTP pushes.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td><strong>Ingest Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingest IP</td>
<td>The IP address of the ingest interface on this server. The ingest IP address is used to establish connectivity to the content provider system.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td>Ingest Subnet Mask</td>
<td>The subnet mask that defines the subnetwork for this interface.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td><strong>General Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td>The IP address for this interface.</td>
<td>All servers</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask that defines the subnetwork for this interface.</td>
<td>All servers</td>
</tr>
</tbody>
</table>
### Chapter 4  Configuring the CDS

#### Server Level Configuration

**Note**
To configure an unconfigured interface, click the **click here** link. The Interface Setup page is displayed. Select the setting for the interface you want to configure and then click **Submit**. The Server Setup page is displayed. Complete the interface configuration by filling in the fields as appropriate. See **Table 4-17** for field descriptions.

**Note**
The Streamer can have a maximum of 12 interfaces configured for stream traffic simultaneously, with a maximum of 12 interfaces configured for cache traffic, or any variation of the two (for example, 8 stream interfaces and 6 cache interfaces). If an interface is configured for both cache and streaming traffic on a Streamer, priority is given to the higher-bandwidth stream traffic provided cache traffic is able to transmit on other interfaces.

**Step 4**
Click **Submit** to save the settings.
To clear the fields and start over, click **Reset**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stream/Cache Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>The IP address for this interface. The IP address set for this interface overrides the default Source IP setting. If you are using Layer 3 communication among Vaults and Streamers, each cache or stream/cache interface must have an IP address. If you are using Layer 2 communication among Vaults and Streamers, IP addresses for cache and stream/cache interfaces are optional.</td>
<td>All servers</td>
</tr>
<tr>
<td>Transport Port</td>
<td>This setting applies only to stream or stream/cache interfaces. This is the UDP port number for stream traffic. The port number set for this interface overrides the default transport port setting.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Cache Port</td>
<td>The UDP port number for cache traffic. The port number set for this interface overrides the default cache port setting.</td>
<td>All servers</td>
</tr>
<tr>
<td>Transport Group ID</td>
<td>The transport group ID this stream interface belongs to. This setting applies only to stream or stream/cache interfaces. For more information about transport groups, see the “Configuring Transport Groups” section on page 4-23.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td><strong>Stream Control Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stream Control IP</td>
<td>The IP address for this interface.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Stream Control Subnet</td>
<td>The subnet mask that defines the subnetwork for this interface.</td>
<td>Streamer, ISV</td>
</tr>
</tbody>
</table>

**Table 4-17  Server Setup Fields (continued)**
Configuring the Route Table

The Route Table allows you to enter separate default gateways for stream and cache traffic, as well as many static routes as necessary. You need to enter a default gateway so that IP destinations without a route to follow will have the Address Resolution Protocol (ARP) applied.

To configure a route, do the following:

---

**Step 1**
Choose Configure > Server Level > Route Tables. The Routing Table page is displayed with all configured routes listed (Figure 4-29).

![Figure 4-29 Route Table Page—Layer 3 Network](image)

**Step 2**
Enter the route settings as appropriate. See Table 4-18 for descriptions of the fields.
Table 4-18  Route Table Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>IP address of the destination network or host. Enter 0.0.0.0 for default gateway.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask of the destination network or host. Enter 0.0.0.0 for default gateway.</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the next hop (primary datagram transmitter and receiver) along the route to the destination network. Enter 0.0.0.0 for a local host.</td>
</tr>
<tr>
<td>Transport Group ID</td>
<td>Select a Transport Group ID associated with this route. See the “Configuring Transport Groups” section on page 4-23 for more information.</td>
</tr>
</tbody>
</table>

To enter a default gateway, enter 0.0.0.0 for the network address and subnet mask.
To enter a local host, enter 0.0.0.0 for the gateway.

**Step 3** Click **Submit**.
To reset the field, click **Reset**.

---

**Network Information**

To edit the network information, do the following:

**Step 1** Enter the network information as appropriate. See Table 4-19 for descriptions of the fields. The default gateway and local network can be the same for both stream and cache traffic.

Table 4-19  Network Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Default Gateway</td>
<td>The default gateway for all stream traffic.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Stream Local Network</td>
<td>Defines the local network (along with the subnet mask) for all stream traffic.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Stream Subnet Mask</td>
<td>The subnet mask for the stream traffic local network.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>Cache Default Gateway</td>
<td>The default gateway for all cache traffic.</td>
<td>All servers except ISVs</td>
</tr>
<tr>
<td>Cache Local Network</td>
<td>The local network for all cache traffic.</td>
<td>All servers except ISVs</td>
</tr>
<tr>
<td>Cache Subnet Mask</td>
<td>The subnet mask for the cache traffic local network.</td>
<td>All servers except ISVs</td>
</tr>
</tbody>
</table>

1. Required only for Layer 3 networks.

**Step 2** Click **Submit**.

To delete a route, select the **Delete** check box next to the applicable route in the Configured Route portion of the page and click **Submit**.
To edit a route or network information, enter the new settings in the Configured Route portion of the page. After making your changes, click Submit.

**Configuring the SNMP Agent**

The SNMP Agent sets up SNMP on the CDS. For more information about SNMP on the CDS, see Appendix B, “SNMP MIB and Trap Information.”

To configure the SNMP Agent settings for a new server, do the following:

**Step 1** Choose **Configure > Server Level > SNMP**. The SNMP Agent page is displayed (Figure 4-30).

![Figure 4-30 SNMP Agent Page](image)

**Step 2** Choose the server’s IP address from the drop-down list and click **Display**.

**Step 3** Enter the settings as appropriate. The fields are described in **Table 4-20**.
Table 4-20  
**SNMP Agent Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Contact</td>
<td>Specify a name used to identify the point of contact for this server. You may specify a name with up to 64 characters.</td>
</tr>
<tr>
<td>SNMP Location</td>
<td>Specify the location of the server. You may enter a name with up to 64 characters.</td>
</tr>
<tr>
<td>Community Name</td>
<td>Enter a community string that will have access to this server through SNMP.</td>
</tr>
<tr>
<td>Permissions</td>
<td>The permissions for the community are:</td>
</tr>
<tr>
<td></td>
<td>• read-only</td>
</tr>
<tr>
<td></td>
<td>• read/write</td>
</tr>
<tr>
<td></td>
<td>The default is read/write.</td>
</tr>
<tr>
<td></td>
<td>If you do not select a permission setting for a community you are adding, read/write privileges will be applied.</td>
</tr>
<tr>
<td>Trap Station</td>
<td>The IP address or Fully Qualified Domain Name (FQDN) of a network management station.</td>
</tr>
<tr>
<td>Version</td>
<td>The SNMP versions supported in the CDSM are:</td>
</tr>
<tr>
<td></td>
<td>• v1</td>
</tr>
<tr>
<td></td>
<td>• v2</td>
</tr>
<tr>
<td></td>
<td>• v2-inform</td>
</tr>
<tr>
<td></td>
<td>SNMP v2-inform sends a <em>message received</em> to the NMS upon receiving an NMS message.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> There is no default for the SNMP version. If you do not select an SNMP version for a trap station you are adding, SNMP communication will not be successful to that station.</td>
</tr>
</tbody>
</table>

**Step 4**  
Click **Submit** to save the settings.  
To clear the fields and start over, click **Reset**.

**Step 5**  
To add another SNMP community or SNMP station, fill in the appropriate fields and click **Submit**.

To edit the SNMP information, choose the server’s IP address from the drop-down list, edit the fields, and click **Submit**.

The SNMP page allows for multiple entries of SNMP communities and stations. If you want to delete an SNMP community or station, check the **Delete** check box associated with the entry and click **Submit**.
Configuring the Server Level DNS Binding

The DNS binding settings are used to configure the DNS services for a specific server.

**Caution**

If you have individual DNS settings configured for a server and you change the Array Level DNS binding settings, the individual DNS settings are overwritten. Therefore, first configure the higher level settings before configuring the individual Server Level settings.

To configure the DNS binding settings for a server, do the following:

**Step 1** Choose **Configure > Server Level > DNS Binding**. The DNS Binding page is displayed (Figure 4-31).

**Figure 4-31  DNS Binding—Server Level Page**

![Figure 4-31 DNS Binding—Server Level Page](image)

**Step 2**

Select the server’s IP address from the drop-down list and click **Display**.

**Step 3**

Enter the DNS binding Server Level settings as appropriate. See Table 4-21 for descriptions of the fields.

**Table 4-21  DNS Binding Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Suffix</td>
<td>Specify, if applicable, the internal domain that is used to fully qualify an unqualified hostname. For example, if you are using OpenStream as the BMS, specify a subdomain consistent with what OpenStream is using, for example, bms.n2bb.com. Accordingly, unqualified hostnames used in CORBA transactions, such as contentstore, resolve correctly to contentstore.bms.n2bb.com.</td>
</tr>
</tbody>
</table>
Chapter 4 Configuring the CDS

**Configuring RTSP Setup**

Real Time Streaming Protocol (RTSP) setup involves different parameters based on the RTSP deployment that was specified during the initial installation of the CDS. Table 4-22 describes each type of deployment.

<table>
<thead>
<tr>
<th>Environment</th>
<th>RTSP Deployment Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorola</td>
<td>RTSP</td>
<td>Streamer acts as the RTSP client and the backoffice acts as the RTSP server.</td>
</tr>
<tr>
<td>IPTV</td>
<td>IPTV</td>
<td>IPTV uses multicasting with Internet Group Management Protocol (IGMP) version 2 for live television broadcasts and RTSP for on-demand programs.</td>
</tr>
<tr>
<td>Scientific Atlanta</td>
<td>DSM-CC</td>
<td>Streamer acts as the RTSP server and the backoffice acts as the RTSP client.</td>
</tr>
<tr>
<td>NGOD (Motorola)</td>
<td>NGOD</td>
<td>The Next Generation On Demand (NGOD) approach uses DSM-CC messaging in a Motorola environment.</td>
</tr>
<tr>
<td>Telenet (Scientific Atlanta)</td>
<td>Telenet</td>
<td>Set-top box (STB) communicates with the backoffice to create a VOD session. Upon session completion, the STB creates an RTSP session with the Streamers. The Streamer acts as an RTSP server and is responsible for accepting the request from the set-top box.</td>
</tr>
<tr>
<td>Quative</td>
<td>Quative</td>
<td>The STB communicates with the backoffice to create a VOD session. Upon completion, the STB creates an RTSP session with the Streamers. The Streamer acts as an RTSP server and is responsible for accepting the request from the STB.</td>
</tr>
<tr>
<td>EventIS</td>
<td>EventIS</td>
<td>The STB communicates with the backoffice to initiate a purchase transaction and generate an entitlement ID. The STB then initiates an RTSP session with the Streamer. The Streamer authenticates the entitlement ID with the backoffice and allocates stream resources. The EventIS deployment with “on vpath” is selected when both session and stream control messages go directly to the RTSP server from the STB. The EventIS deployment with “off vpath” is selected when control messages go through the backoffice before reaching the RTSP server, while the stream control messages go directly to the RTSP server.</td>
</tr>
</tbody>
</table>
RTSP Deployment

To configure the RTSP settings, do the following:

Step 1  Choose Configure > Server Level > RTSP Setup. The RTSP Setup page is displayed.

Step 2  From the Streamer Select drop-down list, choose a Streamer IP address and click Display. The RTSP settings for the specified server are displayed (Figure 4-32).

Figure 4-32  RTSP Setup Page for RTSP Deployment

Step 3  Enter the RTSP settings as appropriate. Table 4-23 describes each field and lists the associated RTSP deployment.
## Table 4-23 RTSP Fields for All Deployment

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>RTSP Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Looping Session Timeout</td>
<td>The activity timeout value for looping streams (carousels). If a GET_PARAMETER request (heartbeat) is received from the backoffice within the specified timeout period, the looping session remains active. If not, the looping session is torn down. The default is 240000 milliseconds (4 minutes).</td>
<td>RTSP</td>
</tr>
<tr>
<td>Session Inactivity Timeout</td>
<td>The timeout value for tearing down a session. The default is 360000 milliseconds (6 minutes). If the Session Inactivity Timeout is set to zero (0), the session liveness is not checked.</td>
<td>RTSP, NGOD, IPTV, Telenet, Quative, EventIS</td>
</tr>
<tr>
<td>Callback Server IP</td>
<td>The IP address of the callback server. The CDS sends announce messages to the callback server whenever an RTSP session is torn down and released by the RTSP server. Announce messages are sent for both normal (STB initiated) and abnormal (timeout) terminations.</td>
<td>Quative</td>
</tr>
<tr>
<td>Callback Server Port</td>
<td>The UDP port number of the callback server.</td>
<td>Quative</td>
</tr>
<tr>
<td>Backoffice Timeout</td>
<td>The timeout value for closing a connection to the backoffice. If a message is not received from the backoffice within the time specified in the Backoffice Timeout, the TCP connection is closed. Setting the Backoffice Timeout to zero (0) is the same as disabling it and the connection will not be closed.</td>
<td>DSM-CC, RTSP, NGOD, Quative</td>
</tr>
<tr>
<td>RTSP Server IP</td>
<td>The IP address of the server that communicates with this Streamer using RTSP.</td>
<td>DSM-CC, RTSP, NGOD, Quative</td>
</tr>
<tr>
<td>RTSP Server Port</td>
<td>The TCP port number the RTSP server is listening on for communication with this Streamer.</td>
<td>DSM-CC, RTSP, NGOD, Quative</td>
</tr>
<tr>
<td>Master Streaming IP</td>
<td>The IP address of the master Streamer.</td>
<td>Telenet, EventIS</td>
</tr>
<tr>
<td>Authentication Manager IP1</td>
<td>The Authentication Manager resides on the master Streamer. Typically, the Authentication Manager IP address is the same as that of the master Streamer. This field is only informational. To modify this field, see the “Configuring the Authentication Manager” section on page 4-14.</td>
<td>Telenet, EventIS</td>
</tr>
<tr>
<td>Authentication Manager Port</td>
<td>The Authentication Manager port number is determined by the properties specifications of the Authentication Manager. If you need to change the port number, contact Cisco technical support. This field is only informational. If you must modify this field, see the “Configuring the Authentication Manager” section on page 4-14. The default is 7792.</td>
<td>Telenet, EventIS</td>
</tr>
</tbody>
</table>
### Table 4-23 RTSP Fields for All Deployment (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>RTSP Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Manager IP*</td>
<td>The Bandwidth Manager resides on the master Streamer. Typically, the Bandwidth Manager IP address is the same as that of the master Streamer. If the Bandwidth Manager IP address is set on the Bandwidth Manager page, then this field is only informational and if you must modify this field, see the “Configuring the Bandwidth Manager” section on page 4-9. If the Bandwidth Manager IP address on the Bandwidth Manager page is set to an asterisk (*) or 0.0.0.0, then you must enter the IP address for the Bandwidth Manager in this field for each Streamer.</td>
<td>Telenet, EventIS on vpath</td>
</tr>
<tr>
<td>Bandwidth Manager Port*</td>
<td>The Bandwidth Manager port number default is 7791. This port number is determined by the configuration settings in the Bandwidth Manager. If the Bandwidth Manager IP address is set on the Bandwidth Manager page, then this field is only informational and if you must modify this field, see the “Configuring the Bandwidth Manager” section on page 4-9. If the Bandwidth Manager IP address on the Bandwidth Manager page is set to an asterisk (*) or 0.0.0.0, then you must enter the port number for the Bandwidth Manager in this field for each Streamer.</td>
<td>Telenet, EventIS on vpath</td>
</tr>
<tr>
<td>Backup Bandwidth Manager IP*</td>
<td>The IP address of the network interface card (NIC) you want the Bandwidth Manager to bind to in case the primary Bandwidth Manager IP and port fail.</td>
<td>EventIS on vpath</td>
</tr>
<tr>
<td>Backup Bandwidth Manager Port*</td>
<td>The port number to listen on for incoming connections from the RTSP server. The default is 7791. The minimum port number you can allocate is 150. The maximum port number is 60000.</td>
<td>EventIS on vpath</td>
</tr>
<tr>
<td>Server IP</td>
<td>The IP address used by the backoffice or Session Resource Manager (SRM) for communication of session control requests to the CDS RTSP server.</td>
<td>EventIS off vpath</td>
</tr>
<tr>
<td>Server Port</td>
<td>The port number used by the backoffice or SRM for communication of session control requests to the CDS RTSP server.</td>
<td>EventIS off vpath</td>
</tr>
<tr>
<td>Stream Control IP</td>
<td>The IP address used by the STB for communication of trickmode requests to the CDS RTSP server. This does not have to be the same IP address as the Control IP.</td>
<td>EventIS off vpath</td>
</tr>
<tr>
<td>Stream Control Port</td>
<td>The port number used by the STB for communication of trickmode requests to the CDS RTSP server.</td>
<td>EventIS off vpath</td>
</tr>
<tr>
<td>Reconnect IP</td>
<td>Only for nABLE Motorola environments. The IP address on the Streamer used to receive the requests to reconnect to the backoffice server. After a connection has been established with the backoffice for RTSP communication, sometimes the backoffice sends a request to reconnect.</td>
<td>RTSP</td>
</tr>
</tbody>
</table>
### Table 4-23  RTSP Fields for All Deployment (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>RTSP Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnect Port</td>
<td>Only for nABLE Motorola environments. The TCP port number on the Streamer used to receive the requests to reconnect.</td>
<td>RTSP</td>
</tr>
<tr>
<td>LSCP Listener IP</td>
<td>The IP address on the Streamer used to receive LSCP requests.</td>
<td>DSM-CC, NGOD</td>
</tr>
<tr>
<td>LSCP Listener Port</td>
<td>The TCP port number on the Streamer that is listening for LSCP commands from the set-top box. The default is 9000.</td>
<td>DSM-CC, NGOD</td>
</tr>
<tr>
<td>LSCP Response Pad</td>
<td>When LSCP Response Padding is enabled, three blank bytes are added to the end of the LSCP response. The default is disabled.</td>
<td>DSM-CC, NGOD</td>
</tr>
<tr>
<td>Component Name</td>
<td>The component name is the name of the master Streamer that is registered with the DNS server. This is a critical communication component and must match the table entry in the DNS server.</td>
<td>NGOD, Telenet</td>
</tr>
<tr>
<td>Logical SOP</td>
<td>The logical Streaming Output Port (SOP) is a domain name of this Streamer for identification purposes to the On Demand Resource Manager (ODRM).</td>
<td>NGOD</td>
</tr>
<tr>
<td>Physical SOP IP</td>
<td>The IP address of the SOP.</td>
<td>NGOD</td>
</tr>
<tr>
<td>Physical SOP Port</td>
<td>The port number of the SOP.</td>
<td>NGOD</td>
</tr>
<tr>
<td>Max History</td>
<td>The number of transactions (trick mode, play, pause) to maintain before sending the RTSP log message to the backoffice. If set to zero (0), the log message is not generated and the history is not returned upon session teardown.</td>
<td>RTSP</td>
</tr>
<tr>
<td>Log Level</td>
<td>From the <strong>Log Level</strong> drop-down list, choose one of the following:</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>• Off—Logging is turned off.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Low—Logging messages are minimal in length (for example, RTSP message received).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• High—Logging messages include all information concerning the event (for example, RTSP message with all syntax of the message).</td>
<td></td>
</tr>
<tr>
<td>Maintenance Mode</td>
<td>From the <strong>Maintenance Mode</strong> drop-down list, choose one of the following:</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>• On—All current sessions will continue until they are finished and all new SETUP requests will receive a “Service Unavailable” response.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off—The Streamer is available for new sessions and will continue streaming current sessions.</td>
<td></td>
</tr>
</tbody>
</table>

1. The Authentication Manager and Bandwidth Manager fields are not displayed if these features are not part of your deployment.
Step 4  Configure the clients that will communicate with the Streamer. The clients consist of the set-top boxes, which typically require only one client definition.

The client configuration is displayed in a delimited string format:

```
1)rtsp | 3636 | 3636 | 65535 | quative | parameters | TCP
```

In this format, `rtsp` is the deployment, 3636 is the receive port on the Streamer and the receive port on the client, 65535 is the receive buffer size, `quative` is the client model, `parameters` is the message payload type, and `TCP` is the transport protocol.

- To edit an existing client, click **Edit** next to the client definition.
- To delete an existing client, click **Delete** next to the client definition.
- To add a new client, click **Add New Client**.

Table 4-24 describes the fields for the client definitions.

### Table 4-24  Client Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive Port</td>
<td>Port used for receiving messages from the client.</td>
</tr>
<tr>
<td>Send Port</td>
<td>Port used to send messages to the client.</td>
</tr>
<tr>
<td>Receive Buffer</td>
<td>Receive buffer size, in bytes, for the listener socket. The receive buffer can be set to either 65535 for TCP transport or 512000 for UDP transport. Quative always uses TCP transport.</td>
</tr>
<tr>
<td>Model</td>
<td>Client model type to use for communication with the client. The types are:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- nCUBE</td>
</tr>
<tr>
<td></td>
<td>- Digeo</td>
</tr>
<tr>
<td></td>
<td>- NGOD</td>
</tr>
<tr>
<td></td>
<td>- Myrio</td>
</tr>
<tr>
<td></td>
<td>- Telenet</td>
</tr>
<tr>
<td></td>
<td>- Quative</td>
</tr>
<tr>
<td></td>
<td>- EventIS</td>
</tr>
<tr>
<td></td>
<td>A client model of nCUBE means the client uses RTSP with nCUBE syntax. A Digeo client model uses Digeo syntax, and so on.</td>
</tr>
<tr>
<td>Transport</td>
<td>Transport protocol, either UDP or TCP, used for streaming. The transport protocol is always TCP for Telenet and Quative.</td>
</tr>
</tbody>
</table>

Step 5  Click **Submit**.

To clear the fields and start over, click **Reset**.
Configuring FSI Setup

The File Service Interface (FSI) allows the backoffice to communicate file-related requests to the Vault. These requests include ingesting content, preparation of content files (for example, trick mode creation), and distribution of the content.

To configure the FSI settings, do the following:

**Step 1** Choose **Configure > Server Level > FSI Setup**. The FSI Setup page is displayed.

**Step 2** From the **Vault Select** drop-down list, choose an IP address and click **Display**. The FSI settings for the specified server are displayed (Figure 4-33).

**Figure 4-33** FSI Setup Page

**Step 3** Enter the FSI settings as appropriate. See **Table 4-25** for descriptions of the fields.

**Table 4-25** FSI Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSI IP Address</td>
<td>The IP address of the Vault used in FSI communications with the backoffice. The recommended configuration is to enter 0.0.0.0 to allow all incoming IP interfaces on the Vault to be used for FSI communications.</td>
</tr>
<tr>
<td>FSI Server Port</td>
<td>The port number on the Vault used in FSI communications with the backoffice. The default is 20004.</td>
</tr>
</tbody>
</table>
### Table 4-25  FSI Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP Client Port</td>
<td>The port used by FSI communications when connecting to the catcher, or other FTP server, in order to pull in content, and when the FTP port is not specified in the ingest URL. The default is 21.</td>
</tr>
<tr>
<td>FTP Out Server Port</td>
<td>The port used by FSI communications for egress (FTP out pulls) from the Vault. The default is 21.</td>
</tr>
<tr>
<td>FTP Out Login TTL</td>
<td>The time, in seconds, an FTP client has to connect and log in to the Vault to perform an FTP out pull with a temporary login. The default is 60.</td>
</tr>
<tr>
<td>Log Level</td>
<td>From the Log Level drop-down list, choose one of the following:</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Off—Logging is turned off.</td>
<td></td>
</tr>
<tr>
<td>Low—Logging messages are minimal in length (for example, RTSP message received).</td>
<td></td>
</tr>
<tr>
<td>High—Logging messages include all information concerning the event (for example, RTSP message with all syntax of the message).</td>
<td></td>
</tr>
<tr>
<td>FSI Content Root Path</td>
<td>The root directory used to store MPEG content files on the Vault. This field is used in both nABLE and NGOD RTSP deployments. The default is /files.</td>
</tr>
<tr>
<td>Async. Callback URL</td>
<td>For IPTV deployments only. The asynchronous callback URL is where the recording completion notification is sent when a scheduled recording completes its capture. This URL is basically used to tell the client the recording is completed.</td>
</tr>
</tbody>
</table>

**Step 4**  
Click **Submit**.  
To clear the fields and start over, click **Reset**.
System Monitoring

The CDSM provides tools that can be used for system monitoring and system diagnostics. The topics covered in this chapter include:

- System Level Monitoring, page 5-1
- Monitoring Content Objects, page 5-4
- Monitoring Stream Objects, page 5-13
- Array Level Monitoring, page 5-21
- Server Level, page 5-22
- Recommended Monitoring Schedule, page 5-31

System Level Monitoring

The System Level Monitoring pages provide an overall view of the health and activity of the CDS. The System Level links are:

- System Health
- System Snapshot

To view the System Level Monitoring pages, click Monitor from any page in the CDSM, and then click System Health or System Snapshot, as appropriate.

System Health

The System Health page provides a top-level view of the overall health of each server in the CDS. Any time there is a system health problem, an alarm is displayed in the CDSM banner. See Figure 5-1.

Figure 5-1 CDSM Banner—System Health Alarm

To view the System Health page, choose Monitor > System Health. See Figure 5-2.
The colored boxes on the System Health Monitor page have the following meaning:

- **Green**—All components are operating.
- **Yellow**—Some components are not operational.
- **Red**—All components have failed.

You can view the details of a monitored area of a server by clicking the box in the appropriate column.

- When you click the **Network** check box you are taken to the NIC Monitor page. See the “NIC Monitor” section on page 5-25 for more information.
- When you click the **Disk** check box you are taken to the Disk Monitor page. See the “Disk Monitor” section on page 5-22 for more information.
- When you click the **Services** check box you are taken to the Services Monitor page. See the “Services Monitor” section on page 5-29 for more information.

The time shown at the bottom of the left-panel menu is not the current time, but rather the CDSM time that is used for the health status and monitoring the system.
System Snapshot

The System Snapshot page provides an overview of the current activity on the CDS. A summary of the state of all streams, content ingests, and disk usage is displayed. See Figure 5-3.

Table 5-1 describes the information displayed on the System Snapshot page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Refresh Rate</td>
<td>How often the information is refreshed. The default is 10 seconds. The range is 10 to 300. All field values that are updated, based on the refresh rate, are initially shown in a green colored font.</td>
</tr>
<tr>
<td>Total Streams</td>
<td>Total number of stream objects the CDS is currently streaming.</td>
</tr>
<tr>
<td>HD Streams</td>
<td>Total number of high-definition stream objects the CDS is currently streaming.</td>
</tr>
<tr>
<td>SD Streams</td>
<td>Total number of standard-definition stream objects the CDS is currently streaming.</td>
</tr>
</tbody>
</table>
Monitoring Content Objects

The content objects links on the Monitor System Level page provides information on the status of content ingests. Table 5-2 describes the different ingest states that are monitored.

### Table 5-2 Monitored Ingest States

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed Ingests</td>
<td>Lists content objects that have been fully ingested.</td>
</tr>
<tr>
<td>Active Ingests</td>
<td>Lists content objects that are in the process of being ingested.</td>
</tr>
<tr>
<td>Package Expiration</td>
<td>Lists Package Expiration information, including expiration dates and all</td>
</tr>
<tr>
<td></td>
<td>associated metadata. Allows for package expiration adjustments.</td>
</tr>
<tr>
<td>Publish Failures</td>
<td>Lists the packages that were not able to be published to the backoffice and</td>
</tr>
<tr>
<td></td>
<td>provides a mechanism to republish the package.</td>
</tr>
</tbody>
</table>

Ingests

To view the details of content object ingests, do the following:

**Step 1** Choose **Monitor > System Level** from any page in the CDSM. and then click the link for the type of content object you want to view:

- Completed Ingests
- Active Ingests
Step 2  Select a content object from the drop-down list and click Display. The details of the content object are displayed. Figure 5-4 shows an example of the ingest details.

By typing the first character of the content object name, you can jump to that section of the list.

In addition, you can perform a text string search by typing the text string you want to search for in the Search Ingests field and clicking Search. A list of content objects that contain the text string are listed. To see the content object details, click the content object name listed. To return to the previous page without selecting a content object, click Back.

