CONTENTS

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

CHAPTER 1

Product Overview 1-1
  Overview 1-1
    TV CDS Software 1-3
      Caching Nodes 1-4
      Streamer Load Balancing 1-4
      CServer Functionality 1-4
      Streamer Content Delivery Applications 1-4
  Content Delivery System Architecture 1-5
    Vault 1-6
    Streamer 1-7
    Caching Node 1-7
    Integrated Streamer-Vault 1-7
    Content Delivery System Manager and Virtual Video Infrastructure Manager 1-7
  Resiliency and Redundancy 1-9
    Vault Disk Redundancy 1-9
    Vault Server Resiliency 1-10
    Vault Group Redundancy 1-10
    Streamer Disk Redundancy 1-10
    Streamer Server Resiliency 1-11
    Caching Node Disk Redundancy 1-11
    Caching Node Resiliency 1-11
    CDSM Redundancy 1-11
    Ethernet Link Resiliency 1-11
  Scalability 1-12
# Network Design

## Overview
- CDS with Vaults and Streamers 2-1
- CDS with ISVs 2-2
- CDS with Caching Nodes 2-2

### TV CDS Topologies and VVI Topologies
- Centralized Topology 2-3
- Decentralized Topology 2-4
- Hybrid Topology 2-5

### TV VVI Management
- Centralized Management 2-7
- Split-Domain Management 2-7

### CDS Workflow
- Streamer Workflow 2-8
- Setup Server 2-8
- Control Server 2-9
- Play Server 2-9
- Caching Node Workflow 2-9
- Vault Workflow 2-10

### BMS Considerations for RTSP Environments
- nABLE Integration 2-11

### Network Connections
- Ingest Interface 2-14
- Management Interface 2-15
- Cache Interfaces 2-15
- Cache/Stream Interfaces 2-15
- Streaming Interface 2-15

# Getting Started

## Initially Configuring the Devices
- Logging In to the TV CDSM 3-1
- Logging Out 3-3

### Initializing the CDS and Activating the Optional Features
- Navigating the CDSM 3-4
- Using Online Help 3-4

### Configuration Workflows
- CDS Workflow 3-5
- VVI Workflow 3-6
Contents

Central Management Workflow 3-6
Split-Domain Management Workflow 3-7
TV MediaX Configuration Workflow 3-8

CHAPTER 4
Configuring the CDS 4-1
System Level Configuration 4-1
  Configuring DNS Services 4-2
  Configuring NTP Services 4-3
  Configuring the Hosts Service 4-3
  Configuring the Array Name 4-4
  Configuring QAM Gateways 4-4
    ARP 4-5
  Configuring the Headend Setup 4-7
  Configuring Stream Destinations 4-8
  Configuring the Bandwidth Manager 4-10
  Configuring the Ingest Manager 4-11
  Configuring the Authentication Manager 4-15
  Configuring Ingest Tuning 4-17
  Configuring IP Nicknames 4-19
  Configuring the Media Importer 4-20
  Configuring Call Signs 4-21
  Configuring Input Channels 4-23
  Configuring Source Output Ports 4-25
    Configuring Multiple SOPs 4-26
Array Level Configuration 4-26
  Configuring the Array Level DNS 4-27
  Configuring the Array Level NTP Server 4-28
  Configuring Stream Groups 4-28
    VVI with Split-Domain Management and HTTP Streamers 4-28
  Locating Cache Groups 4-30
  Configuring Vault Groups 4-32
  Configuring SSV Groups 4-34
  Configuring Cache Groups 4-35
  Mapping Vault Groups to Cache Groups 4-37
  Mapping Stream Groups to Cache-Fill Sources 4-38
  Mapping Vault Groups for Redundancy 4-39
  Configuring the Control and Setup IPs 4-40
  Configuring Cache-Fill Bandwidth Using Thin Pipe Mapping 4-42
  Configuring the Media Scheduler 4-45
Contents

User Preferences 4-45
Scheduling Content for Ingest 4-47
Package Metadata Editor 4-50
Fixing Conflicts in the Media Scheduler 4-52

Server Level Configuration 4-53
Configuring the Interfaces 4-53
Configuring the Servers 4-56
  Configuring QoS Settings 4-63
Configuring the Route Table 4-63
  CServer Source Route Type 4-64
  CServer Destination Route Type 4-65
Stream Control Route Type 4-65
Configuring the SNMP Agent 4-67
Configuring the Server Level DNS 4-69
Configuring the Server Level NTP 4-70
  Other NTP Configurations 4-71
Configuring RTSP Setup 4-73
  RTSP Deployment 4-73
Configuring FSI Setup 4-78

CHAPTER 5

System Monitoring 5-1
System Level Monitoring 5-1
  System Health 5-2
  System Snapshot 5-3
Monitoring Content Objects 5-4
  Ingests 5-5
    Viewing Completed Ingests 5-5
    Viewing Active Ingress 5-10
  Package Expirations 5-10
  Publish Failures 5-12
Monitoring Stream Objects 5-13
  Stream Monitor 5-13
  Stream Failures 5-18
Array Level Monitoring 5-24
  Array Snapshot 5-24
Server Level Monitoring 5-24
  Disk Monitor 5-24
    S.M.A.R.T 5-26
    NIC Monitor 5-27
Server Vitals  5-28
Cache/Fill Bandwidth  5-30
Services Monitor  5-31
Recommended Monitoring Schedule  5-32
   Daily Tasks  5-32
   Weekly Tasks  5-32
      Monitoring Tasks for Streamers and Vaults  5-33
      Monitoring Tasks for Vaults  5-34
      Monitoring Tasks for Streamers  5-34
   Monthly Tasks  5-35
   Other Tasks  5-35

**CHAPTER 6**

*System Reporting*  6-1

Stream Activity  6-1
   Streams by Array  6-2
   Streams by Time  6-6
   Stream Play History  6-9
   Cache/Fill Bandwidth  6-13
   Stream Failures  6-15
   Content Popularity  6-18

Content Activity  6-20
   Content by Ingest Date  6-20
   Unpublished Package Report  6-22

CDSM Audit Logs  6-23

Archived Data  6-25
   CDSM Audit Log Archives  6-26
   Content Reports  6-26
   Stream Reports  6-27
   Stream Failure Reports  6-28
   Stream Activity Reports  6-28

**CHAPTER 7**

*System Maintenance*  7-1

User Access  7-2
   Setting Up Users  7-2
   Editing User Settings  7-3
   Deleting a User  7-3
   Viewing User Settings  7-3
   Changing User Default Settings  7-4
Server Maintenance  7-5
  Restarting a Server  7-5
  shuts Down a Server  7-6
  Offloading a Server  7-6
    Server Offload—Disable  7-7
  Setting System Thresholds  7-7
Restarting the Services  7-9
Software Maintenance  7-9
  Viewing the Software Version and Server Information  7-9
  Uploading an EPG File  7-10
  Identifying Server IDs and Group IDs for VVI with Split-Domain Management  7-10
    Generating Server IDs and Group IDs from the VVIM  7-11
Manuals  7-13

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-6
    Server Configuration Files  A-6
      Description of the .arroyorc Settings  A-7
      Description of the setupfile Settings  A-8
    Identifying the Software Versions or Releases  A-12
      Linux OS Version  A-12
      CDS-Related Releases  A-12
    Using ifstats to Monitor Traffic  A-13
    Kernel Crash  A-14
    Disk Drive Issues  A-15
      CDSM GUI Disk Monitor Page Reports a Disk Warning  A-15
    Memory Issues  A-16
    Network  A-17
      Interface Information  A-18
    Startup Issues  A-20
      BIOS Settings—Operating System Hangs or Goes into KDB Mode  A-20
      Serial Console Port Settings  A-21
Required Services Not Starting or Running Correctly  A-21
Management and Database Issues  A-22
  System Health  A-22
  Cannot Access the CDSM GUI  A-22
  CDSM GUI Does Not Register the Vaults and Streamers  A-22
  Database Monitoring  A-23
Ingest Issues  A-23
  Ingest Interface  A-23
    FSI Starts but Cannot Ingest Content  A-24
    FSI Does Not Start  A-24
    Content Not Ingesting  A-24
    Asset Ingest Manager Restart Causes Endless Loop  A-25
Bad Content  A-26
Network  A-27
Content Processing Issues  A-27
  Listing Content  A-27
  Content Mirroring  A-27
  Verifying GOIDs  A-28
  Trick-Mode Issues  A-29
Cache-Fill Issues  A-29
  Rules for ISV Interoperability with Vaults and Streamers  A-29
Network  A-29
  Stream Stops Playing at the Same Place or Does Not Play at All  A-29
Streaming and Playout Issues  A-30
  Listing of Streams  A-30
  No Streaming  A-30
  Stream Not Playing  A-31
  Poor Video or Audio Quality  A-32
    No Video Displayed  A-32
    RTSP Cannot Start  A-33
    Video Stops Playing  A-33
    No Video Playing on the STB  A-33
    CDS Is Streaming but No Video Is Playing on the STB  A-34
Session Messaging  A-35
  Log File Search Tips  A-35
  Codes  A-36
Database Issues  A-37
  Database Replication  A-38
CDSM GUI Does Not Report All the Ingested Content  A-38
RFC Compliance C-5

APPENDIX D

Engineering Access Level Pages D-1

CDSM or VVIM Diagnostics D-2
  CIDR Calculator D-2
  Stream Trick-Mode Debugger D-2
  Unix Timestamp Tool D-2
  Server Diagrams D-2

CDSM or VVIM Setup D-3
  Deployed CServer Version D-3
  Stream Failover Support D-3
  Stream Steering Mode D-3
  Deployment Network Config D-3
  Installation Type D-3
  Stream Destination D-4
  Parent/Child Service Groups D-4
  Bulk Configuration D-4
  SSV Groups D-5
  Trick Mode Capture D-5
  Vault Redundancy D-5
  RS DVR D-5
  Thin Pipe Management D-6
  Shared Content Store D-6
  Virtual Video Infrastructure D-6

  Configuring Split-Domain Management D-7

  Media Scheduler D-7
  Real-Time Capture Type D-7
  Bandwidth Manager D-7
  Ingest Manager D-8
  RTSP Deployment Type D-8
  Authentication Manager D-8
  Service Group Steering D-8
  CDSM or VVIM NAV Setup D-8
  CDSM or VVIM Health Monitoring D-8

  System Configs D-9
  Group Map 0 D-9
  Servers Group Map D-9
  License Map D-9
  Control IP Map D-9
Add New Server  D-9

APPENDIX  E

Software Licensing Information  E-1

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

This preface describes the audience, use, and organization of the Cisco TV CDS 2.2 RTSP Software Configuration Guide. The preface also outlines the document conventions and support information.

This preface contains the following sections:

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

**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-21787-01</td>
<td>March 26, 2010</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 xvi 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, “Creating Bulk Configuration Files”</td>
<td>Provides information on creating Bulk Configuration XML files.</td>
</tr>
<tr>
<td>Appendix C, “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 D, “Engineering Access Level Pages”</td>
<td>Describes the CDSM pages visible with the Engineering access level.</td>
</tr>
<tr>
<td>Appendix E, “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</strong> font</td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>italic</em> font</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</strong> font</td>
<td>Terminal sessions and information the system displays are in <strong>screen</strong> font.</td>
</tr>
<tr>
<td><strong>boldface screen</strong> font</td>
<td>Information you must enter is in <strong>boldface screen</strong> font.</td>
</tr>
<tr>
<td><em>italic screen</em> font</td>
<td>Arguments for which you supply values are in <em>italic screen</em> font.</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 2.2.1
- Cisco TV CDS 2.2 ISA Software Configuration Guide
- Cisco TV CDS 2.1–2.2 API Guide
- Cisco TV CDS 2.2 Installation, Upgrade, and Maintenance 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 for a Real Time Streaming Protocol (RTSP) environment. This chapter covers the following major topics:

- Overview, page 1-1
- Content Delivery System Architecture, page 1-5

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 five areas:

- Ingest
- Storage
- Caching
- 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>Content Cache</td>
<td>Content distribution between Vaults and Streamers</td>
<td>Caching Node</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 video on demand (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.

There are two types of systems available with the TV CDS: a CDS with an array of Vaults and Streamers, and a Virtual Video Infrastructure (VVI) with an array of Vaults, Caching Nodes, and Streamers. The CDSM manages the Vaults and Streamers in a CDS. The VVIM manages the Vaults, Caching Nodes, and Streamers in a VVI with centralized management. For more information about network design and VVI management, see the “TV CDS Topologies and VVI Topologies” section on page 2-2. Figure 1-1 shows a high-level view of both a CDS and a VVI.

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.

The Cisco TV VVI solution has four major elements:

- One or more Vault Groups consisting of one or more Vaults. The Vaults are responsible for ingest and reliable storage of VOD content. The number of Vaults in the Vault Group, and the number of Vault Groups is driven by the amount of content that the system offers and the degree of redundancy.

- One or more Cache Groups, consisting of one or more Caching Nodes. The Caching Nodes provide more flexibility in designing a multi-tiered Virtual Video Infrastructure (VVI) by acting as a tier between the Vaults and the Streamers. The Caching Nodes facilitate content distribution and remove distribution traffic from the network backbone.

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

- The CDSM is used to manage the Vaults, Streamers, and Caching Nodes in the same array, collect event logs, and provide reporting tools. In a split-domain management system configuration, there is a Stream Manager that manages all the Streamers, and a Virtual Video Infrastructure Manager (VVIM) that manages all the Vaults and Caching Nodes.

**TV CDS Software**

The Cisco TV CDS kernel software, known as the CSer ver, 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 dynamic random access memory (DRAM) or disk cache on the serving Streamer.

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 cache on the Streamer. Requests for content that are not already
in the local cache on the Streamer 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.

**Caching Nodes**

A Caching Node is an intermediary fill source for the Streamers. Caching Nodes are deployed in Virtual
Video Infrastructures (VVIs). The VVI is a deployment type of the TV CDS. In a CDS, servers cannot
communicate with servers in other groups. In a VVI, servers in other groups can communicate with each
other on an as needed basis. Streamers and Caching Nodes dynamically discover fill sources within other
groups. Streamers send cache-fill calls to remote servers (Streamers in other Stream Groups and Caching
Nodes) for content that is not found locally (DRAM, disk cache, or peer Streamers). In a VVI, the
Caching Nodes can communicate with the Streamers by using CCP or HTTP. For more information on
how a Caching Node interfaces with a CCP Streamer and an HTTP Streamer, see the “Caching Node
Workflow” section on page 2-9.

**Streamer Load Balancing**

To ensure that new streams are distributed to the best Streamer in the group, each Stream Group runs a
load distribution protocol among its members. 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 after a new server is in service,
fresh streams are automatically allocated to it. Furthermore, the cache capacity of the group is the sum
of the caches of all Streamers in the group, which provides the most optimal system operation and the
highest cache-hit rate.

**CServer Functionality**

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

**Streamer Content Delivery Applications**

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 electronic program guide (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. In a VVI, the Caching Nodes provide a pure caching layer for a multi-tiered VVI. Figure 1-2 shows the different elements of the TV Content Delivery System and the TV Virtual Video Infrastructure with the addition of the Caching Nodes.

Table 1-2 describes the system elements shown in Figure 1-2.
Chapter 1      Product Overview

Content Delivery System Architecture

Table 1-2  High-Level Description of the TV CDS and TV VVI

<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, Real Time Streaming Protocol (RTSP) and Lightweight Stream Control Protocol (LSCP) 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 four levels of storage (or cache):  
|                                | • All content is stored on the Vault server, as well as mirrored to other Vaults.  
|                                | • Requested content is stored on the Caching Nodes.  
|                                | • Recently requested content, or popular content is stored on the hard drive on the Streamer.  
|                                | • Currently requested content, or popular content, is stored in the random access memory (RAM) on the Streamer. |
| Event Collection                | The Content Delivery System Manager collects logged events for reporting purposes as well as for 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 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 reliably on disk. A Vault Group consists of a scalable number of Vaults that divide the responsibility for ingest and storage among the members of the group. Vault servers can be collocated or distributed to multiple locations across an IP or Ethernet network. Each Vault can simultaneously ingest up to 160 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 or two trick files.
Chapter 1      Product Overview

Content Delivery System Architecture

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 Stream Group is responsible for the personalization and streaming of content in response to user requests.

Caching Node

The Caching Node provides a 10-Gbps throughput to facilitate the distribution of content from the Vaults to the Streamers. The Caching Nodes allow for the ability to create a tier-based hierarchy in the CDS. Caching Nodes are deployed in VVIs. Vaults can be strategically located for storing content on a national network, while the Streamers are located in a regional network. The Caching Node can be colocated with the Vaults or distributed closer to regional locations across an IP or Ethernet network. A Cache Group consists of several Caching Nodes that divide the responsibility for distribution among the members of the group.

The Caching Nodes use CCP to communicate with the Vaults and Streamers. Alternatively, the Caching Nodes can use HTTP instead of CCP to communicate with Streamers.

Integrated Streamer-Vault

The Integrated Streamer-Vault (ISV) server offers the functionality of both a Vault and Streamer in one server.

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 and Virtual Video Infrastructure Manager

The Content Delivery System Manager (CDSM) and the Virtual Video Infrastructure Manager (VVIM) are each a browser-based user interface accessible by a web browser program and designed to manage a TV CDS or a TV VVI network.

The CDSM provides centralized management functions for the TV CDS, including configuration, monitoring, troubleshooting, reporting, and maintenance.

The VVIM provides centralized management function for the TV VVI, including configuration, monitoring, troubleshooting, reporting, and maintenance. The VVIM in a centralized domain management configuration manages the Vaults, Caching Nodes, and Streamers. The VVIM in a split-domain management configuration manages the Vaults and Caching Nodes, while the Streamers are managed by the Stream Manager. For more information about split-domain management, see the “TV VVI Management” section on page 2-6.
In both the CDS and VVI, all Vaults and Streamers are identified by an array ID, a group ID, and a server ID. In the CDSM GUI, the array ID identifies servers that are part of the same system, the group ID identifies servers that are part of the same group (Vault Group or Stream Group), and the server ID is a unique number that identifies the server. Table 1-3 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

Table 1-3  
ID Names in the CDSM GUI and CServer Files

<table>
<thead>
<tr>
<th>CDSM GUI ID Name</th>
<th>CServer Files ID Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array ID on the Array Name page</td>
<td>groupid</td>
</tr>
<tr>
<td>Group ID on the Server-Level pages</td>
<td>groupid</td>
</tr>
<tr>
<td>Stream Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Cache Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Vault Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Stream Group ID on the Configuration Generator page</td>
<td>arrayid</td>
</tr>
</tbody>
</table>

In a VVI with CCP Streamers, similar to a CDS, all Vaults, Streamers, and Caching Nodes are identified by an array ID, a group ID and a server ID. The group ID and server ID in a VVI with CCP Streamers must be unique among other groups and servers in the same system.

In a VVI with HTTP Streamers, the Vaults, Streamers, and Caching Nodes still use an array ID, a group ID and a server ID for identification, but there is additional functionality that allows the Vaults and Caching Nodes to communicate using CCP, while the Caching Nodes communicate with the Streamers using HTTP. It is not required that the group ID and server ID be unique, but it is recommended.

The CDSM and VVIM (as well as the Stream Manager) have three configuration and monitoring levels: system, array, and server. System-wide configuration affects all servers managed by that manager. The array-level configuration affects all the servers of the specified array or group, and the server-level configuration applies changes to a specific server.

The CDSM and VVIM offer a drill-down approach to show 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.

The VVIM monitoring and reporting helps operators manage all aspects of the TV VVI in either a centralized management capacity or a split-domain management capacity. In a split-domain capacity, the VVIM monitors the ingests and the Stream Manager monitors the streams of the Streamers in its domain.

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

The TV Content Delivery System is designed to have 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 time. 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 because of 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 that is 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.

**Vault Group Redundancy**

In addition to the Vault server redundancy, the Cisco TV CDS offers 1:1 redundancy for Vault Groups. When the CDS is configured with Vault Group redundancy and at least two Vault Groups are configured, the system handles the loss of an entire Vault Group without impacting the subscriber. Content is mirrored between two Vault Groups, which may be in different geographic regions. If the primary Vault Group becomes unavailable, because of network, power, or other catastrophic problems, any Streamer or Caching Node that was requesting content from that Vault Group would fail over to the other Vault Group until the primary Vault Group came back online and could again respond to cache-fill requests for content.

With Vault redundancy, at least one copy of each content within a group is mirrored to the configured peer group. Vault Group mirroring runs as a low-priority process, so as not to impact the performance of the guaranteed streaming delivery.

**Note**

The maximum number of Vault Groups for this release is two.

**Streamer Disk Redundancy**

The disks in the Streamer are not used for full content storage as in 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.
Stream 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.

Caching Node Disk Redundancy

The disks in the Caching Node are not used for full content storage like most VOD implementations. Rather, the Caching Node disks are part of the TV CDS multilevel caching architecture. If a disk is lost on a Caching Node, the only impact is a marginal loss of caching capability for the system. Any content that was cached on that Caching Node disk is retrieved again from the Vault.

Caching Node Resiliency

The Cisco TV CDS architecture allows for failed Caching Nodes as well. If a Caching Node fails, any cache-fill transmissions that were in process at the time of the failure are re-requested by the Streamer, and any new requests are responded to by the remaining Cache Nodes in the Cache Group.

CDSM Redundancy

The Cisco TV CDS offers 1+1 redundancy for CDSMs. The primary CDSM, designated by a virtual IP address on the management interface, is used as the representative of the CDSMs to the web browser and northbound integrations, such as HTML API calls and SNMP calls.

All CDS servers keep track of a controller IP address in the .arrayorc file. With CDSM redundancy, both management IP addresses are specified in the .arrayorc file on each CDS server, except the CDSM, which only has the other CDSM IP address.

The statsd process is configured with a virtual IP address that can move from one CDSM to the other. If the primary CDSM becomes unavailable, because of network, power, or other catastrophic problems, the secondary CDSM takes over the virtual IP address and the administrator can connect to the secondary CDSM within 15 seconds.

Login information is not shared between CDSMs. If the administrator is logged in and a failover occurs, the administrator has to log in again to the other CDSM.

The CDS servers (Vault, Caching Node, Streamer, and ISV) participate in replication with both the primary and secondary CDSM in the same manner as occurred without redundancy, including synchronization of tables. However, the CDS servers can only retain up to one hour of reporting data, so if a CDSM is down for over an hour, when the CDSM recovers, it is only able to get the last hour of reporting data from each CDS server, which means the reporting data is not synchronized between the primary and secondary CDSMs. Reporting data is archived in comma-separated value (CSV) files every 24 hours and these CSV files are deleted when they are older than 30 days.

Ethernet Link Resiliency

All Ethernet links used within the Cisco TV CDS architecture incorporate link failure detection with automatic failover. This includes the interconnections 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 to add streaming without affecting storage, and in VVIs, to add distribution nodes without directly affecting storage or streaming. 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 the need to take 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 and VVI Topologies, page 2-2
- CDS Workflow, page 2-7
- BMS Considerations for RTSP Environments, page 2-11
- Network Connections, page 2-12

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.

Stream Groups can be distributed close to the subscriber and linked back to the central Vault locations by way of the Cisco Cache Control Protocol (CCP). Cisco 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; as a result, 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 Vaults and Streamers, MPEG-2 transport stream (TS) video is stored on the Vaults with the associated trick-mode files. Content is transported from the Vaults to the Streamers 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 set-top box (STB) for viewing.
CDS with ISVs

For the smallest networks, Cisco packages the CDS in a single server, the Integrated Streamer-Vault (ISV), offering a solution 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 ISVs and delivered to the QAM devices over a gigabit Ethernet network, and then is modulated onto the HFC plant to the subscriber STB for viewing.

CDS with Caching Nodes

For larger networks, Cisco offers the CDS with Caching Nodes in the Virtual Video Infrastructure (VVI). In a VVI, Caching Nodes are the intermediary fill source for Streamers, which removes a large portion of the distribution traffic from the Vaults.

In a TV VVI, MPEG-2 TS video is stored on the Vaults with the associated trick-mode files. Content is transported from the Vaults to the Caching Nodes as needed, by using CCP over gigabit Ethernet networks. Content is distributed from the Caching Nodes to the Streamers as needed, by using CCP over gigabit Ethernet networks, or by using HTTP over gigabit Ethernet networks. Content is sent unicast from the Streamers and delivered to the QAM devices over a gigabit Ethernet network, and then is modulated onto the HFC plant to the subscriber STB for viewing.

TV CDS Topologies and VVI Topologies

The TV CDS (using Vaults and Streamers, or ISVs) and the TV VVI (using Vaults, Caching Nodes, 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. Caching Nodes separate the ingest and storage of content from the distribution of content, offering greater flexibility and network efficiency.

The TV CDS topology and TV VVI 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 disrupting service. The VVI offers additional flexibility in designing your network. Vaults can be centrally located at a national network, and content may be classified by market (city, state, or a broader region) depending on the AMS or BMS used. Caching Nodes can be located centrally, or distributed closer to the regional networks where the Streamers are located. Using Caching Nodes in the network design takes the distribution traffic off the network backbone.