Figure 5-4  Completed Ingests Page

Table 5-3 describes the content object details that are displayed for each type of ingest.
### Table 5-3  Content Object Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Name</td>
<td>The name of the content object.</td>
</tr>
<tr>
<td>Factory ID</td>
<td>The factory responsible for this content object.</td>
</tr>
<tr>
<td>Ingest IP</td>
<td>The IP address of the Vault’s ingest interface used to download the content.</td>
</tr>
<tr>
<td>File Size</td>
<td>The file size, in bytes, of this content object.</td>
</tr>
<tr>
<td>Rate</td>
<td>The rate of ingest in bits per second (3750000 = 3.75 \text{ Mbps}).</td>
</tr>
<tr>
<td>Create Time</td>
<td>The time and date this content object was created.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>The time and date this content object was last modified.</td>
</tr>
<tr>
<td>Op State</td>
<td>The operational state of this content object. The possible operational states are:</td>
</tr>
<tr>
<td></td>
<td>• Created—Content is loading.</td>
</tr>
<tr>
<td></td>
<td>• In Service—Content is available for streaming.</td>
</tr>
<tr>
<td></td>
<td>• Out of Service—Content is not available for streaming.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this content object. The possible administrative states are:</td>
</tr>
<tr>
<td></td>
<td>• Unprovisioned—Content is loading.</td>
</tr>
<tr>
<td></td>
<td>• In Service—Content is available for streaming.</td>
</tr>
<tr>
<td></td>
<td>• Out of Service—Content is not available for streaming.</td>
</tr>
<tr>
<td>Push Provision</td>
<td>The type of FTP provisioned. The provision types are:</td>
</tr>
<tr>
<td></td>
<td>• FTP pull</td>
</tr>
<tr>
<td></td>
<td>• FTP push</td>
</tr>
<tr>
<td>Content Copies</td>
<td>The Content Copies fields display the following information about the copies of the content object:</td>
</tr>
<tr>
<td></td>
<td>Speed/Direction—The trick-mode speed and direction (fast forward or rewind).</td>
</tr>
<tr>
<td></td>
<td>Server ID—The server ID where the copy is stored.</td>
</tr>
<tr>
<td></td>
<td>Status—The status of the stored content.</td>
</tr>
<tr>
<td>Trick Speeds [1-8]</td>
<td>Trick speeds 1 through 8 show the trick-mode speeds for this content object.</td>
</tr>
<tr>
<td>Full Content ID</td>
<td>The full identification of this content object.</td>
</tr>
<tr>
<td>URL(^1)</td>
<td>The Uniform Resource Locator (URL) address of the content providing the following:</td>
</tr>
<tr>
<td></td>
<td>• Protocol used (for example, FTP)</td>
</tr>
<tr>
<td></td>
<td>• Username and password (for example, videolan:mpeg4ftp)</td>
</tr>
<tr>
<td></td>
<td>• IP address of the content provider’s server (for example, 192.168.100.184)</td>
</tr>
<tr>
<td></td>
<td>• Directory where the content is stored on the provider’s server (for example, videolan)</td>
</tr>
<tr>
<td></td>
<td>• Name of the file (for example, long_encore_3.75.mpg)</td>
</tr>
</tbody>
</table>

\(^1\) Not displayed in Figure 5-4.
List Content

The List Content option on the Completed Ingests page lists all content objects, that meet the criteria (Only Damaged or List All), that are associated with each content.

To list all associated content objects, do the following:

**Step 1** Choose Monitor > System Level > Completed Ingests. The Completed Ingest page is displayed.

**Step 2** In the List Content area, choose Only Damaged to list only the damaged content objects, or choose List All to list all content objects, and click List. The Content List is displayed (Figure 5-5).
Figure 5-5  Completed Ingests—Content List

<table>
<thead>
<tr>
<th>Content Name</th>
<th>Duration</th>
<th>Codel()</th>
<th>Version()</th>
<th>Server ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>100a_KRH_2D1_journey_9Am.mpg</td>
<td>01:04:19</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>Complete</td>
</tr>
<tr>
<td>100b_KRH_2D1_journey_10Am.mpg</td>
<td>02:03:23</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>Complete</td>
</tr>
<tr>
<td>100c_KRH_2D1_journey_11Am.mpg</td>
<td>05:10:55</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>Complete</td>
</tr>
<tr>
<td>100d_KRH_2D1_journey_12Am.mpg</td>
<td>04:32:29</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>Complete</td>
</tr>
</tbody>
</table>

This describes the information displayed in the Content List.
Table 5-4  Content List Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Name</td>
<td>The name of the content.</td>
</tr>
<tr>
<td>Duration</td>
<td>The duration of the content.</td>
</tr>
<tr>
<td>GOID</td>
<td>The Global Object ID for the content object associated with the content.</td>
</tr>
<tr>
<td>Version</td>
<td>The trick-play speed of the content object. The value, IGate, refers to an index file, which allows for the jumps between trick speeds, and so on. The value, redo, is an undo file. When the content is ingested, if there are any changes made during the ingest, the changes are recorded in the redo file. If the content is sent by using FTP Out, the changes are undone and the original file is sent.</td>
</tr>
<tr>
<td>Server ID</td>
<td>The server ID of the Vault that is storing the content object.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the storing process of the content object, either complete or partial.</td>
</tr>
</tbody>
</table>

**Packages**

*Note*  
Package Expirations are part of the optional Ingest Manager feature. This option is only listed on the Monitoring System Level left-panel menu if the Ingest Manager is included in your deployment.

To view the details or adjust the license expiration of a package expiration, do the following:

**Step 1**  
Choose Monitor > Package Expiration. The Package Expiration page is displayed.

**Step 2**  
From the Available Packages drop-down list, choose a package and click Display. The Package Expiration details are displayed.

By typing the first character of the package name, you can jump to that section of the list.  
Figure 5-7 shows an example of the Package Expiration details.
**Table 5-5** describes the package expiration details that are displayed.

**Table 5-5  Package Expiration Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Name</td>
<td>The name of the package.</td>
</tr>
<tr>
<td>License Expiration</td>
<td>The date the package will expire.</td>
</tr>
<tr>
<td>Additional Package Window</td>
<td>The additional time added to the package.</td>
</tr>
<tr>
<td>Actual Package Expiration</td>
<td>The Actual Package Expiration is the License Expiration plus the Additional Package Window.</td>
</tr>
</tbody>
</table>

**Step 3**

To adjust the license expiration, enter the number of days (positive or negative) in the **Adjust License Expiration** field and click **Update**.

The license expiration is adjusted by the number of days you entered. The Additional Package Window is not affected and still is applied to create the Actual Package Expiration.
Step 4  In the Asset Details section, to view the metadata associated with the package expiration, click the plus sign (+) next to the metadata you want to view.

To delete a package, choose the package from the Available Packages drop-down list, click Display and then click Delete in the Package Expiration Details section.

Publish Failures

Note  Publish Failures are part of the optional Ingest Manager feature. This option is only listed on the Monitoring System Level left-panel menu if the Ingest Manager is included in your deployment.

The publish failures lists the packages that were not able to be published to the backoffice and provides a mechanism to republish the package.

To publish an unpublished package, or delete an unpublished package, do the following:

Step 1  Choose Monitor > Publish Failures. The Publish Failures page is displayed.

Step 2  From the Unpublished Packages drop-down list, choose a package and click Display. The Unpublished Package details are displayed.

By typing the first character of the package name, you can jump to that section of the list.

Figure 5-7 shows an example of the Publish Failures details.
Table 5-6 describes the publish failures details that are displayed.

Table 5-6  Publish Failures Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Name</td>
<td>The name of the package.</td>
</tr>
<tr>
<td>Source URL</td>
<td>The location of the original package information.</td>
</tr>
<tr>
<td>Target URL</td>
<td>The location where to place the package information.</td>
</tr>
<tr>
<td>Module Type</td>
<td>An internal identifier for what failed. In the example in Figure 5-7, the publishing of the package failed.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>The date the database record was created for this failure.</td>
</tr>
</tbody>
</table>

**Step 3**  In the Assets section, to view the metadata associated with the unpublished package, click the plus sign (+) next to the metadata you want to view.

**Step 4**  To restart the publishing process and set the creation date to today, click Publish. To delete an unpublished package, click Delete.
## Monitoring Stream Objects

The monitored stream objects consist of:

- Stream Monitor
- Stream Failures

### Stream Monitor

To view the details of stream objects, do the following:

**Step 1** Choose **Monitor > Stream Monitor**. The Stream Monitor page is displayed.

**Step 2** From the **Browse By Session ID** drop-down list, choose the Session ID of the stream object and click **Display**. The stream object details are displayed.

If you do not know the session ID, you can perform a text string search by selecting the field you want to search on, entering the text string in the **Search String** field, and clicking **Search**. A list of stream objects that contain the text string in the field you selected are listed. Click the linked field (Session Handle in Figure 5-8) to see the stream monitor details for the selected object, or click **Back** to return to the previous page.

**Figure 5-8 Stream Search Results**

<table>
<thead>
<tr>
<th>Session Handle</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Client IP</th>
<th>Client Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.12</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
<tr>
<td>192.168.1.42</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
<tr>
<td>192.168.1.42</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
<tr>
<td>192.168.1.42</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
<tr>
<td>192.168.1.42</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
<tr>
<td>192.168.1.42</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
<tr>
<td>192.168.1.42</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
<tr>
<td>192.168.1.42</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
<tr>
<td>192.168.1.42</td>
<td>192.168.1.42</td>
<td>4000</td>
<td>17.1.70.48.254</td>
<td>354</td>
</tr>
</tbody>
</table>

**Figure 5-9** shows an example of the stream object details.
Table 5-7 describes the stream details.
### Table 5-7  Stream Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Handle</td>
<td>The internal unique identifier assigned to the stream session by the Streamer.</td>
</tr>
<tr>
<td>RTSP Session ID</td>
<td>The RTSP identifier of the stream session that is used in communications with the backoffice and set-top box.</td>
</tr>
<tr>
<td>External Session ID</td>
<td>The session identifier generated by the backoffice.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>The IP address used to receive the stream (for example, the QAM or set-top box).</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The port number used to receive the stream (for example, the QAM or set-top box).</td>
</tr>
<tr>
<td>Client IP</td>
<td>The IP address of the set-top box that requested the stream.</td>
</tr>
<tr>
<td>Client Port</td>
<td>The set-top box port number used to send the stream request.</td>
</tr>
<tr>
<td>Session Group ID</td>
<td>An identifier defined by the backoffice for a logical grouping of sessions.</td>
</tr>
<tr>
<td>Allocated Bandwidth</td>
<td>The bandwidth allocated for this stream session.</td>
</tr>
<tr>
<td>Current Operation</td>
<td>The current set-top box operation. The possible operations are:</td>
</tr>
<tr>
<td></td>
<td>• Normal Play</td>
</tr>
<tr>
<td></td>
<td>• Paused</td>
</tr>
<tr>
<td></td>
<td>• Fast Forward</td>
</tr>
<tr>
<td></td>
<td>• Rewind</td>
</tr>
<tr>
<td>Operation Start</td>
<td>The start time of the currently active operation.</td>
</tr>
<tr>
<td>LSCP Mode</td>
<td>The valid LSCP modes are:</td>
</tr>
<tr>
<td></td>
<td>• Open—The server is not transporting a media stream.</td>
</tr>
<tr>
<td></td>
<td>• Pause—The server is not transporting a media stream.</td>
</tr>
<tr>
<td></td>
<td>• Search transport—The server is searching for start NPT (normal play time). When at start NPT, it enters the Transport mode.</td>
</tr>
<tr>
<td></td>
<td>• Transport—The server is transporting the media stream and will pause at the end of the stream. If scale is positive, indicating a forward direction, end of stream is the end of media. If scale is negative, indicating a reverse direction, end of stream is the beginning of media.</td>
</tr>
<tr>
<td></td>
<td>• Transport pause—The server is transporting the media stream and will pause at stop NPT.</td>
</tr>
<tr>
<td></td>
<td>• Search transport pause—The server is transporting the media stream and will pause at stop NPT.</td>
</tr>
<tr>
<td></td>
<td>• Pause search transport—The server is transporting the media stream. It does so until stop NPT, and then transitions to search transport mode.</td>
</tr>
<tr>
<td></td>
<td>• End of stream—The server is not transporting a media stream.</td>
</tr>
<tr>
<td></td>
<td>LSCP is not used in a Motorola environment. In an nABLE Motorola environment, the value will always be 0.</td>
</tr>
<tr>
<td>Stream Looping</td>
<td>This field indicates whether stream looping is turned on or off for this stream.</td>
</tr>
</tbody>
</table>
The Graph This Stream button displays the trick-mode activity of the stream (Figure 5-10).
Figure 5-10  Stream Activity Report

To delete a stream object, display the object and click **Delete**.
Stream Failures

To view the details of Failed Streams, do the following:

**Step 1** Choose **Monitor > Failed Streams**. The Stream Failures page is displayed.

Each failed stream is listed by the date and time the stream failed followed by the session ID of the failed stream.

**Note** Stream Failure monitoring displays only the failed streams for the current day. To view past stream failures, see the “Stream Failures” section on page 6-13.

**Step 2** From the **Stream Failures** drop-down list, choose the timestamp and session ID of the stream object and click **Display**. The stream failure details are displayed. See **Figure 5-11**.

To delete a failed stream, display the object and click **Delete**.

**Figure 5-11  Stream Failures Page**
Table 5-8 describes the stream failure details.

Table 5-8 Stream Failure Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>The session ID of the failed stream.</td>
</tr>
<tr>
<td>Failure Date</td>
<td>The date and time the failure occurred.</td>
</tr>
<tr>
<td>QAM IP</td>
<td>The IP address of the QAM device associated with the failure.</td>
</tr>
<tr>
<td>Service Group</td>
<td>The service group associated with the failure.</td>
</tr>
<tr>
<td>Server ID</td>
<td>The server responsible for streaming this stream object. To view the IP address associated with the Server ID, see the “Configuring the Servers” section on page 4-41.</td>
</tr>
<tr>
<td>Group ID</td>
<td>All servers that are part of the same CDS system (managed by one CDSM) have the same groupid. This groupid should be unique across an enterprise.</td>
</tr>
<tr>
<td>Failed Operation</td>
<td>The operation that was taking place when the stream failed, for example, createStream, LSCP Command(), or createServant, destroy. These are the measurement points or transactional states of the system at the time of the failure.</td>
</tr>
<tr>
<td>Failed Task</td>
<td>A failed task is the event category that provides the type of execution sequence that the call stack was currently in at the time of the failure. The list of the high-level categories are:</td>
</tr>
<tr>
<td></td>
<td>• Tune In</td>
</tr>
<tr>
<td></td>
<td>• Load Application</td>
</tr>
<tr>
<td></td>
<td>• Load Catalog</td>
</tr>
<tr>
<td></td>
<td>• Eligibility Check</td>
</tr>
<tr>
<td></td>
<td>• Select Subscription</td>
</tr>
<tr>
<td></td>
<td>• Purchase Subscription</td>
</tr>
<tr>
<td></td>
<td>• Select Movie</td>
</tr>
<tr>
<td></td>
<td>• Purchase Check</td>
</tr>
<tr>
<td>Error Code</td>
<td>The error code provides a description of the event that caused an error. See Table 5-9 for descriptions of the error codes.</td>
</tr>
</tbody>
</table>
Table 5-9 lists the error codes for internal errors that specifically describe where the error occurred, and errors in the network or network components.

### Table 5-9 Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP_CONNECTION_FAILED</td>
<td>Connection to FTP server failed.</td>
</tr>
<tr>
<td>FTP_SERVER_BIND_FAILED</td>
<td>FTP server can not bind to the port.</td>
</tr>
<tr>
<td>FTP_PUSH_TIMEOUT</td>
<td>FTP push timeout (PASV is not served fast enough).</td>
</tr>
<tr>
<td>FTP_QUIT_RECEIVED_DURING_INGEST</td>
<td>FTP server received QUIT request.</td>
</tr>
<tr>
<td>NOT_ENOUGH_QAM_BANDWIDTH</td>
<td>Not enough QAM bandwidth.</td>
</tr>
<tr>
<td>CONTENT_CAN_NOT_BE_LOCATED</td>
<td>Content is not found in the related content stores.</td>
</tr>
<tr>
<td>SET_DESTINATION_FAILED</td>
<td>Failed while setting destination of the stream.</td>
</tr>
<tr>
<td>RTSP_REQUEST_INVALID</td>
<td>The RTSP request was not understood by the RTSP server. Either the syntax is incorrect or the method is unknown.</td>
</tr>
<tr>
<td>SESSION_NOT_FOUND</td>
<td>The RTSP session ID could not be found in the RTSP server.</td>
</tr>
<tr>
<td>RTSP_METHOD_NOT_VALID_IN_STATE</td>
<td>The RTSP request is not valid for the current RTSP session state.</td>
</tr>
<tr>
<td>RTSP_RANGE_NOT_VALID</td>
<td>The RTSP range header does not have valid values.</td>
</tr>
<tr>
<td>TRANSPORT_UNSUPPORTED</td>
<td>The transport header could not be parsed.</td>
</tr>
<tr>
<td>NO_DESTINATION_DEFINED</td>
<td>The transport header does not have a stream destination value.</td>
</tr>
<tr>
<td>INTERNAL_SERVER_ERROR</td>
<td>There was an internal server error during an RTSP request.</td>
</tr>
<tr>
<td>RTSP_SERVICE_UNAVAILABLE</td>
<td>The RTSP service is unavailable.</td>
</tr>
<tr>
<td>UNSUPPORTED_RTSP_VERSION</td>
<td>The RTSP version is not supported.</td>
</tr>
<tr>
<td>UNSUPPORTED_OPTION</td>
<td>The RTSP require header is not supported.</td>
</tr>
<tr>
<td>STREAMING_ERROR_READING_CONTENT</td>
<td>There was an error reading the content in a stream.</td>
</tr>
</tbody>
</table>
Array Level Monitoring

The Array Level Monitoring pages provide an overall view of the health and activity of a specified array.

Array Snapshot

The Array Snapshot page provides an overview of the current activity for the specified array of servers on the CDS. A summary of the state of all streams, content incepts, and disk usage is displayed. See Figure 5-12.

The fields displayed on the Array Snapshot page are the same fields that are displayed on the System Snapshot page, with the active stream bandwidth and active fill bandwidth shown for each Stream Group. For descriptions of the fields, see Table 5-1.

Figure 5-12  Array Snapshot Page
Server Level

The Server Level Monitoring pages provide detail information on the health and activity of a Vault or Streamer server.

To view the Server Level Monitoring pages, do the following:

**Step 1** Choose Monitor > Server Level, and then click one of the following as applicable:
- Disk Monitor
- NIC Monitor
- Cache/Fill Bandwidth
- Services Monitor

**Step 2** Select the IP address of the server from the drop-down list and click Display.

Disk Monitor

The Disk Monitor page provides real-time information on the status of a disk.

To view the current status of a disk, select a server’s IP address from the drop-down list on the Disk page, click Display, and roll your mouse over one of the disks displayed in the graphic. If the server is a Lindenhurst CDE, click one of the disks displayed in the graphic. Figure 5-13 shows an example of a Streamer server.
For Vault servers, the Disk Availability line graph shows the percentage of disk space available. The gigabytes displayed for “Total Space,” “Available Space,” and “% Used” are the sum of all the disks installed on the Vault server.

The Linux File System Stats table shows the combined total storage space for the partitions of the disk drives, the combined available storage space for the partitions of the disk drives, and the percentage of used storage for each combined partition. In Figure 5-13, the hda2 partition has an alarm indicator because the usage has exceeded the user-defined threshold of 40 percent. For information on setting thresholds, see the “Setting System Thresholds” section on page 7-10.

Table 5-10 describes the information displayed when a disk is selected.
The CDS incorporates S.M.A.R.T. to monitor the reliability of a hard drive, predict drive failures, and to carry out different types of drive self-tests. S.M.A.R.T. is firmware, native to most disk drives, that monitors disk attributes over time, making it possible to perform predictive failure analysis. Advanced warning of predictive failures allows the operator to perform preventative maintenance.

To view the current read/write activity that has occurred in the last five seconds on the selected disk, click Graph Disks. Figure 5-14 shows an example of the Disk Activity graph.
The Disk Activity graph displays an average calculation of the amount of data read (in megabytes per second) and data writes over a five-second period.

**NIC Monitor**

The NIC Monitor page displays the status of each network interface card (NIC) on the server.

To view the current status of a NIC on a server, select a server’s IP address from the drop-down list on the NIC Monitor page, click **Display**, and click one of the NIC ports displayed in the graphic. **Figure 5-15** shows an example of the eth4 interface on a Vault server.
Table 5-11 describes the information displayed for a NIC port.

**Table 5-11 NIC Port Status Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Speed</td>
<td>The speed of the interface in megabits per second (Mbps).</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the port interface. The administrative state is determined at the time the server is booted. The possible administrative states are up or down.</td>
</tr>
<tr>
<td>Op State</td>
<td>The operational state of the port interface. The operational state is either up or down. If the port is not connected to the network or is malfunctioning, the operational state displayed is down.</td>
</tr>
<tr>
<td>Media Type</td>
<td>The physical conduit of the interface. The physical type is either copper or fiber optic.</td>
</tr>
<tr>
<td>Poll Interval</td>
<td>The number of seconds between each disk polling.</td>
</tr>
</tbody>
</table>
To view the average transmit and receive activity that has occurred in the last two seconds for each port on this server, click **Graph Ports**. Figure 5-16 shows an example of the Port Activity graph.

**Figure 5-16**  
**NIC Monitor—Vault Port Activity Graph**

### Table 5-11  
**NIC Port Status Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit</td>
<td>The total number of bytes transmitted since this port has been operational and configured as administratively up.</td>
</tr>
<tr>
<td>Received</td>
<td>The total number of bytes received since this port has been operational and configured as administratively up.</td>
</tr>
</tbody>
</table>

**Cache/Fill Bandwidth**

The Cache/Fill Bandwidth page displays details on the content caching activity on a Streamer.

To view the caching activity on a server, select a server’s IP address from the drop-down list on the Cache/Fill Bandwidth page and click **Display**. Figure 5-17 shows an example.
Table 5-12 describes the services listed in the Cache/Fill Bandwidth page.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Refresh Rate</td>
<td>How often the information is refreshed. The default is 10 seconds. The range is 10 to 300. All field values that are updated, based on the refresh rate, are initially shown in a green-colored font.</td>
</tr>
<tr>
<td>Active Stream Count</td>
<td>The number of active streams on this Streamer.</td>
</tr>
<tr>
<td>Active Stream Bandwidth</td>
<td>The bandwidth (in Mbps) used for streaming on this Streamer.</td>
</tr>
<tr>
<td>Unique Stream Count</td>
<td>The number of unique streams on this Streamer.</td>
</tr>
<tr>
<td>Unique Stream Bandwidth</td>
<td>The bandwidth (in Mbps) used for serving unique streams on this Streamer.</td>
</tr>
<tr>
<td>Fill Receive Stream Count</td>
<td>The number of streams on this Streamer that are retrieving content from the Vault in order to fulfill requests for content.</td>
</tr>
<tr>
<td>Actual Fill Stream Bandwidth</td>
<td>The bandwidth (in Mbps) used on this Streamer for retrieving content from the Vault.</td>
</tr>
</tbody>
</table>
Table 5-12  Cache/Fill Bandwidth Fields (continued)

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Read Stream Count</td>
<td>The number of streams on this Streamer sending content that was retrieved from the Streamer’s disks.</td>
</tr>
<tr>
<td>Disk Read Bandwidth</td>
<td>The bandwidth (in Mbps) used on this Streamer for retrieving locally stored content (content on the Streamer’s disks).</td>
</tr>
</tbody>
</table>

**Services Monitor**

The Services Monitor page displays whether specific processes are running on a server. To view the current status of the services running on a server, select a server’s IP address from the drop-down list on the Services Monitor page and click **Display**. Figure 5-17 shows an example of a Streamer server.

**Figure 5-18  Services Monitor Page—Streamer**

Table 5-13 describes the services listed in the Services Monitor page.
### Table 5-13  CDS Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Cache Server</td>
<td>Both</td>
<td>The Cache server runs on all servers. The Cache server is responsible for the core functions of the CDS.</td>
</tr>
<tr>
<td>Cisco FSI Master</td>
<td>Vault</td>
<td>The File Service Interface (FSI) Master process will be running if you are looking at a master Vault server. The FSI Master serves as the master Vault process for content file-related requests from the backoffice.</td>
</tr>
<tr>
<td>Cisco FSI Server</td>
<td>Vault</td>
<td>The FSI Server runs on every Vault and processes file-related requests from the FSI Master.</td>
</tr>
<tr>
<td>Cisco RTSP Server</td>
<td>Streamer</td>
<td>The RTSP server runs on the Streamer as either a client or server depending on the headend environment. The RTSP server handles messaging between the CDS and the backoffice.</td>
</tr>
<tr>
<td>Cisco Resource Manager</td>
<td>Streamer</td>
<td>The Resource Manager runs on a Streamer server. The Resource Manager handles orphaned streams.</td>
</tr>
<tr>
<td>Cisco DB Server</td>
<td>Both</td>
<td>The DB (database) server runs on all servers and is responsible for keeping track of all data objects in the CDS.</td>
</tr>
<tr>
<td>DB Synchronization Status</td>
<td>Both</td>
<td>Displays the status of the database synchronization among all servers. The states are “OK” and “not OK.”</td>
</tr>
<tr>
<td>Cisco SNMP Server</td>
<td>Both</td>
<td>The SNMP server shows as running when the SNMP agent is running.</td>
</tr>
<tr>
<td>Cisco System Manager</td>
<td>Both</td>
<td>The System Manager runs on each server and facilitates communication to the CDSM.</td>
</tr>
<tr>
<td>Cisco BWMgr Server</td>
<td>Streamer</td>
<td>The Bandwidth Manager process runs on the Streamer provided the optional Bandwidth Manager feature is part of your deployment. It keeps track of allocated streams and VOD network resources.</td>
</tr>
<tr>
<td>Cisco Ingest Manager</td>
<td>Vault</td>
<td>The Ingest Manager process will be running if you are looking at a master Vault server and the optional Ingest Manager feature is part of your deployment.</td>
</tr>
</tbody>
</table>
Recommended Monitoring Schedule

This monitoring schedule is recommended to ensure that the CDS is functioning as expected and identify potential issues that may cause down time.

Caution
Do not attempt to access the Linux command line unless you are familiar with the CDS, the Linux operating system, and have a basic understanding of the Linux command line.

Note
Some error warnings in the logs are only informational and no action is necessary.

Daily Tasks

The following tasks should be performed daily:

- Choose **Monitor > System Level > System Health** and check the System Health Monitor page for red or yellow states on any of the servers. Click any red or yellow boxes to see detail information on disk, NIC, or services. See the “System Health” section on page 5-1 for more information.

- Choose **Monitor > System Level > Failed Ingests** to check for any failed ingests. See the “Ingests” section on page 5-4 for more information.

Weekly Tasks

The following tasks should be performed weekly:

- Monitoring Tasks for Streamers and Vaults
- Monitoring Tasks for Vaults
- Monitoring Tasks for Streamers

Note
All commands require that you log into each server’s Linux operating system as **root**. Some tasks have a CDSM option.

Monitoring Tasks for Streamers and Vaults

To monitor the Streamer and Vaults weekly, do the following:

Step 1
Recover used disk space. Log in to each server using the **root** logon and run the following command:

```
dh -h
```

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hda1</td>
<td>13G</td>
<td>5.2G</td>
<td>7.0G</td>
<td>43%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/hda6</td>
<td>20G</td>
<td>16G</td>
<td>4.3G</td>
<td>78%</td>
<td>/arroyo/log</td>
</tr>
</tbody>
</table>

If the disk usage is greater than 75 percent, recover the disk space using the following methods:

- Search and remove any core files.

  ```
  find /arroyo -name core*
  ```
find /home/isa -name core*
b. Copy any archived logs to an external device and delete them from the /arroyo/archive directory.
c. Check for the presence of old install or upgrade ISO files in the /root directory and delete them.

    find /root -name *.iso
    find /arroyo -name *.iso

### Step 2
Verify the services are running. Choose **Monitor > Server Level > Services Monitor** to check the services for each server, or log in to each server and run the following commands:

```
    su - isa
    show_calypso_services
```

### Step 3
Check the CServer interfaces to verify the status of the Ethernet adapters. Choose **Monitor > Server Level NIC Monitor**, or log in to each server and use the following commands:

a. Use the `grep -i Link` command to verify that all adapters should have a status of “link up,” except those adapters that are not being used.

```
    grep -i Link /proc/net/PRO_LAN_Adapters/*.info
```

b. Use the `grep -i Speed` command to verify that each adapter that has a “link up” status should have a speed of 1000.

```
    grep -i Speed /proc/net/PRO_LAN_Adapters/*.info
```

c. Use the `grep -i State` command to verify that all adapters should have an “up” state, except those adapters that are not being used.

```
    grep -i State /proc/net/PRO_LAN_Adapters/*.info
```

### Step 4
Check the CServer streaming and cache-fill interfaces using the following command:

```
    /home/stats/ifstats
```

### Step 5
Check the database thread count using the following command:

```
    netstat -an | grep 9999
```

Two connections for each Vault and Streamer should be listed with a status of “ESTABLISHED.”