Caution

All Cisco servers are connected through a switch. Because all Vaults, CCP Streamers, and Caching Nodes 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.

**Figure 2-1 Centralized Topology with Vaults and Streamers**

Figure 2-1 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. For a VVI, a decentralized topology provides a three-tiered approach by having the Vaults located in the headend, the Caching Nodes in intermediary sites, and the Streamers in the hub sites. The decentralized topology works well for distributing Streamer Groups 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 2-4 illustrates the decentralized topology.
Figure 2-5 illustrates the decentralized topology with Caching Nodes.

**Figure 2-5  Decentralized Topology with Caching Nodes**

**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 that is based on needs of the system implemented. Figure 2-6 illustrates the hybrid topology.

**Figure 2-6  Hybrid Topology**
Figure 2-7 illustrates the hybrid topology with Caching Nodes.

**Figure 2-7  Hybrid Topology with Caching Nodes**

---

**TV VVI Management**

The TV VVI offers two types of management, centralized and split-domain.

In a CDS, Streamers cannot communicate with Streamers in other groups. In a VVI, Streamers in other groups can communicate with each other on an as-needed basis.

All Vaults, Streamers, and Caching Nodes are identified by an array ID, a group ID, and a server ID. In the CDSM GUI, the array ID identifies servers that are part of the same system. The group ID identifies servers that are part of the same group (Vault Group, Cache Group, and Stream Group), and the server ID is a unique number that identifies the server. Table 2-1 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

**Table 2-1 ID Names in the CDSM GUI and CServer Files**

<table>
<thead>
<tr>
<th>CDSM GUI ID Name</th>
<th>CServer Files ID Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array ID on the Array Name page</td>
<td>groupid</td>
</tr>
<tr>
<td>Group ID on the Server-Level pages</td>
<td>groupid</td>
</tr>
<tr>
<td>Stream Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Cache Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Vault Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Stream Group ID on the Configuration Generator page</td>
<td>arrayid</td>
</tr>
</tbody>
</table>
Chapter 2  Network Design

CDS Workflow

**Centralized Management**

Centralized management uses one Virtual Video Infrastructure Manager (VVIM) to manage the Vaults, Caching Nodes, and Streamers in a VVI.

**Note** Centralized management is only in an RTSP environment.

**Split-Domain Management**

Split-domain management uses one VVIM to manage the domain of Vaults and Caching Nodes, and separate managers, the Stream Managers, to manage each domain of Streamers. The Stream Managers communicate with the VVIM over port 80. If port 80 is not open for communication, the managers cannot communicate with each other and configuration settings need to be uploaded to the Stream Managers from information downloaded from the VVIM.

In a split-domain VVI that uses HTTP for communication between the Caching Nodes and Streamers, and in a split-domain VVI that uses CCP in an RTSP environment, the databases for each domain are separate. The information stored in each database is not shared with the servers in the other domains.

In an ISA environment with a split-domain VVI that uses CCP for communication between the Caching Nodes and Streamers, the database is replicated among all servers in the Vault/Cache domain and the Stream domains. Because the VVI allows intercommunication among different Cache Groups and Stream Groups when CCP Streamers are used, the server ID and group ID must be unique across the system.

**Note** Split-domain management is supported in an RTSP environment and an ISA environment with the Shared Content Store feature and CCP Streamers.

**CDS Workflow**

Content is ingested and stored in the Vault array. The Vault array consists of two or more Vault Groups, which in turn consists of two or more Vaults that are either colocated 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.

**Note** Release 2.2.1 supports the ability to differentiate between a DVD asset and a video asset to support ingest, trick-play creation, and streaming of content files as large as 30 GB. The content files could span multiple days.

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

If a VVI is deployed, content is delivered from the Vault Group to the Cache Group in response to cache-fill calls from the Streamers. The Caching Nodes are explained in more detail in the “Caching Node Workflow” section on page 2-9.

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, because of 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. For RTSP, the Setup server and Control server must be the same server. For both ISA and RTSP environments, 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 this IP address.
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 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. After 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 Play server 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.

Caching Node Workflow

A Cache Group is a configurable group of Caching Nodes that serve content to specified Stream Groups. When a content request is received by a Streamer, the Streamer first checks to see if the content is stored locally, which includes DRAM, disk cache, and Streamers in the same Stream Group. Content on the Streamers is always the most popular content, so user requests are generally served from local storage.

Streamers send cache-fill calls to remote servers for content that is not found locally. The remote servers can be Streamers in other Stream Groups, Caching Nodes in Cache Groups, or Vaults in Vault Groups (Vault Redundancy must be enabled). The cache-fill source selected, whether another Streamer, Caching Node, or Vault, is based on the network capacity and fill-source capacity (disk and memory), as well as the preference configured for that group of servers. Caching Nodes could respond to the request with a message stating the content is not currently cached, but there are other fill sources the Caching Nodes can contact (Caching Nodes in other Cache groups, and Vaults).

The Caching Nodes use CCP to communicate with the Vaults, and use either CCP or HTTP to communicate with Streamers.

Note

ISA environments only support CCP, while RTSP environments only support HTTP for VVI.

HTTP Streamers

HTTP can be used for communication between the Caching Nodes and the Streamers. The HTTP Streamer communicates with a proxy for locating a fill source and pulling content.

A locate service serves as a proxy for a group of Caching Nodes and Vaults. The service is accessed through a highly available virtual IP address hosted by the Caching Node. The virtual IP address is bound to a fill port (Locate Port).
HTTP Streamers request content by HTTP GET requests to the proxy service (the server with the locate service). The proxy server checks its own storage and peer fill sources (servers in the same group) for the content using extended-CCP. If the content is found, the best source is chosen based on capacity and a redirect response is sent to the chosen server. If the content is not found, a cache-fill request is sent to the remote servers.

After the best server is chosen to send the content to the HTTP Streamer, a single cache-fill port on that server is chosen for the HTTP transfer of the content. This is different from CCP transfers, which could potentially use all cache-fill ports to deliver the content.

**HTTP Locate Port**

With respect to resiliency, the Locate Port service is similar to the Setup and Control servers. The primary server of the Locate Port service has the locate port IP address bound to an interface. The backup server becomes the primary if the primary fails.

Peer Caching Nodes advertise among themselves about the ability to host the HTTP Locate Port Service, this includes primary, backup, available, and not usable states. Available means the Caching Node can be either a primary or backup if needed. Not usable means that the server cannot host the service; for the HTTP Locate Port this typically means that there are no usable network ports for the service.

A dedicated network port on the Caching Node is used solely for the HTTP Locate Port service. The primary server determines service availability based on the link status of the dedicated network port. Failover of the service occurs if the network port loses link status. A reestablished link results in the server becoming available.

**CCP Streamers**

The CCP Streamers use CCP to communicate with the Caching Nodes. They do not use the proxy address that was assigned to the Locate Port for HTTP Streamers. CCP Streamers load-balance locate requests across fill sources.

The Streamer or Caching Node sends a locate-and-request message from the proxy server. The Proxy server sends a message to the best source to fill the request.

Streamers or Caching Nodes needing content first query peer sources (servers within the same group). Streamers also query local Streamers, if the content is not found, then a request to the remote sources is sent. Remote sources are queried based on a preference list. Sources are grouped and preferences are assigned for each group.

**Vault Workflow**

The Vaults ingest content using three different methods:

- FTP pull
- FTP push
- Live capture of MPEG-2 transport streams over UDP

With FTP pull, the original content is kept on an FTP server (catcher), for a period of time and mechanisms are in place to restart ingest until they have successfully completed.

With FTP push, only a window of data is buffered by a device that grooms the live (broadcast) feed and pushes the data to the Vault.

With live capture over UDP, the Vault captures the live multicast feed directly.
BMS Considerations for RTSP Environments

The TV CDS integrates with Interactive Services Architecture (ISA) used in business management systems (BMSs) such as the 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.

nABLE Integration

The nABLE BMS uses a combination of eXtensible Markup Language (XML) over Hypertext Transfer Protocol (HTTP) and 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).

Note

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 2-8 illustrates how the CDS integrates with the nABLE BMS.

Figure 2-8   TV CDS Integration into the nABLE BMS
Network Connections

The network connections for a TV CDS with Vaults and Streamers, a TV CDS with ISVs, and a TV VVI with Caching Nodes all have different network connections. Table 2-2 lists the different required interfaces for each CDS server. The interfaces are described in the following sections. Figure 2-9 illustrates a TV CDS with Vaults and Streamers. Figure 2-10 illustrates a TV CDS with ISVs. Figure 2-11 illustrates a TV VVI with Caching Nodes.

Table 2-2  CDS Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vault</th>
<th>Streamer</th>
<th>ISV</th>
<th>Caching Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Ingest</td>
<td>1</td>
<td>—</td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>Cache</td>
<td>1 to 8</td>
<td>1 to 13</td>
<td>1 to 4&lt;sup&gt;1&lt;/sup&gt;</td>
<td>1 to 12</td>
</tr>
<tr>
<td>Stream</td>
<td>—</td>
<td>1 to 13</td>
<td>1 to 4</td>
<td>—</td>
</tr>
</tbody>
</table>

1. The cache interfaces on an ISV are used for content mirroring among ISVs.

Table 2-2 lists the mandatory interfaces for each CDS server. If HTTP Streamers are used in a VVI, each Caching Node must have one interface designated as the Locate interface. Stream Control is an optional interface function. For more information, see the “Configuring the Interfaces” section on page 4-53.

Figure 2-9 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 and the content is ingested by the Vaults. The management network consists of communication between the CDSM and the BMS, as well as communication with the Vaults, Streamers QAM devices, and STBs. The cache network consists of Vaults and Streamers.
Figure 2-9  Vault and Streamer Network Connections

Figure 2-10 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 and the content is ingested by the ISVs. The management network consists of communication between the CDSM and BMS, as well as communication with the ISVs, QAM devices, and STBs.

Figure 2-10  ISV Network Connections
Figure 2-11 shows the different logical networks of a VVI. 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 BMS, as well as communication with the Vaults, Streamers, Caching Nodes, QAM devices, and STBs.

**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.

When using Layer 2 packet forwarding, to segregate all ingest traffic through the switching fabric, we recommend the use of a port-based VLAN.
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 Vaults, Caching Nodes, and Streamers 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, when using Layer 2 packet forwarding, we recommend using a port-based VLAN to ensure delivery of critical management communications.

Cache Interfaces

The CCP uses the cache interfaces on the Vaults, Caching Nodes, and Streamers to send the following data to the servers in the same array:

- Content sent to the Streamers
- Content mirrored among the Vaults
- Messages containing information used for performance optimization exchanged among all the CDS servers

Note

All Cisco CDS servers are connected through a switch fabric. Because all Vaults, Caching Nodes, and Streamers 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.

When using Layer 2 packet forwarding for cache traffic, we recommend the use of a port-based VLAN.

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.

When using Layer 2 packet forwarding for cache and stream traffic, we recommend the use of a port-based VLAN.

Streaming Interface

The streaming interface delivers streaming traffic consisting of MPEG-2 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 3-1
- 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 toward 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, and optionally Caching Nodes, 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, the Cisco Content Delivery Engine 110 Hardware Installation Guide, or the Cisco TV CDS 2.2 Installation, Upgrade, and Maintenance Guide.

Initial configuration of your CDEs includes basic network configuration settings to provide connectivity to the CDSM. After 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.
Consult your as-built documentation for the IP address of the CDSM. If you have redundant CDSMs, use the virtual IP address, not the IP addresses of the physical Ethernet interfaces.

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

**Figure 3-1 System Login Page**

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 as in the following example:

Choose **Maintain > Users > Add Users**.
Chapter 3      Getting Started

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** Choose the options for your deployment and click **Submit**. For more information about the fields on this page, see the “CDSM or VVIM Setup” section on page D-3.

**Step 5** Scroll down to the Media Scheduler section, and click 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 click 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**.

---

**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**

---

Cisco TV CDS 2.2 RTSP Software Configuration Guide
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, to the array level, or to 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.
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. After 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.
  - Contents icon shows and hides the Table of Contents.
  - Print icon prints the page you are viewing.
- From the Help window, you can display the full Cisco TV CDS 2.2 RTSP Software Configuration Guide by clicking the View PDF button.

Configuration Workflows

After 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. The configuration workflow consists of one or more of the following:

- CDS Workflow
- VVI Workflow
- TV MediaX Configuration Workflow

CDS Workflow

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 password</td>
<td>Change the administrator password for the CDSM.</td>
<td>“Editing User Settings,” page 7-3</td>
</tr>
<tr>
<td>Interface setup</td>
<td>Configure the different interfaces on the CDS servers.</td>
<td>“Configuring the Interfaces,” page 4-53</td>
</tr>
<tr>
<td>Server setup</td>
<td>Configure the IP addresses and ports for the interfaces, as well as other settings such as quality of service (QoS).</td>
<td>“Configuring the Servers,” page 4-56</td>
</tr>
<tr>
<td>Route table</td>
<td>Route Table identifies destination subnetworks for cache, stream, and stream control interfaces. Route Table is optional.</td>
<td>“Configuring the Route Table,” page 4-63</td>
</tr>
</tbody>
</table>
The other configuration settings, DNS settings, and so on, can be configured in any order.

**VVI Workflow**

The Virtual Video Infrastructure can be centrally managed or can use split-domain management.

**Central Management Workflow**

Table 3-2 lists the basic tasks, in the recommended order, for configuring the VVI with central management for content delivery with references to the associated sections in each chapter.

**Table 3-2 VVI Configuration Workflow**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change administrator password setup</td>
<td>Change the administrator password for the CDSM.</td>
<td>“Editing User Settings,” page 7-3</td>
</tr>
<tr>
<td>Interface setup</td>
<td>Configure the different interfaces on the CDS servers.</td>
<td>“Configuring the Interfaces,” page 4-53</td>
</tr>
<tr>
<td>Server setup</td>
<td>Configure the IP addresses and ports for the interfaces, as well as other settings such as quality of service (QoS).</td>
<td>“Configuring the Servers,” page 4-56</td>
</tr>
<tr>
<td>Route table</td>
<td>Route Table identifies destination subnetworks for cache, stream, and stream control interfaces. Route Table is optional.</td>
<td>“Configuring the Route Table,” page 4-63</td>
</tr>
<tr>
<td>Stream Groups setup</td>
<td>A Stream Group consists of one or more Streamers. Stream Groups relate to QAM gateways or destination subnetwork by the Stream Group preference.</td>
<td>“Configuring Stream Groups,” page 4-28</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.

Split-Domain Management Workflow

Table 3-3 lists the basic tasks, in the recommended order, for configuring the VVI with split-domain management (VVIM and Stream Manager) for content delivery with references to the associated sections in each chapter. For more information, see the Chapter 2, “Network Design,” and the “CDSM or VVIM Setup” section on page D-3.

Table 3-3  VVI Split-Domain Configuration Workflow

<table>
<thead>
<tr>
<th>Task</th>
<th>Manager</th>
<th>Description</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change administrator password</td>
<td>VVIM and Stream Manager</td>
<td>Change the administrator password for the CDSM.</td>
<td>“Editing User Settings,” page 7-3</td>
</tr>
<tr>
<td>Interface setup</td>
<td>VVIM and Stream Manager</td>
<td>Configure the different interfaces on the CDS servers.</td>
<td>“Configuring the Interfaces,” page 4-53</td>
</tr>
<tr>
<td>Server setup</td>
<td>VVIM and Stream Manager</td>
<td>Configure the IP addresses and ports for the interfaces, as well as other settings such as quality of service (QoS).</td>
<td>“Configuring the Servers,” page 4-56</td>
</tr>
<tr>
<td>Route table</td>
<td>VVIM and Stream Manager</td>
<td>Route Table identifies destination subnetworks for cache, stream, and stream control interfaces. Route Table is optional.</td>
<td>“Configuring the Route Table,” page 4-63</td>
</tr>
<tr>
<td>Stream Groups setup</td>
<td>Stream Manager</td>
<td>A Stream Group consists of one or more Streamers. Stream Groups relate to QAM gateways or destination subnetwork by the Stream Group preference.</td>
<td>“Configuring Stream Groups,” page 4-28</td>
</tr>
<tr>
<td>Control and setup IPs</td>
<td>Stream Manager</td>
<td>Configure the Control server and Setup server IP address for the Stream Groups.</td>
<td>“Configuring the Control and Setup IPs,” page 4-40</td>
</tr>
</tbody>
</table>
Table 3-3  VVI Split-Domain Configuration Workflow (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Manager</th>
<th>Description</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Groups setup</td>
<td>VVIM</td>
<td>A Cache Group consists of one or more Caching Nodes.</td>
<td>“Configuring Cache Groups,” page 4-35</td>
</tr>
<tr>
<td>Stream to cache map</td>
<td>Stream Manager</td>
<td>Cache Groups are mapped to Stream Groups and given a preference.</td>
<td>“Mapping Stream Groups to Cache-Fill Sources,” page 4-38</td>
</tr>
<tr>
<td>QAM gateways(^1)</td>
<td>Stream Manager</td>
<td>Configure the QAM Gateways for the CDS.</td>
<td>“Configuring QAM Gateways,” page 4-4</td>
</tr>
<tr>
<td>Headend setup(^1)</td>
<td>Stream Manager</td>
<td>Associate service groups with Stream Groups.</td>
<td>“Configuring the Headend Setup,” page 4-7</td>
</tr>
<tr>
<td>Ingest tuning</td>
<td>VVIM</td>
<td>Configure the trick-mode speeds for ingested content.</td>
<td>“Configuring Ingest Tuning” section on page 4-17</td>
</tr>
</tbody>
</table>

1. If the Stream Destination feature is enabled, the QAM Gateway page and Headend Setup page are replaced with the Stream Destination page. For more information, see the “Configuring Stream Destinations” section on page 4-8.

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

**TV MediaX Configuration Workflow**

Table 3-4 lists the basic tasks for configuring the TV MediaX Suite CDA with references to the associated sections in each chapter.

Table 3-4  TV MediaX Configuration Workflow

<table>
<thead>
<tr>
<th>Task</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 4-23</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 4-23</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 7-10</td>
</tr>
<tr>
<td>Schedule the ingest of content.</td>
<td></td>
</tr>
<tr>
<td>The Media Scheduler does the following:</td>
<td></td>
</tr>
<tr>
<td>1. Values from the EPG file are combined with the values from the Input Channels page, and the ADI metadata XML file is created.</td>
<td>“Configuring the Media Scheduler” section on page 4-45</td>
</tr>
<tr>
<td>2. The database records are marked according to the Media Scheduler settings (scheduled, unscheduled, marked for scheduling, and so on).</td>
<td>“Configuring the Media Scheduler” section on page 4-45</td>
</tr>
<tr>
<td>3. The ADI metadata is published to the backoffice.</td>
<td>“Configuring the Media Scheduler” section on page 4-45</td>
</tr>
</tbody>
</table>
Chapter 4

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 4-26
- Server Level Configuration, page 4-53

**Note**

If Virtual Video Infrastructure (VVI) with split-domain management is enabled, the CDSM pages associated with the Vaults and Caching Nodes display only on the VVI Manager (VVIM), and the CDSM pages associated with the Streamers display only on the Stream Manager. For more information, see the “Virtual Video Infrastructure” section on page D-6.

**System Level Configuration**

The System Level tab has the following configuration options:

- Configuring DNS Services
- Configuring NTP Services
- Configuring the Hosts Service
- Configuring the Array Name
- Configuring QAM Gateways
- Configuring the Headend Setup
- Configuring Stream Destinations
- Configuring the Bandwidth Manager
- Configuring the Ingest Manager
- Configuring the Authentication Manager
- Configuring Ingest Tuning
- Configuring IP Nicknames
Configuring DNS Services

The System DNS page is used to configure up to 16 domain suffixes and 16 DNS servers.

To view the current DNS System Level settings choose, Configure > System Level > System DNS.

Note

If you are upgrading the TV CDS software to Release 2.2 from Release 2.0 or an earlier release, the system prompts you to Submit any settings that have previous domain suffixes to populate the new DNS database structure.

To configure the DNS service settings, do the following:

Step 1

Choose Configure > System Level > System DNS. The System DNS page is displayed.

Step 2

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

Table 4-1 DNS Service Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New 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>
<tr>
<td>New DNS Server</td>
<td>IP address of the DNS server.</td>
</tr>
</tbody>
</table>

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 Delete Entry.
Configuring NTP Services

The System NTP Server page is used to configure up to 16 NTP servers. The clocks on all CDS servers (Vault, Streamer, and Caching Node) and the CDSM and VVIM in a CDS must be synchronized in order to retrieve the statistics on to the CDSM and VVIM.

To view the current NTP System Level settings, choose Configure > System Level > System NTP Server.

To configure the NTP service settings, do the following:

Step 1 Choose Configure > System Level > System NTP Server. The System NTP Server page is displayed.
Step 2 In the New NTP Server field, enter the IP address of the NTP server.
Step 3 Click Submit.

To clear the fields and start over, click Reset.

To delete the NTP settings, check the Delete check box and click Delete Entry.

For information on setting the time zone on a CDS server or configuring NTP on a CDSM or VVIM, see “Other NTP Configurations” section on page 4-71.

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

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.

Table 4-2 Host Service Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>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>IP address associated with the hostname.</td>
</tr>
</tbody>
</table>
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 1-5.

**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.

**Step 2** Enter the array name 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.

**Note**
The QAM Gateway page is not available if the Stream Destination is set to IPTV. For more information, see the “Stream Destination” section on page D-4.

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 a similar device.

Single-site steering is supported 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 location.

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 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 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 are routed 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 4-63.

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 4-1).

**Note**

If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Browse and Import buttons. To import a Bulk Configuration XML file, click Browse to locate the file, then Import to import the file. The status of the import is displayed in the left panel.

For information on enabling the Bulk Configuration feature, see the “Bulk Configuration” section on page D-4. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating QAM Gateway Bulk Configuration Files” section on page B-2.

**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>IP address of the QAM gateway.</td>
</tr>
<tr>
<td>QAM MAC</td>
<td>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 4-63.</td>
</tr>
</tbody>
</table>
| Stream Group Preferences | Choose 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 4-28. |

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

To edit a QAM gateway, choose the QAM IP address and click Next. Enter the new settings and click Submit.

To delete a QAM gateway, choose the QAM IP address, click Next, and then click Delete QAM.
Configuring the Headend Setup

The Headend Setup page is associated with the Service Group Steering optional feature.

**Note**
The Headend Setup page is not available if the Stream Destination is set to IPTV. For more information, see the “Stream Destination” section on page D-4.

Service Group Steering is used to associate 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**
The Headend Setup page is displayed only if the Service Group Steering feature is enabled. For more information, see the “Service Group Steering” section on page D-8.

**Note**
You must first configure the Stream Groups before you can configure the head end setup for a specific service group. See the “Configuring Stream Groups” section on page 4-28.

To configure the headend setup, do the following:

**Step 1**
Choose Configure > Headend Setup. The Headend Setup page is displayed (Figure 4-2).

**Note**
If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Browse and Import buttons. To import a Bulk Configuration XML file, click Browse to locate the file, then Import to import the file. The status of the import is displayed in the left panel.

For information on enabling the Bulk Configuration feature, see the “Bulk Configuration” section on page D-4. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating Headend Setup Bulk Configuration Files” section on page B-3.

**Figure 4-2**  Headend Setup Page

<table>
<thead>
<tr>
<th>Headend Setup CONFIGURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter New Service Group</td>
</tr>
<tr>
<td>To begin select an existing &quot;Service Group&quot; to edit, or select &quot;Add New&quot; from the list below.</td>
</tr>
<tr>
<td>Select Service Groups:</td>
</tr>
<tr>
<td>Stream Group Name:</td>
</tr>
<tr>
<td>Stream Group 1:</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Stream Group 2:</td>
</tr>
<tr>
<td>Medium</td>
</tr>
</tbody>
</table>

**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  Choose 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 4-28.

Step 5  Click Submit.

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

Configuring Stream Destinations

The Stream Destination page provides a way to associate subnetworks with Stream Groups. The Stream Destination page is an alternative to the QAM Gateway page and Headend Setup page where you associate a Stream Group with a specific QAM device and any applicable service groups. Mapping Stream Groups to specified subnets is appropriate for IPTV networks, where each end-user device has its own IP address.

Note  The Stream Destination page is not available if the Stream Destination is set to Cable. For more information, see the “Stream Destination” section on page D-4.

To configure the Stream Destination, do the following:

Step 1  Choose Configure > Stream Destination. The Stream Destination page is displayed (Figure 4-3).

Note  If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Action on Import option, and the Browse and Import buttons.

To import a Bulk Configuration XML file, click Browse to locate the file, select Add for the Action on Import, then Import to import the file. The status of the import is displayed in the left panel.

To delete the configurations defined in the Bulk Configuration XML file, click Browse to locate the file, select Delete for the Action on Import, then Import. All the subnets defined in the Bulk Configuration XML file are deleted and the status is displayed in the left panel.