### Step 6
Check the protocol timing logs for errors or problems.

a. Look at the protocol timing logs for packet retransmissions.

```
    tail -f /arroyo/log/protocolTiming.log.(date) | grep retransmissions
```

### Step 7
Look for warning messages.

```
    grep -i warning /arroyo/log/protocolTiming.log.<date> | more
```

---
**Note**
The “WARNING” messages can sometimes be misleading; for example, “datawait” and “slow disk” messages occur normally and do not indicate an problem.

### Step 8
The number of GOIDs for a particular content object must be the same on all servers (Vaults and Streamers) that are supposed to have the content. The number of Vaults that must have the same number of GOIDs for a particular content object is determined by the mirrored copy configuration (see the “Configuring the Servers” section on page 4-41). The number of GOIDs is also dependent on the trick speeds configured you configured (see the “Configuring Ingest Tuning” section on page 4-16). If the
GOID is different between a Vault and a Streamer, session setup is not created properly because of an issue of “no content available.” This is because there is no content on the Vault that matches the GOID of the Streamer has.

**Monitoring Tasks for Vaults**

1. Check the available space on the Vault hard drives. Choose Monitor > Server Level > Disk Monitor. The disk availability is shown as a percentage and as a number of gigabytes. Alternatively, view the protocol timing logs by running the following command:
   ```
   tail -f /arroyo/log/protocoltiming.{date} | grep "Capacity Disk:"
   ```
   The number returned indicates the percentage of the disk space available on this server. If the number is 5 or lower, then steps need to be taken to increase storage space by adding more Vaults, replacing drives with higher capacity drives, or removing unused content.
2. Check the /home/isa/fsi logs for ingest errors on each Vault. The master Vault has an additional log.
3. Look for errors in the following log files in the /home/isa/bss/logs/ directory:
   - fsi.log
   - fsi.err
   The fsi.log and fsi.err files are related to the ingest activity on a Vault.

**Monitoring Tasks for Streamers**

1. Look at the streaming log.
   ```
   tail -f /arroyo/log/streamevent.log.<date>
   ```
2. Look for errors in the following log files in the /home/isa/bss/logs/ directory:
   - rtsp.log
   - rtsp.err
   The rtsp.log and rtsp.err files are used to check the stream setup and control on a Streamer.

**Monthly Tasks**

1. Choose Monitor > System Level > System Snapshot and check that the “Disk Available” amount meets the requirements for the expected movie storage in the next three to six months.
2. Run the reports for the last month that are suitable for your requirements and save them as comma-separated value (CSV) files.
3. Using the bandwidth and streaming reports, check that the CDS is not exceeding required usage per service area.
4. Run a quick security check.
   a. Ensure that the CDSM changes can be attributed to individual users and not to a generic admin account.
   b. Reset CDSM passwords if necessary.
   c. Reset Linux passwords if necessary.
d. Check that access policies and firewalls are still enforced.

Other Tasks

If you have access to an anything on demand (XOD) application, do the following:

1. Check the inspect-live log for excessive errors.
2. Check the inspect-live log for excessive communication times with the BMS or CDS.
System Reporting

The CDSM provides tools that can be used for system monitoring and system diagnostics. The topics covered in this chapter include:

- Stream Activity, page 6-1
- Content Activity, page 6-17
- CDSM Audit Logs, page 6-21
- Archived Data, page 6-22

Stream Activity

The Stream Activity reports displays information about streams. The available reports are:

- Streams by Array
- Streams by Time
- Stream Play History
- Cache/Fill Bandwidth
- Stream Failures
- Content Popularity

To access the available Stream Activity reports, choose Report > Stream Activity, and follow the procedure for the specific report described in the following subsections.

Streams by Array

The Stream by Array report lists all streams currently active for a specified group of Streamers. To view the Stream by Array report, do the following:

Step 1 From the Available Reports drop-down list, choose Streams by Array (Figure 6-1).
Stream Activity

Figure 6-1  Available Reports for Stream Activity

![Available Reports for Stream Activity]

Figure 6-2 shows the selection fields for the Streams by Array report.

Figure 6-2  Stream By Array Report Selection Fields

![Stream By Array Report Selection Fields]

**Step 2**  From the Stream Array drop-down list, choose a stream array.

**Step 3**  Select a modifier. See Table 6-1 for a description of each modifier.

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (Date Only)</td>
<td>Filter on date only.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Filters the report by the IP address of the destination device you select in a later step.</td>
</tr>
</tbody>
</table>

**Step 4**  Using the drop-down lists provided, or the calendars, select a From Date and To Date for the report.
Step 5  Select a time breakdown of hourly, daily, weekly, or monthly. The maximum time interval allowed for each breakdown is the following:

- Hourly—31 days
- Daily—2 years
- Weekly—2 years
- Monthly—2 years

Step 6  If you selected a modifier that requires a value, select or specify the filter value.

Step 7  Click Display.

To clear the fields and start over, click Reset.

Figure 6-3 shows an example of the Streams by Array report covering daily activity over a 15-day period with no optional modifiers selected.

Figure 6-3  Streams by Array Report

The report displays:

- Report type (for example, Daily Stream Activity Report for streams by array)
- From and to dates
- Date and time of each stream count
- Total number of standard definition (SD) streams, total number of high-definition (HD) streams, and total streams overall for the time period selected

Click Previous Report to return to the report selection page.

Note  Previous Report returns you to the report selection page or the previous report page in a multi-page report. Next Report takes you to the next page in the report.
Step 8  To see more detail, click the total number of streams link. For example, in Figure 6-3, click 5 total. The Session ID Summary is displayed (Figure 6-4).

Figure 6-4  Session ID Summary

Note  The Session ID Summary is sortable by clicking on each column heading.

The report displays:

- Session ID
- Content name
- Start and end date and time

The Session ID Summary is sortable by clicking on each column heading.

Step 9  To see the stream play history of a specific session, click a session ID (Figure 6-5).

Figure 6-5  Session ID—Stream Play History Drilldown

The report displays:

- Session ID
- Set-top box MAC address
- Termination reason
- Date and time of each play or trick mode action
- Elapsed time of each action
Chapter 6  System Reporting

Stream Activity

At the bottom of each Stream Play History report is a legend mapping the action to a color. Click **Previous Report** to return to the previous page.

---

**Note**  
*Previous Report* returns you to the report selection page or the previous report page in a multi-page report. *Next Report* takes you to the next page in the report.

---

**Step 10**  
To see details about the stream associated with this session, click **Show Stream Data** (Figure 6-6).

**Figure 6-6**  
*Stream Play History–Stream Data*

<table>
<thead>
<tr>
<th>CDMS Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stream Activity Report</strong></td>
</tr>
<tr>
<td>Session ID: 1801206492359216</td>
</tr>
<tr>
<td>STB MAC:</td>
</tr>
<tr>
<td>Termination Reason: Session Timeout</td>
</tr>
</tbody>
</table>

| Dec 08, 2006, 06:44:50 | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 |
| Dec 08, 2006, 06:49:07 | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 |
| Dec 08, 2006, 06:55:35 | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 |

**Stream Details**  
QAM ID: 102.162.1.42  
QAM port: 3000  
Service Group: 156

**Content Details**  
File: /var/nvram/content  
Ingest Date: November 6, 2006, 12:27:29 pm  
Ingest IP: 192.168.0.119  
File Size: 3000000000  
VAULT ID: 19  
Administrative State: InService  
Operational State: InService  
Delivery Rates N/A

---

The Stream Data displays:
- Details about the stream (QAM IP address and port, and service group)
- Details about the content (content name, ingest information, server ID storing the content, and so on)

Click **Hide Stream Data** to hide stream data.

Click **Previous Report** to return to the previous page.

**Step 11**  
To download the report to a comma-separated value (CSV) file, do one of the following:

a. If you are using Internet Explorer as your web browser, click **Download** and then click **Save** or **Open**. **Save** presents a Save As dialog box. **Open** opens the CSV file.

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click **Download** and select **Save Link As**, **Save Link Target As**, or **Save Target As** depending on the web browser you are using. A Save As dialog box is displayed.
Streams by Time

The Streams by Time report summarizes the number of standard-definition and high-definition streams by the selected time breakdown in the specified time period. This report can be used to analyze slow times of day and to plan outages.

To view the Streams by Time report, do the following:

**Step 1** From the Available Reports drop-down list, choose Streams By Time. Figure 6-7 shows the selection fields for the Streams By Time report.

**Figure 6-7 Streams by Time Report Selection Fields**

**Step 2** Using the drop-down lists provided, or the calendars, select a From Date and To Date for the report.

**Step 3** Select the time breakdown.

**Step 4** Click Display.

To clear the fields and start over, click Reset.

Figure 6-8 shows an example of the Streams by Time report with the “per hour” time breakdown selected.
The report displays:

- Report type (for example: Stream Activity Report for streams by time)
- From and to dates
- Time of each stream activity survey
- Total number of streams for each time within the specified from and to dates

Click Previous Report to return to the previous page.

**Note** Previous Report returns you to the report selection page or the previous report page in a multi-page report. Next Report takes you to the next page in the report.

**Step 5** To download the report to a comma-separated value (CSV) file, do one of the following:

a. If you are using Internet Explorer as your web browser, click Download and then click Save or Open. Save presents a Save As dialog box. Open opens the CSV file.

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click Download and select Save Link As, Save Link Target As, or Save Target As depending on the web browser you are using. A Save As dialog box is displayed.
Stream Play History

The Stream Play History report lists the trick mode history for specified streams.

To view the Stream Play History report, do the following:

**Step 1**
From the Available Reports drop-down list, choose Stream Play History. Figure 6-9 shows the selection fields for the Stream Play History report.

**Figure 6-9  Stream Play History Report Selection Fields**

![Stream Play History Report Selection Fields](image)

**Step 2**
Select a modifier. See Table 6-2 for a description of each modifier.

**Table 6-2  Stream Play History Modifiers**

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (Date Only)</td>
<td>Displays a list of all streams (Session ID Summary) filtered by the from and to dates.</td>
</tr>
<tr>
<td>Session Handle</td>
<td>Filters the report by a session handle you specify in a later step.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Filters the report by the IP address of the destination device you select in a later step.</td>
</tr>
</tbody>
</table>

**Step 3**
Using the drop-down lists provided, or the calendars, select a From Date and To Date for the report.

**Note**
Selecting Session ID displays the complete play history for the specified session. The From Date and To Date fields are bypassed.
Note: Selecting None (Date Only) displays the Session ID Summary. To see the play history of a specific session, click a Session ID in the Session ID Summary report.

Step 4: If you selected a modifier, select or specify the filtered value. For example, if you select Service Group as the modifier, you specify which Service Group.

Step 5: Click Display.

To clear the fields and start over, click Reset.

Figure 6-10 shows an example of the Stream Play History report.

Figure 6-10 Stream Play History Report

The Session ID Summary is sortable by clicking on each column heading.

The report displays:
- Session ID
- Content name
- Start and end date and time

Step 6: To see the stream play history of a specific session, click a session ID (Figure 6-11).

Figure 6-11 Session ID Stream Play History Drilldown
The report displays:
- Session ID
- Set-top box MAC address
- Termination reason
- Date and time of each play or trick mode action
- Elapsed time of each action

Click Previous Report to return to the previous page.

**Step 7** To see details about the stream associated with this session, click Show Stream Data (Figure 6-12).

**Figure 6-12 Stream Play History—Stream Data**

The Stream Data displays:
- Details about the stream (QAM IP address and port, and service group)
- Details about the content (content name, ingest information, server ID storing the content, and so on)

Click Hide Stream Data to hide stream data.

Click Previous Report to return to the previous page.

At the bottom of each Stream Play History report is a legend mapping the action to a color.

**Note** Previous Report returns you to the report selection page or the previous report page in a multi-page report. Next Report takes you to the next page in the report.

**Step 8** To download the report to a comma-separated value (CSV) file, do one of the following:

a. If you are using Internet Explorer as your web browser, click Download and then click Save or Open. Save presents a Save As dialog box. Open opens the CSV file.
Cache/Fill Bandwidth

The Cache/Fill Bandwidth report displays details on the content caching activity on a Streamer. To view the Cache/Fill Bandwidth report, do the following:

**Step 1** From the **Available Reports** drop-down list, choose Cache/Fill Bandwidth. **Figure 6-9** shows the selection fields for the Cache/Fill Bandwidth report.

**Figure 6-13  Cache/Fill Bandwidth Report Selection Fields**

<table>
<thead>
<tr>
<th>System Level</th>
<th>Stream Activity</th>
<th>Content Delivery</th>
<th>System Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt; Stream Activity &gt;</td>
<td>&lt; Content Activity &gt;</td>
<td>&lt; COBRAND Logs &gt;</td>
<td>&lt; Archived Data &gt;</td>
</tr>
</tbody>
</table>

Select the report you wish to view from the list. Next, select any optional modifiers (or none) you want and then select the start and end dates for the report, then click **Display**.

**Step 2** From the **Server Array** drop-down list, choose a server array.

**Step 3** Using the drop-down lists provided, or the calendars, select a **From Date** and **To Date** for the report.

**Step 4** From the **Server ID** drop-down list, select a Streamer.

**Step 5** Click **Display**.

To clear the fields and start over, click **Reset**.

**Figure 6-10** shows an example of the Cache/Fill Bandwidth report.
**Figure 6-14  Cache/Fill Bandwidth Report**

The report displays the minimum, average, and maximum bandwidth used for the selected Streamer. Click **Previous Report** to return to the previous page.

**Note**  Previous Report returns you to the report selection page or the previous report page in a multi-page report. **Next Report** takes you to the next page in the report.

**Step 6**  To download the report to a comma-separated value (CSV) file, do one of the following:

a. If you are using Internet Explorer as your web browser, click **Download** and then click **Save** or **Open**. **Save** presents a Save As dialog box. **Open** opens the CSV file.
Stream Failures

The Stream Failures report lists the number of stream failures. To view the Stream Failures report, do the following:

**Step 1** From the **Available Reports** drop-down list, choose **Stream Failures**. Figure 6-15 shows the selection fields for the Stream Failures report.

![Stream Failures Report Selection Fields](image)

**Step 2** Select an error code, if applicable. See Table 5-8 in the “Stream Failures” section on page 5-18 for descriptions of possible error codes.

**Step 3** Select a modifier. See Table 6-3 for a description of each modifier.

---

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click **Download** and select **Save Link As**, **Save Link Target As**, or **Save Target As** depending on the web browser you are using. A Save As dialog box is displayed.
Table 6-3  Stream Failure Modifiers

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Group</td>
<td>Filters the report by the service group you select in a later step.</td>
</tr>
<tr>
<td>Server ID</td>
<td>Filters the report by a server ID that you select in a later step.</td>
</tr>
</tbody>
</table>

**Step 4** Using the drop-down lists provided, or the calendars, select a **From Date** and **To Date** for the report.

**Step 5** Select a time breakdown of hourly, daily, weekly, or monthly. The maximum time interval allowed for each breakdown is the following:
- Hourly—31 days
- Daily—2 years
- Weekly—2 years
- Monthly—2 years

**Step 6** If you selected a modifier, select the filter value.

**Step 7** Click **Display**.

To clear the fields and start over, click **Reset**.

*Figure 6-16* shows an example of the Stream Failures report.

**Figure 6-16  Stream Failures Report**

The report displays:
- Report type
- From and to dates
- Date (and time if applicable) of each time breakdown
- Total number of failures for each time breakdown selected

**Step 8** To see more detail, click the total number of failures link. The Stream Failure Details report is displayed (*Figure 6-17*).
Figure 6-17 Stream Failure Details

The report displays:

- Date and time of the failure
- Session ID of the failed stream
- QAM IP address
- Server ID that was sending the stream at the time of the failure
- Service Group
- Error code

The report is sortable by clicking on each column heading.

**Step 9** To see the stream play history of a specific session, click a session ID.

Click Previous Report to return to the previous page.

**Step 10** To see details about the stream associated with this session, click Show Stream Data.

Click Hide Stream Data to hide stream data.

Click Previous Report to return to the previous page.

**Note** Previous Report returns you to the report selection page or the previous report page in a multi-page report. Next Report takes you to the next page in the report.

**Step 11** To download the report to a comma-separated value (CSV) file, do one of the following:

a. If you are using Internet Explorer as your web browser, click Download and then click Save or Open. Save presents a Save As dialog box. Open opens the CSV file.

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click Download and select Save Link As, Save Link Target As, or Save Target As depending on the web browser you are using. A Save As dialog box is displayed.
Content Popularity

The Content Popularity report lists the content by their filenames and ranks them in order of popularity. To view the Content Popularity report, do the following:

Step 1  From the Available Reports drop-down list, choose Content Popularity. Figure 6-18 shows the selection fields for the Content Popularity report.

![Figure 6-18 Content Popularity Report Selection Fields](image)

Step 2  Using the drop-down lists provided, or the calendars, select a Start Time and End Time for the report.

Step 3  Click Display.

To clear the fields and start over, click Reset.

Figure 6-19 shows an example of the Content Popularity report.

![Figure 6-19 Content Popularity Report](image)

The report displays:

- Report type
- Optional modifiers if applicable
- From and to dates
- Content object name
- Total number of streams for each content streamed in the specified time period
Step 4 To view content details, click the content object name. The Content Detail report is displayed (Figure 6-20).

Figure 6-20 Content Popularity Details

Click Close to close this window.

Click Previous Report to return to the previous page.

Note Previous Report returns you to the report selection page or the previous report page in a multi-page report. Next Report takes you to the next page in the report.

Step 5 To download the report to a comma-separated value (CSV) file, do one of the following:

a. If you are using Internet Explorer as your web browser, click Download and then click Save or Open. Save presents a Save As dialog box. Open opens the CSV file.

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click Download and select Save Link As, Save Link Target As, or Save Target As depending on the web browser you are using. A Save As dialog box is displayed.

Content Activity

The Content Activity report lists all content stored on all Vaults in the specified group and all unpublished packages. The available reports are:

- Content by Ingest Date
- Unpublished Package Report

Content by Ingest Date

To view the Content by Ingest Date report, do the following:

Step 1 Click Report > Content Activity. The Content Activity selection page is displayed.

Step 2 From the Available Reports drop-down list, choose Content By Ingest Date (Figure 6-21).
Figure 6-21  Content Activity Selection Fields

Step 3  From the Array drop-down list, choose an array.
Step 4  Using the drop-down lists provided, or the calendars, select a From Date and To Date for the report.
Step 5  Choose Include Deleted to include content that has been deleted from the array, otherwise choose Exclude Deleted.
Step 6  Click Display.

To clear the fields and start over, click Reset.

Figure 6-22 shows an example of the Content Activity report.

Figure 6-22  Content Activity Report

The report displays:
- Report type
- From and to dates
- Content filenames
To view the details of an in-service content object, click the content filename link (Figure 6-23).

Figure 6-23  Content Detail

Click Close to close this window.

Click Previous Report to return to the previous page.

Note  Previous Report returns you to the report selection page or the previous report page in a multi-page report. Next Report takes you to the next page in the report.

Step 8  To download the report to a comma-separated value (CSV) file, do one of the following:

a. If you are using Internet Explorer as your web browser, click Download and then click Save or Open. Save presents a Save As dialog box. Open opens the CSV file.

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click Download and select Save Link As, Save Link Target As, or Save Target As depending on the web browser you are using. A Save As dialog box is displayed.

Unpublished Package Report

To view the Unpublished Package report, do the following:

Step 1  Choose Report > Content Activity. The Content Activity selection page is displayed.

Step 2  From the Available Reports drop-down list, choose Unpublished Package Report (Figure 6-21).
Step 3 Using the drop-down lists provided, or the calendars, select a From Date and To Date for the report.

Step 4 Click Display.

To clear the fields and start over, click Reset.

Figure 6-22 shows an example of the Unpublished Package report.

Figure 6-25 Unpublished Package Report

The report displays:
- Report type
- From and to dates
- Package names
- Creation date
- Source URL
- Target URL
- Number of assets associated with the package

Step 5 Click New Report to return to the previous page.

Step 6 To download the report to a comma-separated value (CSV) file, do one of the following:
a. If you are using Internet Explorer as your web browser, click Download and then click Save or Open. Save presents a Save As dialog box. Open opens the CSV file.

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click Download and select Save Link As, Save Link Target As, or Save Target As depending on the web browser you are using. A Save As dialog box is displayed.

CDSM Audit Logs

The CDSM Audit log keeps track of every configuration change, deletion of monitored items, and maintenance actions.

To view the CDSM Audit logs, do the following:

Step 1  Choose Report > CDSM Audit logs. Figure 6-26 shows the selection fields for the CDSM Audit logs.

Figure 6-26  CDSM Audit Log Selection Fields

<table>
<thead>
<tr>
<th>System Level</th>
<th>CDSM Audit Logs REPORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Activity</td>
<td>The Cisco CDSM audit logs are available for online viewing to aid in identifying configuration errors. To begin, select the date range you wish to see entries for and then click Display.</td>
</tr>
<tr>
<td>Content Activity</td>
<td>From Date</td>
</tr>
<tr>
<td>CDSM Audit Logs</td>
<td>Dec 1 2006</td>
</tr>
<tr>
<td>Archived Logs</td>
<td>Dec 1 2006</td>
</tr>
</tbody>
</table>

Step 2  Using the drop-down lists provided, or the calendars, select a From Date and To Date for the log.

Step 3  Click Display.

To clear the fields and start over, click Reset.

Figure 6-27 shows an example of the CDSM Audit log.
Archived Data

The log displays:
- From and to dates
- Action taken (Section Descriptor)
- User who took the action
- System used
- Date the action occurred

**Step 4** To get more information about the action taken, click a section descriptor. The CDSM Audit Log Detail is displayed in a new window. Click Close to close the window.

**Step 5** To download the report to a comma-separated value (CSV) file, do one of the following:

a. If you are using Internet Explorer as your web browser, click Download and then click Save or Open. Save presents a Save As dialog box. Open opens the CSV file.

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click Download and select Save Link As, Save Link Target As, or Save Target As depending on the web browser you are using. A Save As dialog box is displayed.

Archived Data

The CSV files are generated every 24 hours and are deleted when they are older than 30 days. The CSV files are accessible by going to the /arroyo/asmrpt directory, or by using an FTP client with the username “asmrpt” and the password “asmrpt.”

Monitoring data is archived in comma-separated value (CSV) format for use in a spreadsheet program, database, or other software. Table 6-4 describes the different archived data.
Chapter 6 System Reporting

 Archived Data

To download an archived data report, do the following:

Step 1 Choose Report > Archived Data. The Archived Data page is displayed.

Step 2 From the Archives drop-down list, choose an archive and click Next.

Step 3 Right-click the HTTP link of the report you want to download and select Save Target As, Save Link As, Save Link Target As, or Save Target As depending on the web browser you are using. A Save As dialog box is displayed (Figure 6-28).

Figure 6-28 Save As Dialog Box

Step 4 Select a location and name for the file and click Save.

Step 5 The CSV file is compressed using gzip (extension .gz). Decompress the file using a decompression tool that includes the gzip compression code, such as Winzip, PowerArchiver 6.1, or 7-zip.

Table 6-4 Archived Data

<table>
<thead>
<tr>
<th>Archive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDSM Audit Log Archives</td>
<td>Log of configuration changes that were made to the system and when the changes were made.</td>
</tr>
<tr>
<td>Content Reports</td>
<td>Archive of content ingested.</td>
</tr>
<tr>
<td>Stream Reports</td>
<td>Archive of all streams.</td>
</tr>
<tr>
<td>Stream Failure Reports</td>
<td>Archive of trick mode and play actions that occurred on all streams.</td>
</tr>
</tbody>
</table>

To download an archived data report, do the following:

Step 1 Choose Report > Archived Data. The Archived Data page is displayed.

Step 2 From the Archives drop-down list, choose an archive and click Next.

Step 3 Right-click the HTTP link of the report you want to download and select Save Target As, Save Link As, Save Link Target As, or Save Target As depending on the web browser you are using. A Save As dialog box is displayed (Figure 6-28).

Figure 6-28 Save As Dialog Box

Step 4 Select a location and name for the file and click Save.

Step 5 The CSV file is compressed using gzip (extension .gz). Decompress the file using a decompression tool that includes the gzip compression code, such as Winzip, PowerArchiver 6.1, or 7-zip.

CDSM Audit Log Archives

The CDSM Audit log archives contain the same information as the CDSM Audit logs. For more information, see the “CDSM Audit Logs” section on page 6-21.
Content Reports

Table 6-5 describes the fields in the Content Report CSV files.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mGoid</td>
<td>Global object identifier. Used by the CDS database.</td>
</tr>
<tr>
<td>mName</td>
<td>The name of the content file.</td>
</tr>
<tr>
<td>mProvider</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mCategory</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mFactoryId</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mOpState</td>
<td>The operational state is not used and is always 2 (In Service).</td>
</tr>
<tr>
<td>mAdminState</td>
<td>The administrative state is not used and is always 2 (In Service).</td>
</tr>
<tr>
<td>mProvisionForPush</td>
<td>The type of FTP provisioned. Values are:</td>
</tr>
<tr>
<td></td>
<td>• 0—FTP pull</td>
</tr>
<tr>
<td></td>
<td>• 1—FTP push</td>
</tr>
<tr>
<td></td>
<td>• 3—Live recording</td>
</tr>
<tr>
<td>mURL</td>
<td>The URL of the content file. This field is only applicable for FTP pull.</td>
</tr>
<tr>
<td>mIngestIpAddress</td>
<td>The IP address of the Vault’s ingest port used to download the content file.</td>
</tr>
<tr>
<td>mIngestFileSize</td>
<td>The content file size, in bytes.</td>
</tr>
<tr>
<td>mCreateTime</td>
<td>The time and date this content file was created. The time and date is represented in seconds since the start of Unix epoch time.</td>
</tr>
<tr>
<td>mLastModifiedTime</td>
<td>The time and date this content file was last modified. The time and date is represented in seconds since the start of Unix epoch time.</td>
</tr>
<tr>
<td>mDeleteTime</td>
<td>The time and date this content file was deleted. The time and date is represented in seconds since the start of Unix epoch time.</td>
</tr>
<tr>
<td>mServerId</td>
<td>The Server ID of the Vault server that is the primary source for this content file.</td>
</tr>
<tr>
<td>mAssetName</td>
<td>The asset name of the content, if populated.</td>
</tr>
<tr>
<td>mEncrypted</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mRate</td>
<td>The transmit rate requirement of the file, in bytes per second.</td>
</tr>
</tbody>
</table>

Stream Reports

Table 6-6 describes the fields in the Stream Report CSV files.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mSessionId</td>
<td>The session ID of the stream.</td>
</tr>
<tr>
<td>mGoid</td>
<td>Global object identifier. Used by the CDS database.</td>
</tr>
</tbody>
</table>
Stream Failure Reports

Table 6-7 describes the fields in the Stream Failure Report CSV files.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mSessionId</td>
<td>The session ID of the failed stream.</td>
</tr>
<tr>
<td>mKey</td>
<td>CDS database key for this record.</td>
</tr>
<tr>
<td>mServerId</td>
<td>The server ID of the Streamer that participated in transmitting the stream.</td>
</tr>
<tr>
<td>mGroupId</td>
<td>The array ID the Streamer is associated with.</td>
</tr>
<tr>
<td>mServiceGroup</td>
<td>The service group that participated in transmitting the stream.</td>
</tr>
<tr>
<td>mQAMIp</td>
<td>The IP address of the QAM device that participated in transmitting the stream. The IP address is represented as an integer. For example, 3232235818 decimal converts to C0A8012A hexadecimal, which translates to 192.168.1.42</td>
</tr>
<tr>
<td>mEventTime</td>
<td>The timestamp of when the event occurred. The timestamp is represented in seconds since the start of Unix epoch time.¹</td>
</tr>
<tr>
<td>mOperation</td>
<td>The operation that was taking place when the stream failed. For example: createStream, LSCP Command(), createServant, destroy. These are the measurement points or transactional states of the system at the time of the failure. See Table 5-8 for more information.</td>
</tr>
<tr>
<td>mErrorCode</td>
<td>The error code provides a description of the event that caused the error. See Table 5-8 for more information.</td>
</tr>
</tbody>
</table>

¹. Unix epoch time is 1970-01-01T00:00:00Z
Stream Activity Reports

The Stream Activity Reports archive contains all trick mode and play actions of all streams within the given 24-hour period. Table 6-8 describes the fields that are exported to the CSV file.