For information on enabling the Bulk Configuration feature, see the “Bulk Configuration” section on page D-4. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating Stream Destination Bulk Configuration Files” section on page B-4.

Step 2  From the Subnet drop-down list, choose enter new.

To edit a subnet, choose the subnet from the Subnet drop-down list.
Step 3  Enter the subnet address and subnet mask and click Submit.

Note  If network address translation (NAT) is used for the STBs, be sure the IP subnet reflects the public, routeable IP address for the NAT device, not the internal private IP address of the STB.

Step 4  Choose the preference for each Stream Group. The preferences are:

- **High**—First preference of Streamer or Stream Group to stream to this subnet.
- **Medium**—Second preference of Streamer or Stream Group to stream to this subnet.
- **Low**—Lowest preference of Streamer or Stream Group to stream to this subnet.
- **None**—Do not use this Streamer or Stream Group to stream to this subnet.

Note  If your CDS network is deployed with a single-site steering configuration, you only see **High** and **None** as Stream Group Preference options, and only one Stream Group can have a preference of high.

For more information on creating Stream Groups, see the “Configuring Stream Groups” section on page 4-28.

Step 5  Click Submit.

To reset the fields, click Reset.

To delete a subnet, choose the subnet from the **Subnet** drop-down list, and click **Delete Subnet**.
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 4-4).

Figure 4-4 Bandwidth Manager Page

Step 2

Enter the Bandwidth Manager settings as appropriate. See Table 4-4 for descriptions of the fields.

Table 4-4 Bandwidth Manager Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Manager IP</td>
<td>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 4-73 for more information.</td>
</tr>
<tr>
<td>Bandwidth Manager Port</td>
<td>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>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>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>
</tbody>
</table>
Chapter 4 Configuring the CDS

System Level Configuration

Table 4-4 Bandwidth Manager Fields (continued) (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync Thread Pool</td>
<td>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 4-5).
Figure 4-5  Ingest Manager Page

To configure the Ingest Manager complete the fields below and click submit at the bottom of the page.

<table>
<thead>
<tr>
<th>General Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingest Manager Host: 16.7.4.124.1</td>
</tr>
<tr>
<td>Callback Port:</td>
</tr>
<tr>
<td>Additional Package Window: 7</td>
</tr>
<tr>
<td>FTP Timeout: 100 Sec.</td>
</tr>
<tr>
<td>Use Asset ID: No</td>
</tr>
<tr>
<td>Manage CORBA Services: No</td>
</tr>
<tr>
<td>Require Notify Service: Yes</td>
</tr>
<tr>
<td>Ingest Manager Debug: Low</td>
</tr>
<tr>
<td>Meta Data Publish: Enable</td>
</tr>
<tr>
<td>Meta Publish URL 1: <a href="https://admin4eps/56.74.124.1">https://admin4eps/56.74.124.1</a></td>
</tr>
<tr>
<td>Meta Publish URL 2:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ingest Interface:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
</tr>
<tr>
<td>INA</td>
</tr>
<tr>
<td>Cisco SOAP</td>
</tr>
<tr>
<td>Prodis SOAP</td>
</tr>
<tr>
<td>Notify Service Factory:</td>
</tr>
<tr>
<td>Event Channel ID:</td>
</tr>
<tr>
<td>Event Channel Kind:</td>
</tr>
<tr>
<td>factories ID:</td>
</tr>
<tr>
<td>factories Kind:</td>
</tr>
<tr>
<td>Package Channel ID:</td>
</tr>
<tr>
<td>Package Channel Kind:</td>
</tr>
<tr>
<td>Package Factory ID:</td>
</tr>
<tr>
<td>Package Factory Kind:</td>
</tr>
<tr>
<td>Package Factory Name:</td>
</tr>
<tr>
<td>Package Factory Server ID:</td>
</tr>
<tr>
<td>Cisco SOAP URL: <a href="http://16.7.4.124.38.75/CiscoSOAP">http://16.7.4.124.38.75/CiscoSOAP</a></td>
</tr>
<tr>
<td>Prodis SOAP URL:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Backoffice Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Retries: 6</td>
</tr>
<tr>
<td>Retry Interval: 3</td>
</tr>
<tr>
<td>Backoffice Timeout: 300 Sec.</td>
</tr>
<tr>
<td>New Backoffice: Choose a Backoffice...</td>
</tr>
<tr>
<td>Backoffice URL:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content Store Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Store: FSI</td>
</tr>
<tr>
<td>Content Store URL: <a href="http://16.6.2/2004/">http://16.6.2/2004/</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encryption Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption: Disable</td>
</tr>
<tr>
<td>Encryption URL:</td>
</tr>
<tr>
<td>Encryption FTP URL:</td>
</tr>
</tbody>
</table>

Submit  Reset

**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>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>Port number to use for listening for inbound connections.</td>
</tr>
<tr>
<td>Callback Port</td>
<td>Port number to use for File Services Interface (FSI) callbacks.</td>
</tr>
<tr>
<td>Additional Package Window</td>
<td>Additional time to wait after the package expiration window has been reached before destroying the content.</td>
</tr>
<tr>
<td>FTP Timeout</td>
<td>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 <strong>No</strong>. If set to <strong>No</strong>, 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>URL where the metadata is published, typically the backoffice.</td>
</tr>
<tr>
<td>Meta Publish URL #2</td>
<td>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: ISA, Cisco SOAP, Prodis SOAP; otherwise choose <strong>Disable</strong> to disable the Ingest Manager.</td>
</tr>
<tr>
<td>Name Service IP and Port</td>
<td>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>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>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>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>Directory extension of the Event Channel ID. The default is Context. ISA-only field.</td>
</tr>
<tr>
<td>Factories ID</td>
<td>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>
<tr>
<td>Factories Kind</td>
<td>Factories ID extension. The default is Context. 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>Package Channel ID</td>
<td>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>Event Channel Package ID extension. The default is Factory. ISA-only field.</td>
</tr>
<tr>
<td>Package Factory ID</td>
<td>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>Factories ID extension. The default is Factory. ISA-only field.</td>
</tr>
<tr>
<td>Package Factory Name</td>
<td>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>Numeric value that identifies the Package Factory Server for all ingests. The default is 90. ISA-only field.</td>
</tr>
<tr>
<td>Cisco SOAP URL</td>
<td>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>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>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>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></td>
<td>If the <strong>Retry Interval</strong> is set to zero, the Ingest Manager retries once every 6000 seconds (100 minutes).</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> By default, the Ingest Manager does not retry an expired package. Set the <strong>Retry Interval</strong>, as well as the <strong>Publish Time Adjustment</strong> field on the Input Channel page, so that if publishing a package fails, a retry can happen at least once before the start time of the recording. See the “Configuring Input Channels” section on page 4-23 for more information.</td>
</tr>
<tr>
<td>Backoffice Timeout</td>
<td>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 <strong>TotalManage</strong> to use the TotalManage backoffice support, otherwise choose <strong>Disable</strong> to disable backoffice support.</td>
</tr>
<tr>
<td>Backoffice URL</td>
<td>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: <strong>ISA</strong>, <strong>FSI</strong>, or <strong>NGOD</strong>. To disable the content store, choose <strong>Disable</strong>.</td>
</tr>
<tr>
<td>Content Store URL</td>
<td>URL where the content store is located.</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 Settings</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Choose Verimatrix, or Widevine to use encryption. Choose Disable to disable encryption.</td>
</tr>
<tr>
<td>Encryption URL</td>
<td>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>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 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 4-6).
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&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Authentication Manager resides on the master Streamer. Typically, the Authentication Manager IP address is the same as the master Streamer.</td>
</tr>
<tr>
<td>Authentication Manager Port&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Authentication Manager port number default is 7792. This port number is determined by the properties specifications of the Authentication Manager. If you need to change the port number, contact Cisco technical support.</td>
</tr>
<tr>
<td>EventIS Hostname</td>
<td>Hostname or IP address of the EventIS server.</td>
</tr>
<tr>
<td>EventIS Port</td>
<td>Port number on the EventIS server used to receive authentication requests.</td>
</tr>
<tr>
<td>TRAXIS SOAP Interface</td>
<td>IP address, port, and logical partition on the Streamer used to receive messages about session teardowns from TRAXIS.</td>
</tr>
<tr>
<td>Server Thread Pool</td>
<td>Number of threads in the Authentication Manager server pool that are used to process authentication requests for the duration of the connection. 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 turned off. Choose Low to have minimal information and error logging. 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 4-7).

**Figure 4-7 Ingest Tuning Page**

<table>
<thead>
<tr>
<th><strong>Ingest Tuning</strong></th>
<th><strong>Configure</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trick-Mode Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Editing the settings below will affect ingest on all vault servers on the Cisco CDSM. You may select up to 8 trick mode speeds, each of which can be either 11 or 19x (x). To change the default trick mode speeds edit the fields below and click Submit.</td>
<td></td>
</tr>
<tr>
<td><strong>Speed 1:</strong></td>
<td>Current Setting</td>
</tr>
<tr>
<td><strong>Speed 2:</strong></td>
<td>Current Setting</td>
</tr>
<tr>
<td><strong>Speed 3:</strong></td>
<td>Choose One...</td>
</tr>
<tr>
<td><strong>Speed 4:</strong></td>
<td>Choose One...</td>
</tr>
<tr>
<td><strong>Speed 5:</strong></td>
<td>Choose One...</td>
</tr>
<tr>
<td><strong>Speed 6:</strong></td>
<td>Choose One...</td>
</tr>
<tr>
<td><strong>Speed 7:</strong></td>
<td>Choose One...</td>
</tr>
<tr>
<td><strong>Speed 8:</strong></td>
<td>Choose One...</td>
</tr>
<tr>
<td>To change the values for these settings edit the fields above and click Submit below.</td>
<td>Submit</td>
</tr>
</tbody>
</table>

| **Ingest HPEG Settings** | | |
| Editing the Ingest HPEG Settings below will affect all ingest performed after the settings have been applied. These settings will be applied to all Vault and EBV servers managed by the CDSM. To change the default values for the Ingest HPEG Settings edit the fields below and click Submit at the bottom. | | |
| **Program ID Standardization:** | Current Setting | Default Value | |
| | Enabled | Disabled | |
| **PST:** | Enabled | Disabled | |
| | Disabled | | |
| | Disabled | | |
| | Disabled | | |
| | Disabled | | |
| To change the default values for these settings edit the fields above and click Submit below. | Submit |  |

**Step 2** Enter the ingest tuning settings as appropriate. See **Table 4-7** for descriptions of the fields.
Table 4-7  Ingest Tuning Fields

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

**Ingest MPEG Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program ID Standardization</td>
<td>If Program Identifier (PID) Standardization is enabled, MPEG-2 video assets have their PIDs standardized at ingest so that most assets use the same PIDs. It may be important that all assets use the same PIDs, for example, if multiple assets are going to be part of a playlist and you cannot guarantee that all assets were created with a consistent set of PIDs. The standard PID assignment follows the CableLabs recommendations (see MD-SP-VOD-CEP2.0-I02-070105). Any changes made to the asset are reversed if an FTP OUT is performed. Only standard audio/video assets that may be used in playlists have their PIDs standardized; data downloads, audio only, carousel files, and such other files are left unmodified. Changing the PIDs does not affect normal VOD playback of the asset.</td>
</tr>
<tr>
<td>PSI</td>
<td>When Program ID Standardization is enabled, you have an option to enable or disable PSI. Enabling Program ID Standardization only standardizes the PIDs, not the Program Specific Information (PSI). If you choose Enabled for PSI, the Program Association Table (PAT) and the Program Map Table (PMT) are standardized so that they do not vary at all between one piece of content and another. Use these settings progressively to try and resolve issues with playlists (black screen or no video after transitions, temporary glitches, and so on). Use Program ID Standardization only first, reingest the content, and play the content. If there are still problems, try both enabling Program ID Standardization and PSI. If there are problems playing the content back that was ingested with both of these options enabled, disable them and reingest the content to see if the issue resolves.</td>
</tr>
<tr>
<td>Sequence End Remove</td>
<td>If Sequence End Remove is enabled, a SEQ END header that is present at the end of the asset (and only at the end) is removed on ingest. Doing this allows fades between assets in a playlist, which can make the playlist appear more seamless. Any changes made to the asset is reversed if an FTP OUT is performed. Removing the SEQ END, if present, makes no difference to the VOD playback of the asset.</td>
</tr>
<tr>
<td>Rate Standardize</td>
<td>If Rate Standardize is enabled, MPEG-2 video assets have their rates standardized at ingest so that most assets use one of two standard rates, 3.75 Mbps for SD assets and 15 Mbps for HD assets. These settings follow CableLabs recommendations. Standardizing the rates can be helpful in certain configurations if playlists are going to be created containing multiple assets and you cannot guarantee that all assets were created with consistent rates. For example, some QAM devices do not handle rate changes during playout. Consult your QAM vendor for guidance on whether to enable Rate Standardize. Any changes to the asset are reversed if an FTP OUT is performed.</td>
</tr>
</tbody>
</table>
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 4-8).

**Step 2** Choose 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, choose an IP address or nickname from the drop-down list and click Display.
Configuring the Media Importer

Note

The Media Importer is part of the MediaX Suite, which is an optional feature.

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, as well as to configure the automatic import function.

To configure the Media Importer, do the following:

Step 1
Choose Configure > System Level > Media Importer. The Media Importer page is displayed (Figure 4-9).

Figure 4-9 Media Importer Page

Step 2
Enter the settings as appropriate. See Table 4-8 for descriptions of the fields.

Table 4-8 Media Importer Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Importer Settings</td>
<td></td>
</tr>
<tr>
<td>Importer Type</td>
<td>To upload the EPG using the CDSM, set the Importer Type to <strong>host</strong>. For information on uploading an EGP file, see the “Uploading an EPG File” section on page 7-10.</td>
</tr>
<tr>
<td>Transformer Type</td>
<td>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>Enable Auto Import</td>
<td>To automatically import the EPG information, check the <strong>Enable Auto Import</strong> check box. The Auto Import fields are displayed.</td>
</tr>
<tr>
<td>FTP Server IP</td>
<td>IP address of the FTP server that is used to send the EPG file.</td>
</tr>
</tbody>
</table>
Chapter 4 Configuring the CDS

System Level Configuration

Configuring Call Signs

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

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.

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 4-10).
Step 2 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>CallSign is a unique identifier for a program channel (content source).</td>
</tr>
<tr>
<td>Multicast IP</td>
<td>Multicast IP address of the device sending a Single Program Transport Stream (SPTS).</td>
</tr>
<tr>
<td>Port</td>
<td>Port associated with the CallSign.</td>
</tr>
</tbody>
</table>

Step 3 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 several 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 7-10.

**Caution** All channel default values specified on the Input Channels page 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 4-11).

**Figure 4-11 Input Channels Page**

<table>
<thead>
<tr>
<th>Input Channels</th>
<th>CONFIGURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>To configure a new channel map select “Add New Channel” from the list, complete the fields below, then click Submit. To remove a channel map select it from the list then click delete. All fields require a value.</td>
<td></td>
</tr>
</tbody>
</table>

- **Select Channel**
  - **Add New Channel**
  - **Channel Name**
  - **Multicast Group IP**
  - **Port**

**Channel Default Settings**

- **Channel Code**
- **Category ID**
- **Product**
- **Product ID**
- **Licensing Window Start**
- **License**
- **Publish Time Adjustment**
- **Audio Type**

- **Channel ID**
- **Category ID**
- **Provider**
- **Program Period**
- **License Window End**
- **Rating**
- **Suggested Price**

- **Submit**
- **Reset**
- **Delete**

**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 for ingesting content.

**Note** The combination of the IP address and port must be unique for each channel.

**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>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>Name of the provider.</td>
</tr>
<tr>
<td>Provider ID</td>
<td>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>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>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>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>Suggested price for each asset on this channel. The format is xx.xx.</td>
</tr>
<tr>
<td>Billing ID</td>
<td>Billing ID for every asset on this channel. This field applies only to the SA Tribune transformer type.</td>
</tr>
<tr>
<td>Audio Type</td>
<td>Audio types available for all assets on this channel (Dolby ProLogic, Dolby Digital, Stereo, Mono, Dolby 5.1).</td>
</tr>
</tbody>
</table>

**Step 6** Click **Submit**.

To reset the field, click **Reset**.
Note
You cannot delete a channel that has future scheduled events.

To view, edit, or delete a current channel setup, from the Select Channel drop-down list choose the channel. The Channel Setup page refreshes with the configuration for the channel selected. To delete the channel, click Delete. To edit the channel configuration, edit the fields and click Submit.

Configuring Source Output Ports

Note
The Source Output Port page is displayed when NGOD is selected as the RTSP Deployment Type on the CDSM Setup page. For more information, see the “RTSP Deployment Type” section on page D-8.

The Multiple SOPs feature introduces the ability to create SOP domains and associate a virtual IP address with each domain. The stream interfaces on the Streamer are grouped by using the Route Tables page and are associated with an SOP domain and virtual IP address. This allows for the grouping of the stream interfaces on a Streamer into two groups, each group associated with an SOP domain and virtual IP address, to direct traffic from the stream interfaces to two different routers.

The logical SOP appears to the other NGOD components as a single interface, but internally to the CDS, the logical SOP could represent multiple physical interfaces on multiple Streamers. All the physical interfaces of a logical SOP are directed to one router, while the interfaces of another logical SOP are directed to a different router. Each Streamer, defined by a logical SOP, connects to a different router.

In Release 2.1.1 and Previous Releases
In Release 2.1.1 and previous releases that were configured for an RTSP environment with an NGOD deployment, the CDSM provided a Server Level configuration page, the RTSP Setup page, which included configuration fields for the physical SOP IP and port and the logical SOP. The physical SOP IP and port were the IP address and port number of the gigabit Ethernet interface that was used as the SOP on the Streamer. The logical SOP was the domain name used for identification purposes to the On Demand Resource Manager (ODRM). The logical SOP (domain name of the SOP) was tied to the entire Streamer. The Streamer is part of a Stream Group, and a system can have multiple Stream Groups in a system, each supporting a different SOP.

The logical SOP domain name, maximum number of streams, and maximum bandwidth for each SOP are provided to the ODRM vendor, who uses this information along with the service group information, QAM device information, and so on, to configure the system.

In Release 2.1.2 and Later Releases
In Release 2.1.2 and later releases that were configured for an RTSP environment with an NGOD deployment, the SOP domain name and a virtual IP address are added through the Source Output Port page. Each group of stream interfaces on a Streamer are represented by a virtual IP address and SOP domain.

The stream interfaces (or stream/cache interfaces) on each Streamer connect to two routers, with half the interfaces directed to one router and the other half of the interfaces directed to the other router. This is accomplished by way of the Route Tables page. For more information, see the “Configuring the Route Table” section on page 4-63.
If there are three Streamers, for example, with stream interfaces 1 to 6 going to router 1 and stream interfaces 7 to 12 going to router 2, the following SOPs need to be created:

- SOP A is defined as interfaces 1 to 6 on Streamer 1, 2, and 3.
- SOP B is defined as interfaces 7 to 12 on Streamers 1, 2, and 3.

The Multiple SOP feature allows for stream routing control, provides balance across the routers, and provides redundancy in case of a transport network failure. If a stream interface fails, another stream interface in the same SOP takes over.

### Configuring Multiple SOPs

The following rules apply for the Multiple SOP feature:

- There is a one-to-one relationship between the SOP virtual IP address and domain name, and the stream interface subnet configured in the Route Tables page.
- SOP virtual IP address and domain name cannot span multiple source subnets and a source subnet cannot span multiple SOPs.
- SOP virtual IP address and domain name cannot span more than one Stream Group.

To configure the Multiple SOP feature, do the following:

**Step 1** Choose Configure > System Level > Source Output Port. The Source Output Port page is displayed.

**Step 2** In the **SOP Name** field, enter the domain name of this Streamer for identification purposes to the On Demand Resource Manager (ODRM). In Release 2.1.1 and previous releases, this was the Logical SOP field on the RTSP Setup page.

**Step 3** In the **Virtual IP** field, enter the virtual IP address for this SOP.

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

**Step 5** Repeat **Step 2** to **Step 4** for each SOP.

The configured SOPs are displayed in the bottom half of the page. To delete an SOP, check the **Delete** check box associated with the SOP and click **Submit**.

To complete the configuration of multiple SOPs, you must define each route in the Route Table page and choose **CServer Source** as the Route Type. For more information, see the “Configuring the Route Table” section on page 4-63.

### Array Level Configuration

The Array Level tab has the following configuration options:

- Configuring the Array Level DNS
- Configuring the Array Level NTP Server
- Configuring Stream Groups
- Locating Cache Groups
- Configuring Vault Groups
- Configuring SSV Groups
Chapter 4  Configuring the CDS

Array Level Configuration

- Configuring Cache Groups
- Mapping Vault Groups to Cache Groups
- Mapping Stream Groups to Cache-Fill Sources
- Mapping Vault Groups for Redundancy
- Configuring the Control and Setup IPs
- Configuring Cache-Fill Bandwidth Using Thin Pipe Mapping
- Configuring the Media Scheduler

Note: The Array Level configuration settings are distributed to all servers in the specified array.

Configuring the Array Level DNS

The Array DNS page is used to configure up to 16 domain suffixes and 16 DNS servers.

To view the current Array DNS settings for an Array Level, Choose Configure > Array Level > Array DNS, choose an array name from the drop-down list, and click Display.

Note: If you are upgrading the TV CDS software to Release 2.2 from Release 2.0 or an earlier release, the system prompts you to Submit any settings that have previous domain suffixes to populate the new DNS database structure.

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

Step 1 Choose Configure > Array Level > Array DNS. The Array DNS page is displayed.
Step 2 From the Array Name drop-down list, choose an array and click Display.
Step 3 Enter the DNS binding Array Level settings as appropriate. See Table 4-11 for descriptions of the fields.

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 Delete Entry.

Table 4-11 Array DNS Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New 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>
<tr>
<td>New DNS Server</td>
<td>IP address of the DNS server.</td>
</tr>
</tbody>
</table>

Cisco TV CDS 2.2 RTSP Software Configuration Guide
Configuring the Array Level NTP Server

The Array NTP Server page is used to configure up to 16 NTP servers. The clocks on all CDS servers (Vault, Streamer, and Caching Node) and the CDSM and VVIM in a CDS must be synchronized in order to retrieve the statistics on to the CDSM and VVIM.

To view the current NTP settings for an Array Level, choose Configure > Array Level > Array NTP Server, choose an array name from the drop-down list, and click Display.

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

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

**Step 2** From the Array Name drop-down list, choose an array and click Display.

**Step 3** In the New NTP Server field, enter the IP address of the NTP server.

**Step 4** Click Submit.

To clear the fields and start over, click Reset.

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

For information on setting the time zone on a CDS server or configuring NTP on a CDSM or VVIM, see “Other NTP Configurations” section on page 4-71.

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 subnet by the Stream Group preference. For more information about Stream Group and QAM gateway associations, see the “Configuring QAM Gateways” section on page 4-4. For more information about destination subnetworks and Stream Groups, see the “Configuring Stream Destinations” section on page 4-8.

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.

VVI with Split-Domain Management and HTTP Streamers

A VVI with split-domain management has one manager (VVIM) that manages the Vaults and Caching Nodes, and one manager (Stream Manager) that manages the Streamers.

When you use CCP Streamers in a VVI, all group IDs and server IDs need to be unique among all servers in the VVI. The VVIM manages all the group IDs and server IDs for the VVI with CCP Streamers. The Stream Manager gets an allotment of group IDs from the VVIM in one of two ways:

- During the initial installation, by way of the CDSM Setup page
- In the first-time configuration of Stream Groups
Communication between the VVI Manager and the Stream Manager is accomplished through database replication when CCP is used as the protocol.

The CDSM Setup page for the Stream Manager has a field for the VVIM IP address. The VVIM IP address is used to send an HTTP GET request to the VVIM for a range of group IDs. If the Stream Manager is unable to reach the VVIM, either because port 80 is not open for communication or some other connectivity reason, the Stream Group page displays a field for entering the beginning group ID. The administrator of the Stream Manager gets the beginning group ID from the administrator of the VVIM. The VVIM gets the beginning group ID on the Configuration Generator page. For more information, see the “Identifying Server IDs and Group IDs for VVI with Split-Domain Management” section on page 7-10.

For more information about the VVI settings on the CDSM Setup page, see the “Virtual Video Infrastructure” section on page D-6.

⚠️ **Caution**

The beginning group ID must be generated by the VVIM, and if manually entered, it must be entered correctly. Entering the wrong ID can cause cache-fill failures and other issues.

To configure a Stream Group, do the following:

**Step 1** Choose **Configure > Array Level > Stream Groups Setup**. The Stream Groups page is displayed (Figure 4-12).

To edit a Stream Group, choose the Stream Group from the drop-down list and click **Display**.

**Figure 4-12 Stream Groups Page**

![Stream Groups Page](image)

**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 use only 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 4-12.

### Table 4-12 Unassigned Streamer Options

<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, choose 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**.

**Caution**

If you delete a Stream Group or edit the members of a Stream Group, and the Stream Destination feature is enabled, you must re-submit each Stream Destination subnet that is associated with the Stream Group that you changed or deleted.

---

### Locating Cache Groups

The Cache Group Locator page is used by the Stream Manager in a VVI with split-domain management to identify and locate the Cache Groups that are managed by the VVIM. Split-domain management uses port 80 to communicate group IDs and server IDs. The databases for each domain are separate.

**Note**

The Cache Group Locator page is available only on the Stream Manager when VVI is enabled. For more information, see the “Virtual Video Infrastructure” section on page D-6.

There are two methods on the Cache Group Locator page for getting the Cache Group information:

- **Import**
- **Upload**

The **Import** option uses an HTTP GET request to communicate with the VVIM in retrieving the Cache Groups. The **Upload** option uploads an XML file that was created by the VVIM. To use the **Import** option, the Stream Manager must know the IP address of the VVIM and must be able to communicate with the VVIM over port 80. The VVIM IP address is set on the CDSM Setup page. See the “Virtual Video Infrastructure” section on page D-6 for more information. To use the Upload option, the XML file must be downloaded from the VVIM and delivered to the administrator of the Stream Manager. For more information on downloading the XML file from the VVIM, see the “Identifying Server IDs and Group IDs for VVI with Split-Domain Management” section on page 7-10.
To identify and locate the Cache Groups, do the following:

**Step 1** Choose **Configure > Array Level > Cache Group Locator**. The Cache Group Locator page is displayed (Figure 4-13).

**Figure 4-13 Cache Group Locator Page**

<table>
<thead>
<tr>
<th>Cache Group Locator CONFIGURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>To add Cache Group Locations, select “Add Cache Group Locations” from the select box below.</td>
</tr>
<tr>
<td>Configured Cache Locations: Add Cache Group Locations</td>
</tr>
</tbody>
</table>

Cache Groups can be created by importing the Cache Group Configurations from the VVIM/Cache Domain CDSM or by uploading the Cache Group Configuration XML file obtained from the VVIM/Cache Domain Administrator. Please choose one of the options below.

- Import
- Upload

**VVIM IP:** 172.32.97.265  
[Import Cache Groups]

**Step 2** From the **Configured Cache Locations** drop-down list, choose **Add Cache Group Locations**.

**Step 3** Choose either **Import** or **Upload**.

If you choose **Import**, do the following:

a. In the **VVIM IP**, enter the IP address of the VVIM.

   If the VVIM IP address was provided in the CDSM Setup page, or previously on the Cache Group Locator page, it is displayed in the **VVIM IP** field.

b. Click **Import Cache Groups**.

   The Stream Manager sends an HTTP GET request over port 80 to the VVIM for the Cache Group information. If the VVIM does not respond with the CacheGroupsConfig.xml file before the timeout period, the Cache Group Locator page displays the **Upload** option.

If you choose **Upload**, do the following:

a. Get the CacheGroupsConfig.xml file from the administrator of the VVIM and save it to a location you can access from the CDSM (for example, to your local machine).

b. Click **Browse** to locate the CacheGroupsConfig.xml file. The Choose File dialog box is displayed.

c. Navigate to the file and click **Open**. The path and filename are displayed in the Cache Groups File Location field.

d. Click **Upload**.

**Step 4** After the CacheGroupsConfig.xml file is either imported or uploaded, the Cache Groups are listed in the **Configured Cache Locations** drop-down list.

To view, edit, or delete a Cache Group Location, do the following:

**Step 1** Choose **Configure > Array Level > Cache Group Locator**. The Cache Group Locator page is displayed.
Step 2  From the Configured Cache Locations drop-down list, choose a Cache Group location. The page refreshes and the Cache Group information is displayed. The Location Virtual IP and Location Subnet fields are informational only.

Step 3  To rename the Cache Group Location, enter a new name in the Cache Location Name and click Submit. To reset the field, click Reset.

Step 4  To delete a Cache Group location, click Delete.

Configuring Vault Groups

A Vault Group consists of one or more Vaults. Vaults within a Vault Group work as a team with regard to content ingest, cache-fill responses, load distribution, and bandwidth usage. Vault Groups interact with other Vault Groups by passing cache-fill requests among each other based on performance qualification and cost considerations. For more information on Vault Group redundancy, see the “Mapping Vault Groups for Redundancy” section on page 4-39.

Note  The Vault Groups Setup page is part of the Vault Redundancy feature and is displayed only if Vault Redundancy is enabled. For more information, see the “Vault Redundancy” section on page D-5. If VVI is enabled, The Vault Groups Setup page is displayed only on the VVIM. For more information, see the “Virtual Video Infrastructure” section on page D-6.

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

When grouping Vaults you should consider network costs, bandwidth usage, and geographic locations of Vaults, Caching Nodes, and Streamers. All Vaults in a group are considered to have the same cost to reach a destination.

Note  In Release 2.2, the maximum number of Vault Groups is two.
To configure a Vault Group, do the following:

**Step 1** Choose **Configure > Array Level > Vault Groups Setup**. The Vault Groups Setup page is displayed (Figure 4-14).

![Vault Groups Setup Page](image)

**Figure 4-14  Vault Groups Setup Page**

- **Select Vault Group to View/Edit**
  - No
  - Display

  **"GO" Configuration**

  **Group Members**

<table>
<thead>
<tr>
<th>Server Hostname</th>
<th>New Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.22.97.161</td>
<td>No Change</td>
</tr>
<tr>
<td>172.22.97.55</td>
<td>No Change</td>
</tr>
</tbody>
</table>

  **Unassigned Vault Servers**

<table>
<thead>
<tr>
<th>Server Hostname</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.22.97.261</td>
<td>Don't Change</td>
</tr>
<tr>
<td>172.22.97.202</td>
<td>Don't Change</td>
</tr>
</tbody>
</table>

**Step 2** From the **Select Vault Group to View/Edit** drop-down list, choose **Add New Vault Group** and click **Display**.

To edit a Vault Group, choose the Vault Group from the drop-down list and click **Display**.

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

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

**Step 4** Add the Vaults to the Vault Group.

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

| Table 4-13  Unassigned Vault Options |
|-------------|-------------------------------------|
| **Unassigned Vault Option** | **Description** |
| No Change | Do not make any changes to the Vault Group assignment. |
| Vault Group Name | Add this Vault to this Vault Group. |
| None | Remove this Vault from this Vault Group. Applicable only to Vaults assigned to the selected Vault Group. |

**Step 5** Click **Submit**.

To reset the field, click **Reset**.
To view the members of a Vault Group, choose the Vault Group from the drop-down list and click Display.

To delete a Vault Group, first remove all Vaults from the group, then click Delete Group.

### Configuring SSV Groups

An SSV Group consists of one or more ISVs. ISVs within an SSV Group work as a team with regard to content ingest, cache-fill responses, load distribution, and bandwidth usage. SSV Groups interact with other SSV Groups by passing cache-fill requests among each other based on performance qualification and cost considerations.

The SSV Groups Setup page is part of the SSV Group feature and is displayed only if SSV Group is enabled. For more information, see the “SSV Groups” section on page D-5. The Vault Redundancy Map page and the Thin Pipe Map page are also displayed when SSV Groups is enabled. The Vault Redundancy Map page can be used to map SSV Groups for mirroring. For more information, see the “Mapping Vault Groups for Redundancy” section on page 4-39. The Thin Pipe Map page can be used to configure low-bandwidth connections among SSV Groups. For more information, see the “Configuring Cache-Fill Bandwidth Using Thin Pipe Mapping” section on page 4-42.

An ISV can never be a member of more than one SSV Group.

The term SSV used in the CDSM GUI is the same as the ISV. The terms are interchangeable.

When grouping ISVs you should consider network costs, bandwidth usage, and the geographic locations of the ISVs. All ISVs in a group are considered to have the same cost to reach a destination.

In Release 2.2, the maximum number of SSV Groups is two.

To configure an SSV Group, do the following:

**Step 1** Choose Configure > Array Level > SSV Groups Setup. The SSV Groups Setup page is displayed.

**Step 2** From the Select SSV Group to View/Edit drop-down list, choose Add New SSV Group and click Display.

To edit an SSV Group, choose the SSV Group from the drop-down list and click Display.

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

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

**Step 4** Add the SSVs (ISVs) to the SSV Group.

The unassigned SSVs are listed along with a drop down-list for each that offers the options described in Table 4-14.
Configuring Cache Groups

A Cache Group consists of one or more Caching Nodes. Caching Nodes within a Cache Group work as a team with regard to content caching, load distribution, and bandwidth usage. Cache Groups interact with other Cache Groups by passing cache-fill requests among each other based on performance qualification and cost considerations. If a Cache Group must give up a cache-fill task to another group, Cache Group preferences set on the Stream to Cache Map page are followed.

A Caching Node can never be a member of more than one Cache Group.

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

To configure a Cache Group, do the following:

Step 1 Choose Configure > Array Level > Cache Groups Setup. The Cache Groups Setup page is displayed (Figure 4-15).
Chapter 4      Configuring the CDS

Array Level Configuration

Step 2  From the Select Cache Group to View/Edit drop-down list, choose Add New Cache Group and click Display.

To edit a Cache Group, choose the Cache Group from the drop-down list and click Display.

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

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

Step 4  For a VVI that uses HTTP for communication between the Caching Nodes and Streamers, do the following:

a. In the Location Virtual IP field, enter the IP address this Cache Group uses as the virtual IP address for the Locate Port service. The virtual IP address is bound to the Locate IP and Port. For more information about the Locate Port service, see the “HTTP Streamers” section on page 2-9.

b. In the Location Subnet Mask field, enter the subnet mask for the Location IP address.

Step 5  Add the Caching Nodes to the Cache Group.

The unassigned Caching Nodes are listed along with a drop-down list for each that offers the options described in Table 4-15.

Table 4-15  Unassigned Caching Node Options

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

Step 6  Click Submit.
To reset the field, click Reset.

To view the members of a Cache Group, choose the Cache Group from the drop-down list and click Display.

To delete a Cache Group, first remove all Caching Nodes from the group, then click Delete Group.

**Mapping Vault Groups to Cache Groups**

The Cache To Vault Map page is used to map Vault Groups to Cache Groups in a VVI. Before you can map Vault Groups to Cache Groups, you must create them. For more information, see the “Configuring Cache Groups” section on page 4-35 and the “Configuring Vault Groups” section on page 4-32.

**Note**
The Cache To Vault Map page only displays on the VVIM and is available only when Vault Redundancy and VVI are both enabled. For more information, see the “Vault Redundancy” section on page D-5 and the “Virtual Video Infrastructure” section on page D-6.

To map Vault Groups to Cache Groups, do the following:

**Step 1** Choose Configure > Array Level > Cache To Vault Map. The Cache To Vault Map page is displayed.

**Step 2** From the Cache Group drop-down list, choose a Cache Group and click Select. All available Vault Groups are displayed. By default, all preferences are set to None.

**Step 3** Choose the preference setting for each Vault Group. Following are the possible preferences:
- High—First preference as a source for cache-fill requests.
- Medium—Second preference as a source for cache-fill requests.
- Low—Lowest preference as a source for cache-fill requests.
- None—Do not use this Vault Group as a cache-fill source.

Groups with the same preference level are considered equally as a cache-fill source. At least one Vault Group must have a preference higher than None.

**Step 4** Click Submit.

To reset the field, click Reset.

To view the Vault Group mappings of a Cache Group, choose the Cache Group from the drop-down list and click Display.

To delete a Cache Group or a Vault Group, see the “Configuring Cache Groups” section on page 4-35 or the “Configuring Vault Groups” section on page 4-32. When a Cache Group is deleted, the mapping for the Cache Group is also deleted, and any mapping to the Cache Group in the Stream To Cache Map page is also deleted. When a Vault Group is deleted, the Vault Group is removed from each Cache Group mapping; any mapping for the Vault Group in the Vault Redundancy Map page is also deleted.
Mapping Stream Groups to Cache-Fill Sources

The Stream To Cache Map page is used to map Cache Groups to Stream Groups in a VVI. Before you can map Cache Groups to Stream Groups, you must create them. See the “Configuring Stream Groups” section on page 4-28 and the “Configuring Cache Groups” section on page 4-35 for more information.

In a VVI with split-domain management, the Stream Manager must know about the Cache Groups to map the Stream Groups to the Cache Groups. See the “Locating Cache Groups” section on page 4-30 for more information.

**Note**

The Stream To Cache Map page is available only on the Stream Manager when VVI is enabled. For more information, see the “Virtual Video Infrastructure” section on page D-6.

Streamers can be used as cache-fill sources when Streamer is Cache is enabled on the Server Setup page (“Configuring the Servers,” page 4-56). A Stream Group is available on the Stream To Cache Map page when at least one Streamer in a Stream Group has Streamer is Cache enabled.

To map Cache Groups to Stream Groups, do the following:

**Step 1** Choose Configure > Array Level > Stream To Cache Map. The Stream To Cache Map page is displayed (Figure 4-16).

**Figure 4-16 Stream To Cache Map Page**

To begin select a Stream Group from the list, then select a preference for each Cache Group, as cache capable Stream Group, for the selected Stream Group. Cache Groups that have been configured but currently have no member Cache servers are highlighted, and may only have a preference of None. Click Submit at the bottom of the form to save the configuration.

**Step 2** From the Stream Group drop-down list, choose a Stream Group and click Select. All available Cache Groups and Stream Groups are displayed. By default, all preferences are set to None.

**Step 3** Choose the preference setting for each Cache Group and Stream Group. The possible preferences are:

- High—First preference as a source for cache-fill requests.
- Medium—Second preference as a source for cache-fill requests.
- Low—Lowest preference as a source for cache-fill requests.
• None—Do not use this Cache Group or Stream Group as a cache-fill source. Groups with the same preference level are considered equally as a cache-fill source. At least one Cache Group must have a preference higher than None.

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

To view the Cache Group mappings of a Stream Group, choose the Stream Group from the drop-down list and click Display.

To delete a Stream Group or Cache Group, see the “Configuring Stream Groups” section on page 4-28 or “Configuring Cache Groups” section on page 4-35. When a Stream Group is deleted, the mapping for the Stream Group is also deleted. When a Cache Group is deleted, the Cache Group is removed from each Stream Group mapping, and any mapping for that Cache Group in the Vault To Cache Map page is also deleted. When a Vault Group is deleted, the Vault Group is removed from each Stream Group mapping, and any mapping for the Vault Group in the Vault Redundancy Map page is also deleted.

Mapping Vault Groups for Redundancy

The Vault Redundancy Map page is used to map Vault Groups to each other. Before you can map Vault Groups for redundancy, you must create them. See the “Configuring Vault Groups” section on page 4-32 for more information.

Note
The Vault Redundancy Map page is part of the Vault Redundancy feature and is displayed only if Vault Redundancy is enabled. If VVI is enabled, The Vault Redundancy Map page is displayed only on the VVIM. For more information, see the “Virtual Video Infrastructure” section on page D-6 and the “Vault Redundancy” section on page D-5.

Note
In Release 2.2, the maximum number of Vault Groups is two.

Vault Groups interact with other Vault Groups by passing cache-fill requests among each other based on performance qualification and cost considerations. If a Vault Group must give up a cache-fill task to another group, Vault Group preferences set on the Vault Redundancy Map page are followed. For more information on Vault Group redundancy, see the “Vault Group Redundancy” section on page 1-10.

To map a Vault Group to another Vault Group, do the following:

Step 1
Choose Configure > Array Level > Vault Redundancy Map. The Vault Redundancy Map page is displayed (Figure 4-17).
Step 2  From the Vault Group drop-down list, choose Vault Group and click Select. All available Vault Groups are displayed. By default, all preferences are set to Ignore.

Step 3  Choose the preference setting for the Vault Group. The possible preferences are:

- **Mirror**—Content is mirrored to this Vault Group, and this Vault Group becomes the source for content requests from Streamers or Caching Nodes if the primary Vault Group becomes unavailable.

- **Ignore**—Do not use this Vault Group for mirroring or as a backup source of content.

Groups with the same preference level are considered equally as a cache-fill source. At least one Cache Group must have a preference higher than None.

Step 4  Click Submit.

To reset the field, click Reset.

To view the Vault Group mappings, choose the Vault Group from the drop-down list and click Display.

To delete a Vault Group, see the “Configuring Vault Groups” section on page 4-32. When a Vault Group is deleted, the mapping for the Vault Group is also deleted.

### 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. In an RTSP environment, the Setup server and Control server must be the same server.

**Note**

In an RTSP environment that uses VVI with split-domain management, each Stream Manager is allotted two Setup IDs for the Setup servers. If the Stream Manager uses both Setup IDs, it contacts the VVIM for additional Setup IDs. If the VVIM is unreachable, the Control/Setup IP page displays the Setup ID field for manual entry of the new Setup IDs. For more information, see the “Identifying Server IDs and Group IDs for VVI with Split-Domain Management” section on page 7-10.
Chapter 4  Configuring the CDS

Array Level Configuration

The Control server is used to communicate with Lightweight Stream Control Protocol (LSCP) clients or
Real Time Streaming Protocol (RTSP) clients. Each Control server handles up to 6000 clients. You must
configure a Control server for each group of up to 6000 clients. For instance, if you have 7000 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 2-8.

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**

<table>
<thead>
<tr>
<th>Stream Group</th>
<th>Control/Setup IP</th>
<th>Subnet Mask</th>
<th>IP Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>#91</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>Control/Setup IP</td>
</tr>
<tr>
<td>#92</td>
<td>192.168.2.2</td>
<td>255.255.255.0</td>
<td>Control/Setup IP</td>
</tr>
<tr>
<td>#96</td>
<td>192.168.3.3</td>
<td>255.255.255.0</td>
<td>Control/Setup IP</td>
</tr>
</tbody>
</table>

**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 4-16** for descriptions of the types.

**Table 4-16  Control/Setup Types**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control IP</td>
<td>IP address used only for LSCP or RTSP client control.</td>
</tr>
<tr>
<td>Setup IP</td>
<td>IP address of the Setup server.</td>
</tr>
<tr>
<td>Control/Setup IP</td>
<td>Control/Setup IP address used for LSCP or RTSP client control.</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 Cache-Fill Bandwidth Using Thin Pipe Mapping

The Thin Pipe Map page allows you to configure low-bandwidth connections between local and remote groups. A local group consists of servers in the same group, for example, all the Streamers in a Stream Group are considered part of the same group, or local group. A local group consists of CDS servers in the same local area network (LAN). A remote group consists of all the servers in the other Stream Groups, Cache Groups, and Vault Groups. A remote group consists of all the CDS servers that are reachable by way of a wide area network (WAN).

There can be multiple thin pipes configured for each local group. As an example, a site with Caching Nodes organized into a Cache Group could have one 500-Mbps thin pipe going to a site with a Vault Group, and a second 500-Mbps thin pipe going to a location with a Stream Group. The thin pipes are completely independent of each other.

The Thin Pipe Map page also allows for the configuration of thin pipes in a hierarchy, where a remote group must be reached through several pipes. For example, a Cache Group could have a 500 Mbps thin pipe over which it streams to multiple Stream Groups. Each Stream Group could have separate 100 Mbps thin pipes. In this case, the Cache Group traffic on egress to all Stream Groups is limited to 500 Mbps, while ingress traffic to each Stream Group from this Cache Group is limited to 100 Mbps. In this example, the Cache Group would have four thin pipes configured: one 500 Mbps pipe to all three Stream Groups, and a total of three 100 Mbps pipes, one to each individual Stream Group.

---

**Note**

The Thin Pipe Map page is displayed only if Thin Pipe Management is enabled. See the “Thin Pipe Management” section on page D-6 for more information.

For CCP traffic to work properly in the CDS, the following configuration must exist:

- Thin pipe mapping must be configured in the CDS.
- DiffServ AF settings must be configured on the CDS servers.
- Routers must support the bandwidths that are configured for the thin pipe mapping on the CDS.

---

**Note**

The configured bandwidth for CCP on the Thin Pipe Map page must be the minimum bandwidth reserved for the AF class. The sum of the bandwidths of all physical links configured for CCP among all sites must be less than the bandwidth configured for the AF class reserved for CCP.

CCP is used as the protocol among Vaults and Caching Nodes in a VVI that uses HTTP, and among all servers in a VVI that uses CCP and in all non-VVIs. The AF class is configured on each CDS server. See the “Configuring the Servers” section on page 4-56 for more information.

As an example, Figure 4-19 shows the maximum bandwidth available for the various groups in a Virtual Video Infrastructure (VVI) system with two super headends (SHEs), three caching sites, and one streaming site.
The maximum bandwidth available is dictated by the physical link, as well as by any network design constraints placed on bandwidth availability. If a switched network has further restrictions, for example, Vault Group 1 (VG1) to Vault Group 2 (VG2) and Cache Group 3 (CG3) share a 3 Gbps link on the route between VG1 and the other two sites, then another thin pipe must be configured to specify this 3-Gbps restriction.

Table 4-17 lists the thin pipe mappings that would be configured for the different Vault Groups illustrated in Figure 4-19.

### Table 4-17 Thin Pipe Mappings for Thin Pipe Example

<table>
<thead>
<tr>
<th>Thin Pipe Map</th>
<th>Remote Group</th>
<th>Bandwidth (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vault Group 1 (VG1)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VG1toAll</td>
<td>Vault Group 2, Cache Group 1, Cache Group 2, Cache Group 3</td>
<td>5</td>
</tr>
<tr>
<td>VG1toVG2</td>
<td>Vault Group 2</td>
<td>4</td>
</tr>
<tr>
<td>VG1toCG1</td>
<td>Cache Group 1</td>
<td>2</td>
</tr>
<tr>
<td>VG1toCG2</td>
<td>Cache Group 2</td>
<td>2</td>
</tr>
<tr>
<td>VG1toCG3</td>
<td>Cache Group 3</td>
<td>2</td>
</tr>
<tr>
<td><strong>Vault Group 2 (VG2)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VG2toAll</td>
<td>Vault Group 1, Cache Group 1, Cache Group 2, Cache Group 3</td>
<td>4</td>
</tr>
<tr>
<td>VG2toCG1</td>
<td>Cache Group 1</td>
<td>2</td>
</tr>
<tr>
<td>VG2toCG2</td>
<td>Cache Group 2</td>
<td>2</td>
</tr>
<tr>
<td>VG2toCG3</td>
<td>Cache Group 3</td>
<td>2</td>
</tr>
<tr>
<td><strong>Cache Group 1 (CG1)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CG1toAll</td>
<td>Vault Group 1, Vault Group 2, Cache Group 2, Cache Group 3</td>
<td></td>
</tr>
</tbody>
</table>
The thin pipes configured in Table 4-17 ensure that the bandwidth for Vault Group 1 never exceeds the maximum bandwidth available for Vault Group 1, which is 5 Gbps. This means that even if all remote groups were requesting cache fills from Vault Group 1, which would be a maximum throughput of 9 Gbps, the actual maximum bandwidth of cache-fill traffic coming from Vault Group 1 would never exceed 5 Gbps.

To configure a Thin Pipe Map, do the following:

Choose Configure > Array Level > Thin Pipe Map. The Thin Pipe Map page is displayed (Figure 4-20).

**Figure 4-20 Thin Pipe Map Page**

<table>
<thead>
<tr>
<th>Thin Pipe Map</th>
<th>Remote Group</th>
<th>Bandwidth (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CG2toSG1</td>
<td>Stream Group 1</td>
<td>3</td>
</tr>
<tr>
<td><strong>Cache Group 2 (CG2)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CG2toAll</td>
<td>Vault Group 1, Vault Group 2, Cache Group 1, Cache Group 3</td>
<td>2</td>
</tr>
<tr>
<td><strong>Cache Group 3 (CG3)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CG3toAll</td>
<td>Vault Group 1, Vault Group 2, Cache Group 1, Cache Group 3</td>
<td>2</td>
</tr>
</tbody>
</table>

The maximum bandwidth entered applies to each server in the group. For example, if the maximum bandwidth between two groups is designed as 5 Gbps (5000 Mbps) and there are two servers in each group, then the entered amount should be 2500 Mbps (5000 Mbps divided by the number of servers in the group).
Note: The maximum bandwidth threshold is 75 percent of the Max Bandwidth field.

Step 9: In the Available Remote Groups area, check the check box next to each remote group that you want to use this maximum bandwidth restriction.

Step 10: Check the Limit HTTP check box if this thin pipe is to limit the bandwidth between Caching Nodes and Streamers in a VVI that uses HTTP as the caching protocol.

Step 11: Click Submit.
   To reset the field, click Reset.

To delete a thin pipe mapping, choose the pipe name from the Configured Pipes drop-down list, click Select, and click Delete.

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 7-10 and the “Configuring Input Channels” section on page 4-23 for more information.

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

Note: 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 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 4-21).