### Table 6-8 Stream Activity Report Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mSessionId</td>
<td>The session ID of the stream.</td>
</tr>
<tr>
<td>mActionTime</td>
<td>The timestamp when the stream activity occurred. The timestamp is represented in seconds since the start of Unix epoch time.¹</td>
</tr>
<tr>
<td>mServerId</td>
<td>The server ID of the Streamer that is providing the stream.</td>
</tr>
<tr>
<td>mOpState</td>
<td>The operational state is not used and is always zero (0).</td>
</tr>
<tr>
<td>mStreamState</td>
<td>Stream state is not used and is always zero (0).</td>
</tr>
<tr>
<td>mSpeed</td>
<td>Speed direction is as follows:</td>
</tr>
<tr>
<td></td>
<td>1 means play</td>
</tr>
<tr>
<td></td>
<td>0 means not paused/stopped</td>
</tr>
<tr>
<td></td>
<td>n means n times fast-forward</td>
</tr>
<tr>
<td></td>
<td>-n means n times rewind</td>
</tr>
<tr>
<td>mMntOffset</td>
<td>The current point in time (milliseconds) where the stream is on the set-top box, based on from NPT and to NPT.</td>
</tr>
<tr>
<td>mDestroyedReason</td>
<td>This field is only populated if the stream is destroyed by the CDS orphan stream handler. The CDS orphan stream handler only destroys a stream for one of the following two reasons:</td>
</tr>
<tr>
<td></td>
<td>Orphan session is detected</td>
</tr>
<tr>
<td></td>
<td>LSCP timeout maximum has been reached</td>
</tr>
</tbody>
</table>

¹ Unix epoch time is 1970-01-01T00:00:00Z
System Maintenance

This chapter explains how to perform common administrative tasks including, updating system software, restarting services, and shutting down the Vault and Streamer servers. This chapter covers the following topics:

- **User Access**, page 7-1
- **Server Maintenance**, page 7-6
- **Restarting the Services**, page 7-11
- **Software Maintenance**, page 7-13
- **Manuals**, page 7-15

---

**Note**

You must have read/write privileges to perform the functions described in this chapter.

---

**Caution**

Many of the functions discussed in this chapter involve rebooting a CDS server. Rebooting a Vault server does not interrupt stream services, but causes current ingests to fail. If your CDS does not have stream failover, rebooting a Streamer without offloading it will interrupt all stream services. If possible, you should perform functions that require a system restart during times when the least number of users are actively connected to your system.

---

**User Access**

The CDS consists of one of the following network configurations:

- One or more Vault servers, one or more Streamer servers, and one CDSM
- One or more ISV servers and one CDSM

All the components of your CDS are configured, monitored, and managed centrally through the CDSM. The CDSM is a browser-based interface that runs on its own server. However, there are some ISV systems that include the CDSM functions.

The CDS provides three levels of user access:

- **Read only** access provides viewing access to the configuration settings and monitoring capabilities.
- **Read/write** access provides the ability to change the configuration settings and monitor all aspects of the system. In addition, a user with read/write access can perform software upgrades, restart servers, and restart services in a CDS.
• Master access has all the privileges of the read/write level and can add, delete, and change the level of access of the other users.

• Engineering access is primarily used for initializing the CDS at the time of installation and for CDS diagnostics. Once your CDS has been configured, you should not require a user with engineering access level for day-to-day operations.

There is one built-in user, “admin,” that has master user capabilities. This is the only user that exists on a new system.

### Setting Up Users

The CDS provides one built-in user, “admin,” that has master level access and cannot be deleted. The master user can add additional users with different levels of access.

To add a user, do the following:

#### Step 1
Choose Maintain > Users > Add User. The Add User page is displayed (Figure 7-1).

![Add User Page](image)

#### Step 2
Fill in the fields as described in Table 7-1.

<table>
<thead>
<tr>
<th>Table 7-1</th>
<th>Add User Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>New User</td>
<td>The user login ID. A user name may have up to 25 characters. Any 7-bit characters from the American National Standards Institute (ANSI) character set are allowed.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the user login name. The password must be at least 5 characters. The maximum is 20.</td>
</tr>
<tr>
<td>Access</td>
<td>Select the appropriate access level from the drop-down list. See the beginning of this section, the “User Access” section on page 7-1 for descriptions of the access levels.</td>
</tr>
</tbody>
</table>
Step 3  Click **Add User** to add this user.
To clear the fields and start over, click **Reset**.

---

**Editing User Settings**

To change a user’s password and access level, do the following:

Step 1  Choose **Maintain > Users > Edit User**. The Edit User page is displayed (Figure 7-2).

![Figure 7-2 Edit User Page](image)

Step 2  From the **Action** drop-down list, choose **Change Password** or **Change Access**.

Step 3  From the **User Name** drop-down list, choose a user name.

Step 4  Fill in the new password or select the access as appropriate. See **Table 7-2** for descriptions of these fields.

**Table 7-2 Edit User Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Password</td>
<td>The password associated with the user’s login name. The range is 5 to 20 characters.</td>
</tr>
<tr>
<td>Access</td>
<td>Select the appropriate access level from the drop-down list. See the beginning of this section, the “User Access” section on page 7-1, for descriptions of the access levels.</td>
</tr>
</tbody>
</table>

Step 5  Click **Submit** to save the changes.
To clear the fields and start over, click **Reset**.
Deleting a User

To delete a user from the list of users, do the following:

**Step 1** Choose Maintain > Users > Edit User. The Edit User page is displayed (Figure 7-2 on page 7-3).

**Step 2** From the Action drop-down list, choose Delete User.

**Step 3** From the User Name drop-down list, choose a user.

**Step 4** Click Submit to delete the user.

To clear the fields and start over, click Reset.

Changing User Default Settings

The User Default Settings page allows you to specify your settings for the Media Scheduler page so that each time you log in to the CDSM your settings are recalled. If you have master level access, you can specify the settings for all users. For more information about the Media Scheduler, see the “Configuring the Media Scheduler” section on page 4-31.

To change the default settings for a user, do the following:

**Step 1** Choose Maintain > Users > User Default Settings. The User Default Settings page is displayed.

**Step 2** From the Select User drop-down list, choose a user. The User Default Settings page refreshes and displays the user settings (Figure 7-2).
**Step 3** In the Media Scheduler Preferences section of the page, make your selections as appropriate. See Table 7-3 for descriptions of the fields.

**Table 7-3 Media Scheduler Preferences**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action on Recurring Schedules</td>
<td>Choose either Preserve Exiting Schedules or Overwrite Existing Schedules. This option is only for user-generated schedules and is not for uploaded electronic program guide (EPG) data. Preserving Existing Schedules keeps any content that is currently scheduled for the day and channel you selected and fills in only the empty timeslots. Overwrite Existing Schedules overwrites any content that is currently scheduled for the day and channel you selected.</td>
</tr>
<tr>
<td>Package Name Generation</td>
<td>When you schedule an event that originated from an uploaded EPG file, the Media Scheduler creates a package name combining the channel name, title brief, and the word “package.” If the package name already exists and you want a new package name auto-generated, choose Enable and the start time is added to the package name. If the package name already exists and you want to create the package name using the Metadata Editor, choose Disable.</td>
</tr>
</tbody>
</table>

**Step 4** In the Input Channels Displayed on Media Scheduler section of the page, check the check boxes for the channels you want to schedule, or check the Select All check box to choose all channels.

**Step 5** If you have master level access and you want to apply the user default settings of this page to all users, check the Apply To All Users check box.

**Step 6** Click Save to save the changes.

To clear the fields and start over, click Reset.

---

**Viewing User Settings**

To view all user settings you must log in with master access level.

Choose Maintain > Users > View Users. The View Users page is displayed (Figure 7-4).
Server Maintenance

The Server Maintenance pages provides the ability to offload and shutdown a server for maintenance, and to restart a server without shutting it down. The Server Maintenance pages include the following:

- Restarting a Server
- Shutting Down a Server
- Offloading a Server
- Setting System Thresholds

Restarting a Server

⚠️ Caution

Restarting a Vault or Streamer server while there are still active ingests and streams causes the current ingests and streams to fail. Restarting a server briefly shuts down the unit, then restarts it using the installed version software image. This action does not power off the unit.

To restart a server, do the following:

Step 1  Choose Maintain > Servers > Server Restart. The Server Restart page is displayed. See Figure 7-5.
Step 2  From the Server IP drop-down list, choose a server’s IP address or nickname and click Display. The server type and ID, as well as the array ID, are displayed.

Step 3  From the Restart drop-down list, choose Yes and click Submit.

### Shutting Down a Server

**Caution**  Shutting down a Vault or Streamer server while there are still active ingest and streams causes the current ingest and streams to fail.

Shutting down by simply powering off the unit using the chassis power button is not recommended, as this may result in corruption of the unit’s configuration information, including system status when the shutdown occurred.

Shutting down and restarting using the CDSM is the recommended procedure. the Server Shutdown shuts down and powers off the selected unit.

To shut down and power off a server, do the following:

Step 1  Choose Maintain > Servers > Server Shutdown. The Server Shutdown page is displayed. See Figure 7-6.
Step 2  From the **Server IP** drop-down list, choose a server’s IP address or nickname and click **Display**. The server type and ID, as well as the array ID, are displayed.

Step 3  From the **Shutdown** drop-down list, choose **Yes** and click **Submit**.
## Offloading a Server

The Server Offload page lets you enable or disable the server offload. When Server Offload is enabled on a server, the server is configured to reject new provisioning.

To enable Server Offload, do the following:

### Step 1
Choose **Maintain > Servers > Server Offload**. The Server Offload page is displayed. See **Figure 7-7**.

**Figure 7-7  Server Offload Page**

<table>
<thead>
<tr>
<th>Maintaining Servers</th>
<th>Server Offload Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Select the server IP of the specific server that you wish to offload and then click **Display**.

Server IP: 10.22.216.111  Display

Current status for 10.22.216.111. To change the offload status of this server, select the desired status below, either Disable or Enable, and then click **Submit** below.

**Vault**

Server ID: 11  Array ID: 199190

Server Offload Status

- Disable
- Enable

Changing these settings may cause the server to lose connection to the network, please double-check your entries prior to submitting.

Submit  Reset

### Step 2
From the **Server IP** drop-down list, choose a server’s IP address or nickname and click **Display**. The server type and ID, as well as the array ID, are displayed.

### Step 3
Select **Enable** and click **Submit**.

After enabling Server Offload, current traffic activity can be monitored, and when the server offload is complete, the software can be updated. To view activity on a Vault server, see the “Monitoring Content Objects” section on page 5-4. To view activity on a Streamer, see the “Monitoring Stream Objects” section on page 5-13. If the server is an ISV, verify that activity is completed for both content objects and stream objects before updating the software.

**Note**

The Server Offload setting is persistent through a system reboot.
Server Offload—Disable

Once the software upgrade or maintenance is complete, you need to disable the server offload so that the server can again participate in the system.

To disable Server Offload, do the following:

---

**Step 1** Choose Maintain > Servers > Server Offload.

**Step 2** From the Server IP drop-down list, choose a server’s IP address or nickname and click Display. The server type and ID, as well as the array ID, are displayed.

**Step 3** Select Disable and click Submit.

---

Setting System Thresholds

The System Thresholds page allows you to set thresholds for loss and usage of the CDS resources, as well as enable or disable monitoring of the CDS services. The Performance Parameters section of the page has threshold values; the System Services section of the page enables or disables monitoring of the specific services. To view the system services monitored, see the “Services Monitor” section on page 5-29. Table 7-4 lists each threshold in the Performance Parameters section, and where each threshold is monitored.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Monitoring Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Loss</td>
<td>The Network indicator box on the “System Health” section on page 5-1.</td>
</tr>
<tr>
<td>Disk Loss</td>
<td>The Disk indicator box on the “System Health” section on page 5-1.</td>
</tr>
<tr>
<td>Disk Capacity Notify</td>
<td>The “Disk Monitor” section on page 5-22.</td>
</tr>
<tr>
<td>Disk Capacity Warning</td>
<td>The “Disk Monitor” section on page 5-22.</td>
</tr>
<tr>
<td>Linux File System Usage</td>
<td>The “Disk Monitor” section on page 5-22.</td>
</tr>
</tbody>
</table>

To set the system thresholds and enable or disable the system services, do the following

---

**Step 1** Choose Maintain > Servers > System Thresholds. The System Thresholds page is displayed (Figure 7-8).
**Restarting the Services**

Each server runs services that allow the server to function with other components in the CDS. Services are not automatically restarted each time there is a configuration change. If you need to restart a service, the Services Restart page provides this option. This action does not power cycle the unit. Table 7-5 describes the different services.

**Figure 7-8 System Thresholds Page**

Table 7-5 describes the different services.

<table>
<thead>
<tr>
<th>Performance Parameter</th>
<th>Current Value</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Loss %</td>
<td>18</td>
<td>15</td>
</tr>
<tr>
<td>Disk Loss %</td>
<td>23</td>
<td>20</td>
</tr>
<tr>
<td>Disk Capacity Notify %</td>
<td>77</td>
<td>75</td>
</tr>
<tr>
<td>Disk Capacity Warning %</td>
<td>85</td>
<td>85</td>
</tr>
<tr>
<td>Linux Disk System Usage%</td>
<td>75</td>
<td>75</td>
</tr>
</tbody>
</table>

**Step 2** Enter the threshold settings and enable or disable the services as appropriate.

**Step 3** Click **Submit** to save the settings.

To clear the fields and start over, click **Reset**.

To restore the default settings, click **Restore**. The default values are shown in a separate column on the page.
Chapter 7  System Maintenance

Restarting the Services

To restart a service, do the following:

**Step 1**  Choose **Maintain > Services**. The Services Restart page is displayed. See Figure 7-9.

**Figure 7-9   Services Restart Page**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reload Bandwidth Manager</td>
<td>Optional feature. Any time there are changes to the Bandwidth Manager configuration, it is necessary to reload the bandwidth manager.</td>
</tr>
<tr>
<td>RTSP nABLE</td>
<td>Any time there are changes to the RTSP Setup page, it is necessary to restart the RTSP nABLE service.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Any time there are changes to the SNMP configuration, it is necessary to restart the SNMP service.</td>
</tr>
</tbody>
</table>

To restart a service, do the following:

**Table 7-5  Restart Services Options**

**Step 2**  From the **Server IP** drop-down list, choose a server’s IP address or nickname and click **Display**. The server type and ID, as well as the array ID, are displayed.

**Step 3**  Select the check box next to each service you want to restart and click **Submit**.

To clear the fields and start over, click **Reset**.
Software Maintenance

The Software Maintenance pages provides the ability to update the CDS software or upload an electronic program guide (EPG) file.

Updating the System Software

To upgrade the software image on a server, you first need to offload a server for maintenance. See the “Offloading a Server” section on page 7-9. Once the server has been fully offloaded, you can upgrade the software.

To upgrade the software, do the following:

Step 1  Choose Maintain > Software. The Software Upgrade page is displayed. See Figure 7-10.

**Figure 7-10   Software Upgrade Page**

Step 2  From the Server IP drop-down list, choose a server’s IP address or nickname and click Display. The server type and ID, as well as the array ID, are displayed.

Step 3  From the Available Versions drop-down list, choose a software image file and click Submit. To clear the fields and start over, click Reset.
Once the software has been updated, disable the server offload. See the “Server Offload—Disable” section on page 7-10.

Uploading an EPG File

The EPG File Upload page can be used to upload an electronic program guide (EPG) file into the CDS for use with the Media Scheduler. The EPG file is an XML file.

Note

Before you can upload an EPG file, you need to enter the channel information. See the “Configuring Input Channels” section on page 4-21 for more information.

To upload an EPG file, do the following:

Step 1 Choose Maintain > Software > EPG Upload. The EPG File Upload page is displayed. See Figure 7-11.

Figure 7-11  TEPG File Upload Page

Step 2 Enter the full path and filename in the EPG File Location field, or click Browse to locate the file using the Browse window.

Step 3 Once the full path and filename of the EPG File is entered, click Upload.

To clear the fields and start over, click Reset.
Manuals

The CDS manuals are available in PDF format through the CDSM.

Note
You need Adobe Acrobat Reader to view the manuals. To download a free Acrobat Reader, visit the Adobe website at www.adobe.com. The Acrobat Reader installation program installs a plug-in for your browser program.

To view the manuals, do the following:

Step 1 Choose Maintain > Manuals. The Manual page is displayed.
Step 2 Click the link to the manual you want to view. The manual is displayed using the Acrobat Reader plug-in for your browser.

Tip To download the manual to your computer, right-click the link of the manual and save the manual to a location on your hard drive for later viewing.

See the “Related Documentation” section on page xiv for information on other documentation for the Cisco Content Delivery System.
Troubleshooting

This appendix presents troubleshooting procedures for the CDS by showing the symptoms, probable causes, and recommended actions for a variety of issues. The topics covered in this appendix include:

- General Issues, page A-2
- Startup Issues, page A-17
- Management and Database Issues, page A-19
- Ingest Issues, page A-21
- Content Processing Issues, page A-25
- Cache-Fill Issues, page A-27
- Streaming and Playout Issues, page A-28
- Session Messaging, page A-33
- Database Issues, page A-35
- Advanced Features and Applications, page A-38
- Frequently Asked Questions, page A-39
- CDS Content Quality Guidelines, page A-44

There are a variety of possible combinations of CDS topologies, backoffice environments, middleware, and so on. The engineers using this troubleshooting appendix is expected to know their system well enough that they can extrapolate the relevant troubleshooting guidelines. With all connectivity issues, physical integrity of cables and ports should be verified, as well as VLAN configuration if applicable.

All Linux commands described in this appendix require console access to the server, or Secure Shell (SSH) access to the server.

Caution

Do not attempt to access the Linux command line unless you are familiar with the CDS, the Linux operating system, and have an understanding of the Linux command line.

Note

It is important to verify at each step that the correct user account is being used. The root and isa user accounts are the only ones required to manipulate the files. The root user account uses the # as a prompt. The isa user account uses the $ as a prompt. We strongly recommend that you change these passwords as soon as possible using the passwd command.
General Issues

This section describes the CDS file system, log files, configuration files, and general troubleshooting methods. This section includes the following:

- File System
- Log Files
- Server Configuration Files
- Identifying the Software Versions or Releases
- Using ifstats to Monitor Traffic
- Kernel Crash
- Disk Drive Issues
- Memory Issues
- Network

File System

The CDSM file system differs from the file system on the other servers (Vault, Streamer, ISV).

CDSM

The CDSM has the following directory structures:

- /arroyo/asmrpt—Contains comma-separated values (CSV) files that are created by extracting information from the database every 24 hours. These files are accessible through the Reports > Archived Data page. The asm_archiver job must be installed and added to the crontab for these files to be generated. For more information, see the “ Archived Data” section on page 6-22.
- /arroyo/db—Contains the database binaries, this roughly maps to the /home/isa/Berkeley directory on Streamers and Vaults.
- /arroyo/db/DATADIR—Contains the database files and indexes.
- /arroyo/image—The staging area for CDS software image files. This directory also includes backup directories when a software upgrade is performed on the server.
- /arroyo/msa—Contains the Managed Services Architecture (MSA) logs that are created by extracting information from the database. The logs are processed by the iVAST MSA agent.
- /arroyo/www—Contains the HTTP files for the CDSM GUI. The subdirectory, .../www/htdocs, contains the PHP files for the CDSM GUI.
- /arroyo/www/modules—The link library for htdocs files.
- /home/isa/—Contains configuration and log files.

Report Archiving

The CSV files are generated every 24 hours and are deleted when they are older than 30 days. The CSV files are stored in the /arroyo/asmrpt directory. In order for the CSV files to be generated, the report archiver needs to be installed and configured. The CSV files are accessible by going to the /arroyo/asmrpt directory, or by using an FTP client with the username “asmrpt” and the password “asmrpt.”
Vault, Streamer, and ISV

The Vault, Streamer, and ISV have the following directory structures:

- /arroyo/db
- /arroyo/log
- /arroyo/test/
- /arroyo/archive
- /home/isa

In addition to the above directories, the Vault, Streamer, and ISV have the following directories specific to the RTSP environment.

- /home/isa/bss
- /home/isa/bss/bin—Contains the VOD server binaries
- /home/isa/bss/database—Contains the database files
- /home/isa/bss/etc—Contains the configuration files for the binaries
- /home/isa/bss/lib—Contains the shared application libraries
- /home/isa/bss/log—Contains the application log files
- /home/isa/bss/log/archive—Contains the archived log files
- /home/isa/bss/run—Contains process ID (PID) files for running the application
- /home/isa/bss/scripts—Contains general scripts

Log Files

There are three types of log files in an RTSP environment:

- **Linux Log Files**
- **CServer Log Files**
- **RTSP Log Files**

The CServer log files are automatically archived and moved to the /arroyo/archive directory when the disk storage reaches a certain level. The RTSP log files are automatically archived and moved to the /home/isa/bss/log archive directory whenever the FSI or RTSP process is restarted, or the log file reaches close to 50 MB in size. A total of nine revisions are kept of each log file, with the eight oldest being compressed and moved to the archive directory.

Linux Log Files

The Linux operating system has the following useful log files:

- /var/log/debugmessages—Syslog messages
- /var/log/messages—Includes useful bootup status messages
CServer Log Files

The CDS has the following useful log files:

- `/arroyo/log/c2k.log <date>`—This log has information about content read issues. The date extension for the log filename has the format of ddmmyyyy (for example, 01152008 is January 15, 2008). To increase the verbosity of this log file, use the following command:
  
  `# echo "6" > /proc/calypso/tunables/c2kVerbosedump`

- `/arroyo/log/protocoltiming.log <date>`—Provides information about any network interface issues and any disk issues.

- `/arroyo/log/avsdb.log <date>`—Provides information about any database issues.

- `/arroyo/log/statsd.log <date>`—Provides system statistics information.

- `/arroyo/log/stresstest.log <date>`—Provides CPU uptime information.

- `/root/avslauncher.log <date>`—Provides information about the startup of the avslauncher module.

Other CServer log files that may be useful are the following:

- `/arroyo.log/controlblocktiming.log <date>`
- `/arroyo.log/debug.log <date>`
- `/arroyo.log/decommissioned.log <date>`
- `/arroyo.log/deleted.log <date>`
- `/arroyo.log/executiontiming.log <date>`
- `/arroyo.log/objectRepair.log <date>`
- `/arroyo.log/serverinfo.log <date>`
- `/arroyo.log/streamevent.log <date>`
- `/arroyo.log/systemstats.log <date>`

**Note**
The files with the extension `<date>` use the format mmddyyyy. The date is the Coordinated Universal Time (UTC) date.

CServer Error Codes

CServer error codes that appear in the c2k.log.<date> file do not necessarily mean an error has occurred. An actual error has “err” listed in the entry, as opposed to “out” or “ntc.” Following is a list of important CServer error and status codes:

**Error Codes**

- 5—Completion of a task.
- 25—Insufficient resources.

**Status Codes**

- 0—Content is okay (cnOK).
- 1—Stream has ended (cnEnd).
- 2—Stream has been paused (cnPaused).
- 3—Error has occurred (cnError).
• 4—Next element is being processed (cnNextElement).
• 5—Live content has resumed (cnResumeLive).
• 6—Next content object is being processed (cnNextContent).
• 7—Next iteration is being processed (cnNextIteration).
• 9—There has been a failover (cnFailover).
• 8—Stream has been destroyed (cnDestroyed).

RTSP Log Files

The Linux user isa is the owner of the application files in an RTSP environment. To change from the root use the su – isa command.

All application log files are located in /home/isa/bss/log directory. When a log file reaches around 50 MB in size, it is archived and moved to the archive directory. When the RTSP or FSI is restarted, all current log files are archived and moved to the archive directory. The latest archived log files remain uncompressed, while the rest are gzipped. The archive directory always maintains the ten latest archives of each log file. The older log files are deleted.

If the RTSP application or the FSI application does not start, check the following files for possible reasons:
• rtsp.err
• rtsp.out
• fsi.err
• fsi.out

These files are located in the /home/isa/bss/log/ directory.

The CDS RTSP environment has the following useful log files:
• /home/isa/bss/log/fsi.log
• /home/isa/bss/log/rtsp.log
• /home/isa/bss/log/aim.log
• /home/isa/bss/log/library.log—Logs the cache2app library information

To change the log levels while the RTSP application is not running, edit the arroyo-env.sh file.

$ cd /home/isa/bss/scripts/
$ vi arroyo-env.sh

Change the value for the ARROYO_LOG_LEVEL variable to OFF, LOW, or HIGH. The default setting is LOW.

To change the log level whether the RTSP application is running or not, use the RTSP Setup page. For more information, see the “Configuring RTSP Setup” section on page 4-52.
Server Configuration Files

The server configuration settings are stored in the .arroyorc file and the setupfile file. This section describes the different parameters for each file.

Note
This section is informational only. All changes to the configuration files should be accomplished through the initial configuration and CDSM GUI.

Description of the .arroyorc Settings

This section describes the different line entries of the .arroyorc file. The .arroyorc file is located in the /home/isa directory and is created during the initial configuration procedure outlined in the Cisco Content Delivery Engine 205/220/420 Hardware Installation Guide.

self
This number represents what type of server the CDE is:
- 0 = ISV (also known as SSV)
- 1 = Vault
- 2 = Streamer
- 3 = CDSM

groupid
All servers that are part of the same CDS system (managed by one CDSM) have the same group ID. This group ID should be unique across an enterprise. The purpose of the group ID is to allow servers in a group to recognize each other as belonging to the same group. If two server groups were on the same VLAN and they had the same group number they would conflict and cause issues. This is much more likely to be an issue in a lab environment with shared resources than an actual production deployment but this should still be managed.

serverid
Every server in the group has to have a unique ID ranging from 1 to 255. It is a good idea to use a standardized numbering solution; for example, all 1xx serverids are Streamers and all 2xx server IDs are Vaults.

vault
This parameter has the IP address of a Vault in the system. Each “vault” line represents an individual Vault. There may be multiple vault lines.

streamer
This is the IP address of a Streamer in the system. Each “streamer” line represents an individual Streamer. There may be multiple streamer lines.

controller
This is the IP address of the CDSM. There is only one controller line. This line is not needed in the file for the CDSM, but is used on Vaults and Streamers to point to the CDSM.
mirroring
This controls local mirroring, which is to say this determines the number of copies of a given piece of content that is stored locally.

partno
This allows the server to identify itself properly to the CDSM. The CDSM can then display the appropriate server graphic in the GUI and manage the appropriate number of disks, Ethernet ports, and so on.

mgmtif
The index of the management interface starting at eth0. Typically this remains 0.

ingestif
This parameter is only for Vaults. The index of the ingest interface starting at eth0. Typically this remains 0 but may have the value of 1 as well.

dbdomsock
This is the “file handle” where the applications address messages intended for the database.

dbnetport
This is the port number where the applications address messages intended for the database.

controlif
The index of the stream control interface starting at eth0. This is an optional configuration that is used when you want to separate the Setup and Control interface.

Description of the setupfile Settings

This section describes the different parameters of the setupfile file. The setupfile file is located in the /arroyo/test directory. Some values for the parameters in the setupfile file are set during the initial configuration (serverid, groupid, streamer vault), others are set by using the CDSM.

Note
The localip # line entry has been deprecated. Ignore this line entry.