Figure 4-21  Media Scheduler Page—User Preferences

<table>
<thead>
<tr>
<th>Media Scheduler CONFIGURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Preferences</td>
</tr>
<tr>
<td>Preference Editor:</td>
</tr>
<tr>
<td>○ Hide On Return</td>
</tr>
<tr>
<td>○ Show On Return</td>
</tr>
<tr>
<td>Action on Recurring Sched (Only for user generated schedules)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Package Name Preferences</td>
</tr>
<tr>
<td>You can choose between auto generating a package name using the start time stamp or entering the package name manually, if the package name we tried to create already exists.</td>
</tr>
<tr>
<td>○ Auto generate</td>
</tr>
<tr>
<td>○ Don’t auto generate</td>
</tr>
<tr>
<td>Channels To Schedule</td>
</tr>
<tr>
<td>[Select All]</td>
</tr>
<tr>
<td>Channel1</td>
</tr>
<tr>
<td>Channel2</td>
</tr>
<tr>
<td>Channel3</td>
</tr>
<tr>
<td>Channel4</td>
</tr>
<tr>
<td>Channel5</td>
</tr>
<tr>
<td>Channel6</td>
</tr>
</tbody>
</table>

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 Existing 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 4-50.

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.
To create new channels, see the “Configuring Input Channels” section on page 4-23.

**Step 6**

Click **Save** to save the settings. The calendar is displayed (Figure 4-22).

**Figure 4-22**  **Media Scheduler Page—Calendar**

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

---

**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 4-22). If Show On Return was selected in the User Preferences, the User Preferences are displayed (Figure 4-21).

**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 4-23).
Depending on the status of the schedule, the schedule 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 4-24).
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 4-50.

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

Tip  The Bulk Schedule option allows you to schedule the events for multiple channels at the same time. To schedule all channels or a group of channels for a whole day, click Bulk Schedule. The Bulk Schedule dialog box is displayed. Check the check box next to each channel and click Submit. If all required metadata information is available, this method schedules all the timeslots for the day. To check all the channels, check Select All. To uncheck all the channels, check Unselect All. The field alternates from Select All to Unselect All fields.

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.
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 4-25).

**Figure 4-25  Package Metadata Editor—User-Generated Timeslot**

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 4-26).

*Figure 4-26  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 4-18** for descriptions of the Recurring Schedule fields.

**Table 4-18  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>Recurrence Pattern is repeated for one year from the metadata Start Time.</td>
</tr>
<tr>
<td></td>
<td>End After</td>
<td>Recurrence Pattern is repeated the number of times you specify in the occurrences field.</td>
</tr>
<tr>
<td></td>
<td>End By</td>
<td>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 4-45 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 4-27).

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

**Figure 4-27 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>02:00:00</td>
<td>03:00:00</td>
</tr>
<tr>
<td>3</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>03:00:00</td>
<td>03:30:00</td>
</tr>
<tr>
<td>4</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>04:00:00</td>
<td>04:30:00</td>
</tr>
<tr>
<td>5</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>05:00:00</td>
<td>05:30:00</td>
</tr>
<tr>
<td>6</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>06:00:00</td>
<td>07:00:00</td>
</tr>
<tr>
<td>7</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>07:00:00</td>
<td>08:00:00</td>
</tr>
<tr>
<td>8</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>08:00:00</td>
<td>09:00:00</td>
</tr>
<tr>
<td>9</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>09:00:00</td>
<td>10:00:00</td>
</tr>
<tr>
<td>10</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>10:00:00</td>
<td>11:00:00</td>
</tr>
<tr>
<td>11</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>11:00:00</td>
<td>12:00:00</td>
</tr>
<tr>
<td>12</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>12:00:00</td>
<td>13:00:00</td>
</tr>
<tr>
<td>13</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>13:00:00</td>
<td>14:00:00</td>
</tr>
<tr>
<td>14</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>14:00:00</td>
<td>15:00:00</td>
</tr>
<tr>
<td>15</td>
<td>CHAN1</td>
<td>June-3-2008</td>
<td>15:00:00</td>
<td>16:00:00</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 4-25). Fill in the metadata as required and click **Submit.** The Package Metadata Editor window closes.

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

After a server has been initially configured (see the “Initially Configuring the Devices” section on page 3-1), the CDSM detects it and the IP address or nickname of the server 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
- Configuring the Server Level NTP
- 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 4-19.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Reserves an Ethernet interface to allow optimal configuration.</td>
</tr>
<tr>
<td>Management</td>
<td>Communicates with other network devices with regards to condition of the server, stream control, and ISA communications.</td>
</tr>
<tr>
<td>Ingest</td>
<td>Establishes connectivity with a content provider system and to ingest content on to a Vault or an ISV.</td>
</tr>
<tr>
<td>Cache</td>
<td>Transports content between Vaults and Streamers, or in the case of VVI, between Vaults, Caching Nodes, and Streamers.</td>
</tr>
<tr>
<td>Stream/Cache</td>
<td>Used on the Streamer for both cache and streaming traffic. If an interface is configured for both cache and streaming traffic on a Streamer, priority will 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>Transports streams to the QAM devices, or to subnets in the case of IPTV.</td>
</tr>
</tbody>
</table>
Chapter 4      Configuring the CDS

Server Level Configuration

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, stream/cache, stream control, or locate, as appropriate for the server

To configure the interface settings, do the following:

**Step 1** Choose **Configure > Server Level > Interface Setup**. The Interface Setup page is displayed (Figure 4-28).

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

---

<table>
<thead>
<tr>
<th>Table 4-19 CDS Interfaces (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stream Control</strong></td>
</tr>
<tr>
<td><strong>Locate</strong></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, stream/cache, stream control, or locate, as appropriate for the server
Step 3  Choose 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

After a server has been initially configured, the CDSM detects it and the IP address or nickname of the server 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 the IP address or nickname of the server and click **Display**.

**Step 3** The fields differ for a Vault, Streamer, and ISV server. Figure 4-29 shows the Server Setup for a Vault. Figure 4-30 shows the Server Setup for a Streamer. The ISV server setup page has a combination of the Vault and Streamer fields. See Table 4-21 for descriptions of the fields and to which server they apply. The fields for the Caching Node setup page are described in Table 4-21.

Table 4-20 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

<table>
<thead>
<tr>
<th>CDSM GUI ID Name</th>
<th>CServer Files ID Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array ID on the Array Name page</td>
<td>groupid</td>
</tr>
<tr>
<td>Group ID on the Server-Level pages</td>
<td>groupid</td>
</tr>
<tr>
<td>Stream Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Cache Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Vault Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Stream Group ID on the Configuration Generator page</td>
<td>arrayid</td>
</tr>
</tbody>
</table>
### Figure 4-29  Server Setup–Vault Server Page

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

<table>
<thead>
<tr>
<th>Server IPs</th>
<th>172.22.97.181</th>
<th>Display</th>
</tr>
</thead>
</table>

Current settings for (172.22.97.181). To make changes to these settings, edit the field you wish to change and click Submit Below.

**4U SATA 1U: Vault**

- **Server ID:** 691  **Group ID:** 69182

<table>
<thead>
<tr>
<th>Hostname</th>
<th>a181</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL</td>
<td>10</td>
</tr>
<tr>
<td>NAT Screening</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Default Streams/Cache Settings**

- **Source IP:** 10.166.287.155
- **Cache Port:** 40070

**Ingest MPEG Settings**

- **Bit Standardization:** Disabled
- **Receive End Pt:** Disabled
- **Rate Standardization:** Disabled

**Jumbo Frames Support**

- **Cache Jumbo Frames:** Enabled/Disabled

**Server Status**

- **Server Upgrade:** Disabled
- **Vault Mirror Copies:** 2
- **Vault Local Copies:** 1

**Cache IP Packets**

- **Cache Differentiated Services Code Point:** 8 (63)

**Cache Priority**

- **Current Forwarding Class:** AF11

**FTP Out Settings**

- **FTP Out Interface:** Management
- **FTP Out Bandwidth:** max 1000Mbps
- **FTP Out Sessions:** 0-10

**Ethernet Interface Settings**

#### 4U (Management)

- **Management IP:** 172.22.97.181
- **Gateway:** 172.22.97.255
- **Subnet Mask:** 255.255.255.0

#### 4U (Ingress)

- **Ingress IP:** 102.168.102.181
- **Ingress Subnet Mask:** 255.255.255.0

#### 4U (Egress)

- **Egress IP:** 102.168.102.181
- **Egress Subnet Mask:** 255.255.255.0
Figure 4-30  Server Setup—Streamer Server Page

Server Setup CONFIGURE

Select the ID of the specific server that you wish to add and click Display.

Server ID: 192.22.37.150  Display

Current settings for (192.22.37.150). To make changes to these settings, edit the field you wish to change and click Submit below.

**CDR228-ZE2-Cs Streamer**

Server Name:

**Server ID:** 190  **Group ID:** 190190

Hostname: streamer190

TTL: 10

Null Streaming: Enabled

Default Stream/Cache Settings

**Source IP:** 192.0.0.2

**Starting Transport Port:** 4473

**Ending Transport Port:** 4473

**Cache Port:** 4473

**Stream Group Info**

**Stream Group Name:** StreamGroup

**Stream Group ID:** 1

**Stream In Cache:** Enabled

**Jumbo Frame Support**

**Enable Jumbo Frames:** Enabled

**Enable Jumbo Frames:** Disabled

**Server Status**

**Server Status:** Disabled

**Transport/Cache IP Packets**

**Transport**

**Differential Services Code Point:** 0 (0x0)

**Cache**

**Differential Services Code Point:** 0 (0x0)

**HTTP**

**Differential Services Code Point:** 0 (0x0)

**Cache Priority**

**Enabled Forwarding Class:** 0.75

**Ethernet Interface Settings**

**eth0 (Management)**

**Management IP:** 192.22.37.150

**Gateway:** 192.22.37.129

**Subnet Mask:** 255.255.255.0

**eth1 (Not Used)**

**eth2 (Stream/Cache)**

**Source IP:** 192.168.195.2

**Transport Port:**

**Cache Port:**

**Source IP:**

**Transmit Rate:**

**Receive Rate:**

**Stream/Cache**

**Source IP:**

**Transmit Rate:**

**Receive Rate:**
### Table 4-21 Server Setup Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Fully qualified hostname for this server. The name can be up to 64 characters long. 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, Caching Node, Streamer, ISV</td>
</tr>
<tr>
<td>TTL</td>
<td>IP time to live (TTL) for data packets. The IP TTL default is 16 hops. Valid entries range from 0 to 255.</td>
<td>All servers</td>
</tr>
<tr>
<td>Null Streaming</td>
<td>From the <strong>Null Streaming</strong> drop-down list, choose <strong>Enabled</strong> to allow the streaming of null MPEG files, or <strong>Disabled</strong> to prevent the streaming of null MPEG files.</td>
<td>All servers</td>
</tr>
<tr>
<td>Default Stream/Cache Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>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>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>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>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>Ingest MPEG Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PID Standardization</td>
<td>This field is informational only. If this field is set to enable, then MPEG-2 video assets have their program identifiers (PIDs) standardized at ingest so that most assets use the same PIDs. To change the settings of the Ingest MPEG fields, see the “Configuring Ingest Tuning” section on page 4-17.</td>
<td>Vault</td>
</tr>
<tr>
<td>Sequence End Remove</td>
<td>This field is informational only. If this field is set to enable, a SEQ END header that is present at the end of the asset (and only at the end) is removed on ingest. To change the settings of the Ingest MPEG fields, see the “Configuring Ingest Tuning” section on page 4-17.</td>
<td>Vault</td>
</tr>
<tr>
<td>Rate Standardize</td>
<td>This field is informational only. If this field is set to enable, then MPEG-2 video assets have their rates standardized at ingest so that most assets use one of two standard rates, 3.75 Mbps for SD assets or 15 Mbps for HD assets. To change the settings of the Ingest MPEG fields, see the “Configuring Ingest Tuning” section on page 4-17.</td>
<td>Vault</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 informational only. To configure Stream Groups, see the “Configuring Stream Groups” section on page 4-28.</td>
<td>Streamer, ISV</td>
</tr>
</tbody>
</table>
Chapter 4  Configuring the CDS

Server Level Configuration

Streamer Is Cache

If Streamer Is Cache is enabled, the Streamer can be used as a possible cache-fill source by a Streamer in a different Stream Group. All Stream Groups that have at least one Streamer with Streamer Is Cache enabled are displayed on the Stream to Cache Map page, where the Stream Group can be selected as a possible cache-fill source and given a preference. Only the Streamers with Streamer Is Cache enabled are used as possible cache-fill sources. The protocol used for cache-fill responses from Streamers is always CCP. For more information, see the “Mapping Stream Groups to Cache-Fill Sources” section on page 4-38.

### Cache Group Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Group ID</td>
<td>These fields display the Cache Group Name and Cache Group ID the Caching Node is a member of. The Cache Group Name is informational only. To configure Cache Groups, see the “Configuring Cache Groups” section on page 4-35.</td>
<td>Caching Node</td>
</tr>
</tbody>
</table>

### Vault Group Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vault Group ID</td>
<td>These fields display the Vault Group Name and Vault Group ID the Vault is a member of. The Vault Group Name is informational only. To configure Vault Groups, see the “Configuring Vault Groups” section on page 4-32.</td>
<td>Vault</td>
</tr>
</tbody>
</table>

### Jumbo Frames Support

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<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 have 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 have 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 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>
</tbody>
</table>

### Server Status

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Offload</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>Choose 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 are stored on this server.</td>
<td>Vault, ISV</td>
</tr>
</tbody>
</table>
**Table 4-21  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, and HTTP IP Packets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport 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 to 63.</td>
<td>All servers</td>
</tr>
<tr>
<td>Cache Differentiated Services Code Point</td>
<td>Note: DSCP is set separately for cache and transport interfaces. DSCP can also be set for HTTP Streamers when HTTP is selected as the cache-fill protocol for VVI on the CDSM Setup page.</td>
<td></td>
</tr>
<tr>
<td>Cache Priority</td>
<td>From the Cache Priority drop-down list, choose an AF class. For more information, see the “Configuring QoS Settings” section on page 4-63.</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>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. The range is 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>IP address of the management interface on this server.</td>
<td>All servers</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the gateway to the network.</td>
<td>All servers</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask that defines the subnetwork for this server.</td>
<td>All servers</td>
</tr>
<tr>
<td>FTP Listener</td>
<td>Choose 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>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>Subnet mask that defines the subnetwork for this interface.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td><strong>Locate Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locate Interface IP</td>
<td>IP address for this interface. The Locate Interface is used by the Locate Port service for communications with third-party streamers that use HTTP to communicate.</td>
<td>Caching Node</td>
</tr>
<tr>
<td>Locate Port</td>
<td>Port number used for communication with HTTP Streamers. CCP Streamers do not use the Locate Port; instead, they load-balance locate requests across fill sources. For more information on HTTP Streamers and CCP Streamers, see the “HTTP Streamers” section on page 2-9.</td>
<td>Caching Node</td>
</tr>
<tr>
<td><strong>General Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td>IP address for this interface.</td>
<td>All servers</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>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

Table 4-21  Server Setup Fields (continued)

<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>IP address for this interface. The IP address set for this interface overrides the default Source IP setting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you are using Layer 3 communication among Vaults, Caching Nodes, and Streamers, each cache or stream/cache interface must have an IP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you are using Layer 2 communication among Vaults, Caching Nodes, and Streamers, IP addresses for cache and stream/cache interfaces are optional.</td>
<td></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></td>
</tr>
<tr>
<td>Cache Port</td>
<td>UDP port number for cache traffic. The port number set for this interface overrides the default cache port setting.</td>
<td></td>
</tr>
</tbody>
</table>

| **Stream Control Interface** |
| Stream Control IP    | IP address for this interface.                                                                         | Streamer, ISV |
| Stream Control Subnet| Subnet mask that defines the subnetwork for this interface.                                             | Streamer, ISV |

**Note**

The **Auto Populate Source IPs** button is available when the first applicable interface (for example, the first stream interface) is configured with an IP address. Clicking **Auto Populate Source IPs** automatically enters the next consecutive IP address as the Source IP for the next interface, and continues to populate all Source IPs until they are all filled. Any preexisting IP addresses in the Source IP fields are overwritten.

**Note**

To configure an unconfigured interface, click the **click here** link. The Interface Setup page is displayed. Choose 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 4-21 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 that 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**.
Configuring QoS Settings

There needs to be a dedicated Differentiated Services (DiffServ) Assured Forwarding (AF) class for the CCP traffic. The Assured Forwarding PHB guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, if available. There are four AF classes, AF1x through AF4x. Within each class, there are three drop probabilities (low, medium, and high).

The sum of all bandwidths configured for CCP traffic cannot exceed the bandwidth configured for the AF classes reserved for CCP. CCP is used as the protocol among Vaults and Caching Nodes in a VVI that uses HTTP, and among all servers in a VVI that uses CCP and in all non-VVIs.

Table 4-22 lists the four AF classes and the data types for each drop probability. To set the AF class on each server, use the Cache Priority drop-down list in the Server Setup page.

<table>
<thead>
<tr>
<th>AF1x Class</th>
<th>AF2x Class</th>
<th>AF3x Class</th>
<th>AF4x Class</th>
<th>Data Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF11</td>
<td>AF21</td>
<td>AF31</td>
<td>AF41</td>
<td>The following data types are set to low drop probability:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Lost packet recovery for committed rate traffic (Vault or Caching Node or Streamer to Vault or Caching Node or Streamer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- High-priority lost packet recovery for committed rate traffic (Vault or Caching Node or Streamer to Vault or Caching Node or Streamer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- iGate and index file transmission (Vault or Caching Node to Streamer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- First part of mirror data going to a new Vault (Vault to Vault)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Control traffic</td>
</tr>
<tr>
<td>AF12</td>
<td>AF22</td>
<td>AF32</td>
<td>AF42</td>
<td>Committed rate traffic (Vault or Caching Node or Streamer to Vault or Caching Node or Streamer) is set for medium drop.</td>
</tr>
<tr>
<td>AF13</td>
<td>AF23</td>
<td>AF33</td>
<td>AF43</td>
<td>The following data types are set to high drop probability:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Remote smoothing traffic (Vault to Vault) and prefetched traffic (Vault to Caching Node to Streamer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Mirroring traffic for creating additional mirrored copies (Vault to Vault)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Repair traffic that is recovering striped data lost because of a drive failure (Vault to Vault)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Mirroring of live ingest traffic (Vault to Vault)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Lost packet recovery of mirroring traffic (Vault to Vault)</td>
</tr>
</tbody>
</table>

Configuring the Route Table

In earlier releases, the Route Table included a section called “Network Information,” which had the default gateway and local network for cache traffic, and the default gateway and local network for stream traffic. The same default gateway and local network could be used for both stream and cache traffic.
Interfaces were grouped into transport groups that could separate stream traffic to multiple transport networks. The transport mechanism did not work on cache-fill interfaces. The streaming network and cache-fill network were treated as distinct entities, which disallowed an interface to function as both a streaming interface and a cache-fill interface.

Release 2.1 introduced the ability to define multiple subnets on a server. Multiple subnets replace the transport group mechanism and applies equally to stream and cache-fill interfaces. With multiple subnets you have the ability to group interfaces into separate subnets. One of the uses for multiple subnets is to configure half of the interfaces on the server to connect to one switch or router, and the other half of the interfaces to connect to a different switch or router for redundancy. The Route Table page allows for multiple subnets for cache, stream, and stream/cache interfaces.

The Route Table page has three different route types:

- **CServer Source** (written to the SubnetTable file)
- **CServer Destination** (written to the RoutingTable file)
- **Stream Control** (written to the Linux OS route table)

Each route type has a different function, and each route type is written to a different file on the CDS server.

**Note**

You cannot have intersecting subnets for any defined routes for CServer Source or CServer Destination.

### CServer Source Route Type

When **CServer Source** is selected from the **Route Type** drop-down list, a subnet is defined and written to the SubnetTable file. Subnets can only be defined for stream, cache, or stream/cache interfaces. Interfaces are defined on the Interface Setup page (“Configuring the Interfaces,” page 4-53), and IP addresses for the interfaces are set on the Server Setup page (“Configuring the Servers,” page 4-56). Figure 4-31 shows an example of interfaces configured for multiple subnets on a Streamer.

**Figure 4-31  Subnet Configuration Example on Streamer**

Table 4-23 shows the possible configuration settings to use to define the subnets described in Figure 4-31.
The Route Table entry for the subnet is defined by a network and subnet mask, and also includes a default gateway. ARP is applied for any data packets that have a destination IP address within the defined subnet, and the MAC address is returned. Any data packets outside the subnet are sent to the default gateway.

**CServer Destination Route Type**

When **CServer Destination** is selected from the Route Type drop-down list, an alternate gateway for a destination subnet (based on the Network and Subnet Mask fields) is defined and written to the RoutingTable file. The alternate gateway is used whenever the destination IP address of the data packet falls within the destination subnet defined with the Route Type of **CServer Destination**.

**Stream Control Route Type**

When **Stream Control** is selected from the Route Type drop-down list, a subnet and default gateway is defined for all stream control traffic, and the information is written to the Linux OS routing table file. The Stream Control route type is available only when one of the interfaces is set to Stream Control in the Interface Setup page. See the “Configuring the Interfaces” section on page 4-53 for more information. The Linux OS routing table file is also used to store route information for the ingest and management interfaces.

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Network</th>
<th>Subnet Mask</th>
<th>Gateway</th>
<th>Route Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet 1</td>
<td>192.168.1.0</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>CServer Source</td>
</tr>
<tr>
<td>Subnet 2</td>
<td>192.168.2.0</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
<td>CServer Source</td>
</tr>
</tbody>
</table>

The WarningAfter being upgraded to Release 2.1 or later, any servers with incompatible routes are listed in red in the drop-down list. You can review the Route Table configuration for each of these servers, modify or delete the routes, and click **Submit** to apply the changes. The routes are converted to the Release 2.1 format and the server is listed in black. When all servers with incompatible routes are fixed, the warning message is removed and the entry in the system alarm drop-down list in the GUI banner is removed.

To configure a route, do the following:

**Step 1** Choose **Configure > Server Level > Route Tables**. The Routing Table page is displayed (Figure 4-32).
Step 2  From the drop-down list, choose a server and click Display. Any configured routes are displayed.

Step 3  Enter the route settings as appropriate. See Table 4-24 for descriptions of the fields.

Table 4-24  Route Table Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>IP address of the network.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask of the network.</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the next hop (primary datagram transmitter and receiver) along the route to the network.</td>
</tr>
<tr>
<td>Route Type</td>
<td>From the Route Type drop-down list, choose one of the following route types:</td>
</tr>
<tr>
<td></td>
<td>• CServer Source—Used to configure a subnet and default gateway for a group of stream, cache, or stream/cache interfaces on this server.</td>
</tr>
<tr>
<td></td>
<td>• CServer Destination—Used to configure a default gateway for a specified destination subnetwork. Typically this is used to configure the default gateway to reach the QAM devices.</td>
</tr>
<tr>
<td></td>
<td>• Stream Control—Used when configuring a subnet route for the stream control traffic. This option is available only on Streamers, and is available only when one of the interfaces on the Streamer is configured as a Stream Control interface. See the “Configuring the Interfaces” section on page 4-53 for more information.</td>
</tr>
</tbody>
</table>

Note  For multiple SOPs used for NGOD RTSP deployments, you must choose CServer Source as the Route Type.

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

### Configuring the SNMP Agent

The SNMP Agent sets up SNMP on the CDS. For more information about SNMP on the CDS, see Appendix C, “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 Agent**. The SNMP Agent page is displayed (Figure 4-33).

**Note** If Bulk Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse** and **Import** buttons. To import a Bulk Configuration XML file, click **Browse** to locate the file, then **Import** to import the file. The status of the import is displayed in the left panel.

For information on enabling the Bulk Configuration feature, see the “Bulk Configuration” section on page D-4. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating SNMP Agent Bulk Configuration Files” section on page B-6.

**Figure 4-33 SNMP Agent Page**

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

**Step 3** Enter the settings as appropriate. The fields are described in Table 4-25.
Table 4-25  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 choose a permission setting for a community you are adding, read/write privileges are 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 message received to the NMS upon receiving an NMS message.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>There is no default for the SNMP version. If you do not choose an SNMP version for a trap station you are adding, SNMP communication is not 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 IP address of the server 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**.

**Note**  The Cisco TV CDS MIBs are available for download at the bottom of the SNMP Agent page.
Configuring the Server Level DNS

The Server DNS page is used to up to 16 domain suffixes and 16 DNS servers.

**Note**
If you are upgrading the TV CDS software to Release 2.2 from Release 2.0 or an earlier release, the system prompts you to **Submit** any settings that have previous domain suffixes to populate the new DNS database structure.

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

---

**Step 1**
Choose **Configure > Server Level > Server DNS**. The Server DNS page is displayed (Figure 4-34).

---

**Note**
If Bulk Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse** and **Import** buttons. To import a Bulk Configuration XML file, click **Browse** to locate the file, then **Import** to import the file. The status of the import is displayed in the left panel.

For information on enabling the Bulk Configuration feature, see the “Bulk Configuration” section on page D-4. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating DNS Server Bulk Configuration Files” section on page B-7.

---

**Figure 4-34**  **Server DNS Page**

---

**Step 2**
Choose the IP address of the server from the drop-down list and click **Display**.
Step 3 Enter the DNS binding Server Level settings as appropriate. See Table 4-26 for descriptions of the DNS binding fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New 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>
<tr>
<td>New DNS Server</td>
<td>IP address of the 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 Delete Entry.

Configuring the Server Level NTP

The NTP Server page is used to configure up to 16 NTP servers. The clocks on all CDS servers (Vault, Streamer, and Caching Node) and the CDSM and VVIM in a CDS must be synchronized in order to retrieve the statistics on to the CDSM and VVIM.

To configure the NTP settings for a server, do the following:

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

*Note* If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Browse and Import buttons. To import a Bulk Configuration XML file, click Browse to locate the file, then Import to import the file. The status of the import is displayed in the left panel.

For information on enabling the Bulk Configuration feature, see the “Bulk Configuration” section on page D-4. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating NTP Server Bulk Configuration Files” section on page B-8.

Step 2 Choose the IP address of the server from the drop-down list and click Display.
Step 3 In the New NTP Server field, enter the IP address of the NTP server.
Step 4 Click Submit.
To clear the fields and start over, click Reset.

To delete the NTP settings, check the Delete check box and click Delete Entry.
Other NTP Configurations

In addition to configuring the IP addresses of the NTP servers, you need to set the time zone on each CDS server, as well as configure the NTP servers for the CDSM and VVIM.

Setting the Time Zone on a CDS Server

To set the time zone on a CDS server, log in to the CDS server as root, and use the Linux link command to link the time zone to the /etc/localtime file.

The following are examples of the command used to set UTC and several different US time zones:

- UTC option:
  \[ \text{ln -sf /usr/share/zoneinfo/UTC /etc/localtime} \]

- EST option:
  \[ \text{ln -sf /usr/share/zoneinfo/US/Eastern /etc/localtime} \]

- Central option:
  \[ \text{ln -sf /usr/share/zoneinfo/US/Central /etc/localtime} \]

- Mountain option:
  \[ \text{ln -sf /usr/share/zoneinfo/US/Mountain /etc/localtime} \]

- Pacific option:
  \[ \text{ln -sf /usr/share/zoneinfo/US/Pacific /etc/localtime} \]

Find the time zone for your specific location in the /usr/share/zoneinfo directory.

Configuring the NTP Server on the CDSM and VVIM

Configuring the NTP server on the CDSM or VVIM involves the following:

1. Adding the NTP servers to the /etc/ntp.conf file
2. Setting the run levels for the Network Time Protocol daemon (ntpd)
3. Setting the time zone
4. Setting the server date and time
5. Starting the NTP service
6. Synchronizing the server clock with the NTP server
7. Synchronizing the hardware clock on the server

Specific NTP configuration details should be obtained from your system administrator to add the NTP servers to the /etc/ntp.conf file.

To setup the NTP server on the CDSM or VVIM, do the following:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the CDSM or VVIM as root.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Set the run levels for the NTP service.</td>
</tr>
</tbody>
</table>

\[ \text{# chkconfig --level 2345 ntpd on} \]

To check the run level settings, enter the following command:

\[ \text{# chkconfig --list ntpd} \]
You will see the following:

```
ntpd               0:off    1:off    2:on    3:on    4:on    5:on    6:off
```

**Step 3** Stop the ntpd service.
```
# service ntpd stop
```

**Step 4** Set the time zone by linking the time zone to the /etc/localtime file. The following command shows an example of setting the time zone to UTC.
```
# ln -sf /usr/share/zoneinfo/UTC /etc/localtime
```
Find the time zone for your specific location in the /usr/share/zoneinfo directory.

**Step 5** Set the system date and time to a date and time close to the NTP server date and time by entering the `date -s` command, for example:
```
# date -s "16:55:30 Nov 7, 2010"
```

**Step 6** Synchronize the server clock to the NTP server.
```
# ntpd -q
```

**Note** If the system clock is off by a significant amount, the command takes a considerable amount of time to return.

**Step 7** Start the ntpd service.
```
# service ntpd start
```

**Step 8** Synchronize the hardware clock.
```
# /sbin/hwclock --systohc
```

**Step 9** Check the NTP synchronization.
```
# ntpq -p
```

**Step 10** Reboot the CDSM or VVIM.
```
# init 6
```
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 4-27 describes each type of deployment.

Table 4-27 RTSP 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>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.

**Note**  If Bulk Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse** and **Import** buttons. To import a Bulk Configuration XML file, click **Browse** to locate the file, then **Import** to import the file. The status of the import is displayed in the left panel.

For information on enabling the Bulk Configuration feature, see the “Bulk Configuration” section on page D-4. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating RTSP Setup Bulk Configuration Files” section on page B-10.

**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 4-35).
Step 3  Enter the RTSP settings as appropriate. Table 4-28 describes each field and lists the associated RTSP deployment.

Table 4-28  RTSP Fields for All Deployment

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>RTSP Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Streaming IP</td>
<td>Informational only. The IP address of the master Streamer. To configure the Master Streaming IP address, see the “Configuring the Control and Setup IPs,” page 4-40.</td>
<td>All</td>
</tr>
<tr>
<td>Looping Session</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>Timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Inactivity</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, Quative, EventIS</td>
</tr>
<tr>
<td>Timeout</td>
<td></td>
<td></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>
</tbody>
</table>
### Table 4-28 RTSP Fields for All Deployment (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>RTSP Deployment</th>
</tr>
</thead>
<tbody>
<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 is not 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>Authentication Manager IP&lt;sup&gt;1&lt;/sup&gt;</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 4-15.</td>
<td>EventIS</td>
</tr>
<tr>
<td>Authentication Manager Port&lt;sup&gt;1&lt;/sup&gt;</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 4-15. The default is 7792.</td>
<td>EventIS</td>
</tr>
<tr>
<td>Bandwidth Manager IP&lt;sup&gt;1&lt;/sup&gt;</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 4-10. 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>EventIS on vpath</td>
</tr>
<tr>
<td>Bandwidth Manager Port&lt;sup&gt;1&lt;/sup&gt;</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 4-10. 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>EventIS on vpath</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>RTSP Deployment</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Backup Bandwidth Manager IP¹</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 Port¹</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>
<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</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>
</tbody>
</table>
Chapter 4  Configuring the CDS

Server Level Configuration

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.

Table 4-28  RTSP Fields for All Deployment (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>RTSP Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Level</td>
<td>From the Log Level drop-down list, choose one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off—Logging is turned off.</td>
<td>All</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 Maintenance Mode drop-down list, choose one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On—All current sessions continue until they are finished and all new SETUP requests receive a “Service Unavailable” response.</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>• Off—the Streamer is available for new sessions and continues 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.

The client configuration is displayed in a delimited string format:

```
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 4-29 describes the fields for the client definitions.

Table 4-29  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>
</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.

**Note**  If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Browse and Import buttons. To import a Bulk Configuration XML file, click Browse to locate the file, then Import to import the file. The status of the import is displayed in the left panel.

For information on enabling the Bulk Configuration feature, see the “Bulk Configuration” section on page D-4. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating FSI Setup Bulk Configuration Files” section on page B-9.

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 4-36).
Figure 4-36   FSI Setup Page

![FSI Setup Page](image)

Step 3  Enter the FSI settings as appropriate. See Table 4-30 for descriptions of the fields.

Table 4-30   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>
<tr>
<td>FTP Client Port</td>
<td>The port used by FSI communications when connecting to the catcher, or other FTP server, 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: Off—Logging is turned off. Low—Logging messages are minimal in length (for example, RTSP message received). High—Logging messages include all information concerning the event (for example, RTSP message with all syntax of the message).</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 5-24
- Server Level Monitoring, page 5-24
- Recommended Monitoring Schedule, page 5-32

Note

If Virtual Video Infrastructure (VVI) with split-domain management is enabled, the CDSM pages associated with the Vaults and Caching Nodes display only on the VVI Manager (VVIM), and the CDSM pages associated with the Streamers display only on the Stream Manager. For more information, see the “Virtual Video Infrastructure” section on page D-6.

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 group in the CDS and each server in each group. Any time there is an alarmed event, an alarm is displayed in the CDSM banner. The Alarms menu is displayed when you roll your mouse over the alarm icon. See Figure 5-1. Clicking the alarmed event in the Alarm menu takes you to the CDSM page that has more information. For example, in Figure 5-1, clicking System health problems reported takes you to the System Health page.

Figure 5-1    CDSM Banner—System Health Alarm

To view the System Health page, choose Monitor > System Health. See Figure 5-2.

Figure 5-2    System Health Page

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 5-27 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 5-24 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 5-31 for more information.

• When you click the **Vitals** check box you are taken to the Server Vitals Monitor page. See the “Server Vitals” section on page 5-28 for more information.

---

**Note**
The Vitals column is displayed only if the CDSM Health Monitor feature is enabled. For more information, see the “CDSM or VVIM Health Monitoring” section on page D-8.

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.

**Figure 5-3  System Snapshot Page**

<table>
<thead>
<tr>
<th>System Snapshot MONITOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displayed below is a rollup of all current streams and all stored content. To change the Data Refresh Rate enter a new value between 10 and 300 seconds in the field below.</td>
</tr>
<tr>
<td><strong>Data Refresh Rate:</strong></td>
</tr>
<tr>
<td><strong>Streams</strong></td>
</tr>
<tr>
<td>Total Streams:</td>
</tr>
<tr>
<td>HD Streams:</td>
</tr>
<tr>
<td>SD Streams:</td>
</tr>
<tr>
<td>Active Stream Bandwidth:</td>
</tr>
<tr>
<td>Active Fill Bandwidth:</td>
</tr>
<tr>
<td><strong>Content</strong></td>
</tr>
<tr>
<td>Total Content:</td>
</tr>
<tr>
<td>Active Ingests:</td>
</tr>
<tr>
<td>Completed Ingests:</td>
</tr>
<tr>
<td>Prev. (push) Ingests:</td>
</tr>
<tr>
<td>Failed Ingests:</td>
</tr>
<tr>
<td>Temp Out OF Service:</td>
</tr>
<tr>
<td>Total Disk:</td>
</tr>
<tr>
<td>Disk Used:</td>
</tr>
<tr>
<td>Disk Available:</td>
</tr>
</tbody>
</table>

Table 5-1 describes the information displayed on the System Snapshot page.
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>
<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>
<tr>
<td>Active Stream Bandwidth</td>
<td>Total bandwidth, in megabits, used for active streams.</td>
</tr>
<tr>
<td>Active Fill Bandwidth</td>
<td>Total bandwidth, in megabits, used for caching content among Vaults and Streamers.</td>
</tr>
<tr>
<td>Total Content</td>
<td>Total number of content objects currently stored, ingested, provisioned for ingest, and failed ingest on the CDS.</td>
</tr>
<tr>
<td>Active Ingests</td>
<td>Total number of content objects currently being ingested on the CDS.</td>
</tr>
<tr>
<td>Completed Ingests</td>
<td>Total number of content objects currently stored on the CDS.</td>
</tr>
<tr>
<td>Prov. (push) Ingests</td>
<td>Total number of content objects that have been requested for ingestion, but have not yet begun active ingestion.</td>
</tr>
<tr>
<td>Failed Ingests</td>
<td>Total number of content objects that failed to complete the ingest process.</td>
</tr>
<tr>
<td>Temp Out of Service</td>
<td>Total number of content objects that are in a Temp Out of Service state. The backoffice may put a content object into this state for a certain amount of time.</td>
</tr>
<tr>
<td>Total Disk</td>
<td>Total disk space, in bytes, on the CDS.</td>
</tr>
<tr>
<td>Disk Used</td>
<td>Total used disk space, in bytes, on the CDS.</td>
</tr>
<tr>
<td>Disk Available</td>
<td>Total available disk space, in bytes, on the CDS.</td>
</tr>
</tbody>
</table>

Monitoring Content Objects

In a VVI with split-domain management, the Stream Manager displays the following completed ingest details: Content Name, File Size, Rate, Create Time, and Last Modified. For the other completed ingests fields, see the same content asset on the VVIM.
Ingests

Viewing Completed Ingests is a different procedure than viewing the other types of monitored ingests. This section contains the following topics:

- Viewing Active Ingests
- Viewing Completed Ingests

Viewing Completed Ingests

To view the details of completed ingests, do the following:

**Step 1** Choose Monitor > System Level > Completed Ingests.

**Step 2** The following methods can be used to display a list of content objects:

- Enter the first character of the content object name in the text box. A drop-down list of content objects is displayed. If there are more than 25 content objects that start with that first character you entered, you are prompted to continue entering the next character of the content object name or click Display. You can continue to enter characters to reduce the list (you can also delete characters to increase the list) and at any point click Display. After you click Display, a list of content objects is displayed that has the same beginning characters that you entered in the text box.

- In the Browse Content box, click one of the characters. A list of content objects that begin with that character is displayed.

- In the Quick Lists box, the following options are offered:
  - Most Recent Ingests (max 100)—Lists the 100 most recent completed ingests sorted by ingest date.
  - List All Contents—Lists all completed ingests sorted by content name. This option is available only if the number of completed ingests is less than 100.
  - Content Status—Lists status information for each completed ingest.
  - Content Status (Damaged Only)—Lists status information only for damaged completed ingests.

After you perform one of these methods, a list is displayed. The list of content objects can span several pages. To view the next page, click the page number.

Figure 5-4 shows an example of the Completed Ingests list generated with any of the methods, except the Content Status options. The content names and the date they were ingested are displayed.
Figure 5-5 shows an example of the Content Status information that displays when you choose Content Status or Content Status (Damaged Only).
Figure 5-5  Completed Ingests List—Content Status

<table>
<thead>
<tr>
<th>Content Name</th>
<th>Duration</th>
<th>GOID(s)</th>
<th>Version(s)</th>
<th>Server ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider:kvodegaid.mp4</td>
<td>02:01:28</td>
<td>IGate 139</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provider:srcheeky_cat.mp4</td>
<td>02:58:15</td>
<td>IGate 139</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5-3  Content Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Name</td>
<td>Name of the content.</td>
</tr>
<tr>
<td>Duration</td>
<td>Duration of the content.</td>
</tr>
<tr>
<td>GOID</td>
<td>Global Object ID for the content object associated with the content.</td>
</tr>
<tr>
<td>Version</td>
<td>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>Server ID of the Vault that is storing the content object.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the storing process of the content object, either complete or partial.</td>
</tr>
</tbody>
</table>
Step 3  To view the details of a content object, click the content name. The Ingest Details are displayed (Figure 5-6).

**Figure 5-6  Completed Ingests—Ingest Details**

<table>
<thead>
<tr>
<th>Completed Ingests Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>To view the details for a Completed Ingest begin typing the content name, then select the content name from the list provided.</td>
</tr>
</tbody>
</table>

**Ingest Details**

**Content Name:** Provider Moreno 211.mpg

**Ingest IP:** 172.22.21.10

**File Size:** 1251112702

**Size:** 3756800

**Create Time:** January 19, 2010, 4:50:02 pm

**Last Modified:** January 19, 2010, 4:50:02 pm

**Op Status:** inService

**Admin Status:** inService

**Push Provision:** $5 m/s

**Content Engine**

<table>
<thead>
<tr>
<th>Speed / Direction</th>
<th>Server ID</th>
<th>Status</th>
</tr>
</thead>
</table>

**Full Content ID**