Required Settings

The following line entries are required in every setupfile file:

serverid #
An identifier that uniquely identifies the server within a group of servers identified by the group ID. See the “serverid” section on page A-6 for more information.

groupid #
An identifier that identifies the group of servers within the CDS. See the “groupid” section on page A-6 for more information.
streamer <0 or 1> vault <0 or 1>
To run the server as a Streamer, set streamer to 1, otherwise set streamer to 0. To run the server as a Vault, set vault to 1, otherwise set vault to 0. Setting both streamer and vault to 0 is not a valid option.

service address <ip in dot notation> setup <setup portno> control <control portno>
The service address is used to specify whether this server can assume the role of the Setup server, the Control server, or both the Setup and Control servers for the specified IP address. This parameter applies only to Streamers.
- setup portno—A value of 0 means the server is not available to assume the role of the Setup server for the specified IP address. A value of 1 means to use the default port number 3300.
- control portno—A value of 0 means the server is not available to assume the role of the Control server for the specified IP address. A value of 1 means to use the default port number 9000.

e1000 <index>: streaming <0 or 1> fill <0 or 1> ip <ip in dot notation> tport <transport portno> cport <cache portno> tgid <transport groupid>
The e1000 is used to configure the network interfaces for cache-fill and transport/streaming. Each "e1000" line represents an individual Ethernet port. Include one line per interface.
- index—Refers to the interface index as known to the e1000 driver. In the case of servers with the Lindenhurst chipset, this matches one for one with the number for the eth# interface.
- streaming—For transport/streaming. A value of 1 means this interface is used for streaming, otherwise set streaming to 0.
- fill—For cache-fill. A value of 1 means this interface is used for cache-fill, otherwise set fill to 0.
- ip—Each interface requires a source IP address. This assumes Layer 3 networks only.
- tport—The transport port number used as the source in transporting (streaming) packets. A value of 0 means to use the default port number 1026 (unless affected by the optional default source IP entry).
- cport—The cache port number used as the source in caching (fill) packets. A value of 0 means to use the default port number 48879 (unless affected by the optional default source IP entry).
- tgid—The transport group ID for this interface. The transport group ID is used in conjunction with the TransportGroupIdTable file located in the /arroyo/test directory to determine which interface to use to transport the packet. This is based on packet’s destination IP address or subnet. The default value is 0, which means this interface is available to any transport group. Any other value means the interface is dedicated to a particular transport group.

vault mirror copies <number of copies>
The Vault mirror copies is a numeric value representing the number of copies of each content to store on the Vaults.

Optional Settings

The following line entries are optional in the setupfile file:

management eth#
Specifies the interface used for management. The default is eth0.

ingest eth#
Specifies the interface used for live ingests (FTP push or UDP capture). By default, the management interface is used. This parameter is only applicable to Vaults.
Appendix A  Troubleshooting

General Issues

e1000 adapters: maxrate <rate in Mbps>
Controls the maximum transmit bandwidth on this interface, either for streaming, for caching, or for both. The default is 975 Mbps.

ibg adapters
The maximum transmit bandwidth of the ibg adapters. The default is 975 Mbps.

disks #
Specifies the number of hard drives (disks) installed on a server. The default is 12 disks for a Streamer, and 24 disks for a Vault. If you have a server with 12 disks, you must add this entry and specify 12 disks; otherwise, warning messages stating disks are non-operational will be logged to the protocol timing log file.

test #
Specifies the test mode of the server. The default is 4, which means to run the server in production mode.

cache_dscp #
Used to set the DSCP bits on cache-fill packets. The default value is 0.

cache_ecn #
Used to set the ECN bits on cache-fill packets. The default value is 0. This parameter should not be used.

transport_dscp #
Used to set the DSCP bits on transport/streaming packets. The default value is 0.

transport_ecn #
Used to set the ECN bits on transport/streaming packets. The default value is 0. This parameter should not be used.

trickspeedsv2 ########
Used to specify up to 8 speeds for generating trick objects during ingest. This parameter is only applicable to Vaults. The defaults are 5,–5,10,–10,32,–32. The highest speeds are –127. An entry larger than 127 defaults to 127. A value of 0 is ignored.

ftpout if eth# max utilization mbps # max sessions #
Used to specify which interface on the Vault is used for FTP out, the maximum bandwidth utilization for all active sessions (in Mbps), and the maximum number of simultaneous sessions allowed. By default the maximum sessions is 0, meaning that FTP out is not allowed. The default for bandwidth utilization is 0, which means unlimited usage. The default interface chosen is the management interface. For FTP out to function properly, the entire content must exist on the Vault.

bypass_isacheck <0 or 1>
Used in the RTSP environments to bypass global object ID (GOID) checks at startup.

arrayid #
Specifies the Streamer array this server belongs to. The array ID is used in conjunction with the StreamDestinationMap file located in the /arrayo/test directory to determine which play servers are available for selection. The selection is based on the packet’s destination IP address or subnet. The default value is 0.
default source ip <ip in dot notation> tport <minportno> - <maxportno> cport <portno>

Used to affect source packets if no specific information is provided in the individual mandatory e1000 interface entries.

- **ip**—The default source IP address for an interface. This value is overridden by the mandatory e1000 interface entry. This IP address is not meaningful in a Layer 3 network. However, today it must have a non-zero value for the other values to be looked at.

- **tport**—Once a stream is started, a random port within the range specified is used as the source port for transport/streaming packets of the stream (assuming no specific port was selected for tport in the mandatory e1000 interface entries).

- **cport**—The source port to use for cache-fill packets (assuming no specific port was selected for cport in the mandatory e1000 interface entries).

**Note**
The default source IP is useful in a Layer 2 network. For Layer 3 networks, an IP address is required for each interface, so the value in the default source IP is superseded by the individual entries for the interfaces. However, the default source IP setting specifies other defaults (transport port and cache port). If you would like to specify a range of transport ports, then the default source IP could have a value of zero.

**Note**
The default source IP can be used in conjunction with the mandatory e1000 interface entries. For example, the default source IP can be used to specify a range for the source transport port. However, the generation of a random port does not currently work on every stream start. Therefore, it is best not use this option.

bms address <ip> <port>

The IP address and port of the backoffice.

### Identifying the Software Versions or Releases

The following sections describe the commands for identifying the software versions on the server.

#### Linux OS Version

To identify the software version of the Linux operating system (OS) on the CDSM, enter the following command:

```bash
# cat /proc/version or “uname -a”
Linux version 2.6.18-92.el5 (brewbuilder@ls20-bc2-13.build.redhat.com) (gcc version 4.1.2 20071124 (Red Hat 4.1.2-41)) #1 SMP Tue Apr 29 13:16:15 EDT 2008
```

To identify the software version of the Linux OS on the Vault, Streamer, or ISV, enter the following commands:

```bash
# cat /proc/version
Linux version 2.6.18-53.el5.kernel.2_6_18.2008.10.07.01 (arroyoqa@build-svr) (gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)) #1 SMP Mon Nov 17 18:21:51 PST 2008
# uname -a
Linux stm74 2.6.18-53.el5.kernel.2_6_18.2008.10.07.01 #1 SMP Mon Nov 17 18:21:51 PST 2008 i686 i686 i386 GNU/Linux
```
**CDS-Related Releases**

The RTSP CDS software is a combination of an RTSP overlay, statsd software, and the CServer code. The following sections describe how to identify the software version of each.

**RTSP Environment**

To identify the software version of the CDS RTSP overlay image, enter the following command:

```
# cat /arroyo/image/tags
```

```
linux/linux              kernel-2_6_18-2009-01-15-01
snmp/statsd              statsd-2009-01-14-03
snmp/agent.S31           snmpd-2009-01-16-01
cserver                  cserver-e013-2009-01-16-06
export                   export-e013-2008-10-06-01
avsdb                    avsdb-2009-01-06-01
cache2app                 r_2_0v1-isa-e008-2009-01-15-01
isa                       r_2_0v1-isa-e008-2009-01-15-01
bss                       bss-r20-2009-01-15-01
avslauncher              avslauncher-2009-01-13-01
framework                frmwk-r20-2008-10-28-02
tavsdb                    tavsdb-2009-01-14-01
ui/http/httpd-2.2.9      asm-2008-09-21-01
ui/http/php-5.2.6        asm-2009-01-13-01
upscripts                upgrade-2009-1-8-01
packager                  1
flav_inst                 1
```

**statsd Program**

To identify the software version of the statsd program, enter the following command:

```
# strings /home/stats/statsd |grep Rel
```

```
STATSD Release TOP_OF_TREE (arroyoqa@build-svr) (gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)) #1-Nstatsd-2008-11-07-02 Mon Nov 17 18:34:15 PST 2008
```

**CServer Code**

To identify the software version of the CServer on the Streamer, Vault, or ISV, enter the following command:

```
# strings avs_cserver.ko |grep CServer
```

```
Average setup time spent in CServer =
AVS CServer Release #1-Ncserver-e013-2008-11-17-05 Mon Nov 17 18:54:01 PST 2008
ENV_ISA_SR DEBUG
AVS CServer Information ENV_ISA_SR DEBUG (arroyoqa@build-svr) (gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)) #1-Ncserver-e013-2008-11-17-05 Mon Nov 17 18:54:01 PST 2008
```

To view the CServer settings, status, and version, enter the following command:

```
# cat /proc/calypso/status/server_settings
```

```
AVS CServer Information ENV_ISA_SR PROD (arroyoqa@build-svr) (gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)) #1-Ncserver-e013-2009-01-20-03 Tue Jan 20 17:54:28 PST 2009

Server Settings:
Server is operational
Cache2App is operational
```
Appendix A  Troubleshooting

General Issues

TSCs Per Second is 2333447000

Network Settings:
- Running in L3 Network Mode
- Allow Jumbo Frames
- Transport/Stream Data Payload: 1316
- Cache/Fill Data Payload: 7680
- Cache/Fill Control Maximum Packet Size: 8048

Using ifstats to Monitor Traffic

The `ifstats` command shows real-time traffic on each Ethernet interface on the server.

```
# /home/stats/ifstats
ifstats - 11:12:22

<table>
<thead>
<tr>
<th>Int#</th>
<th>R-Mbps</th>
<th>X-Mbps</th>
<th>R-Bytes</th>
<th>X-Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>0</td>
<td>0</td>
<td>56760511</td>
<td>166307653</td>
</tr>
<tr>
<td>eth1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>eth2</td>
<td>4</td>
<td>457</td>
<td>3439241508</td>
<td>3497139080</td>
</tr>
<tr>
<td>eth3</td>
<td>4</td>
<td>457</td>
<td>3439172148</td>
<td>3099124288</td>
</tr>
<tr>
<td>eth4</td>
<td>4</td>
<td>457</td>
<td>3441836680</td>
<td>2945489644</td>
</tr>
<tr>
<td>eth5</td>
<td>4</td>
<td>472</td>
<td>3443060380</td>
<td>2736156168</td>
</tr>
<tr>
<td>eth6</td>
<td>4</td>
<td>471</td>
<td>3438423816</td>
<td>2613199736</td>
</tr>
<tr>
<td>eth7</td>
<td>5</td>
<td>464</td>
<td>3440066492</td>
<td>2419935662</td>
</tr>
<tr>
<td>eth8</td>
<td>4</td>
<td>449</td>
<td>3439982812</td>
<td>2266582156</td>
</tr>
<tr>
<td>eth9</td>
<td>4</td>
<td>465</td>
<td>3441251384</td>
<td>2164010982</td>
</tr>
<tr>
<td>eth10</td>
<td>5</td>
<td>465</td>
<td>3439982136</td>
<td>1915437726</td>
</tr>
<tr>
<td>eth11</td>
<td>4</td>
<td>464</td>
<td>3438935192</td>
<td>397577442</td>
</tr>
<tr>
<td>eth12</td>
<td>5</td>
<td>464</td>
<td>3440343164</td>
<td>300903930</td>
</tr>
<tr>
<td>eth13</td>
<td>4</td>
<td>465</td>
<td>3439540716</td>
<td>4454799830</td>
</tr>
</tbody>
</table>
```

Kernel Crash

The kernel debugger (KDB) provides information (in the form of a core dump file) when the server processing fails.

If a server has crashed after being started automatically from the `/etc/rc.local` directory, you need to boot in single-user mode. To boot in single-user mode, perform the following steps:

**Step 1** Reboot the server.
**Step 2** When a blue screen displays a list of Linux versions, press the E key to edit the kernel entry.
**Step 3** Multiple lines are displayed. Use the **Up Arrow** and **Down Arrow** keys to highlight the second line. You may need to press the E key again to edit the line. A square cursor appears at the end of the line.
**Step 4** Remove the 115200 from the console parameter (for example, console=ttys0,115200n8).
**Step 5** Add the word, “Single” or the letter “S” to the end of the line.
**Step 6** Press **Enter**.
**Step 7** Press the B key to boot the Linux kernel into single-user mode.
**Step 8** Wait for the server to finish booting up.
**Step 9** Edit the `/etc/rc.local` file and comment out the line `/arroyo/test/vault/run`. 
Step 10
Reboot the server.

To view the contents of the core dump file from the Linux prompt, do the following:

Step 1
Run the GNU debugger (gdb), and specify the core file and binary file.

```
gdb --core=<core-file> <binary-file>
```

The core-file parameter is the core filename and the binary-file is the binary file that produced the core file.

Step 2
Once the GNU debugger has started, enter the backtrace command, `bt`, at the gdb prompt and press `Enter`.

```
gdb> bt
```

The callback stack is displayed, which shows the history of the current function calls that were made at the time of the crash.

Disk Drive Issues

When reinserting disk drives after transporting a chassis, or transferring disk drives from one chassis to another, the disk drive order is irrelevant.

To view the statistics of the internal boot drive, the disk drive that contains the software, enter the `df -k` command.

```
# df -k
Filesystem          1k-blocks  Used  Available  Use%  Mounted on
/dev/hda1            10317828 3764936   6028776  39%  /
/dev/hda2            20641788 1711372  17881776   9%  /arroyo
/dev/hda3            8254272  32828  7802148   1%  /arroyo/db
/dev/hda6            35641880 1185880  32645480   4%  /arroyo/log
none                 1681200         0  1681200   0%  /dev/shm
```

To view the statistics of a removable SATA or SCSI disk drive, use the following commands:

```
# cat /proc/calypso/status/streamer/diskinfo
Disk Info:
    Disks(12) Op(12)
    Storage: T(804G) A(21%) U(0)
    BW: (99%) w(1.35M/s) r(0/s)
    I/O Util: w(1:0%) e(0) a(0%)
Disk[ 2][67.0G] A[20%] B[0x]
Disk[ 3][67.0G] A[21%] B[0x]
Disk[ 4][66.5G] A[22%] B[0x]
Disk[ 5][67.0G] A[20%] B[0x]
Disk[ 6][67.0G] A[21%] B[0x]
Disk[ 7][67.0G] A[20%] B[0x]
Disk[ 8][67.0G] A[20%] B[0x]
Disk[ 9][67.0G] A[21%] B[0x]
Disk[10][67.0G] A[20%] B[0x]
Disk[12][67.0G] A[20%] B[0x]
```
CDSM GUI Disk Monitor Page Reports a Disk Warning

If the CDSM GUI Disk Monitor page reports a disk warning, check the disk drive status in the /arroyo/log/protocoltiming.log.<date> log file and the /var/log/debugmessages log file.

```bash
# grep drives /arroyo/log/protocoltiming.log.11132007
WARNING: 5 disk drives are non-operational
WARNING: 5 disk drives are non-operational
...  
WARNING: 5 disk drives are non-operational
WARNING: 5 disk drives are non-operational
```

```bash
# grep disks /var/log/debugmessages
Nov 20 19:02:44 vault219 kernel: RAMDISK driver initialized: 16 RAM disks of 16384K size 4096 blocksize
Nov 20 19:03:34 vault219 kernel: Waiting for 2 disks to finish initializing
Nov 20 19:03:34 vault219 kernel: Waiting for 4 disks to finish initializing
Nov 20 19:03:35 vault219 kernel: Waiting for 3 disks to finish initializing
Nov 20 19:03:36 vault219 kernel: Waiting for 2 disks to finish initializing
Nov 20 19:03:36 vault219 kernel: Waiting for 1 disks to finish initializing
Nov 20 19:03:36 vault219 kernel: Waiting for 5 disks to finish initializing
Nov 20 19:03:42 vault219 kernel: Waiting for 6 disks to finish initializing
Nov 20 19:03:42 vault219 kernel: Waiting for 5 disks to finish initializing
Nov 20 19:03:43 vault219 kernel: Waiting for 4 disks to finish initializing
Nov 20 19:03:45 vault219 kernel: Waiting for 11 disks to finish initializing
Nov 20 19:03:46 vault219 kernel: Waiting for 10 disks to finish initializing
Nov 20 19:03:46 vault219 kernel: Waiting for 9 disks to finish initializing
Nov 20 19:03:46 vault219 kernel: Waiting for 8 disks to finish initializing
Nov 20 19:03:47 vault219 kernel: Waiting for 7 disks to finish initializing
Nov 20 19:03:47 vault219 kernel: Waiting for 6 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 5 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 4 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 3 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 2 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 1 disks to finish initializing
Nov 20 19:03:50 vault219 kernel: Total disk space = 24.0TB on 24 disk drives (Lost disks = 0)
```

Memory Issues

To slow down the CDSM bootup in order to see the memory counter, do the following:

**Step 1**  Reboot the server.

**Step 2**  To enter the BIOS Setup Utility, press the **Delete** key on your keyboard when you see the following text prompt:

```
Press DEL to runSetup
```

**Note**  In most cases, the **Delete** key is used to invoke the setup screen. There are a few cases where other keys are used, such as **F1**, **F2**, and so on.

**Step 3**  Use the **Right Arrow** key to navigate to the Boot menu.
**Step 4**  Choose the **Boot Settings** configuration option *(Figure A-1).*

**Step 5**  Choose **Quick Boot** and set it to **Disabled**.

**Figure A-1**  **BIOS Setup Utility—Boot Settings**

<table>
<thead>
<tr>
<th>Boot Settings Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Boot</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Quiet Boot</td>
<td>[Disabled]</td>
</tr>
<tr>
<td>AddOn ROM Display Mode</td>
<td>[Force BIOS]</td>
</tr>
<tr>
<td>Bootup Mem Lock</td>
<td>[Dbl]</td>
</tr>
<tr>
<td>PS/2 Mouse Support</td>
<td>[Auto]</td>
</tr>
<tr>
<td>Wait For ‘F1’ If Error</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Hit ‘DEL’ Message Display</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Interrupt 19 Capture</td>
<td>[Enabled]</td>
</tr>
</tbody>
</table>

![BIOS Setup Utility—Boot Settings](image)

**Step 6**  Press **F10** to save and exit the BIOS Setup Utility.

---

**Network**

The following commands are useful for checking your network configuration and activity.

To view the ARP table, enter the following command:

```
# arp -a
```

jetsam.v.com (111.0.110.151) at 00:00:0C:07:AC:00 [ether] on eth0
cds17-m1.v.com (111.0.210.170) at 00:30:48:58:5B:A1 [ether] on eth0
? (111.0.210.175) at 00:30:48:32:0A:5A [ether] on eth0
cds17-s1.v.com (111.0.210.172) at 00:04:23:D8:89:44 [ether] on eth0
cds17-s1.v.com (111.0.210.172) at 00:04:23:D8:89:44 [ether] on eth0

To view the IP routing table, enter the following command:

```
# netstat -rn
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS</th>
<th>Window</th>
<th>irtt</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>111.0.210.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
<tr>
<td>111.0.0.0</td>
<td>0.0.0.0</td>
<td>255.0.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>0.0.0.0</td>
<td>255.0.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>lo</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>111.0.210.1</td>
<td>0.0.0.0</td>
<td>UG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
</tbody>
</table>

To view the CDS routing table, enter the following command:

```
# cat /arroyo/test/RoutingTable
```

default gateway 111.1.13.1
network 111.1.13.1 netmask 255.255.255.240 gateway 0.0.0.0
To view the CDS remote server table, enter the following command:

```
# cat /arroyo/test/RemoteServers
remote server
   id 141
   ip 111.1.9.20
   ip 111.1.9.21
   ip 111.1.9.22
   ip 111.1.9.23
   ip 111.1.9.24
end remote server

remote server
   id 143
   ip 111.1.9.25
   ip 111.1.9.26
end remote server

remote server
   id 144
   ip 111.1.9.27
   ip 111.1.9.28
   ip 111.1.9.29
   ip 111.1.9.30
end remote server
```

### Interface Information

To view basic interface information, use the `ifconfig` command.

```
# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:04:23:D8:9A:80
inet addr:111.0.110.41  Bcast:111.0.110.255  Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:13946269 errors:0 dropped:0 overruns:0 frame:0
TX packets:11594110 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueue len:1000
RX bytes:3085199261 (2942.2 Mb)  TX bytes:1317620721 (1256.5 Mb)
   Interrupt:24 Base address:0x3000 Memory:dd240000-0
```

For detailed interface information, view the interface information file in the `/proc/net/` directory.

```
# cat /proc/net/PRO_LAN_Adapters/eth0.info
Description                      Intel® Gigabit Ethernet Network Connections
Part_Number                      ffffff-0ff
Driver_Name                      igb
Driver_Version                   1.2.22-CDS
PCI_Vendor                       0x8086
PCI_Device_ID                    0x10a7
PCI_Subsystem_Vendor             0x15d9
PCI_Subsystem_ID                 0x10a7
PCI_Revision_ID                  0x02
PCI_Bus                         14
PCI_Slot                         0
PCI.Bus_Type                     UNKNOWN
PCI_Bus.Speed                    UNKNOWN
PCI_Bus_Width                    UNKNOWN
IRQ                              194
System_Device_Name               eth0
Current_HWaddr                   00:30:48:C3:26:9E
Permanent_HWaddr                 00:30:48:C3:26:9E
```
Appendix A  Troubleshooting

Startup Issues

This section includes the following topics:

- BIOS Settings—Operating System Hangs or Goes into KDB Mode
- Serial Console Port Settings
- Required Services Not Starting or Running Correctly
BIOS Settings—Operating System Hangs or Goes into KDB Mode

When a single bit error occurs in the memory of a server, it causes the Linux OS to lock up, which puts the server into kernel debugger (KDB) mode. This is due to the BIOS Error Correcting Code (ECC) Type being set incorrectly.

To correct the ECC Error Type setting in the BIOS Setup Utility, do the following.

---

**Step 1**  During the server bootup, press the **Delete** key to enter the BIOS Setup Utility.

**Step 2**  Navigate to the Advanced menu and choose **Advanced Chipset Control**.

**Step 3**  Choose **ECC Error Type** and change the setting to **NMI** (Figure A-2).

---

**Step 4**  Press **F10** to save and exit.

---

Serial Console Port Settings

The CDE servers ship with the following serial console settings: 115200 baud rate, no parity, 8 data bits, and 1 stop bit (115200-N-8-1). To verify the serial console settings, check the following:

- **BIOS Settings**—Determines the speed during the very beginning of the boot process up to and including the GRUB menu. In the BIOS Setup Utility, check that the Console Redirection in the Advanced menu is set to VT100.
• /etc/boot/menu.lst—Determines the speed once the kernel is loaded.
• /etc/inittab—Determines the speed once the OS is loaded. Enter the following:
  ```
  $ cat /etc/inittab | grep S0
  S0:2345:respawn:/sbin/agetty ttyS0 115200 vt100
  ```

  The CDE100 may have the following serial console settings: 9600 baud rate, no parity, 8 data bits, and 1 stop bit (9600-N-8-1).

---

**Required Services Not Starting or Running Correctly**

From the CDSM GUI, view the Services page for each server by clicking **Monitor > Server Level > Services**. For more information, see the “Services Monitor” section on page 5-29. If the required services are not started, or they are not running correctly, check that there is two-way database connectivity between the Streamers and Vaults, and the CDSM.

  ```
  $ netstat -an | grep 9999
  tcp 0 0 0.0.0.0:9999 0.0.0.0:* LISTEN
  tcp 0 0 172.22.97.193:9999 172.22.97.197:56998 ESTABLISHED
  tcp 0 0 172.22.97.193:34743 172.22.97.197:9999 ESTABLISHED
  tcp 0 0 172.22.97.193:9999 172.22.97.192:50343 ESTABLISHED
  tcp 0 0 172.22.97.193:39158 172.22.97.196:9999 ESTABLISHED
  tcp 0 0 172.22.97.193:46030 172.22.97.192:9999 ESTABLISHED
  tcp 0 0 172.22.97.193:9999 172.22.97.196:55780 ESTABLISHED
  tcp 0 0 172.22.97.193:9999 172.22.97.191:50950 ESTABLISHED
  tcp 0 0 172.22.97.193:60598 172.22.97.191:9999 ESTABLISHED
  tcp 0 0 172.22.97.193:9999 172.22.97.194:37543 ESTABLISHED
  tcp 0 0 172.22.97.193:56376 172.22.97.194:9999 ESTABLISHED
  ```

Two connections for each Vault and Streamer should be listed with a status of “ESTABLISHED.”

If the connection states do not say “ESTABLISHED,” check the configuration of /home/isa/.arroyorc file to make sure the settings are correct, then restart the database.

Log in to the server as `isa` and start the database.

  ```
  $ arroyo start avsdb
  ```

Log into the server as `root` and start the statsd.

  ```
  $ /home/stats/statsd
  ```

Check that the RTSP listener is running on the correct port.

  ```
  $ arroyo status
  $ netstat -an | grep 554
  ```

---

**Management and Database Issues**

This section includes the following topics:

- System Health
- Cannot Access the CDSM GUI
- CDSM GUI Does Not Register the Vaults and Streamers
- Database Monitoring
System Health

The colored boxes on the System Health Monitor page have the following meaning:
- Green—All components are operating; occasionally click each check box to verify.
- Yellow—Some components are not operational.
- Red—All components have failed.

Cannot Access the CDSM GUI

If you cannot access the CDSM GUI, log in as root and verify that the Apache server is running on the CDSM.

```
# ps -aef | grep http
```

```
root    4023     1  0 Aug09 ?        00:01:44 /arroyo/www/bin/httpd
nobody  4033  4023  0 Aug09 ?        00:00:53 /arroyo/www/bin/httpd
nobody  4034  4023  0 Aug09 ?        00:00:53 /arroyo/www/bin/httpd
nobody  4035  4023  0 Aug09 ?        00:00:53 /arroyo/www/bin/httpd
nobody  4036  4023  0 Aug09 ?        00:00:53 /arroyo/www/bin/httpd
nobody  4037  4023  0 Aug09 ?        00:00:53 /arroyo/www/bin/httpd
nobody  4085  4023  0 Aug09 ?        00:00:52 /arroyo/www/bin/httpd
nobody  4086  4023  0 Aug09 ?        00:00:53 /arroyo/www/bin/httpd
nobody  4572  4023  0 Aug10 ?        00:00:52 /arroyo/www/bin/httpd
root   11598 30692  0 16:12 pts/0    00:00:00 grep http
```

If the Apache server is not running, restart the server.

```
#/arroyo/www/bin/apachectl start
```

CDSM GUI Does Not Register the Vaults and Streamers

If the CDSM GUI is not able to register that the Vaults and Streamers are part of the array or CDS, do the following:

**Step 1** Log in to the Vault or Streamer as root.

**Step 2** Verify two-way database connectivity with the CDSM.

```
# netstat -an | grep 9999
```

**Step 3** Verify statsd is running.

```
# ps -aef | grep statsd
```

**Step 4** Verify the correct version and permissions for /home/stats/svrinit or svrinit_15 are being used.

```
# ls -l /home/stats/
```

**Step 5** On the Vault and the Streamer, initialize the CDS host in the database by using svrinit_15. Use the following options:
- Option -i for the server’s physical IP address (eth0)
- Option -s for the subnet mask of the network
- Option -h for the host name
• Option -d to deregister

For example, first deregister the CDS host using the -d option, then initialize the CDS host.

```
# svrinit_15 -i <ip_address> -s <subnet_mask> -h <host_name> -d
# svrinit_15 -i <ip_address> -s <subnet_mask> -h <host_name>
```

**Step 6** If you still have trouble getting the tables initialized, then log in to the CDSM GUI with an engineering access user account and add the Streamer or Vault by clicking the **Maintain > Software > System Configs** page and using the **Add New Server** option.

---

**Database Monitoring**

To monitor a stuck database thread problem, use the following command:

```
netstat -an | grep 9999
```

Two connections for each Vault and Streamer should be listed with a status of “ESTABLISHED.” If two-way connection does not exist, run `db_shutdown` on all servers including the CDSM, then start the database using the following commands:

```
# su – isa
$ arroyo start avsdb
```

If the database is stuck and `db_shutdown` does not take effect, use `ps –ef |grep avsdb` to query the process ID (PID), then use the `kill -9 {pid}` command to kill the avsdb process, and lastly restart the database.

---

**Ingest Issues**

This section includes the following ingest issues:

- Ingest Interface
- Bad Content
- Network

---

**Ingest Interface**

This section includes the following topics on troubleshooting the ingest interface:

- FSI Starts but Cannot Ingest Content
- FSI Does Not Start
- Content Not Ingesting
- Asset Ingest Manager Restart Causes Endless Loop
Ingest Issues

Appendix A    Troubleshooting

FSI Starts but Cannot Ingest Content

**Cause 1:** FSI mode selected is incorrect.

**Action 1:** Check the FSI mode on the server by viewing the /home/isa/bss/log/fsi.log when FSI is started.

```
11/05/2008|19:04:50.035191|fsid.cc|444|366702208| Initializing fsi daemon...
11/05/2008|19:04:50.035470|fsid.cc|445|366702208| main(): Thread ID: 366702208
11/05/2008|19:04:50.035520|fsid.cc|447|366702208| Initializing FSI configuration...
11/05/2008|19:04:50.035654|DatabaseConnection.cc|62|366702208| Successfully connected database socket.
11/05/2008|19:04:50.048468|fsid.cc|459|366702208| Setting FSI running mode to "1" as specified by commandline.
```

FSI Does Not Start

**Cause 1:** Invalid port address.

```
cat fsi.err | grep FSID
```

**Action 1:** Change the FSI port to a nonzero value (default=20004).

```
Using the CDSM GUI, choose Configure > Server Level > FSI Setup and enter a new port number in the FSI Server Port field. See the “Configuring FSI Setup” section on page 4-58 for more information.
```

**Action 2:** Log in to the server as *isa* and start the FSI service.

```
$ arroyo start fsi
```

**Cause 2:** Cannot open cache2app reported in fsi.log and fsi.err.

**Action 1:** Verify that the CSserver process is running

```
Log in to the server as root and enter the lsmod command to check if the avs_cservlet is running.
If the avs_cservlet is not running, enter the rpm -qa | grep cserver command to see if it is installed.
- If avs_cservlet is installed, enter the /arroyo/test/run command to start avs_cservlet.
- If avs_cservlet is not installed, call Cisco Technical Support.
```

Content Not Ingesting

**Cause 1:** Cannot connect to the FTP server (for example, Lysis Content Ingest Server).

**Action 1:** Check the network connectivity and user access.

```
Check the network connectivity, access control lists (ACLs), user access privileges, and so on for the FTP server.
```

**Action 2:** Verify the manual FTP request.

```
Verify that a manual FTP request to the FTP server from the user isa is working and list the content to be ingested.
```

**Cause 2:** Content is not correctly named in the ADI XML file.
Action 1: View the aim.log file.

```
cat aim.log | grep FTPP
```

11/23/2007|12:00:59.383279|AIMListenThread |0144|06151|CALLBACK
RECVD|FSICALLBACK|2251799813686769|400|FTPProcess:|run_ftp(): FTP Failed:

In this example, 6663_3800p.mpg does not exist on the FTP server. Make sure the FTP server content matches the content listed in the ADI XML file.

Cause 3: The Asset Ingest Manager (AIM) is not getting a message from the FTP server.

Action 1: Do the following:

1. Identify the master Vault by looking at the /sbin/ifconfig file and locating the eth0:1 interface.
2. On the master Vault, enter the `tail -f aim.log` command.
3. Retry the transfer from the FTP server.
4. If there is a connectivity issue, the aim.log is not updated.
5. Restart the AIM process by entering the `arroyo stop aim` command followed by the `arroyo start aim` command.
6. If necessary, restart the FTP server.

Asset Ingest Manager Restart Causes Endless Loop

Cause 1: AIM has orphaned threads.

Action 1: Check the aim.log for endless looping message.

```
12/12/2007|11:47:16.677035|AVSIngestMgrISA |0178|01024|******************* AIMd starting*******************
12/12/2007|11:47:16.684145|pRunMaster        |0035|01024|Current process is the master
12/12/2007|11:47:16.684597|AIMCache          |0164|01024|Trying to load dynamic libs........
12/12/2007|11:47:16.745753|AIMCache          |0182|01024|Shared lib error[libAVSNGOD_AIM.so: cannot open shared object file: No such file or directory]
12/12/2007|11:47:16.745911|AIMCache          |0182|01024|Shared lib error[libAVSISA_AIM.so: cannot open shared object file: No such file or directory]
12/12/2007|11:47:16.746031|AIMCache          |0182|01024|Shared lib error[libAVSVideovision_AIM.so: cannot open shared object file: No such file or directory]
.....
12/12/2007|15:55:20.31800|AIMDbManager      |0021|02051|AIM config change detected.....
12/12/2007|15:55:20.322220|ATMDBManager      |0316|02051|DB Tag[.0.0.0:20004/]
12/12/2007|15:55:20.322670|ATMDBManager      |0054|02051|Config change from [http://.0.0.0:20004/]
12/12/2007|15:55:20.33040|ATMDBManager      |0055|02051|Config change to [.0.0.0:20004/]
12/12/2007|15:55:20.325100|ATMDBManager      |0054|02051|Config change from [/totalmanage/vod][5001]
Ingest Issues

12/12/2007|15:55:20.325500|AIMDbManager |0055|02051|Config change to [nage/vod][]
12/12/2007|15:56:20.443830|pDbConfigObject |0257|02051|Db errcode[55]
12/12/2007|15:56:20.444500|AIMDbManager |0021|02051|AIM config change detected.....
12/12/2007|15:56:20.445230|AIMCache |0316|02051|DB Tag[0004/]
12/12/2007|15:56:20.445690|AIMDbManager |0054|02051|Config change from [.0.0.0:20004/]
12/12/2007|15:56:20.446060|AIMDbManager |0055|02051|Config change to [0004/]
12/12/2007|15:56:20.446460|AIMCache |0316|02051|DB Tag[here.there:8082/totalmanage/vod][]
12/12/2007|15:56:20.446900|AIMDbManager |0054|02051|Config change from [omeplace.here.there:8082/totalmanage/vod][]
12/12/2007|15:56:20.447270|AIMDbManager |0055|02051|Config change to [here.there:8082/totalmanage/vod][]
12/12/2007|15:56:20.448310|AIMDbManager |0054|02051|Config change from [nage/vod][]
12/12/2007|15:56:20.448700|AIMDbManager |0055|02051|Config change to [][]

Action 1: Check for orphaned AIM threads during the AIM service being stopped.

Log in as isa and stop the AIM service, verify there are no orphaned AIM threads, and restart the AIM service.

$ arroyo stop aim

$ ps -aef | grep AVSIngestMgr

isa 7291 7243 0 20:59 pts/0 00:00:00 grep AVSIngestMgr

$ arroyo start aim

Cause 2: The master Vault AIM is in a degraded state.

Check the aim.log on the slave Vault to verify it is in a waiting state.

12/12/2007|14:57:08.954182|AVSIngestMgrISA |0178|01024|******* AIMd starting****
12/12/2007|14:57:08.955726|pTCP|0065|01024|Host info 10.212.17.12:5555
12/12/2007|14:57:08.961349|pTCP|0065|01024|Host info *:5555
12/12/2007|14:57:08.961442|pRunMaster|0029|01024|process is not the master, waiting on notification

Action 1: Cause a failover between the master and slave Vaults.

On the master Vault, stop the stds and Ingest Manager (AIM) services, thereby causing Vault failover. The AIM service on the new master Vault should immediately start processing Vault requests.

On the old master Vault, log in as root and restart the stds service, log in as isa and restart the AIM service. This Vault becomes the new standby and the AIM process is in waiting mode.

Bad Content

Variable bit rate (VBR) encoded content is not currently supported. Refer to the “CDS Content Quality Guidelines” section on page A-44 for constant bit rate (CBR) guidelines.

Network

Ensure that the network maximum transmission unit (MTU) is appropriately set. If jumbo frames are enabled on the CDS, then the network must support jumbo frames. We recommend that the network support jumbo frames even when the jumbo frame option is disabled.
If a Layer 2 network is used for CDS, then appropriate MAC addresses (ARP entries) have to be configured on the switches and routers. Ensure that the CDS Vault and Streamer interfaces are in the same VLAN. If a Layer 3 network is used for the CDS, then ensure that the corresponding default gateways are correctly configured on CDS Vaults and Streamers for the various interfaces and Stream Groups.

Ensure that the content source (catcher, FTP server, and so on) is reachable from the Vaults or ISVs, and that manual content transfer using FTP works correctly.

For more information about the status of the network interfaces, network routing tables, ARP and so on see the “Network” section on page A-15.

## Content Processing Issues

This section includes the following content processing issues:

- Listing Content
- Content Mirroring
- Verifying GOIDs
- Trick-Mode Issues

### Listing Content

To view the actual stored content versus what the database reports, enter the following commands:

```sh
$ su - isa
$ cd /arroyo/db
$ ./AVSDBUtil <<- EOF > db_content_list
  > 1
  > 2
  > 0
  > EOF
$ cat db_content_list
```

### Content Mirroring

To enable content mirroring locally on one Vault, do the following:

**Step 1** Modify the /home/isa/.arroyorc file by adding the following line:

```diff
  cserver_opts "vault local copy count 2"
```

**Step 2** Verify that the change has propagated to the /arroyo/test/vault/setupfile file.

The line, “vault local copy count 2,” should be added to the setupfile file.

Alternatively, enable local mirroring using the tunables. You can also use the tunables to verify the settings.

```sh
echo 2 > /proc/calypso/tunables/vaultlocalcopycount
```
Appendix A      Troubleshooting

Content Processing Issues

Note

Using the `echo 2` command to enable local mirroring in the tunable file, only changes the local copy count temporarily. The local copy count resets to its original value on reboot. To configure the local copy count permanently, for any value other than 1, edit the `/arroyo/test/vault/setupfile` or use the CDSM GUI.

To enable content mirroring between two Vaults, do the following:

---

**Step 1**
In the CDSM GUI, choose **Configure > Server Level > Server Setup**. The Server Setup page is displayed.

For more information, see the “Configuring the Servers” section on page 4-41.

**Step 2**
From the **Server IP** drop-down list, choose the IP address of the server.

**Step 3**
From the **Vault Mirror Copies** drop-down list, choose 2.

**Step 4**
Click **Submit**.

**Step 5**
Verify the change has propagated by looking at `/arroyo/test/vault/setupfile` and `/arroyo/log/protocoltiming.log.<date>` files.

```
# grep mirror /arroyo/test/setupfile
vault mirror copies 2

# grep LocalMirror /arroyo/log/protocoltiming.log.11202007
-LocalMirror Active=0:0 comp=0% obj=0.0/s read=0b/s write=0b/s copies=1
-LocalMirror Active=0:0 comp=0% obj=0.0/s read=0b/s write=0b/s copies=1
```

---

Verifying GOIDs

You cannot verify that the global object identifiers (GOIDs) among Vaults and Streamers are correct by comparing the total number of GOIDs on each server. There are actually multiple chains of GOIDs. If you list the GOID chains you can verify that the GOIDs are correct, because listing the GOIDs provides a summary at the end of the listing that reports any issues.

To list the GOIDs, enter the following command:

```
echo 2 > /proc/calypso/tunables/cm_logserverinfo
```

To list all GOID chains, enter the following command:

```
echo 4 > /proc/calypso/tunables/cm_logserverinfo
```

The log file that contains information about the GOIDs is the `/arroyo/log/serverinfo.log.<date>` log file.

---

Trick-Mode Issues

Verify the trick-mode settings in the CDSM GUI and the Vault setupfile file.

- From the CDSM GUI, choose **Configure > System Level > Ingest Tuning** to view the trick-mode settings.

- To check the trick-mode setting in the setupfile on the Vault, enter the following command:

```
$ grep trick /arroyo/test/setupfile
trickspeedsv2    4 10 32 -32 -10 -4
```
Check the `/arroyo/log/c2k.log.<date>` log file and the session message logs during playout to verify that the trick-mode files are being streamed.

### Cache-Fill Issues

This section covers the following cache-fill issues:

- Rules for ISV Interoperability with Vaults and Streamers
- Network

### Rules for ISV Interoperability with Vaults and Streamers

The following rules apply for ISVs to interoperate with Vaults and Streamers:

- An ISV can cache-fill both a colocated Streamer and a dedicated remote Streamer.
- An ISV at one location cannot cache-fill a Streamer associated with an ISV at another location.
- Two ISVs can mirror content with each other, but an ISV and a Vault cannot mirror content with each other.
- A Vault cannot cache-fill an ISV.

### Network

**Note**

For more network troubleshooting methods, see the “Network” section on page A-24.

### Stream Stops Playing at the Same Place or Does Not Play at All

**Cause 1:** Jumbo frames are not supported or configured on the cache-fill network switch.

**Check 1:** Search the c2k.log file and the rtsp.log file for content read errors.

```bash
15-Jan-2008 20:42:33 UTC :out:c2k_p_setcontentbundle: stream 3 localStreamHandlePtr 00000000 remoteServer 00000000
15-Jan-2008 20:42:33 UTC :out:c2k_p_setcontentbundlecontinue: stream 3 localStreamHandle 0
15-Jan-2008 20:42:33 UTC :out:c2k_p_setdestination: stream 3 localStreamHandle 0 ip 0xe0016401 port 10000
15-Jan-2008 20:42:41 UTC :out:iGate::ReadClose(goid 0): ERROR: Never saw header
15-Jan-2008 20:42:41 UTC :out:iGate::ReadClose(goid 0): ERROR: Never saw EOF record
15-Jan-2008 20:42:44 UTC :out:iGate::ReadClose(goid 0): ERROR: Never saw header
15-Jan-2008 20:42:44 UTC :out:iGate::ReadClose(goid 0): ERROR: Never saw EOF record
15-Jan-2008 20:42:47 UTC :out:iGate::ReadClose(goid 0): ERROR: Never saw header
15-Jan-2008 20:42:47 UTC :out:iGate::ReadClose(goid 0): ERROR: Never saw EOF record
```

**rtsp.log**

```bash
01/15/2008|21:43:03.585614|MyrioSession.cc|385|Successfully sent message to IPTV STB
01/15/2008|21:43:03.585785|StreamImpl.cc|1980|***** Stream State (after Callback receipt) *****
01/15/2008|21:43:03.585899|StreamImpl.cc|1982|Current Operation : = 0
01/15/2008|21:43:03.585957|StreamImpl.cc|1983|Operation Time (ms) : = 1200429783585
```
01/15/2008|21:43:03.586011|StreamImpl.cc|1984|Stream State : = stopped
01/15/2008|21:43:03.586062|StreamImpl.cc|1985|************************************************
01/15/2008|21:43:03.586191|MyrioSession.cc|375|IPTV STB Message:
ANNOUNCE * RTSP/1.0
CSeq: 30539779
Session: 13762563
x-notice: 4400 "Error Reading Content Data" event-date=20080115T204303.586Z
01/15/2008|21:43:03.586259|MyrioSession.cc|385|Successfully sent message to IPTV STB

### Check 2: Ping between the two devices.

Ping between the two devices on the cache-fill VLAN using a packet size greater than 1500 bytes.

### Action 1: If the ping fails, verify that jumbo frames and cache-fill interfaces are configured correctly.

Verify that jumbo frames are enabled on the switch ports for the cache-fill VLAN, and verify that the cache-fill interfaces are configured correctly on the Streamers and Vaults. See the “Configuring the Servers” section on page 4-41 for information on configuring the cache-fill interfaces.

---

### Streaming and Playout Issues

This section includes the following streaming and playout issues:

- Listing of Streams
- No Streaming
- Stream Not Playing
- Poor Video or Audio Quality

---

### Listing of Streams

To monitor streams based on various criteria, go to the Stream Monitor page in the CDSM GUI by clicking **Monitor > System Level > Stream Monitor**. For more information, see the “Monitoring Stream Objects” section on page 5-13.

---

### No Streaming

Some common causes for streaming problems are the following:

- Server is in the process of being offloaded.
- QAM device has no available bandwidth.
- Tuning failure as a result of one of the following:
  - Error in the ARP table
  - QAM device is down
  - Network problem
- Backoffice is out of synchronization with the CDS ContentStore, resulting in content not being found.
Stream Not Playing

The rtsp.log file has the entry, “error reading content data.” This means that a callback was received from the CServer with a completion code of 3.

**Cause 1:** A piece of the content is missing.

In this case, a user can typically stream part of the content, but at some point the stream stops and the error message is returned in the ANNOUNCE message. The content needs to be validated at the CServer level.

**Action 1:** Set up a stream to play to a multicast address.

If this is successful, then there is a network issue, which is either a default gateway or unreachable remote client. You can verify whether it is successful by looking at the /home/stats/ifstats file.

**Action 2:** If ifstats information does not detect a problem, try streaming to another multicast IP address. Repeat streaming to a multicast address with different content and, if possible, ingest known good content. Check the protocoltiming.log.<date> for damaged GOIDs by using the following command:

```
tail -f protocoltiming.log.<latest date> | grep GOIDs
```

**Cause 2:** There is a reachability problem to the destination QAM device.

The CServer returns the same completion code, so the same error is returned in the announce message. In this case, the content does not stream at all. The play request and play response are separated by about 10 to 15 seconds, instead of the typical subsecond separation. This is due to the ARP timeout process the CServer is going through to reach the destination. Once stream response fails, the CServer calls back with the completion code of 3, which causes the “error reading content data” message.

**Action 1:** Check that the interfaces involved in the streaming are up and operating at the correct speed.

Using the CDSM GUI, choose Monitor > Server Level > NIC Monitor, select the IP address of the server, and verify the participating interfaces are up and operating at gigabit Ethernet speeds. For more information, see the “NIC Monitor” section on page 5-25.

**Action 2:** Set up a stream to play to a multicast address.

If this is successful, then there is a network problem, which is either a default gateway or unreachable remote client. You can verify whether it is successful by looking at the /home/stats/ifstats information.

**Action 3:** If streaming to a multicast address is not successful, check that the Vaults can be reached.

Check the /arroyo/log/protocoltiming.log.<date> log file for the number of reachable remote servers. Additionally, if there is a cache-fill issue, you will see a large megabit value for the re-xmit buffer.

You can also check the /arroyo/log/c2k.log.<date> log file for any unreachable Vaults.

**Cause 3:** The c2k.log file reports “no streamer available, out of capacity.”

The protocoltiming.log file reports “remote vaults 0 caches 0.” This means the Streamer and Vault have lost connection with each other.

**Action 1:** Check the route configured on the servers.

Use the `cat /arroyo/test/RoutingTable` command to verify correct route table entries.

Check the routing table using the CDSM GUI by clicking Configure > Server Level > Route Tables. For more information, see the “Configuring the Route Table” section on page 4-47.
Appendix A      Troubleshooting

Streaming and Playout Issues

Action 2: Use the `cat /arroyo/test/RemoteServers` to check if the remote server is configured correctly.
Action 3: Check the routing table on the switch or router.

Poor Video or Audio Quality

This section includes the following issues that result in poor video or audio quality:

- **No Video Displayed**
- **RTSP Cannot Start**
- **Video Stops Playing**
- **No Video Playing on the STB**
- **CDS Is Streaming but No Video Is Playing on the STB**

No Video Displayed

When content is streamed to a client device, if there is no video picture displayed on the client device and the audio is working fine, use the following troubleshooting methods:

- Verify that the source is working properly and that the original content is of good quality.
  - Verify that the appropriate bit rates are being sent from the server using the following command on all Streamers:
    ```
    /home/stats/ifstats
    ```
  - Verify that the content plays locally, and on a test client device (for example, a VLC client).
  - Test playing the content on an alternate player with an AVC plug-in.

- Verify that the CDS is configured correctly.

  - Check the run script in the `/arroyo/test/run` directory. There is a tunable set for Telenet to stream null packets when the end of the stream is reached. This should be commented out or removed in a non-Telenet environment.

  - The interface that you are using for real-time ingest needs to be configured for the CServer. There are a couple of settings that define the interrupt for the real-time ingest interface and ensure that a single central processing unit (CPU) is responsible for receiving the packets for the ingest. Without these settings, packets can be out of order, which can cause problems with the video picture.

  To fix this, use the `cat /proc/interrupts` command to display the interrupts and find the interrupt value associated with the interface you are using for ingest. Once you know this value, add the following lines to the `/arroyo/test/run` script:

  ```
  echo 1 > /proc/irq/<interrupt_value>/smp_affinity
  echo <interrupt_value> > /proc/calypso/test/bypass_disable_irq
  ```

  You can enter these lines at the Linux command line as well by doing so you do not have to reboot your system in order for them to take effect. Any content that you have previously ingested should be considered invalid.
RTSP Cannot Start

The owner and group permission of the RTSP binary file are incorrect. To correct this, enter the following commands:

```
# cd /home/isa/bss/bin
# chown root:root AVSRTSPServer
# chmod u+s AVSRTSPServer
# su - isa arroyo start rtsp
```

Video Stops Playing

If the video stops playing after a fixed interval (for example, five minutes), check to see that the interval the video played for matches the session inactivity timeout setting in the CDSM GUI Configure > Server Level > RTSP Setup page.

If the interval matches the setting, check the /home/isa/bss/log/rtsp.log file for the STB responses within the inactivity timeout interval.

This scenario could be caused by the STB possibly not responding, or the STB response may be getting lost in the network.

No Video Playing on the STB

Check the /home/isa/bss/log/rtsp.log file on the relevant Streamer. If you see a successful setup request and response, and do not see a play request for the same session, there is some issue with the STB communication to the RTSP server. The RTSP server should also be receiving a get_parameter request as a heartbeat in order to keep the session alive. If this does not happen, the session is torn down after the session inactivity timeout is exceeded, and a "session timed-out" message is sent.

Following is an example of the rtsp.log file showing the setup, response, teardown, and timeout messages.

```
SETUP rtsp://10.212.16.18:554/?AssetId=CAN36099.mpg RTSP/1.0 CSeq: 10 User-Agent: OpenTV VOD 1 Transport: MP2T/DVBC/QAM;unicast;client=168892769.6501124101;destination=172.23.68.2;client_port=1
06/13/2007|20:23:33.548631|RTSPTCPListener.cc|298|Valid RTSP request received, port = 554
06/13/2007|20:23:33.548788|RTSPMsgHandler.cc|671|Current session count = 0
06/13/2007|20:23:33.548868|RTSPMsgHandler.cc|283|Created session id of: = 1179649
06/13/2007|20:23:33.549422|StreamImpl.cc|111|Stream handle set to: = 1
06/13/2007|20:23:33.549200|StreamImpl.cc|1745|Stream setup - URL = CAN36099.mpg, downstream address = -10.0.0.0172.23.68.2
06/13/2007|20:29:13.075941|LivenessManager.cc|213|Session has timed-out, initiating teardown process. Session: 1179649
06/13/2007|20:29:13.076127|RTSPMsgHandler.cc|671|Current session count = 1
```

Notice:5402 Event-Date=20070613T182913.076Z "Client Session Terminated"
CDS Is Streaming but No Video Is Playing on the STB

Check the /home/isa/bss/log/rtsp.log file on the relevant Streamer for any of the following message flows:

- Setup request is sent from Quative, followed by setup okay response returned from CDS.
- Describe request is sent from the STB, followed by describe ok response and details returned from CDS.
- Play request is sent from STB, followed by play ok response sent from CDS.
- Teardown request is sent from STB, followed by teardown performed by CDS.

The possible causes for the above message flows are the following:

- STB is not tuning to the correct frequency or program ID, or the session resource manager (SRM) is returning incorrect information.
- SRM is providing the wrong edge QAM device to the CDS. In the rtsp.log file, check the IP address in the setup RTSP header.
- Edge QAM device port mapping may be wrong. Check the edge QAM device configuration.
- Radio frequency (RF) is not reaching the STB.

Following is an example of the rtsp.log file showing the request and response messages.

```
SETUP rtsp://87.231.193.114:554/?AssetId=CAN0000095932.mpg RTSP/1.0^M CSeq: 2^M User-Agent: OpenTV VOD 1^M Transport: MP2T/DVBC/QAM;unicast;client=170027388.4312020202;destination=172.23.77.2;client_port=16^M
11/29/2007|16:10:56.952766|RTSPTCPListener.cc|298|Valid RTSP request received, port  = 554
11/29/2007|16:10:56.952938|RTSPMsgHandler.cc|644|Current session count = 0
11/29/2007|16:10:56.953163|RTSPMsgHandler.cc|311|Created session id of: = 30801921
11/29/2007|16:10:56.954630|QuativeSession.cc|786|SETUP Response: RTSP/1.0 200 OK^M CSeq: 2^M Session: 30801921;timeout=300^M Transport: MP2T/DVBC/QAM;unicast;client=170027388.4312020202;destination=172.23.77.2;client_port=16^M Location: rtsp://87.231.193.114:554^M
11/29/2007|16:10:56.954832|PersistenceConnection.cc|137|Repository operation successfully completed
11/29/2007|16:10:57.195911|QuativeSession.cc|684|Message: RTSP/1.0 200 OK^M CSeq: 90^M Session: 30801921^M Content-Type:application/sdp^M Content-Length: 170^M v=0^M o=- 3405337857 3405337857 IN IP4 10.236.141.67^M s=RTSP Session^M t=0 0 0^M m=video 0 udp M2T^M c=IN IP4 0.0.0.0^M i=CAN0000095932.mpg^M a=type:vod^M a=range:npt=0.0-3814.142
11/29/2007|16:10:57.195975|QuativeSession.cc|694|Successfully sent message to STB
11/29/2007|16:10:57.377758|RTSPTCPListener.cc|155|Messages: PLAY * RTSP/1.0^M CSeq: 91^M Session: 30801921^M Range: npt=0.0-0^M
11/29/2007|16:10:57.377850|RTSPTCPListener.cc|298|Valid RTSP request received, port  = 554
11/29/2007|16:10:57.377986|RTSPMsgHandler.cc|644|Current session count = 1
11/29/2007|16:10:57.378120|StreamImpl.cc|1121|Play(*, from: 0 to: 2147483647)
11/29/2007|16:10:57.378179|StreamImpl.cc|588|handleContent(), url: *, play content now: 1, flush: 0
11/29/2007|16:10:57.378235|StreamImpl.cc|697|handlePlay(), loop content: 0, play content now: 1, no flush: 0
11/29/2007|16:10:57.385838|QuativeSession.cc|684|Message: RTSP/1.0 200 OK^M CSeq: 91^M Session: 30801921^M Range: npt=0.0-0^M
11/29/2007|16:10:57.385895|PersistenceConnection.cc|137|Repository operation successfully completed
11/29/2007|16:10:57.385971|QuativeSession.cc|694|Successfully sent message to STB
```
Session Messaging

This section includes the following topics on session messaging:

- Log File Search Tips
- Codes

Log File Search Tips

To search for general RTSP errors, use the following commands:

grep "RTSP/1.0 4" rtsp.log
grep "RTSP/1.0 5" rtsp.log

To search for content read errors, use the following command:

grep "Error Reading Content Data" rtsp.log

To search for stopped sessions, use the following command:

grep "stream_session: stopped" rtsp.log

To search for SETUP requests, use the following command:

grep "SETUP rtsp" rtsp.log

Use the CSeq header value in the rtsp.log file to match RTSP requests to responses.

Use the Session header value in the rtsp.log file to trace a single RTSP session from setup to teardown.
Codes

The ANNOUNCE method is a mechanism for RTSP servers to signal RTSP clients about start of stream or end of RTSP session events. An ANNOUNCE request must include a “CSeq” header and “Notice.” Following are the Notice codes:

- 1103 Playout Stalled (from VOD server only)
- 1104 Playout Resumed (from VOD server only)
- 1500 New Scale (from VOD server only)
- 2101 EOS (end of stream) (from VOD server only)
- 2104 BOS (beginning of stream); can happen in case of rewind or reverse play (from VOD server only)
- 2401 Ticket Expired; the playout has stopped (from the MS server only).
- 4400 Error Reading Content Data; the playout has stopped (from VOD server only); from the Streamer to the client referring to a hole in the content or a delay in getting the content
- 5200 Server Resources Unavailable; the playout has stopped (from MS server only)
- 5402 Client Session Terminated; teardown has been initiated by the server, the session is closed (from MS server only)
- 5403 Server Shutting Down; the playout has stopped. If from MS server, the session is closed. If from VOD server, the client must issue a teardown of the session (first configuration only).
- 5502 Internal Server error; the playout has stopped. The client must issue a teardown of the session.

After receiving and interpreting a request message, the recipient responds with an RTSP response message. The status code returned in the RTSP response message must be in the range 100 to 599 (per RFC 2326). If the server returns another value, the client must treat the error according to the range value:

- 1xx: Informational—Request received, continuing process.
- 2xx: Success —Action was successfully received, understood, and accepted.
- 3xx: Redirection—Further action must be taken in order to complete the request.
- 4xx: Client Error—Request contains bad syntax or cannot be fulfilled.
- 5xx: Server Error—Server failed to fulfill an apparently valid request.