```
295036211: Moreno 211.mpg
```

**URI**

```
http://172.22.21.10:8080/RedCam/Moreno 211.mpg
```

Table 5-4 describes the content object details that are displayed for each type of ingest.
### Table 5-4  Content Object Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Name</td>
<td>Name of the content object.</td>
</tr>
<tr>
<td>Factory ID</td>
<td>Factory responsible for this content object.</td>
</tr>
<tr>
<td>Ingest IP</td>
<td>IP address of the ingest interface on the Vault used to download the content.</td>
</tr>
<tr>
<td>File Size</td>
<td>File size, in bytes, of this content object.</td>
</tr>
<tr>
<td>Rate</td>
<td>Rate of ingest in bits per second ($3750000 = 3.75$ Mbps).</td>
</tr>
<tr>
<td>Create Time</td>
<td>Time and date this content object was created.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Time and date this content object was last modified.</td>
</tr>
<tr>
<td>Op State</td>
<td>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>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>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>These fields display the following information about the copies of the content:</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>Full identification of this content object.</td>
</tr>
<tr>
<td>Ior$^1$</td>
<td>Interoperable Object Reference (IOR) for this content object.</td>
</tr>
<tr>
<td>URL$^1$</td>
<td>Uniform Resource Locator (URL) address of the content has 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 server (for example, 192.168.100.184)</td>
</tr>
<tr>
<td></td>
<td>• Directory where the content is stored on the provider server (for example, videolan)</td>
</tr>
<tr>
<td></td>
<td>• Name of the file (for example, long_encore_3.75.mpg)</td>
</tr>
<tr>
<td>Asset Ior$^1$</td>
<td>Asset IOR associated with this content object.</td>
</tr>
</tbody>
</table>

$^1$ Not displayed in Figure 5-6.
Viewing Active Ingests

To view the details of active ingests, do the following:

**Step 1** Choose Monitor > System Level > Active.

**Step 2** Choose a content object from the drop-down list and click Display. The details of the content object are displayed. Figure 5-6 on page 5-8 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.

Table 5-4 on page 5-9 describes the content object details that are displayed for active ingests.

Package Expirations

**Note**

Package Expirations are part of the optional Ingest Manager feature. This option is listed only 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 5-8 shows an example of the Package Expiration details.
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 is still 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.

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>Name of the package.</td>
</tr>
<tr>
<td>License Expiration</td>
<td>Date the package expires.</td>
</tr>
<tr>
<td>Additional Package Window</td>
<td>Additional time added to the package.</td>
</tr>
<tr>
<td>Actual Package Expiration</td>
<td>Actual Package Expiration is the License Expiration plus the Additional Package Window.</td>
</tr>
</tbody>
</table>

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 listed only on the Monitoring System Level left-panel menu if the Ingest Manager is included in your deployment.

The Publish Failures page 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 5-8 shows an example of the Publish Failures details.

Figure 5-8 Publish Failures Page

Table 5-6 describes the publish failures details that are displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Name</td>
<td>Name of the package.</td>
</tr>
<tr>
<td>Source URL</td>
<td>Location of the original package information.</td>
</tr>
<tr>
<td>Target URL</td>
<td>Location where to place the package information.</td>
</tr>
</tbody>
</table>
Chapter 5      System Monitoring

Monitoring Stream Objects

The monitored stream objects consist of:

- Stream Monitor
- Stream Failures

Stream Monitor

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

Step 2  The following methods can be used to display a stream object or a list of stream objects:

- **Enter the first character of the session handle in the text box. A drop-down list of stream objects is displayed.** If there are more than 25 objects that start with that first character you entered, you are prompted to continue entering the next character of the object name or choose one that is listed. You can continue to enter characters to reduce the list (you can also delete characters to increase the list) and at any point choose one. After you choose one, the stream details are displayed (Figure 5-10).

- In the Quick Lists box, the following options are offered:
  - **Most Recent 100**—Lists the 100 most recent stream objects.
  - **All Streams**—Lists all streams. This option is available only if the number of streams is less than 100.

- **Destination IP, Destination Port, Client IP, Client Port**—If you do not know the session handle, 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 as seen in Figure 5-9) to see the stream monitor details for the selected object, or click **Back** to return to the previous page.

After you perform one of these methods, a list is displayed. The list of stream objects can span several pages. To view the next page, click the page number.

**Figure 5-9** shows an example of the stream object list generated by clicking **Most Recent 100** or **All Streams**. The Session IDs and the stream start time are displayed.
Chapter 5      System Monitoring

Monitoring Stream Objects

The stream object list generated by entering the destination IP, destination port, client IP, or client port in the Quick List box, displays the session ID, stream start time, destination IP, destination port, client IP, and client port.

Figure 5-9  Stream Monitor — Stream List

Step 3 To view the details of a stream object, click the session handle. The Stream Details are displayed.

Figure 5-10 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>Internal unique identifier assigned to the stream session by the Streamer.</td>
</tr>
<tr>
<td>RTSP Session ID</td>
<td>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>Session identifier generated by the backoffice.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>IP address used to receive the stream (for example, the QAM or set-top box).</td>
</tr>
</tbody>
</table>
### Table 5-7 Stream Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Port</td>
<td>Port number used to receive the stream (for example, the QAM or set-top box).</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address of the set-top box that requested the stream.</td>
</tr>
<tr>
<td>Client Port</td>
<td>Set-top box port number used to send the stream request.</td>
</tr>
<tr>
<td>Session Group ID</td>
<td>Identifier defined by the backoffice for a logical grouping of sessions.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Identifier of the client that is receiving the stream.</td>
</tr>
<tr>
<td>Service Group</td>
<td>Service group used for this session.</td>
</tr>
<tr>
<td>Service Area</td>
<td>Logical name that describes the service group, which is a logical grouping of subscribers.</td>
</tr>
<tr>
<td>Entitlement</td>
<td>This is an identifier that specifies if this a valid SETUP request. This is used to pass back to the authentication server during the setup process. This is only used in an EventIS environment.</td>
</tr>
<tr>
<td>Allocated Bandwidth</td>
<td>Bandwidth allocated for this stream session.</td>
</tr>
<tr>
<td>Current Operation</td>
<td>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>Start time of the currently active operation.</td>
</tr>
<tr>
<td>Stream State</td>
<td>Stream state has the following possible values: playing, paused, stopped.</td>
</tr>
<tr>
<td>LSCP Mode</td>
<td>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 pauses 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 pauses at stop NPT.</td>
</tr>
<tr>
<td></td>
<td>- Search transport pause—The server is transporting the media stream and pauses 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>LSCP is not used in a Motorola environment. In an nABLE Motorola environment, the value is always 0.</td>
<td></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 Stream** button displays the trick-mode activity of the stream (Figure 5-11).

If Trick Mode Capture is disabled, the **Graph Stream** is not displayed. For information on enabling the Trick Mode Capture, see the “Trick Mode Capture” section on page D-5.

**Figure 5-11 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 6-15.

**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 5-12.

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

*Figure 5-12 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>Session ID of the failed stream.</td>
</tr>
<tr>
<td>Failure Date</td>
<td>Date and time the failure occurred.</td>
</tr>
<tr>
<td>QAM IP</td>
<td>IP address of the QAM device associated with the failure.</td>
</tr>
<tr>
<td>Service Group</td>
<td>Service group associated with the failure.</td>
</tr>
<tr>
<td>Server ID</td>
<td>Server responsible for streaming this stream object.</td>
</tr>
<tr>
<td></td>
<td>To view the IP address associated with the Server ID, see the “Configuring</td>
</tr>
<tr>
<td></td>
<td>the Servers” section on page 4-56.</td>
</tr>
<tr>
<td>Group ID</td>
<td>All servers that are part of the same CDS system (managed by one CDSM) have</td>
</tr>
<tr>
<td></td>
<td>the same Group ID. This Group ID corresponds to the CDSM GUI array ID and</td>
</tr>
<tr>
<td></td>
<td>should be unique across an enterprise. Table 5-9 describes the ID mapping</td>
</tr>
<tr>
<td></td>
<td>between the CDSM GUI and the CServer.</td>
</tr>
<tr>
<td>Failed Operation</td>
<td>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>Failed task is the event category that provides the type of execution</td>
</tr>
<tr>
<td></td>
<td>sequence that the call stack was currently in at the time of the failure.</td>
</tr>
<tr>
<td></td>
<td>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>• Purchase Movie</td>
</tr>
<tr>
<td></td>
<td>• Purchase Check</td>
</tr>
<tr>
<td>Error Code</td>
<td>Error code provides a description of the event that caused an error.</td>
</tr>
<tr>
<td></td>
<td>See Table 5-10 for descriptions of the error codes.</td>
</tr>
</tbody>
</table>

Table 5-9 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

Table 5-9  ID Names in the CDSM GUI and CServer Files

<table>
<thead>
<tr>
<th>CDSM GUI ID Name</th>
<th>CServer Files ID Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array ID on the Array Name page</td>
<td>groupid</td>
</tr>
<tr>
<td>Group ID on the Server-Level pages</td>
<td>groupid</td>
</tr>
<tr>
<td>Stream Group ID on the Server Setup</td>
<td>arrayid</td>
</tr>
<tr>
<td>Cache Group ID on the Server Setup</td>
<td>arrayid</td>
</tr>
</tbody>
</table>
Table 5-9  ID Names in the CDSM GUI and CServer Files (continued)

<table>
<thead>
<tr>
<th>CDSM GUI ID Name</th>
<th>CServer Files ID Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vault Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Stream Group ID on the Configuration Generator page</td>
<td>arrayid</td>
</tr>
</tbody>
</table>

Table 5-10 lists the error codes for internal errors that specifically describe where the error occurred, and errors in the network or network components.

Table 5-10  Error Codes

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2024</td>
<td>FTP_CONNECTION_FAILED</td>
<td>Connection to FTP server failed.</td>
</tr>
<tr>
<td>2025</td>
<td>FTP_SERVER_BIND_FAILED</td>
<td>FTP server can not bind to the port.</td>
</tr>
<tr>
<td>2026</td>
<td>FTP_PUSH_TIMEOUT</td>
<td>FTP push timeout (PASV is not served fast enough).</td>
</tr>
<tr>
<td>2027</td>
<td>FTP_QUIT_RECEIVED_DURING_INGEST</td>
<td>FTP server received QUIT request.</td>
</tr>
<tr>
<td>2036</td>
<td>NOT_ENOUGH_QAM_BANDWIDTH</td>
<td>Not enough QAM bandwidth.</td>
</tr>
<tr>
<td>2041</td>
<td>CONTENT_CAN_NOT_BE_LOCATED</td>
<td>Content is not found in the related content stores.</td>
</tr>
<tr>
<td>3006</td>
<td>SET_DESTINATION_FAILED</td>
<td>Failed while setting destination of the stream.</td>
</tr>
<tr>
<td>6001</td>
<td>RTSP_REQUEST_INVALID</td>
<td>RTSP request was not understood by the RTSP server.</td>
</tr>
<tr>
<td>6002</td>
<td>SESSION_NOT_FOUND</td>
<td>RTSP session ID could not be found in the RTSP server.</td>
</tr>
<tr>
<td>6003</td>
<td>RTSP_METHOD_NOT_VALID_IN_STATE</td>
<td>RTSP request is not valid for the current RTSP session state.</td>
</tr>
<tr>
<td>6004</td>
<td>RTSP_RANGE_NOT_VALID</td>
<td>RTSP range header does not have valid values.</td>
</tr>
<tr>
<td>6005</td>
<td>TRANSPORT_UNSUPPORTED</td>
<td>Transport header could not be parsed.</td>
</tr>
<tr>
<td>6006</td>
<td>NO_DESTINATION_DEFINED</td>
<td>Transport header does not have a stream destination value.</td>
</tr>
<tr>
<td>6007</td>
<td>INTERNAL_SERVER_ERROR</td>
<td>There was an internal server error during an RTSP request.</td>
</tr>
<tr>
<td>6008</td>
<td>RTSP_SERVICE_UNAVAILABLE</td>
<td>RTSP service is unavailable.</td>
</tr>
<tr>
<td>6009</td>
<td>UNSUPPORTED_RTSP_VERSION</td>
<td>RTSP version is not supported.</td>
</tr>
<tr>
<td>6010</td>
<td>UNSUPPORTED_OPTION</td>
<td>RTSP require header is not supported.</td>
</tr>
<tr>
<td>6011</td>
<td>STREAMING_ERROR_READING_CONTENT</td>
<td>There was an error reading the content in a stream.</td>
</tr>
</tbody>
</table>

Table 5-11 lists the error codes for errors that could occur during ingest or during trick-mode file creation, which cause stream failures.
### Table 5-11  MPEG Error Codes

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8001</td>
<td>TRICK_INGEST_NO_INGEST_OBJECTS</td>
<td>Ingest fails. Check available system memory.</td>
</tr>
<tr>
<td>8002</td>
<td>TRICK_INGEST_TOO_MANY_SPEEDS</td>
<td>Too many trick speeds. Change trick speed configuration.</td>
</tr>
<tr>
<td>8003</td>
<td>TRICK_INGEST_NULL_INGEST_OBJECTS</td>
<td>Ingest fails. Check available system memory.</td>
</tr>
<tr>
<td>8004</td>
<td>TRICK_INGEST_INVALID_SPEED_DENOMINATOR</td>
<td>Ingest fails. Change trick speed configuration.</td>
</tr>
<tr>
<td>8005</td>
<td>TRICK_INGEST_INVALID_SPEED_LT_2X</td>
<td>Ingest fails. Change trick speed configuration.</td>
</tr>
<tr>
<td>8006</td>
<td>TRICK_INGEST_NULL_DERIVED_INGEST_OBJECTS</td>
<td>Ingest fails. Check available system memory.</td>
</tr>
<tr>
<td>8007</td>
<td>TRICK_RSDVR_DYNAMIC_TRICK_CREATION_FAILS</td>
<td>RS-DVR trick-mode file creation fails. Change trick speed configuration.</td>
</tr>
<tr>
<td>8008</td>
<td>TRICK_INGEST_CDNN_AVCC_UNSUPPORTED</td>
<td>Do not attempt to ingest an Advanced Video Coding (AVC) stream on a VVI system.</td>
</tr>
<tr>
<td>8009</td>
<td>TRICK_RSDVR_BAD_STREAM_TYPE</td>
<td>RS-DVR trick-mode file creation fails. Stream should already have failed ingest.</td>
</tr>
<tr>
<td>8010</td>
<td>TRICK_INGEST_ABORTED</td>
<td>General ingest failure. Check ingest feed.</td>
</tr>
<tr>
<td>8011</td>
<td>TRICK_INGEST_INSUFFICIENT_DATA</td>
<td>Ingest fails. Check ingest feed.</td>
</tr>
<tr>
<td>8012</td>
<td>TRICK_INGEST_STREAM_TOO_BIG</td>
<td>Ingest fails. The limit is 162 GB or about 12 hours at a known bitrate.</td>
</tr>
<tr>
<td>8013</td>
<td>TRICK_RSDVR_WRITE_OVERFLOW</td>
<td>RS-DVR trick-mode file creation fails. Check ingest feed.</td>
</tr>
<tr>
<td>8014</td>
<td>TRICK_INGEST_VBR_UNSUPPORTED</td>
<td>Ingest fails. Check ingest feed.</td>
</tr>
<tr>
<td>8015</td>
<td>TRICK_INGEST_RATE_FORCED</td>
<td>Streaming rate may be incorrect. Check ingest feed.</td>
</tr>
<tr>
<td>8016</td>
<td>TRICK_INGEST_PAT_NOT_FOUND</td>
<td>Program association table (PAT) not found. Check ingest feed.</td>
</tr>
<tr>
<td>8017</td>
<td>TRICK_INGEST_DEFAULTING_PMT_PID</td>
<td>Program map table (PMT) process ID (PID) not determined. Check ingest feed.</td>
</tr>
<tr>
<td>8018</td>
<td>TRICK_INGEST_DEFAULTING_PROGRAM_NUMBER</td>
<td>Program number not determined. Check ingest feed.</td>
</tr>
<tr>
<td>8019</td>
<td>TRICK_INGEST_DEFAULTING_VIDEO_PID_AND_TYPE</td>
<td>Video PID or type not determined. Check ingest feed.</td>
</tr>
<tr>
<td>8020</td>
<td>TRICK_INGEST_BITRATE_INDETERMINATE</td>
<td>Bitrate cannot be determined. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8021</td>
<td>TRICK_INGEST_FIRSTPTS_NOT_FOUND</td>
<td>First presentation time stamp (PTS) not determined. Check ingest feed.</td>
</tr>
<tr>
<td>8022</td>
<td>TRICK_INGEST_CANNOT_DETERMINE_FRAMERATE</td>
<td>Frame rate not determined. Check ingest feed.</td>
</tr>
<tr>
<td>8023</td>
<td>TRICK_INGEST_PMT_NOT_FOUND</td>
<td>PMT not found. Check ingest feed.</td>
</tr>
<tr>
<td>8024</td>
<td>TRICK_INGEST_MULTIPLE_VIDEO_PIDS</td>
<td>Multiple video PIDs found. Check ingest feed.</td>
</tr>
<tr>
<td>8025</td>
<td>TRICK_INGEST_PID REPLACEMENT_CANCELED</td>
<td>PIDs could not be standardized. Check ingest feed.</td>
</tr>
</tbody>
</table>
Table 5-11    MPEG Error Codes (continued)

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8026</td>
<td>TRICK_INGEST_OVERFLOW</td>
<td>Ingest fails because of ring buffer overflow. Check ingest feed.</td>
</tr>
<tr>
<td>8027</td>
<td>TRICK_INGEST_WRITE_ERROR</td>
<td>Ingest fails because of a 1x write problem. Check ingest feed.</td>
</tr>
<tr>
<td>8028</td>
<td>TRICK_INGEST_OVERFLOW_ON_RETRY</td>
<td>Ingest fails even after a retry (ring buffer overflow). Check ingest feed.</td>
</tr>
<tr>
<td>8029</td>
<td>TRICK_INGEST_KNOBS_FAILURE</td>
<td>Ingest fails. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8030</td>
<td>TRICK_INGEST_KNOBS_FAILURE_PAT_PMT</td>
<td>Ingest fails. No PAT or PMT found. Check ingest feed or adjust ingest parameters.</td>
</tr>
<tr>
<td>8031</td>
<td>TRICK_INGEST_KNOBS_FAILURE_BITRATE</td>
<td>Ingest fails. Bitrate cannot be computed. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8032</td>
<td>TRICK_INGEST_KNOBS_FAILURE _DISCONTINUITIES</td>
<td>Ingest fails. Too many discontinuities. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8033</td>
<td>TRICK_INGEST_KNOBS_FAILURE_CONTINUITY _COUNTERS</td>
<td>Ingest fails. Too many continuity counter errors. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8034</td>
<td>TRICK_INGEST_KNOBS_FAILURE_SYNC</td>
<td>Ingest fails. Too many sync errors. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8035</td>
<td>TRICK_INGEST_KNOBS_FAILURE_SYNC_TIME</td>
<td>Ingest fails. Sync loss too long. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8036</td>
<td>TRICK_INGEST_KNOBS_FAILURE_PIC_GAPS</td>
<td>Ingest fails. Too many picture gaps. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8037</td>
<td>TRICK_INGEST_KNOBS_FAILURE_PIC_GAP_TIME</td>
<td>Ingest fails. Picture gap too long. Check ingest feed or adjust ingest configuration parameters.</td>
</tr>
<tr>
<td>8038</td>
<td>TRICK_INGEST_SEQUENCE_HEADER_NOT_FOUND</td>
<td>Ingest fails. Could not find a Sequence Header. Check ingest feed.</td>
</tr>
<tr>
<td>8039</td>
<td>TRICK_INGEST_SPS_NOT_FOUND</td>
<td>Ingest fails. Could not find an SPS. Check ingest feed.</td>
</tr>
<tr>
<td>8040</td>
<td>TRICK_INGEST_CDN_SEQ_WRITE_FAILED</td>
<td>Ingest fails because of a Sequence Header write error. Check ingest feed.</td>
</tr>
<tr>
<td>8041</td>
<td>TRICK_INGEST_CDN_NONCONFORMAL _FRAME_START</td>
<td>VVI: Ingest fails. Invalid frame start. Check ingest feed.</td>
</tr>
<tr>
<td>8042</td>
<td>TRICK_INGEST_SPLIT_SEQEND_SEQ_PAIR</td>
<td>Ingest fails. SequenceEnd/SequenceHeader pair not consecutive. Check ingest feed.</td>
</tr>
<tr>
<td>8043</td>
<td>TRICK_INGEST_PIC_SIZE_CHANGED</td>
<td>Ingest fails. Picture size changed. Check ingest feed.</td>
</tr>
<tr>
<td>8044</td>
<td>TRICK_INGEST_PIC_SIZE_H_OR_V_ZERO</td>
<td>Ingest fails. Picture size H or V zero. Check ingest feed.</td>
</tr>
<tr>
<td>8045</td>
<td>TRICK_INGEST_HORIZONTAL_PIC_SIZE_EXCEEDS _MAX</td>
<td>Ingest fails. Horizontal size exceeds max (1920). Check ingest feed.</td>
</tr>
</tbody>
</table>
Table 5-11  MPEG Error Codes (continued)

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8046</td>
<td>TRICK_INGEST_VERTICAL_PIC_SIZE_EXCEEDS_MAX</td>
<td>Ingest fails. Vertical size exceeds max (1088). Check ingest feed.</td>
</tr>
<tr>
<td>8047</td>
<td>TRICK_INGEST_SEQUENCE_HEADER_CHANGED</td>
<td>VVI: Ingest fails. Sequence Header changed. Check ingest feed.</td>
</tr>
<tr>
<td>8048</td>
<td>TRICK_INGEST_SEQUENCE_HEADER_CHANGE_NO_SEQEND</td>
<td>Ingest fails. Sequence Header changed with no preceding Sequence End.</td>
</tr>
<tr>
<td>8049</td>
<td>TRICK_INGEST_SEQUENCE_HEADER_CHANGE_BAD_PRIOR_STARTCODE</td>
<td>Ingest fails. Sequence Header changed with no immediately preceding Sequence End.</td>
</tr>
<tr>
<td>8050</td>
<td>TRICK_INGEST_SEQUENCE_HEADER_CHANGE_NO_PRIOR_STARTCODE</td>
<td>Ingest fails. Sequence Header changed with no preceding start code</td>
</tr>
<tr>
<td>8051</td>
<td>TRICK_INGEST_ILLEGAL_FRAMERATE</td>
<td>Illegal frame rate code. Check ingest feed.</td>
</tr>
<tr>
<td>8052</td>
<td>TRICK_INGEST_CDN_ILLEGAL_PES_PACKETISATION</td>
<td>VVI: Ingest fails. Illegal PES packetization. Check ingest feed.</td>
</tr>
<tr>
<td>8053</td>
<td>TRICK_INGEST_CDN_STREAM_STARTS_WITH_P_FRAME</td>
<td>VVI: Ingest fails: Stream begins with a P-frame. Check ingest feed.</td>
</tr>
<tr>
<td>8054</td>
<td>TRICK_INGEST_CDN_STREAM_STARTS_WITH_B_FRAME</td>
<td>VVI: Ingest fails: Stream begins with a B-frame. Check ingest feed.</td>
</tr>
<tr>
<td>8055</td>
<td>TRICK_INGEST_ZERO_BITRATE</td>
<td>Check ingest feed. Bitrate indeterminate.</td>
</tr>
<tr>
<td>8056</td>
<td>TRICK_INGEST_CDN_STREAM_STARTS_WITH_BAD_I_FRAME</td>
<td>VVI: Ingest fails: Stream begins with a malformed I-frame. Check ingest feed.</td>
</tr>
</tbody>
</table>

Table 5-12 lists the Managed Services Architecture (MSA) error codes for the optional Ingest Manager feature.

Table 5-12  MSA Error Codes for the Optional Ingest Manager Feature

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7000</td>
<td>MSA_BAD_XML</td>
<td>There was an XML parsing error. Check the ADI XML for errors.</td>
</tr>
<tr>
<td>7001</td>
<td>MSA_BAD_REQUEST</td>
<td>The request for content was bad. Check the target backoffice URL.</td>
</tr>
<tr>
<td>7002</td>
<td>MSAUNKNOWN_HOST</td>
<td>The host is unknown. Check the target backoffice URL.</td>
</tr>
<tr>
<td>7003</td>
<td>MSA_CONNECTION_DROP</td>
<td>The connection was dropped. Check the URL. The Ingest Manager possibly misformatted the ADI XML.</td>
</tr>
<tr>
<td>7004</td>
<td>MSA_BACKOFFICE_TIMEOUT</td>
<td>The backoffice did not respond within the allowed time interval.</td>
</tr>
<tr>
<td>7005</td>
<td>MSA_UNKNOWN</td>
<td>An unknown error occurred. Check the /home/isa/bss/log/aim.log.</td>
</tr>
<tr>
<td>7006</td>
<td>MSA_FAILED_POST</td>
<td>The Ingest Manager failed to post the ADI to the backoffice.</td>
</tr>
<tr>
<td>7007</td>
<td>MSA_PKG_EXPIRED</td>
<td>The package has expired and the retry record is removed.</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 ingests, and disk usage is displayed.

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 on page 5-4.

Server Level Monitoring

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
- Server Vitals
- Cache/Fill Bandwidth
- Services Monitor

**Step 2** Choose 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, choose the IP address of the server 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.

To change how often the information is refreshed, enter the number of seconds in the Data Refresh Rate field. 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 font.
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 7-7.

Table 5-13 describes the information displayed when a disk is selected.
Server Level Monitoring

Chapter 5  System Monitoring

5.26

Cisco TV CDS 2.2 RTSP Software Configuration Guide

Chapter 5  System Monitoring

Table 5-13  Disk Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Temp</td>
<td>The current temperature of the hard disk.</td>
</tr>
<tr>
<td>Smart Status</td>
<td>The Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status of a disk as determined by the manufacturer in accordance with the relevant ATA/SCSI standards. S.M.A.R.T. is logic embedded in the firmware that determines when a disk is going bad.</td>
</tr>
<tr>
<td>Number of Reads</td>
<td>Number of bytes read from the disk since it was powered on.</td>
</tr>
<tr>
<td>Number of Writes</td>
<td>Number of bytes written to the disk since it was powered on.</td>
</tr>
</tbody>
</table>

S.M.A.R.T

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.

Figure 5-14  Disk Monitor—Vault 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.

Table 5-13  Disk Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Temp</td>
<td>The current temperature of the hard disk.</td>
</tr>
<tr>
<td>Smart Status</td>
<td>The Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status of a disk as determined by the manufacturer in accordance with the relevant ATA/SCSI standards. S.M.A.R.T. is logic embedded in the firmware that determines when a disk is going bad.</td>
</tr>
<tr>
<td>Number of Reads</td>
<td>Number of bytes read from the disk since it was powered on.</td>
</tr>
<tr>
<td>Number of Writes</td>
<td>Number of bytes written to the disk since it was powered on.</td>
</tr>
</tbody>
</table>

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, choose the IP address of the server 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.

To change how often the information is refreshed, enter the number of seconds in the Data Refresh Rate field. 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 font.

**Figure 5-15   NIC Monitor—Vault Page**

![NIC Monitor—Vault Page](image)

Table 5-14 describes the information displayed for a NIC port.

**Table 5-14   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>
</tbody>
</table>
Server Level Monitoring

Chapter 5      System Monitoring

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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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>

Table 5-14    NIC Port Status Fields (continued)

Server Vitals

The Server Vitals page provides current values for monitored system components. Server components are monitored and if a threshold is exceeded, the System Health Monitor page reports the event and an SNMP trap is sent to the Network Management System (NMS).

Note

The Server Vitals page is displayed only if the CDSM Health Monitor feature is enabled. For more information, see the “CDSM or VVIM Health Monitoring” section on page D-8.
To view the current values of the monitored components, as well as the threshold settings, choose the IP address of the server from the drop-down list on the Server Vitals page and click **Display**.

To change how often the information is refreshed, enter the number of seconds in the **Data Refresh Rate** field. 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.

To change the temperature format to Fahrenheit, choose **°F** for the **Temperature Format**. The default is Celsius (°C).

The monitored components are different for each Content Delivery Engine (CDE) model. Figure 5-17 shows an example of the Server Vitals page for a Vault (CDE420).

*Figure 5-17  Server Vitals Page*

<table>
<thead>
<tr>
<th>Server Vitals MONITOR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select the name or IP of the specific server that you wish to monitor and click Display.</strong></td>
</tr>
<tr>
<td><strong>Server IP:</strong></td>
</tr>
<tr>
<td><strong>Data Refresh Rate:</strong></td>
</tr>
<tr>
<td><strong>Temperature Format:</strong></td>
</tr>
</tbody>
</table>

**Temperatures**

<table>
<thead>
<tr>
<th><strong>Current</strong></th>
<th><strong>Max</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Front Temp:</td>
<td>69°C/99.6°F</td>
</tr>
<tr>
<td>Rear Temp:</td>
<td>69°C/99.6°F</td>
</tr>
<tr>
<td>Ambient Temp:</td>
<td>28°C/82.6°F</td>
</tr>
</tbody>
</table>

**Fan Speed**

<table>
<thead>
<tr>
<th><strong>Current</strong></th>
<th><strong>Min</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Front Fan:</td>
<td>4532</td>
</tr>
<tr>
<td>Front Fan:</td>
<td>4532</td>
</tr>
<tr>
<td>Front Fan:</td>
<td>4532</td>
</tr>
<tr>
<td>Front Fan:</td>
<td>4532</td>
</tr>
<tr>
<td>Front Fan:</td>
<td>4532</td>
</tr>
</tbody>
</table>

**Voltages**

<table>
<thead>
<tr>
<th><strong>Current</strong></th>
<th><strong>Min/Max</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Voltage:</td>
<td>1.47</td>
</tr>
<tr>
<td>CPU2 Voltage:</td>
<td>1.14</td>
</tr>
<tr>
<td>12V Voltage:</td>
<td>1.22v</td>
</tr>
<tr>
<td>+5V Voltage:</td>
<td>1.62</td>
</tr>
<tr>
<td>+5VStandby:</td>
<td>0.96</td>
</tr>
<tr>
<td>+12V Voltage:</td>
<td>11.71</td>
</tr>
<tr>
<td>+3.3V Voltage:</td>
<td>4.94</td>
</tr>
<tr>
<td>-5V Voltage:</td>
<td>4.94</td>
</tr>
<tr>
<td>-12V Voltage:</td>
<td>2.3</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, choose the IP address of the server from the drop-down list on the Cache/Fill Bandwidth page and click Display. Figure 5-18 shows an example.

To change how often the information is refreshed, enter the number of seconds in the Data Refresh Rate field. 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 font.

**Figure 5-18 Cache/Fill Bandwidth Page**

![Cache/Fill Bandwidth Page](image)

The Cache/Fill Bandwidth page displays details on the content caching activity on a Streamer. To view the caching activity on a server, choose the IP address of the server from the drop-down list on the Cache/Fill Bandwidth page and click Display. Figure 5-18 shows an example. To change how often the information is refreshed, enter the number of seconds in the Data Refresh Rate field. 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 font.

**Table 5-15** describes the services listed in the Cache/Fill Bandwidth page.

**Table 5-15 Cache/Fill Bandwidth Fields**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 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>
<tr>
<td>Disk Read Stream Count</td>
<td>The number of streams on this Streamer sending content that was retrieved from the disks on the Streamer.</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 disks on the Streamer).</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, choose the IP address of the server from the drop-down list on the Services Monitor page and click **Display**. Figure 5-18 shows an example of a Streamer server.

**Figure 5-19 ** Services Monitor Page—Streamer

Table 5-16 describes the services listed on the Services Monitor page.

**Table 5-16  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 is 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>
</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 5-2 for more information.

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

Note

All commands require that you log into the 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

Filesystem Size Used Avail Use% Mounted on
/dev/hda1 13G 5.2G 7.0G 43% /
/dev/hda6 20G 16G 4.3G 78% /arroyo/log

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

a. 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. Also, 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 a 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 4-56). The number of GOIDs is also dependent on the trick speeds configured you configured (see the “Configuring Ingest Tuning” section on page 4-17). 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**

In addition to the weekly monitoring tasks for both the Vaults and Streamers, the Vaults can also be monitored in the following ways:

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**

In addition to the weekly monitoring tasks for both the Vaults and Streamers, the Streamers can also be monitored in the following ways:

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**

The monthly monitoring tasks consist of the following:

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 6-20
- CDSM Audit Logs, page 6-23
- Archived Data, page 6-25

**Note**

If Virtual Video Infrastructure (VVI) with split-domain management is enabled, the CDSM pages associated with the Vaults and Caching Nodes display only on the VVI Manager (VVIM), and the CDSM pages associated with the Streamers display only on the Stream Manager. For more information, see the “Virtual Video Infrastructure” section on page D-6.

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).

Figure 6-1 **Available Reports for Stream Activity**

![Figure 6-1](image1)

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

**Figure 6-2** **Stream By Array Report Selection Fields**

![Figure 6-2](image2)

**Step 2**

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

**Step 3**

Choose a modifier. See Table 6-1 for a description of each modifier.
Step 4 Using the drop-down lists provided, or the calendars, choose a **From Date** and **To Date** for the report.

Step 5 Choose 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, choose 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

<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 choose in a later step.</td>
</tr>
</tbody>
</table>

<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 choose in a later step.</td>
</tr>
</tbody>
</table>

The report displays:

- Report type (for example, Daily Stream Activity Report for streams by array)
Stream Activity

- 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

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

The Session ID Summary can be sorted 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).

Note If Trick Mode Capture is disabled, the session ID does not link to the stream play history. For information on enabling the Trick Mode Capture, see the “Trick Mode Capture” section on page D-5.
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

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).
Stream Activity

Chapter 6      System Reporting

Figure 6-6  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.

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

### Step 3
Choose 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 choose **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 6-13 shows the selection fields for the Stream Play History report.

Figure 6-9 Stream Play History Report Selection Fields