Table A-1 describes the RTSP status codes.

<table>
<thead>
<tr>
<th>State</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>200</td>
<td>return &quot;OK&quot;</td>
</tr>
<tr>
<td>BAD_REQUEST</td>
<td>400</td>
<td>return &quot;Bad Request&quot;</td>
</tr>
<tr>
<td>FORBIDDEN</td>
<td>403</td>
<td>return &quot;Forbidden&quot;</td>
</tr>
<tr>
<td>NOTFOUND</td>
<td>404</td>
<td>return &quot;Not Found&quot;</td>
</tr>
<tr>
<td>METHOD_NOT_ALLOWED</td>
<td>405</td>
<td>return &quot;Method Not Allowed&quot;</td>
</tr>
<tr>
<td>NOT_ACCEPTABLE</td>
<td>406</td>
<td>return &quot;Not Acceptable&quot;</td>
</tr>
<tr>
<td>REQUEST_TIMEOUT</td>
<td>408</td>
<td>return &quot;Request Time-out&quot;</td>
</tr>
<tr>
<td>UNSUPPORTED_MEDIA_TYPE</td>
<td>415</td>
<td>return &quot;Unsupported Media Type&quot;</td>
</tr>
</tbody>
</table>
Database Issues

This section covers the following database issues and troubleshooting methods:

- Database Replication
- Corruption Recovery

Database Replication

This section covers the following database issues:

- CDSM GUI Does Not Report All the Ingested Content
- Errors in Log File
- Many Log Files

Table A-1  RTSP Status Codes (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVALID_PARAMETER</td>
<td>451</td>
<td>return &quot;Parameter Not Understood&quot;</td>
</tr>
<tr>
<td>NO_BANDWIDTH</td>
<td>453</td>
<td>return &quot;Not Enough Bandwidth&quot;</td>
</tr>
<tr>
<td>SESSION_NOT_FOUND</td>
<td>454</td>
<td>return &quot;Session Not Found&quot;</td>
</tr>
<tr>
<td>INVALID_METHOD</td>
<td>455</td>
<td>return &quot;Method Not Valid in This State&quot;</td>
</tr>
<tr>
<td>INVALID_HEADER</td>
<td>456</td>
<td>return &quot;Header Filed Not Valid for Resource&quot;</td>
</tr>
<tr>
<td>INVALID_RANGE</td>
<td>457</td>
<td>return &quot;Invalid Range&quot;</td>
</tr>
<tr>
<td>UNSUPPORTED_TRANSPORT</td>
<td>461</td>
<td>return &quot;Unsupported transport&quot;</td>
</tr>
<tr>
<td>DESTINATION_UNREACHABLE</td>
<td>462</td>
<td>return &quot;Destination unreachable&quot;</td>
</tr>
<tr>
<td>DESTINATION_REQUIRED</td>
<td>463</td>
<td>return &quot;Destination required&quot; (nCUBE extension)</td>
</tr>
<tr>
<td>INTERNAL_SERVER_ERROR</td>
<td>500</td>
<td>return &quot;Internal Server Error&quot;</td>
</tr>
<tr>
<td>NOT_IMPLEMENTED</td>
<td>501</td>
<td>return &quot;Not Implemented&quot;</td>
</tr>
<tr>
<td>SERVICE_UNAVAILABLE</td>
<td>503</td>
<td>return &quot;Service Unavailable&quot;</td>
</tr>
<tr>
<td>UNSUPPORTED_VERSION</td>
<td>505</td>
<td>return &quot;RTSP Version not supported&quot;</td>
</tr>
<tr>
<td>UNSUPPORTED_OPTION</td>
<td>551</td>
<td>return &quot;Option not supported&quot;</td>
</tr>
</tbody>
</table>

NGOD Extensions for Session Setup Failure (SSF)

| SSF_ASSET_NOT_FOUND           | 771  | return "Server Setup Failed - Asset Not Found"        |
| SSF_SOP_NOT_AVAILABLE         | 772  | return "Server Setup Failed - SOP Not Available"      |
| SSF_UNKNOWN_SOP_GROUP         | 773  | return "Server Setup Failed - Unknown SOP Group"       |
| SSF_UNKNOWN_SOP_NAMES         | 774  | return "Server Setup Failed - Unknown SOP Names"       |
| SSF_INSUFF_VOLUME_BW          | 775  | return "Server Setup Failed - Insufficient Volume Bandwidth" |
| SSF_INSUFF_NETWORK_BW         | 776  | return "Server Setup Failed - Insufficient Network Bandwidth" |
| SSF_INVALID_REQUEST           | 777  | return "Server Setup Failed - Invalid Request"         |
| SSF_INTERNAL_ERROR            | 778  | return "Server Setup Failed - Internal Error"          |
CDSM GUI Does Not Report All the Ingested Content

First, verify that the package has not already expired.

Second, check for index errors in the CDSM database logs, using the following command:

```bash
$ grep index /arroyo/log/avsdb.log.20071106
```

The example output indicates that the Vault and CDSM databases are not synchronized, possibly due to the server times not being synchronized, a network connectivity issue, a server failure, or some other similar issue.

For resolution, refer to the “Corruption Recovery” section on page A-37.

Errors in Log File

If the error “FSI_ENV:XX:YY was not found in the database” occurs repeatedly in the logs (see the following example), there could be two causes for this issue.


**Cause 1:** The databases are not synchronized.
If you are sure you entered an FSI configuration into the CDSM and the FSI is still giving this message, the configuration did not get replicated to the server where the FSI process is running.

**Cause 2:** The FSI configuration not existing in the database.
The FSI process can run without an existing database configuration by using its internal defaults.

Many Log Files

If one of the following conditions exist, it indicates that there were database replication errors:

- Many log files with a filename similar to log.00000XXXX in the /home/isa/Berkeley/DATADIR directory.
- Database could not be started. See the “Services Monitor” section on page 5-29 for more information.
- Bidirectional connections are lost between servers. See the “Required Services Not Starting or Running Correctly” section on page A-19.
- The following error message is listed in the /arroyo/log/avsdb-err.log.yyyyMMdd file, “tavsdb: unable to allocate memory for mutex; resize mutex region.”

```bash
# tail -f avsdb-err.log.20081111
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
```
Database Issues

- The /home/isa/Berkeley/DATADIR/REPLAY.db file increases to several GB in size.

```
$ ls -ltr
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002824
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002825
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002826
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002837
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002838
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002839
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002841
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002840
-rw-r--r-- 1 isa isa 5726769152 Nov 12 15:23 REPLAY.db
```

For resolution, refer to the “Corruption Recovery” section on page A-37.

### Corruption Recovery

⚠️ **Caution**

Escalate to tier-three support before making any intrusive database changes.

If the CDSM database is corrupted and the Vault database is not corrupted, do the following:

**Step 1**  
As user `root`, stop the CDSM database.

```
# /usr/bin/db_shutdown
```

**Step 2**  
Check to ensure the database is shut down.

```
# ps -ef | grep avsd
isa 2646 1 0 Jan09 ? 00:14:50 /arroyo/db/avsdb
root 26088 26059 0 13:23 pts/1 00:00:00 grep avsd
```

Make sure there is no avsd process returned. If the avsd hangs, use the process ID (2646 in the above example) with the `kill` command.

```
# kill -9 2646
```

**Step 3**  
Delete all files in the /arroyo/db/DATADIR directory.

**Step 4**  
As user `root`, stop the Vault database.

```
# /usr/bin/db_shutdown
```

**Step 5**  
Check to ensure the database is shut down.

```
# ps -ef | grep avsd
```

**Step 6**  
Copy all files in /arroyo/db/DATADIR directory from the Vault to the CDSM.

**Step 7**  
As user `root`, restart the Vault database.
Advanced Features and Applications

This section covers the Media Scheduler feature (live multicast ingest).

Live Multicast Ingest

Live multicast ingest is available as part of the Media Scheduler feature or the Real-Time Capture feature.

Ingest with Media Scheduler

Using Media Scheduler for live multicast ingest requires the following procedures:

1. Enable live ingest by setting both the Media Scheduler and the Ingest Manager to ON in the CDSM Setup. See the “Initializing the CDS and Activating the Optional Features” section on page 3-3 for more information.

2. Use the CDSM Input Channels page to configure the input channels. See the “Configuring Input Channels” section on page 4-21 for more information.

3. Upload channel schedules by importing the electronic program guide (EPG). See the “Uploading an EPG File” section on page 7-14 for more information.

Ingest without Media Scheduler

Using Real-Time Capture for live multicast ingest requires the following procedures:

1. Enable live ingest by configuring Ingest Manager ON and setting Real-Time Capture Type to Real-Time Capture (non-Media Scheduler) in the CDSM Setup page. Activate the Ingest Manager. Because the Ingest Manager is an optional feature, an activation key is required. See the “Initializing the CDS and Activating the Optional Features” section on page 3-3 for more information.

2. Use the CDSM CallSign Setup page to configure call signs with multicast IP addresses.

Ingest Troubleshooting

If the message “ERROR: Unable to login to the ftp location,” is present in the /home/isa/bss/log/aim.log file, check the FTP server configured in the Ingest Manager by using the ps -ef | grep ftp command. If the FTP service is not running, enter the service vsftpd start command to start it.
Frequently Asked Questions

Many of the frequently asked questions (FAQs) responses were based on an ISV system, but guidelines can be easily extrapolated for a Vault and Streamer. This section covers the following topics:

- Reliability and Availability
- Serviceability and Manageability
- Content
- Other

Reliability and Availability

Q. How do I enable stream resiliency?
A. Log in to the CDSM with engineering access. The CDSM Setup page is displayed. For Stream Failover Support, select “ON” and click Submit. For more information, see the “CDSM Setup” section on page C-2.

Q. How do I check and make sure the database is running properly?
A. After starting the database, you should see two sockets (listening and non-listening) connecting to the database on each of the remote servers on port 9999. You can check them by using the netstat -an | grep 9999 command.

For example, the following output of the netstat command shows that the server (172.22.97.194) has both the listening and non-listening sockets binding on port 9999 to echo the four remote servers (172.22.97.192, 172.22.97.193, 172.22.97.195 and 172.22.97.191).

```
# netstat -an | grep 9999
 tcp 0 0 172.22.97.194:9999 172.22.97.195:48652 ESTABLISHED
 tcp 0 0 172.22.97.194:9999 172.22.97.191:42732 ESTABLISHED
 tcp 0 0 172.22.97.194:54563 172.22.97.195:9999 ESTABLISHED
 tcp 0 0 172.22.97.194:39342 172.22.97.191:9999 ESTABLISHED
 tcp 0 0 172.22.97.192:9999 172.22.97.192:40207 ESTABLISHED
 tcp 0 0 172.22.97.195:41815 172.22.97.192:9999 ESTABLISHED
 tcp 0 0 172.22.97.193:9999 172.22.97.193:33196 ESTABLISHED
 tcp 0 0 172.22.97.194:43269 172.22.97.193:9999 ESTABLISHED
 tcp 0 0
```

If you cannot see both listening and non-listening sockets binding on port 9999 for each of the remote servers, the database is not running properly. Check that you have the correct replication group members in your /home/isa/.arroyorc file.

Serviceability and Manageability

Q. How do I check the calypso server status?
A. Log in to the server as root and enter the cat /proc/calypso/status/server_settings command.

Q. How do I check central processing unit (CPU)?
A. Log in to the server as root and enter the cat /proc/cpuinfo command.
**Frequently Asked Questions**

**Q.** How do I check the kernel network driver version?

**A.** Log in to the server as root and list the e1000.ko file to check the date and time it was created using the following command:

```bash
ls -l /lib/modules/<current running kernel name>/kernel/drivers/net/e1000/e1000.ko
```

The following example shows that the e1000.ko file is based on the kernel 2.5.18-53.el5.kernel.2_6_18.2009.01.08.01.

```bash
# ls -l /lib/modules/2.6.18-53.el5.kernel.2_6_18.2009.01.08.01/kernel/drivers/net/e1000/e1000.ko
-rw-r--r-- 1 root root 2617502 Jan 8 18:13 /lib/modules/2.6.18-53.el5.kernel.2_6_18.2009.01.08.01/kernel/drivers/net/e1000/e1000.ko
```

**Q.** How do I stop, start, and restart the Apache server on the CDSM?

**A.** Log in to the server as root and enter the following command:

```bash
# /arroyo/www/bin/apachectl stop
# /arroyo/www/bin/apachectl start
# /arroyo/www/bin/apachectl restart
```

**Q.** How do I check the Streamer static ARP table?

**A.** Log in to the server as root and enter the following command:

```bash
# cat /arroyo/test/ArpTable
ip 192.168.2.42 mac 000000000002
ip 192.168.2.43 mac 000000000002
```

**Q.** How do I view the ARP Table dump file?

```bash
# echo 1 > /proc/calypso/test/arp_dumpstate
```

**Q.** How do I recover the system from the kernel debugger (KDB) after a reboot?

**A.** If the server starts the KDB tool instead of rebooting, modify the /etc/grub.conf file as follows:

```bash
kdb=off panic=1
kernel /boot/vmlinuz-2.4.32avs ro root=/dev/hda1 console=tty0 console=ttyS0,115200
kdb=off panic=1
```

**Q.** What do I do if the KDB prompt is displayed when the server restarts after a failure?

**A.** Boot into single user-mode (see the “Kernel Crash” section on page A-12).

**Q.** How do I identify any holes in the content?

**A.** Log in to the server as root and enter the following commands:

```bash
# echo 2 > /proc/calypso/tunables/cm_logserverinfo
# cat /arroyo/log/serverinfo.log.01132009
```

Look at the last two lines of output. If there are no holes, the last two lines should be the following:

```
BeingDeleted=0 HasHoles=0 CopyHoles=0 SectorHoles=0
Object Status Check Complete.
```

**Q.** How do I clear cached video blocks (data cache) on the Streamer?

**A.** Log in to the server as root and enter the `echo 1 > /proc/calypso/test/clearcache` command.
Q. How do I clear the data cache in memory?
A. Log in to the server as *root* and enter the `echo 1 > /proc/calypso/test/clearmem` command.

**Note** Make sure there are no streams running before you use this command. If there are streams, the data cache in memory is not cleared.

Q. How do I destroy all streams?
A. Log in to the server as *root*, stop the services, change to the database table directory, remove the session table, and restart the services.

```
# arroyo stop
# cd /home/isa/bss/database/DATADIR
# rm RTSP_SESSION.db, RTSP_ANNEX.db
# arroyo start
```

All sessions are removed, and upon restarting the services, all streams that do not have an associated session are stopped.

Q. How do I delete an individual stream from the database?
A. Log in to the server as *root* and enter the following commands:

```
# su - isa
$ cd bss/database
$ ./AVSDBUtil
  5 -> RTSP SESSIONS
  2 -> GET ALL SESSIONS
  1 -> DELETE SESSIONS
Enter the Session Handle:
```

Q. How do I destroy all streams when none of the above methods work?
A. Log in to the server as *root* and enter the following commands:

```
[root@ssv3 root]# /usr/bin/db_shutdown
[root@ssv3 root]# ps -ef |grep avs
```

Wait for all avs processes to stop, then reboot the server.
```
[root@ssv3 root]# reboot
```

Q. How do I check the routing table and gateway?
A. Log in to the server as *root* and check the file `/arroyo/test/RoutingTable`.

```
# cat /arroyo/test/RoutingTable
default gateway 192.169.131.250
network 192.169.131.0 netmask 255.255.255.0 gateway 0.0.0.0
default cache gateway 192.169.131.250
local cache network 192.169.131.0 netmask 255.255.255.0
```
Content

Q. How do I get information on a content stream that seems corrupted; for example, there is macroblocking, the stream stops and restarts, and so on?
A. Log in to the server as root and enter the following commands:

```
# echo 2 > /proc/calypso/tunables/cm_logserverinfo
# cat /arroyo/log/serverinfo.log.01132009
```

Check the last set of output lines to see the current content states.

Object Count=37708 LengthUnknown=0
CouldNotRepair=0 IsDamaged=0 BeingRepaired=0 BeingCopied=0
needCrcValidate=37708 isFragFlag=0 isFragd=0 Defrag=0 Smooth=0
BeingFilled=0 OutOfService=0 NeedsISACheck=0
BeingDeleted=0 HasHoles=0 CopyHoles=0 SectorHoles=0
Object Status Check Complete.

Q. How do I know if a content object has “holes”?
A. Log in to the server as root and view the /var/log/debugmessages. There is a message in the debug messages file regarding the GOID and the content holes.

Q. What do I do if content ingest is not working?
A. Log in to the server as root, enter the less /home/isa/ContentStore/server/GenericLog.log command, and review the log for anomalies.

Q. How do I delete ingests that are “stuck” in the active ingest state?
A. Log in to the server as root and enter the following commands:

```
# su - isa
$ ./arroyo/db/AVSDBUtil
```

```
log4cxx: No appender could be found for logger (cdscommon.db).
log4cxx: Please initialize the log4cxx system properly.
************************************************
1: CONTENT
2: FSI LOG
3: FSI LPI
4: RTSP Config
5: RTSP SESSIONS
0: EXIT
```

Enter [1/2/3/4/5] or 0? :
************************************************

Choose the option 1 (CONTENT). In the next menu, choose option 1 (DELETE CONTENT). Enter the content ID of the “stuck” ingest, then choose the exit option for each menu until you are back at the Linux prompt.

Q. How do I manually ingest content from the command line?
A. Log in to the server as root and enter the following commands:

```
# su - isa
# cd ~/.SDClient
```

Update the SDClient.cfg file with the local IP address.

```
# ./sdClient
```
Follow the SDClient menus.

**Other**

**Q.** How do I view the CServer code configuration file?

**A.** Log in to the server as root and enter the `cat /arroyo/test/<server type>/setupfile` command. The server type is one of the following: vault, streamer, or ssv.

```
# cat /arroyo/test/<server type>/setupfile
# CServer core configuration. Changes to this file require
# a server reboot.

local 0 0 2 remote 0 0 2 fill 3 1 maxrate 900000 localip 0c0a80040
localip 0c0a80040
e1000 adapters: maxrate 965
e1000 0: streaming 1 fill 0
e1000 1: streaming 1 fill 0
e1000 3: streaming 0 fill 1

streamer 1 vault 1
serverid        64
groupid         64
maxpacketsize   1316
management      eth0
ingest          eth0
trickspeedsv2    10 0 0 0 0 0 0 0
ftpout if eth0 max utilization mbps 0 max sessions 0
fake cylindermap 1
test 4
```

**Q.** How do I know if a subsystem on a server is overloaded?

**A.** View the `.arroyo.log.protocoltiming.log.<date>` file. When you see the “COST REQUEST NO CAPACITY.” message, it means that the server is running out of capacity and it cannot accept new streaming requests.

Also, when you see a line in the `/arroyo/log/c2k.log.<date>` file that says the following:

```
01-May-2007 17:40:44 UTC :err:ServeStream::reserveStream: refused streamhandle 4 for
gold a445c9780e7f8f due to its load 3750, current load 0
```

This entry typically means there are no stream ports linked. In the ten-second snapshot of the `/arroyo/log/protocoltiming.log.<date>` file, there is a line that shows load values for each of the major subsystems (LAN, memory, CPU, and so on). More than likely one of the subsystems is at 100, which is the subsystem that is having the problem.

**Q.** How do I enable debugging?

**A.** Log in to the server as root and enter the following commands:

```
# su - isa
# cd ~/StreamsDriver
# touch DEBUGGING_ON
# ~/IntegrationTest/debugging_on_off
# ./stop_driver
# ./run_driver
```

**Q.** How do I update the remote servers from /arroyo/test/RemoteServers?
A. Log in to the server as root and enter the following commands:

```
# echo 1 > /proc/calypso/test/readremoteservers
```

CDS Content Quality Guidelines

This section covers the following topics:

- Supported Elementary Stream Types
- Scrambling
- Transport Bit Rate
- Stream Length
- Format Restrictions
- Preferred Formats

Supported Elementary Stream Types

Video-only, audio-only (as well as audio streams with only a few or occasional video frames) and data-only streams are supported in addition to the customary multiplex of both audio and video.

Scrambling

The transport layer cannot be scrambled, meaning the transport header and any adaptation field must be in the clear. Streams whose Elementary Streams (ESs) are fully scrambled, including all start codes, are capable of being ingested and streamed, but are incapable of trick play.

For trick-play capability, the following cannot be scrambled:

- Packetized Elementary Stream (PES) headers
- Program Association Table (PAT) and Program Map Table (PMT)
- Closed-caption data (if scrambled, the data is incorrectly included in tricks)

Transport Bit Rate

All transport streams are constant bit rate (CBR). Variable bit rate (VBR) is not supported. The maximum bit rate is 35 Mbps. There is no minimum bit rate. The ES video bit rate, as specified in the MPEG-2 sequence header, is ignored. The bit rates of individual ESs do not matter. The CBR for an individual ES (in particular the video) is not required. All that is required is that the aggregate transport stream be CBR.

Streams containing MPEG-2 or AVC video are expected to conform to the appropriate buffer models spelled out in ISO/IEC 13818-1and 14496-10.
Stream Length

All content must be at least one second in length. A content item must be under 12 hours in length or 81 GB in size, whichever comes first.

Format Restrictions

Following are the format restrictions for Advanced Video Coding (AVC), H.264, and MPEG-4:

- Sequence Parameter Set (SPS) seq_parameter_set_id flag must be zero.
- SPS pic_order_count_type flag must be zero.
- SPS seq_scaling_matrix_present_flag must be zero.
- SPS profile_idc flag must only be Baseline, Main, or High profile.

Preferred Formats

Using the following guidelines improves the performance of the system, the quality of the tricks, and the trick transitions.

1. All content should be encoded as a Single Program Transport Stream (SPTS). If multiple programs must be included (for example, a Picture-in-Picture (PIP) stream), ensure that the “real” program is encoded with the lowest program number.
2. All content should follow the process ID (PID) numbering specified in the Content Encoding Profiles 2.0 Specification (MD-SP-VOD-CEP2.0-I02-070105), section 6.7.5. Regardless, the audio and video PIDs should be above 0x20.
3. All content should be preceded with a Program Association Table (PAT) and then a Program Map Table (PMT), and then a Program Clock Reference (PCR) before the first audio or video frame. Optionally, the discontinuity bit can be set.
4. All content should use the same PID for both PCR and video.
5. All content should begin with a closed Group Of Pictures (GOP) for MPEG-2 or with an Instantaneous Decoder Refresh (IDR) frame for AVC. This first frame is always accompanied by a sequence header for MPEG-2 or by an SPS for AVC.
6. In order to guarantee relatively smooth looking trick modes, the minimum I/IDR-frame frequency should be eight per second. If the minimum trick speed is 4x or less, the I/IDR-frame frequency should be at least two per second. In no case should two I/IDR frames be more than two seconds apart.
7. Each I frame should be preceded by a sequence header and GOP header if any exist for an MPEG-2 video. Each I/IDR frame should be preceded by an SPS and Picture Parameter Set (PPS) for H.264 video.
8. Avoid mixing frame data from multiple video frames in the same transport packet. Specifically, no data belonging to the prior frame exists following the Packetized Elementary Stream (PES) packet header for the next frame. Breaking this rule may improve encoding efficiency slightly, but degrades the quality of the tricks on certain set-top boxes (STBs).
9. All content must be encoded as a single sequence, with no changes in horizontal or video resolutions, or changes in encoding parameters in the middle of the content.
10. The GOP size may be variable, but GOPs should generally not exceed two seconds in length. Using longer GOPs may improve encoding efficiency, but the quality of lower-speed tricks (3x, 4x) may suffer.
11. No more than four B-frames should be used between each pair of I-frames or P-frames.
12. There should be no continuity counter errors in the content.
13. There should be no discontinuities in the content, other than an optional one on the first PCR.
14. The accuracy requirements for PCRs, +/-five parts per million (5 ppm), as stated in ISO/IEC 13818-1 must be adhered to throughout the stream.
15. Audio and video are expected not to overflow the appropriate target buffer model specified.
16. A reasonable bit rate to use when encoding MPEG-2 standard definition (SD) video is 3.75 Mbps.
17. A reasonable bit rate to use when encoding MPEG-2 high definition (HD) video is 15 Mbps.
18. Appropriate bit rates for carriage of AVC are still being established, and while they are expected to be at least half the bit rates of MPEG-2, no specific recommendations can be offered.
19. There may be PIDs in the content that are not specified in the PMT. Such use is beyond the scope of this document.
20. All PATs and PMTs should be identical, with the same version number throughout.
21. The CDS support up to 30 Mbps MPEG-2 video encoding.
22. Content is filtered out if three occurrences of one-second synchronization lost is identified.
23. Content is filtered out if five seconds of null frames are identified.
SNMP MIB and Trap Information

This appendix describes the Simple Network Management Protocol (SNMP) traps sent by the CDS. The topics covered in this appendix include:

- **Overview, page B-1**
- **SNMP Management Objects and Traps, page B-2**
- **RFC Compliance, page B-7**

**Overview**

You can manage the servers by way of SNMP from a Network Management System (NMS). To implement SNMP management, the servers must be configured with a management IP address, SNMP community strings, and contact information. For more information about configuring the server for SNMP communication, see the “Configuring the SNMP Agent” section on page 4-49.

**Note**

We recommend configuring a VLAN for management traffic.

SNMP management features on the servers include:

- SNMP version 1 or version 2c
- Standard MIBs

**SNMP Agent**

The server’s SNMP agent uses certain variables that are included in a Cisco proprietary Management Information Base (MIB) file. By default, the SNMP agent is not started automatically. To start the SNMP agent, login to the server as `root` and enter the following command:

```
# nice -n 19 /usr/local/bin/snmpd
```

To have the SNMP agent start automatically after a reboot, use the Linux vi editor to add the following to the `/etc/rc.local` file:

```
nice -n 19 /usr/local/sbin/snmpd
```

To verify the SNMP agent has started, enter the `ps -ef | grep snmpd` command.
SNMP Management Objects and Traps

The CDS SNMP agent and Management Information Base (MIB) files are compliant with the Internet Engineering Task Force (IETF) standards for SNMP v1 and SNMP v2c. For a list of SNMP-associated Request For Comment (RFC) specifications, see the “RFC Compliance” section on page B-7.

The MIB files are located in the /usr/local/share/snmp/mibs/ directory.

The CDS MIBs describe the following groups of trapped events:

- Device
- Configuration
- Health
- Statistics

Some MIBs (for example, Device) do not have any associated traps.

Table B-1 describes the management objects defined in the Device MIB.

<table>
<thead>
<tr>
<th>Management Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arDeviceRole</td>
<td>The server type:</td>
</tr>
<tr>
<td></td>
<td>- Streamer</td>
</tr>
<tr>
<td></td>
<td>- Vault</td>
</tr>
<tr>
<td></td>
<td>- SSV (ISV)</td>
</tr>
<tr>
<td></td>
<td>- Controller (CDSM)</td>
</tr>
<tr>
<td>arDevicePartNo</td>
<td>The part number of the device.</td>
</tr>
<tr>
<td>arDeviceServerId</td>
<td>The server ID of this server.</td>
</tr>
<tr>
<td>arDeviceGroupId</td>
<td>All servers that are part of the same CDS (managed by one CDSM) have the same group ID. This group ID should be unique across an enterprise.</td>
</tr>
</tbody>
</table>

Table B-2 describes the management objects defined in the Configuration MIB for an ISA environment.

<table>
<thead>
<tr>
<th>Management Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arConfigISANamingServiceIp</td>
<td>The IP address of the CORBA Naming Service used by the OpenStream system.</td>
</tr>
<tr>
<td>arConfigISANamingServicePort</td>
<td>The port of the Naming Service used by the OpenStream system.</td>
</tr>
<tr>
<td>arConfigISANotifyServiceIp</td>
<td>The IP address of the CORBA Notification Service used by the OpenStream system.</td>
</tr>
<tr>
<td>arConfigISANotifyServicePort</td>
<td>The port of the Notification Service used by the OpenStream system.</td>
</tr>
</tbody>
</table>
### Table B-2 Configuration MIB (continued)

<table>
<thead>
<tr>
<th>Management Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arConfigISANotifyEventChannelFactory</td>
<td>The name used to locate the Notify Service through corbaloc protocol (DefaultEventChannelFactory in OpenStream).</td>
</tr>
<tr>
<td>arConfigISAContentServiceMasterIp</td>
<td>The IP address for the master Content Service.</td>
</tr>
<tr>
<td>arConfigISAContentServiceMasterPort</td>
<td>The port number for the master Content Service.</td>
</tr>
<tr>
<td>arConfigISAStreamServiceMasterIp</td>
<td>The IP address for the master Streamer Service.</td>
</tr>
<tr>
<td>arConfigISAStreamServiceMasterPort</td>
<td>The port number for the master Streamer Service.</td>
</tr>
<tr>
<td>arConfigISAWebServicePort</td>
<td>The port number for the ISA web services.</td>
</tr>
<tr>
<td>arConfigISAConfigFile</td>
<td>The filename of the ISA configuration file.</td>
</tr>
<tr>
<td>arConfigISAEventChannels_Id</td>
<td>A simple name that identifies the root directory of the Event Channel where all event channels need to register.</td>
</tr>
<tr>
<td>arConfigISAEventChannelsKind</td>
<td>The directory extension of the Event Channel ID.</td>
</tr>
<tr>
<td>arConfigISAContentChannels_Id</td>
<td>A simple name that identifies the Content Event Channel where all events concerning content objects are published.</td>
</tr>
<tr>
<td>arConfigISAContentChannelsKind</td>
<td>The Event Channel Content ID extension.</td>
</tr>
<tr>
<td>arConfigISAStreamChannels_Id</td>
<td>A simple name that identifies the Stream Event Channel where all events concerning stream objects are published.</td>
</tr>
<tr>
<td>arConfigISAStreamChannelsKind</td>
<td>The Event Channel Stream ID extension.</td>
</tr>
<tr>
<td>arConfigISAFactories_Id</td>
<td>A simple name that identifies the root directory of the Factories where all factories need to register.</td>
</tr>
<tr>
<td>arConfigISAFactoriesKind</td>
<td>The Factories ID extension.</td>
</tr>
<tr>
<td>arConfigISAEventChannelFactory</td>
<td>A simple name that identifies the Event Channel Factory, which is used to create event channels, and resolves the Notification Service name.</td>
</tr>
<tr>
<td>arConfigISALoadQueryInterval</td>
<td>The time interval, in seconds, in which ISA gets the current load heuristics of all servers in the Vault/Streamer arrays in order to make a provisioning decision.</td>
</tr>
<tr>
<td>arConfigISAContentStoreFactoryId</td>
<td>The name of the CDS Content Store Factory that is registered with the OpenStream system. The Content Store Factory allows the creation of Content Store objects, and the Content Store objects act as factories for content objects.</td>
</tr>
<tr>
<td>arConfigISAContentStoreKind</td>
<td>The Content Store Factory ID extension.</td>
</tr>
<tr>
<td>arConfigISAContentStoreNumThreads</td>
<td>The number of threads allocated to the ISA Content Store service.</td>
</tr>
<tr>
<td>arConfigISAFTPServerPort</td>
<td>The port used when the Vault receives a request from the OpenStream system to act as an FTP server and receives an FTP put command from the content provider acting as an FTP client.</td>
</tr>
<tr>
<td>Management Object</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>arConfigISAFTPClientPort</td>
<td>The port used when the Vault receives a request from the OpenStream system to act as an FTP client and sends an FTP get command to the content provider acting as an FTP server.</td>
</tr>
<tr>
<td>arConfigISAFTPClientNumAttempts</td>
<td>The number of times the FTP client attempts to connect to the FTP server before considering the transaction failed.</td>
</tr>
<tr>
<td>arConfigISAFTPPollTimeout</td>
<td>The polling timeout for FTP.</td>
</tr>
<tr>
<td>arConfigISASTreamSourceIPConfig</td>
<td>The Stream Source IP address. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Control IP</td>
</tr>
<tr>
<td></td>
<td>• Default Stream Source IP</td>
</tr>
<tr>
<td></td>
<td>• Stream Interface IP</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td>arConfigISASTreamServiceId</td>
<td>The name of the Stream Service.</td>
</tr>
<tr>
<td>arConfigISASTreamServiceKind</td>
<td>The Service ID extension.</td>
</tr>
<tr>
<td>arConfigISASTreamNumThreads</td>
<td>The number of threads created by the Stream Service.</td>
</tr>
<tr>
<td>arConfigISATME</td>
<td>Whether Trick-Mode Event (TME) enhancements are enabled.</td>
</tr>
<tr>
<td>arConfigISASTreamingSourcePort</td>
<td>The streaming source port number.</td>
</tr>
<tr>
<td>arConfigISALSCPServerPort</td>
<td>The port on the Streamer that is listening for LSCP commands from the set-top box.</td>
</tr>
<tr>
<td>arConfigISASTreamingMode</td>
<td>The stream mode.</td>
</tr>
<tr>
<td></td>
<td>Mode 1 is used by the Scientific Atlanta QAMs.</td>
</tr>
<tr>
<td></td>
<td>Mode 2 is used by the Scientific Atlanta GQAM, the Harmonic NSG, and the Motorola SEM.</td>
</tr>
<tr>
<td>arConfigISASTreamHeadendId</td>
<td>The headend ID for the Stream Service.</td>
</tr>
<tr>
<td>arConfigISAPlayNumThreads</td>
<td>The Lightweight Stream Control (LSC) number of threads.</td>
</tr>
<tr>
<td>arConfigISALSCPResponsePadding</td>
<td>The response padding used in LSCP transactions.</td>
</tr>
<tr>
<td>arConfigISAResourceManagerName</td>
<td>The name of the CDS Resource Service Manager that monitors orphan sessions.</td>
</tr>
<tr>
<td>arConfigISASessionsPollTime</td>
<td>The time interval between polling for orphan sessions.</td>
</tr>
<tr>
<td>arConfigISASTreamTimeout</td>
<td>The maximum time allowed before a stream object is played. If the stream object is not played within the timeout period, it is destroyed.</td>
</tr>
<tr>
<td>arConfigISAPreEncryptionEnabled</td>
<td>Indicates whether support for Motorola pre-encryption is enabled or disabled.</td>
</tr>
<tr>
<td>arConfigISACoContentStoreName</td>
<td>The Content Store name.</td>
</tr>
<tr>
<td>arConfigISAMSAEnabled</td>
<td>Indicates whether Managed Services Architecture (MSA) is enabled or disabled. MSA routes successful events to the ISA event channels and error events to either the Event Posting Agent (EPA) or Event Log Agent (ELA).</td>
</tr>
</tbody>
</table>
Table B-2  Configuration MIB\(^1\) (continued)

<table>
<thead>
<tr>
<th>Management Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arConfigISAFTPServerOutPort</td>
<td>The port number used by ISA 1.5 FTP out feature.</td>
</tr>
<tr>
<td>arConfigISAMSALSCPClientProto</td>
<td>The way LSCP clients communicate with the Streamers. The options are:</td>
</tr>
<tr>
<td></td>
<td>• TVGuide—For Scientific Atlanta clients—TV Guide</td>
</tr>
<tr>
<td></td>
<td>• RTI—For Tandberg clients</td>
</tr>
<tr>
<td></td>
<td>• VODLink—For SeaChange clients</td>
</tr>
<tr>
<td></td>
<td>• CV—For SeaChange clients with Cablevision</td>
</tr>
<tr>
<td></td>
<td>• Cisco (RTSP)</td>
</tr>
<tr>
<td></td>
<td>• TTV (RTSP)</td>
</tr>
</tbody>
</table>

1. All management objects in the Configuration MIB are for an ISA environment. If an ISA-specific management object is requested in an RTSP environment, an invalid response is generated (either blank or a standard error message that the element was not found).

Table B-3 describes the readable (with SNMP, GET or GETNEXT) defined in the Health MIB and Table B-4 describes the health traps in the Health MIB.

Table B-3  Health MIB

<table>
<thead>
<tr>
<th>Management Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arDiskHealthMonitorIndex</td>
<td>The unique value that identifies the disk being monitored.</td>
</tr>
<tr>
<td>arDiskHealthDiskName</td>
<td>The name assigned to the disk device. This object is the driver assigned</td>
</tr>
<tr>
<td></td>
<td>name for the disk specified.</td>
</tr>
<tr>
<td>arDiskHealthState</td>
<td>The state of the disk health are:</td>
</tr>
<tr>
<td></td>
<td>• 0 means okay. The disk is healthy and ready.</td>
</tr>
<tr>
<td></td>
<td>• 1 means not okay. The disk is not ready. It may be abandoned, removed,</td>
</tr>
<tr>
<td></td>
<td>or in a transient state.</td>
</tr>
<tr>
<td>arDiskHealthTotalErrors</td>
<td>The total number of errors reported by the disk to the disk driver.</td>
</tr>
<tr>
<td>arDiskHealthErrorsReported</td>
<td>The number of errors reported to CServer. These are the errors that cannot</td>
</tr>
<tr>
<td></td>
<td>be resolved by the disk driver in a timely manner.</td>
</tr>
<tr>
<td>arDiskHealthTotalResets</td>
<td>The total number of resets (soft and hard) for this disk. A soft reset</td>
</tr>
<tr>
<td></td>
<td>affects a single device only and is the first recourse in resolving an</td>
</tr>
<tr>
<td></td>
<td>unresponsive device.</td>
</tr>
<tr>
<td>arDiskHealthHardResets</td>
<td>The number of hard resets for the disk. A hard reset may affect all</td>
</tr>
<tr>
<td></td>
<td>devices connected to the same bus or controller.</td>
</tr>
<tr>
<td>arDiskHealthTotalRequests</td>
<td>The total number of read and write requests submitted to this disk.</td>
</tr>
<tr>
<td>arDiskHealthRequestsRetried</td>
<td>The number of times requests were retried by the driver.</td>
</tr>
<tr>
<td>arDiskHealthBytesRead</td>
<td>The number of bytes read from this disk.</td>
</tr>
<tr>
<td>arDiskHealthBytesWritten</td>
<td>The number of bytes written to this disk.</td>
</tr>
</tbody>
</table>
Table B-4  Health MIB Traps

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arDiskHealthUp</td>
<td>Signifies that the previously inactive disk is now active and ready, that</td>
</tr>
<tr>
<td></td>
<td>is, the disk has returned to the ok (0) state.</td>
</tr>
<tr>
<td>arDiskHealthDown</td>
<td>Signifies that the active disk is now inactive, that is, it has left the</td>
</tr>
<tr>
<td></td>
<td>ok (0) state.</td>
</tr>
<tr>
<td>arMSAEvent</td>
<td>Signifies that an MSA event (error) has occurred.</td>
</tr>
<tr>
<td>arMSAEventmSessionId</td>
<td>The session ID sent to the MSA.</td>
</tr>
<tr>
<td>arMSAEventmServerId</td>
<td>The server ID of the Streamer associated with the session ID.</td>
</tr>
<tr>
<td>arMSAEventmGroupId</td>
<td>The array ID the Streamer is a member of.</td>
</tr>
<tr>
<td>arMSAEventmServiceGroup</td>
<td>The service group ID associated with the session ID.</td>
</tr>
<tr>
<td>arMSAEventmQAMIp</td>
<td>The QAM IP address associated with the session ID.</td>
</tr>
<tr>
<td>arMSAEventmEventTime</td>
<td>The timestamp associated with this session ID.</td>
</tr>
<tr>
<td>arMSAEventmErrorCode</td>
<td>The error code associated with this session ID.</td>
</tr>
<tr>
<td>arMSAEventmErrorCodeInt</td>
<td>The error code integer associated with the session ID. For a description</td>
</tr>
<tr>
<td></td>
<td>of the error code, see the “Stream Failures” section on page 5-18.</td>
</tr>
</tbody>
</table>

Table B-5 describes the management objects defined in the Statistics MIB.

Table B-5  Statistics MIB

<table>
<thead>
<tr>
<th>Management Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arCacheStatsFillReceiveStreamCount</td>
<td>The number of streams received through cache-fill.</td>
</tr>
<tr>
<td>arCacheStatsFillStreamActualBWinKbits</td>
<td>The bandwidth used (in kilobits per second [kbps]) for cache-fill streams.</td>
</tr>
<tr>
<td>arCacheStatsFillStreamCommittedBWinKbits</td>
<td>The bandwidth reserved (in kbps) for cache-fill streams.</td>
</tr>
<tr>
<td>arCacheStatsDiskReadStreamCount</td>
<td>The number of streams that retrieved content from local disk storage.</td>
</tr>
<tr>
<td>arCacheStatsDiskReadBWinKbits</td>
<td>The bandwidth used (in kbps) in retrieving streams from local disk storage.</td>
</tr>
<tr>
<td>arStreamStatsActiveStreamCount</td>
<td>The number of active streams.</td>
</tr>
<tr>
<td>arStreamStatsActiveStreamBWinKbits</td>
<td>The bandwidth used (in kbps) for active streams.</td>
</tr>
<tr>
<td>arStreamStatsUniqueStreamCount</td>
<td>The number of unique streams.</td>
</tr>
<tr>
<td>arStreamStatsUniqueStreamBWinKbits</td>
<td>The bandwidth used (in kbps) for unique streams.</td>
</tr>
</tbody>
</table>
RFC Compliance

Table B-6 is a list of SNMP RFC standards.

<table>
<thead>
<tr>
<th>RFC Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1155 (STD0016)</td>
<td>Structure and Identification of Management Information for TCP/IP-based Internets</td>
</tr>
<tr>
<td>RFC 1157 (STD0015)</td>
<td>Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 1212 (STD0016)</td>
<td>Concise MIB Definitions</td>
</tr>
<tr>
<td>RFC 1213 (STD0017)</td>
<td>Management Information Base for Network Management of TCP/IP-based Internets: MIB-II</td>
</tr>
<tr>
<td>RFC 2790 (Draft Standard)</td>
<td>Host Resources MIB</td>
</tr>
<tr>
<td>RFC 1901 (Historic)</td>
<td>Introduction to Community-based SNMPv2</td>
</tr>
<tr>
<td>RFC 1903 (Draft Standard)</td>
<td>Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)</td>
</tr>
<tr>
<td>RFC 1910 (Historic)</td>
<td>User-based Security Model for SNMPv2</td>
</tr>
<tr>
<td>RFC 2011 (Proposed Standard - Updates RFC 1213)</td>
<td>SNMPv2 Management Information Base for the Internet Protocol using SMIV2</td>
</tr>
<tr>
<td>RFC 2012 (Proposed Standard)</td>
<td>SNMPv2 Management Information Base for the Transmission Control Protocol using SMIV2</td>
</tr>
<tr>
<td>RFC 2013 (Proposed Standard)</td>
<td>SNMPv2 Management Information Base for the User Datagram Protocol using SMIV2</td>
</tr>
<tr>
<td>RFC 2096 (Proposed Standard)</td>
<td>IP Forwarding Table MIB</td>
</tr>
<tr>
<td>RFC 2863 (Draft Standard)</td>
<td>The Interfaces Group MIB</td>
</tr>
<tr>
<td>RFC 3410 (Informational)</td>
<td>Introduction and Applicability Statements for Internet-Standard Management Framework</td>
</tr>
<tr>
<td>RFC 3412 (STD0062)</td>
<td>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</td>
</tr>
</tbody>
</table>
### Table B-6 SNMP RFC Standards (continued)

<table>
<thead>
<tr>
<th>RFC Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3413 (STD0062)</td>
<td>Simple Network Management Protocol (SNMP) Applications</td>
</tr>
<tr>
<td>RFC 3414 (STD0062)</td>
<td>User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)</td>
</tr>
<tr>
<td>RFC 3415 (STD0062)</td>
<td>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 3417 (STD0062)</td>
<td>Transport Mappings for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 3418 (STD0062)</td>
<td>Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 2570 (Informational)</td>
<td>Introduction to Version 3 of the Internet-standard Network Management Framework</td>
</tr>
<tr>
<td>RFC 2571 (Draft Standard)</td>
<td>An Architecture for Describing SNMP Management Frameworks</td>
</tr>
<tr>
<td>RFC 2572 (Draft Standard)</td>
<td>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 2573 (Draft Standard)</td>
<td>SNMP Applications</td>
</tr>
<tr>
<td>RFC 2575 (Draft Standard)</td>
<td>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 2578 (STD0058)</td>
<td>Structure of Management Information Version 2 (SMIv2)</td>
</tr>
<tr>
<td>RFC 2579 (STD0058)</td>
<td>Textual Conventions for SMIv2</td>
</tr>
<tr>
<td>RFC 2580 (STD0058)</td>
<td>Conformance Statements for SMIv2</td>
</tr>
</tbody>
</table>
Engineering Access Level Pages

This appendix describes the CDSM pages available through the Engineering access level. The Engineering access level provides the following pages:

- CDSM Diagnostics, page C-1
- CDSM Setup, page C-2
- System Configs, page C-5

The Engineering access level is primarily used for initializing the CDS at the time of installation and for CDS diagnostics. Once your CDS has been configured, you should not require an engineering access level user for day to day operations.

When you log in to the CDSM with a user account that has Engineering access level, the first page that is displayed is the CDSM Setup page. All the other CDSM pages that are available with the Master access level are still available with the Engineering access level.

In an RTSP environment, the Configure > Server Level > RTSP Setup page displays four additional fields:

- Database Connect Size
- UDP Packet Size
- Threadpool Size
- Max Sessions

These fields are only for diagnostic purposes, and their values should not be changed.

CDSM Diagnostics

To access the CDSM Diagnostics page, choose Maintain > Software > CDSM Diagnostics. The first section of this page provides configuration information that is useful in diagnosing an issue. The following remaining sections of the CDSM Diagnostic page are:

- CIDR Calculator
- Stream Trickmode Debugger
- Unix Timestamp Tool
- Server Diagrams
CIDR Calculator

By entering an IP address and network mask, and clicking Submit, the Classless Inter-Domain Routing (CIDR) Calculator provides the following TCP/IP network information:

- Network address
- Broadcast address
- Number of hosts
- Range of IP addresses for the hosts

Stream Trick-Mode Debugger

To view the trick-mode data for a Session ID enter the Session ID and click Submit. The CDSM Diagnostic page refreshes and a View Data button is displayed next to the Submit button. Click View Data to see the raw trick-mode data. A new window displays the data. Right-click in that window and choose View Source in the pop-up menu. A formatted version of the raw data is displayed.

Unix Timestamp Tool

Clicking on a day in the calendar displays the Unix start time and end time. The time is represented in seconds since the start of Unix epoch time, which is 1970-01-01T00:00:00.

Server Diagrams

Choose a server from the Server Diagrams drop-down list and a graphic of the server is displayed.

CDSM Setup

The CDSM Setup page is used to initially configure the CDS. After you have set the CDSM Setup fields for your CDS, click Submit. Configuration and start up messages are displayed in the left panel.

Deployed CServer Version

For Release 2.0, this field is always set to 2.0.x.

Stream Failover Support

Stream failover support is available for both the ISA and RTSP environments in Release 2.0. If a Streamer fails, another Streamer in the same Stream Group takes over any active stream sessions without loss of state and backoffice independence.
Stream Steering Mode

Stream steering determines which Streamers serve streams to a QAM device. There are two types of stream steering:

- Single site
- Multi-site

Single-site steering uses only one Stream Group to serve streams to a QAM device. Multi-site steering can use more than one Stream Group to serve streams to a QAM device.

Note: Multi-site steering is only available with ASI streaming in an ISA environment.

Deployment Network Config

Specify whether your CDS network topology is a Layer 2 or Layer 3 network.

Installation Type

The only options for Release 2.0 are “ISA 2.0” and “RTSP 2.0.”

Media Scheduler

The Media Scheduler is an optional feature and requires a software activation key to enable it. For more information about activating the Media Scheduler, see the “Initializing the CDS and Activating the Optional Features” section on page 3-3. The Media Scheduler allows live ingests from multicast IP addresses and uses the Input Channels page to map multicast IP addresses to channels. You can enable either Media Scheduler or Real-Time Capture Type, but not both.

Real-Time Capture Type

Real-Time Capture allows live ingests from multicast IP addresses and uses the CallSign Setup page to map the multicast IP addresses to call signs. You can enable either Media Scheduler or Real-Time Capture Type, but not both.

Playout Scheduler

The Playout Scheduler is not supported in Release 2.0.

Bandwidth Manager

The Bandwidth Manager is an optional feature and is only for RTSP environments. The Bandwidth Manager keeps track of allocated streams and VOD network resources.
### Ingest Manager

The Ingest Manager is an optional feature and requires an software activation key to enable it. For more information about activating the Ingest Manager, see “Initializing the CDS and Activating the Optional Features” section on page 3-3. The Ingest Manager takes care of provisioned content objects by collecting the metadata, sending messages to the appropriate subsystem to ingest the content, and sending messages to expire the content when the expiration period has passed.

### RTSP Deployment Type

The RTSP Deployment type is only applicable to RTSP environments. The options are the following:

- DSM-CC
- RTSP
- NGOD
- IPTV
- Telenet
- Quative
- EventIS (on vpath and off vpath)

The deployment configuration differs depending on the type of headend.

### Authentication Manager

The Authentication Manager is an optional feature and is only for specific RTSP environments (EventIS or Telenet). The Authentication Manager communicates with the backoffice to validate a request received from a set-top box before setting up a session.

### Service Group Steering

Service Group Steering is an optional feature and is only for RTSP environments. When the Service Group Steering option is turned on, the **Configure > System Level > Headend Setup** page is available to steer Stream Groups to specific service groups.

### CDSM NAV Setup

The CDSM NAV Setup changes what displays in the CDSM GUI.

### CDSM Health Monitoring

The CDSM Health Monitoring is not supported in Release 2.0.
System Configs

The System Configs page contains critical CDS parameters that are set at the time of the initial installation of the CDS. Generally, the default settings are appropriate for all environments.

Caution
If these parameters are changed once the CDS is in service, your CDS may not function properly.

Group Map 0

Specifies whether the Group Map 0 parameter is for an ISA or RTSP environment.

Servers Group Map

Specifies whether the Servers Map 0 parameter is for an ISA or RTSP environment.

License Map

This is the CDS license, and is set at the time of installation.

Control IP Map

The Control IP Map is always set to one.

Add New Server

Should you experience problems adding a new server into the CDS, and you have tried the solutions covered in the “CDSM GUI Does Not Register the Vaults and Streamers” section on page A-20, you can use the Add New Server section.
Software Licensing Information

This appendix provides software license information related to the TV CDS.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, that is, both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the license texts. Both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL, please contact openssl-core@openssl.org.

OpenSSL License:
Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”. 


4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)/”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Product Warranties

The following sections detail Cisco Systems, Inc. warranty policies.

Standard Warranty

Cisco Systems, Inc. (“Cisco Systems, Inc.”) warrants that all hardware shall be free from defects in material and workmanship for a period of thirty (30) days under normal operating conditions from the product shipment date. Cisco Systems, Inc., at its sole option, will either repair or replace the nonconforming hardware. Hardware replaced under the terms of this warranty may be refurbished or new equipment substituted at the option of Cisco Systems, Inc. Any replacement or repaired equipment provided to you will not extend the period of the original warranty. You acknowledge and agree that the provisions of this warranty constitute the sole and exclusive remedy available to it with regard to defective hardware. This limited warranty shall not apply to defects resulting from neglect, misuse, electrical or electro-magnetic stress, accident, fire and other hazard, unauthorized alteration, modification or repair, including without limitation, installation of unauthorized parts, improper testing, handling, storage, operation, interconnection with installation or any other cause beyond the range of normal use of the hardware.

Returns

Any hardware can be returned only with the prior approval of Cisco Systems, Inc. Any such return shall reference a return material authorization (RMA) number issued by authorized Cisco Systems, Inc. service personnel. Transportation costs, if any, incurred in connection with the return of defective hardware to Cisco Systems, Inc. shall be borne by you. Cisco Systems, Inc. shall pay any transportation costs incurred with the redelivery of a repaired or replaced item. If Cisco Systems, Inc. determines that the allegedly defective hardware is not covered by the terms of this warranty or that a warranty claim is made after the warranty period, the cost of repair by Cisco Systems, Inc., including all shipping expenses, shall be paid by you.
Infringement

Cisco Systems, Inc. retains the exclusive right to defend and pay damages finally awarded and/or settle any claim(s) by a third party against you based upon on a Cisco Systems, Inc. product (excluding any Third Party content therein) infringing a patent, trademark, or copyright or misappropriation of any trade secret. The foregoing obligations are conditioned on your providing Cisco Systems, Inc. with prompt written notice of claim(s) or any threat of such a claim(s), and giving Cisco Systems, Inc. full assistance in connection with such defense and/or settlement and on your not being in breach of your obligations hereunder. If the Cisco Systems, Inc.’s product becomes or is likely to become the subject of such a claim, Cisco Systems, Inc. at its sole option may settle any such claim(s), procure for you the right to continue using the product or replace or modify the Product to avoid infringement asserted. Cisco Systems, Inc. will have no obligation or liability relating to or arising from (a) any use of any product (i) not in accordance with this agreement or for purposes not intended by Cisco Systems, Inc. (ii) in combination with other products, equipment, software or data not supplied by Cisco Systems, Inc. or (b) any modification of the product by any person other than Cisco Systems, Inc. or its authorized subcontractor. This infringement section states Cisco Systems, Inc.’s entire liability and your sole and exclusive remedy for infringement claims and actions.

No Other Warranties

THE SOFTWARE IS PROVIDED “AS IS” WITH ALL FAULTS. EXCEPT FOR THE EXPRESS WARRANTIES REGARDING THE HARDWARE SET FORTH ABOVE, UNLESS UNENFORCEABLE OR UNLAWFUL UNDER APPLICABLE LAW, CISCO SYSTEMS, INC. DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE; AND THE LIABILITY OF CISCO SYSTEMS, INC., IF ANY, FOR DAMAGES RELATING TO OR RESULTING FROM ANY PRODUCT (INCLUDING ANY HARDWARE AND/OR SOFTWARE THEREIN) OR ITS USE, WHETHER ALLEGEDLY DEFECTIVE OR OTHERWISE (INCLUDING WITHOUT LIMITATION A CLAIM FOR LOSS OF USE OR LOSS OF DATA OR LOSS OF PROFITS) SHALL UNDER ANY TORT, CONTRACT, OR OTHER LEGAL THEORY BE LIMITED TO THE ACTUAL PRICE PAID FOR SUCH HARDWARE AND/OR SOFTWARE AND SHALL IN NO EVENT INCLUDE INCIDENTAL, CONSEQUENTIAL, SPECIAL OR INDIRECT DAMAGES OF ANY KIND, EVEN IF CISCO SYSTEMS, INC. IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. CISCO SYSTEMS, INC. SHALL NOT BE LIABLE UNDER THIS WARRANTY IF YOU OR ANY THIRD PARTY ALTERS, MISUSES, NEGLECTS, OR ABNORMALLY STRESSES THE HARDWARE AND SOFTWARE.

Cisco Software License

Subject your compliance with the terms of this license and payment of all amounts owed for your use of the software, Cisco grants to you a non-exclusive license to the Content Delivery Applications (the “Software”), solely for your internal business purposes and solely in accordance with the Documentation. You may use the Software on the provided installed system (the “Hardware”) or may transfer the Software to a single hard disk, provided you remove the Software from the original Hardware. You may create one copy of the Software for archival purposes. Any use of the Software other than in accordance with this license will result in immediate termination of the license.

In connection with your use of the Software you acknowledge that the Software constitutes valuable trade secrets of Cisco. Accordingly, you agree not to (a) modify, adapt, or otherwise create derivative works from the Software; (b) sublicense, loan, or otherwise transfer the Software except in connection
with a transfer of the Hardware to which the software relates provided that Licensee does not retain any copies of the Software to any third party; or (c) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code for the Software.

All rights in and to the Software not expressly granted to you in this license are reserved by Cisco. You may not assign or transfer any of its rights under this license to any third party without Cisco’s prior written consent except in connection with a transfer of the Hardware to which the Software relates. This license will be governed by the laws of the State of California.

**GNU General Public License**

Certain items of software included with the Licensed Software are subject to the GNU General Public License (“GPL”), the Lesser GNU General Public License (“LGPL”), or other “open source” or “free software” licenses (Open Source Software”). Some of the Open Source Software is owned by third parties. The Open Source Software is not subject to any warranties by Cisco Systems, Inc. Instead, each item of Open Source Software is licensed under the terms of the end-user license that accompanies such Open Source Software. In particular, nothing in this document restricts any right to copy, modify, and distribute that Open Source Software subject to the terms of the GPL and LGPL. As required by the terms of the GPL and LGPL, Cisco Systems makes the Open Source Software provided available under the GPL and LGPL, and Cisco Systems, Inc.’s modification to that Open Source Software are available by written request at the notice address below.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706