```
Stream Activity REPORTS

Available Reports:  Stream Play History

Modifiers:
- None (Date Only)
- Session Handle
- Destination IP

From Date
- Nov 6 2008

To Date
- Nov 6 2008

Destination IP:  Choose One...
```

Please only click the 'Display' button once, some large reports take several seconds to process.

Step 2
Choose 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 choose in a later step.</td>
</tr>
</tbody>
</table>

Step 3
Using the drop-down lists provided, or the calendars, choose 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.
Stream Activity

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, choose or specify the filtered value. For example, if you choose Service Group as the modifier, you specify which Service Group.

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

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

Figure 6-14 shows an example of the Stream Play History report.

**Figure 6-10  Stream Play History Report**

The report displays:

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

**Note**  The Session ID Summary can be sorted by clicking on each column heading.

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

**Note**  If Trick Mode Capture is disabled, the session ID does not link to the stream play history. For information on enabling the Trick Mode Capture, see the “Trick Mode Capture” section on page D-5.
The report displays:

- Session ID
- Set-top box MAC address
- Termination reason
- Server ID of the Play server that served the trick mode
- 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).
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.

b. If you are using another major web browser (for example, Netscape, Firefox, Opera), right-click **Download** and choose **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.
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 6-13 shows the selection fields for the Cache/Fill Bandwidth report.

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

![Figure 6-13 Cache/Fill Bandwidth Report Selection Fields](image)

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

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

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

**Step 5** Click Display.

To clear the fields and start over, click Reset.

Figure 6-14 shows an example of the 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.

**Figure 6-15 Stream Failures Report Selection Fields**

**Step 2**
Choose 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**
Choose a modifier. See Table 6-3 for a description of each modifier.
Stream Activity

Chapter 6      System Reporting

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 that you choose in a later step.</td>
</tr>
<tr>
<td>Server ID</td>
<td>Filters the report by a server ID that you choose in a later step.</td>
</tr>
</tbody>
</table>

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

Step 5  Choose 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, choose 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 can be sorted by clicking on each column heading.

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

Note If Trick Mode Capture is disabled, the session ID does not link to the stream play history. For information on enabling the Trick Mode Capture, see the “Trick Mode Capture” section on page D-5.

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 choose 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**

**Step 2**
Using the drop-down lists provided, or the calendars, choose 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**

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).

![Content Detail Report](image)

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 choose 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 6-24).

**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, choose 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 6-25** shows an example of the Content Activity report.
The report displays:

- Report type
- From and to dates
- Content filenames
- Creation date
- Destroyed date

**Step 7**

To view the details of an in-service content object, click the content filename link (Figure 6-23).

**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 choose 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 6-24).

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

**Step 4** Click Display.

To clear the fields and start over, click Reset.

Figure 6-25 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 choose 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.
Step 2 Using the drop-down lists provided, or the calendars, choose 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.

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.
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.

Table 6-4  Archived Data Types

<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 choose 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).
Step 4  Choose 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 6-23.

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>
</tbody>
</table>
Table 6-5  Content Report Archive Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mURL</td>
<td>The URL of the content file. This field is applicable only for FTP pull.</td>
</tr>
<tr>
<td>mIngestIpAddress</td>
<td>The IP address of the ingest interface on the Vault 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>

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

Stream Reports

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

Table 6-6  Stream Report Archive 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>mGoid</td>
<td>Global object identifier. Used by the CDS database.</td>
</tr>
<tr>
<td>mTsIdOut</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mTsIdIn</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mProgramNumber</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mBandwidthUsed</td>
<td>This field is applicable only when Streaming Mode is set to ASI.</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>mQAMPPort</td>
<td>The port the QAM device is using to receive the stream object.</td>
</tr>
<tr>
<td>mSetTopMac</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mServiceGroup</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mStartTime</td>
<td>The timestamp of when the stream was created. The timestamp is represented in seconds since the start of Unix epoch time.</td>
</tr>
<tr>
<td>mLastTime</td>
<td>Not applicable.</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 on page 5-19 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 on page 5-19 for more information.</td>
</tr>
<tr>
<td>mOperand</td>
<td>The operand that was being operated on at the time of the failure, for example, the StreamID is the operand if a stream was being created or controlled at the time of failure.</td>
</tr>
<tr>
<td>mTask</td>
<td>The failed task is the event category indicating the type of execution sequence that the call stack was currently within at the time of the failure. See Table 5-8 on page 5-19 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>
<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>
</tbody>
</table>

¹. Unix epoch time is 1970-01-01T00:00:00Z
### Table 6-8 Stream Activity Report Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>mNptOffset</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 7-2
- Server Maintenance, page 7-5
- Restarting the Services, page 7-9
- Software Maintenance, page 7-9
- Manuals, page 7-13

**Note**

If Virtual Video Infrastructure (VVI) with split-domain management is enabled, the CDSM pages associated with the Vaults and Caching Nodes display only on the VVI Manager (VVIM), and the CDSM pages associated with the Streamers display only on the Stream Manager. For more information, see the “Virtual Video Infrastructure” section on page D-6.

**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 interrupts 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. After 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.

**Step 2** Fill in the fields as described in Table 7-1.

**Step 3** Click **Add User** to add this user.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Choose the appropriate access level from the drop-down list. See the beginning of this section, the “User Access” section on page 7-2 for descriptions of the access levels.</td>
</tr>
</tbody>
</table>
## Editing User Settings

To change a user password and access level, do the following:

**Step 1** Choose Maintain > Users > Edit User. The Edit User page is displayed.

**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 choose 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 login name. The range is 5 to 20 characters.</td>
</tr>
<tr>
<td>Access</td>
<td>Choose the appropriate access level from the drop-down list. See the beginning of this section, the “User Access” section on page 7-2, 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 7-1 on page 7-4).

**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**.

## 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.
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 4-45.

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 7-1).

**Figure 7-1 User Default Settings Page**

To configure default values for a user select the user from the list, edit the values below, then click Save at the bottom of the page.

- **Select User**:

**Media Scheduler Preferences**

Below are the preferences set for a user, to edit the preferences change the settings below and click Save.

- **Auto on Recurring Scheduling**: (Only for user generated schedules)
  - Presence Existing Schedules
  - Overwrite Existing Schedules

You can choose between auto generating a package name using the start time stamp, or entering the package name manually. If the package name we tried to create already exists.

- **Package Name Auto-Generation**:
  - Enable
  - Disable

**Input Channels Displayed On Media Scheduler**

- [ ] D1-12
- [ ] JUNK-1
- [ ] DCH-1
- [ ] DCH-34
- [ ] DCH-222
- [ ] SUITE-223

**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 <strong>Preserve Exiting Schedules</strong> or <strong>Overwrite Existing Schedules</strong>. 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 <strong>Enable</strong> 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 <strong>Disable</strong>.</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**.

### 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:
Shutting Down a Server

Caution

Shutting down a Vault or Streamer server while there are still active ingests and streams causes the current ingests 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 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.
Step 2 From the Server IP drop-down list, choose the IP address or nickname of the server 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; that is, do not allow new ingests on a Vault and do not allow new streams on a Streamer and move existing streams to another Streamer gracefully.

To enable Server Offload, do the following:

Step 1 Choose Maintain > Servers > Server Offload. The Server Offload page is displayed.
Step 2 From the Server IP drop-down list, choose the IP address or nickname of the server and click Display. The server type and ID, as well as the array ID, are displayed.
Step 3 Choose 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**

After 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:

2. From the Server IP drop-down list, choose the IP address or nickname of the server and click Display. The server type and ID, as well as the array ID, are displayed.
3. Choose 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 5-31. 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 5-2.</td>
</tr>
<tr>
<td>Disk Loss</td>
<td>The Disk indicator box on the “System Health” section on page 5-2.</td>
</tr>
<tr>
<td>Disk Capacity Notify</td>
<td>The “Disk Monitor” section on page 5-24.</td>
</tr>
<tr>
<td>Disk Capacity Warning</td>
<td>The “Disk Monitor” section on page 5-24.</td>
</tr>
<tr>
<td>Linux File System Usage</td>
<td>The “Disk Monitor” section on page 5-24.</td>
</tr>
</tbody>
</table>

To set the system thresholds and enable or disable the system services, do the following

1. Choose Maintain > Servers > System Thresholds. The System Thresholds page is displayed (Figure 7-2).
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.
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.

<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</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:

**Step 1** Choose **Maintain > Services**. The Services Restart page is displayed.

**Step 2** From the **Server IP** drop-down list, choose the IP address or nickname of the server 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 check box next to each service you want to restart and click **Reset**.

Software Maintenance

The Software Maintenance pages provides the ability to view the CDS software, upload an electronic program guide (EPG) file, generate server IDs and group IDs for Video Virtualization Infrastructure (VVI), and upload a topology file. This section covers the following topics:

- Viewing the Software Version and Server Information
- Uploading an EPG File
- Identifying Server IDs and Group IDs for VVI with Split-Domain Management

Viewing the Software Version and Server Information

To view the TV CDS software version and server information, choose **Maintain > Software > Software Version**. The Software Version page is displayed. From the **Server IP** drop-down list, choose the IP address or nickname of the server and click **Display**. The following information is displayed:

- Server type (Vault, Streamer SSV (ISV))
- Software version
- Server ID
- Array ID
- Product ID (PID)—CDE model (for example, CDE220)
- Version ID (VID)—Hardware version (for example, V01)
- Serial number—Serial number of the CDE
- Additional string—Model variation (for example, 4A-C)

### 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 4-23 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.

**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** After the full path and filename of the EPG File is entered, click **Upload**. To clear the fields and start over, click **Reset**.

### Identifying Server IDs and Group IDs for VVI with Split-Domain Management

The VVIM manages all the identifiers, and the Stream Managers get a range of group IDs and server IDs from the VVIM and uses them for the Streamers it manages.

Table 7-6 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

<table>
<thead>
<tr>
<th>CDSM GUI ID Name</th>
<th>CServer Files ID Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array ID on the Array Name page</td>
<td>groupid</td>
</tr>
<tr>
<td>Group ID on the Server-Level pages</td>
<td>groupid</td>
</tr>
<tr>
<td>Stream Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Cache Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Vault Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Stream Group ID on the Configuration Generator page</td>
<td>arrayid</td>
</tr>
</tbody>
</table>
Generating Server IDs and Group IDs from the VVIM

The Configuration Generator page is used to generate group IDs and server IDs for the Stream Managers. When the Stream Manager contacts the VVIM during the initial configuration using the cdsconfig script, the VVIM generates the IDs, sends them to the Stream Manager, and populates the table on the Configuration Generator page. This is done by an HTTP GET request over port 80.

If the Stream Manager is unable to contact the VVIM during the initial configuration, the cdsconfig script prompts the Stream Manager administrator to contact the VVIM administrator for the server ID. The VVIM administrator would then go to the Configuration Generator page to generate the IDs for the Stream Manager.

For HTTP streamers, if the Stream Manager is unable to reach the VVIM, either because port 80 is not open for communication or because of some other connectivity reason, the Stream Manager administrator can contact the VVIM administrator for the needed information. This information consists of the following:

- Stream Group IDs
- Cache Group information

Using the Configuration Generator page, the VVIM administrator can look up the group ID and server ID ranges, and if necessary generate them. The VVIM administrator can provide the beginning group ID for the Stream Groups, which the Stream Manager administrator enters on the Stream Groups Setup page, if prompted to do so.

The Cache Group information is contained in an XML file, called CacheGroupsConfig.xml. The VVIM administrator can click the Download link to view the CacheGroupsConfig.xml file, and right-click the Download link to save the XML file locally. This XML file can be sent to the Stream Manager administrator and the Stream Manager can upload it through the Cache Group Locator page.

To generate new IDs or view the existing IDs, do the following:

---

**Step 1** Choose **Maintain > Software > Configuration Generator**. The Configuration Generator page is displayed (Figure 7-3).

---
Figure 7-3  Configuration Generator Page

The table on the Configuration Generator page lists the Stream Domain Name, Stream Manager IP address, and the ID ranges assigned for each Stream Manager.

Stream Group ID Range and Server ID Range
Sometimes the group IDs and Server IDs show as “not generated” in the table. To generate the IDs, click the Not Generated text in the Stream Group ID Range column. A dialog box is displayed asking if you want to generate the IDs now. Click OK.

Stream Manager IP Address
The IP address of the Stream Manager is not included in the table on the Configuration Generator page until the Stream Manager is configured using the CDSM Setup page. It is possible that the Stream Manager IP address failed to be captured, in which case the entry is displayed as “Not Captured.” Click the Not Captured link to enter the IP address manually. A text box is displayed with an Update icon (plus sign) and a Cancel icon (X).

Step 2 In the Stream Domain Name field, enter the name of the Stream Manager that you are generating IDs for.

Step 3 In the Stream Manager IP field, enter the IP address of the Stream Manager that you are generating IDs for.

Step 4 Click Generate New IDs.
Setup ID Range

Setup IDs are only used in RTSP environments that have split-domain management and are using CCP Streamers. The VVIM only generates two setup IDs for each Stream Domain. A setup ID is used to identify the Setup server in a Stream Group. The Setup and Control servers are configured for each Stream Group on the Control/Setup IP page. See the “Configuring the Control and Setup IPs” section on page 4-40 for more information. If the Stream Manager uses the two allotted setup IDs, it contacts the VVIM for a new set of setup IDs. If the connection between the Stream Manager and VVIM fails, the Stream Manager administrator contacts the VVIM administrator for the IDs. The new setup IDs can be generated by clicking the Generate new Setup ID range icon in the Setup ID Range column.

Note
CCP Streamers are not supported in a VVI split-domain management for RTSP environments.

Manuals

To view the manual, chooseMaintain > Manuals. The Manual page is displayed. Click the link to the manual. The manual is displayed by means of 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.
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-20
- Management and Database Issues, page A-22
- Ingest Issues, page A-23
- Content Processing Issues, page A-27
- Cache-Fill Issues, page A-29
- Streaming and Playout Issues, page A-30
- Session Messaging, page A-35
- Database Issues, page A-37
- Advanced Features and Applications, page A-40
- Frequently Asked Questions, page A-41
- CDS Content Quality Guidelines, page A-46

There are a variety of possible combinations of CDS topologies, backoffice environments, middleware, and so on. The engineers using this troubleshooting appendix are 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 `#` symbol as a prompt. The `isa` user account uses the `$` symbol as a prompt. We strongly recommend that you change these passwords as soon as possible by 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 6-25.
- /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 arroyo/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. 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. 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 yyyymmdd (for example, 20090115 is January 15, 2009). To increase the verbosity of this log file, use the following command:

  ```
  # echo "6" > /proc/calypso/tunables/c2k_verbosedump
  ```

- `/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 yyyymmdd. 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).

**Protocoltiming Warning Messages**

Table A-1 describes some of the warning messages that might be seen in the Protocoltiming log.

<table>
<thead>
<tr>
<th>Warning Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING: Fill transmit bus hold offs</td>
<td>System bus is overloaded or network transmissions are not occurring fast enough and transmission of data is being delayed. The counts following these numbers may be low, this is not a concern because the delay is only 2 microseconds (ms). However, if the counts are high, this can cause stream data delivery problems.</td>
</tr>
<tr>
<td>WARNING: Fill Data Wait</td>
<td>Vault or Caching Node is unable to deliver data to a waiting Caching Node or Streamer because the data is not yet available. If the numbers are low, this is not a concern because the delay is only 2 ms. If the counts are high, this can cause stream data delivery problems.</td>
</tr>
<tr>
<td>WARNING Data Low</td>
<td>Data being streamed has less than 100 ms buffered ahead of the current stream point. Normally there should be a 2-second elasticity buffer for data being transmitted, except for a short interval when the stream first starts and the data is still “bursting” to fill the elasticity buffer. There are no problems as a result of this warning, but it is a precursor to the Fill Data Wait warning.</td>
</tr>
<tr>
<td>WARNING: Disk Refetches</td>
<td>Warning does not indicate any problems with streaming content, just that the disk bandwidth was not being used as efficiently as possible.</td>
</tr>
<tr>
<td>WARNING: No capacity 5 percent</td>
<td>Server was not accepting any new requests, which were sent to it during five percent of the preceding ten-second sample period, because it was out of capacity. Other statistics in the protocoltiming log need to be examined to determine why the server determined it was out of capacity. If Caching Nodes or Streamers are unable to find an alternate server to provide the data they need, a stream failure may occur.</td>
</tr>
</tbody>
</table>
| WARNING: Cannot stripe disk writes | Indicates one of the following two conditions:  
  - Some disk drives are completely full and data can no longer be written to them.  
  - The disk system is under a full-bandwidth load such that some drives are fully committed to reading stream data and are never getting any time to write data to the drive. 

The data storage pattern is not efficient when this happens because the data cannot be spread equally across all the drives. Check other load statistics to determine why the disk system cannot stripe to some drives is useful in determining why these warnings are occurring. |
| WARNING: Mirror Recovery degraded - some remote vaults (0:1) are inaccessible | The configured mirroring has not occurred because 1 or more required Vaults are down, or a partner Vault is up but configured to be in a different Vault Group. |
RTSP Log Files

The Linux user \textit{isa} is the owner of the application files in an RTSP environment. To change from the \textit{root} use the \texttt{su – isa} command.

All application log files are located in \/home\textbackslash{}isa\textbackslash{}bss\textbackslash{}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:

\begin{itemize}
  \item rtsp.err
  \item rtsp.out
  \item fsi.err
  \item fsi.out
\end{itemize}

These files are located in the \/home\textbackslash{}isa\textbackslash{}bss\textbackslash{}log/ directory.

The CDS RTSP environment has the following useful log files:

\begin{itemize}
  \item \/home\textbackslash{}isa\textbackslash{}bss\textbackslash{}log\textbackslash{}fsi.log
  \item \/home\textbackslash{}isa\textbackslash{}bss\textbackslash{}log\textbackslash{}rtsp.log
  \item \/home\textbackslash{}isa\textbackslash{}bss\textbackslash{}log\textbackslash{}aim.log
  \item \/home\textbackslash{}isa\textbackslash{}bss\textbackslash{}log\textbackslash{}library.log—Logs the cache2app library information
\end{itemize}

To change the log levels while the RTSP application is not running, edit the arroyo-env.sh file.

\begin{verbatim}
$ cd /home/isa/bss/scripts/
$ vi arroyo-env.sh
\end{verbatim}

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 \textit{“Configuring RTSP Setup”} section on page 4-73.

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.

\begin{itemize}
  \item \textcolor{red}{Note} This section is informational only. All changes to the configuration files should be accomplished through the initial configuration and CDSM GUI.
\end{itemize}

Table A-2 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.
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 server IDs 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.

---

### Table A-2 ID Names in the CDSM GUI and CServer Files

<table>
<thead>
<tr>
<th>CDSM GUI ID Name</th>
<th>CServer Files ID Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array ID on the Array Name page</td>
<td>groupid</td>
</tr>
<tr>
<td>Group ID on the Server-Level pages</td>
<td>groupid</td>
</tr>
<tr>
<td>Stream Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Cache Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Vault Group ID on the Server Setup page</td>
<td>arrayid</td>
</tr>
<tr>
<td>Stream Group ID on the Configuration Generator page</td>
<td>arrayid</td>
</tr>
</tbody>
</table>
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-7 for more information.
**groupid #**
An identifier that identifies the group of servers within the CDS. See the “groupid ” section on page A-7 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 destination IP address or subnet of the packets. 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.

**Note**
The transport group ID (tgid) has been deprecated. Use the SubnetTable instead. See the “Network” section on page A-17.
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 applicable only to Vaults.

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 are logged to the protocoltiming 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 applicable only 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 selected 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 array this server belongs to. The array ID is used in conjunction with the StreamDestinationMap file located in the /arroyo/test directory to determine which play servers are available for selection. The selection is based on the destination IP address or subnet of the packets. The default value is 0.

**remote site manager <ip address> for arrayid #**

Specifies the IP address of a remote site manager for a specified array. The remote site manager has a list of all the servers that it can connect to that are located at the same site (the servers are listed in the RemoteServers list on the remote site manager). When this server comes up, it contacts the remote site manager and asks for a referral for a server that is in the specified array. The remote site manager returns the IP address of a server from that array. This server sets up connections with all the referred remote servers, and once every minute, checks to see if there are connections with all remote array servers. If for some reason one is not available, this server contacts the remote site manager for another referral.

---

**Note**

You must add the allow new L3 remote servers 1 directive to the setupfile for both this server and the server that gets referred. If you do not add this directive, this server cannot establish a connection with the referred remote server.

---

**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 to be looked at.
- **tport**—After 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:

```
# 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:

```
# 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/statstd             statsd-2009-01-14-03
snmp/agent.531           snmpd-2009-01-16-01
cserver                 cserver-e013-2009-01-16-06
export                   export-e013-2008-10-06-01
avsdbr                   avsdbr-2009-01-06-01
cache2app                r_2_Ov1-isa-e008-2009-01-15-01
isa                      r_2_Ov1-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
tavsdbr                  tavsdbr-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
```

CSserver 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
AVS CServer Release #1-Ncserver-e013-2008-11-17-05 Mon Nov 17 18:54:01 PST 2008
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
  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
=================================================================================================
Int#   R-Mbps  X-Mbps  R-Bytes  X-Bytes
eth0   0       0       56760511  166307653
eth1   0       0       0       0
eth2   4       457     3439241508 3497139080
eth3   4       457     3439172148 3099124288
eth4   4       457     3441836680 2945489644
eth5   4       472     3443060380 2736115618
eth6   4       471     3438423816 2613199736
eth7   5       464     3440066492 2419935662
eth8   4       449     3439982812 2266582156
eth9   4       465     3443251384 2164010982
eth10  5       465     3439982136 1915437726
eth11  4       464     3438935192 397577442
eth12  5       464     3440343164 300903930
```
Kernel Crash

The kernel debugger (KDB) provides information (in the form of a core dump file) when the server processing fails. For the server to enter KDB when the server has crashed, the /proc/sys/kernel/panic parameter must be zero. If the panic parameter is non-zero, the system reboots automatically without entering KDB.

In addition to KDB, there is a kdump service. The kdump service allows you to take a kernel dump of memory. The kdump service runs automatically if the server is configured to reboot automatically after a crash (which means the panic parameter is non-zero). The kdump service stores the kernel memory dump in the /var/arroyo/crash directory. After the kernel memory is dumped, the system reboots into the normal operating system.

If the server is configured to enter KDB (which means the panic parameter is zero), the server enters KDB mode. The kdump command allows you to take a kernel memory dump while the server is in KDB mode. The kdump command reboots the server into kdump mode, takes a kernel memory dump, and reboots the server into the normal operating system.

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=ttySO,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: After 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
```

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>1k-blocks</th>
<th>Used</th>
<th>Available</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hda1</td>
<td>10317828</td>
<td>3764936</td>
<td>6028776</td>
<td>39%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/hda2</td>
<td>20641788</td>
<td>1711372</td>
<td>17881776</td>
<td>9%</td>
<td>/arroyo</td>
</tr>
<tr>
<td>/dev/hda3</td>
<td>8254272</td>
<td>32828</td>
<td>7802148</td>
<td>1%</td>
<td>/arroyo/db</td>
</tr>
<tr>
<td>/dev/hda6</td>
<td>35641880</td>
<td>1185880</td>
<td>32645480</td>
<td>4%</td>
<td>/arroyo/log</td>
</tr>
<tr>
<td>none</td>
<td>1681200</td>
<td>0</td>
<td>1681200</td>
<td>0%</td>
<td>/dev/shm</td>
</tr>
</tbody>
</table>

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.

```
# 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

```
# 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 19:03:47 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)

**Note**

Sometimes on the CDE400, the bus and host resets are used to reset the SATA driver because the Linux
SATA driver, sats_mv.ko, does not provide a device reset vector. If the device is reset when there are no
outstanding requests, warning messages are displayed on the console. These warning messages are
informational and do not indicate a failure.

---

### Memory Issues

To slow down the CDSM bootup 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**.
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:7A:00:00 [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
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window Irtt Iface
111.0.210.0 0.0.0.0 255.255.255.0 U 0 0 0 0 eth0
111.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 0 eth0
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 0 lo
0.0.0.0 111.0.210.1 0.0.0.0 UG 0 0 0 0 eth0
```

To view the CDS subnet table, enter the following command:
```
# cat /arroyo/test/SubnetTable
network 111.1.13.1 netmask 255.255.255.240 gateway 111.1.13.1 transport_source_ip 0
```

**Note**
In Release 2.1, the local networks and their gateways are specified in the SubnetTable file. For backward compatibility, the local subnet and gateway in the RoutingTable are still supported and are used if the SubnetTable file does not exist. The Routing Table can still be used to specify static routes.
To view the CDS routing table, enter the following command:

```bash
# 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:

```bash
# 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.

```bash
# 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 txqueuelen: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.

```bash
# 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
```
Appendix A  Troubleshooting

General Issues

<table>
<thead>
<tr>
<th>IRQ</th>
<th>194</th>
</tr>
</thead>
<tbody>
<tr>
<td>System_Device_Name</td>
<td>eth0</td>
</tr>
<tr>
<td>Current_HWaddr</td>
<td>00:30:48:C3:26:9E</td>
</tr>
<tr>
<td>Permanent_HWaddr</td>
<td>00:30:48:C3:26:9E</td>
</tr>
<tr>
<td>Link</td>
<td>up</td>
</tr>
<tr>
<td>Speed</td>
<td>1000</td>
</tr>
<tr>
<td>Duplex</td>
<td>Full</td>
</tr>
<tr>
<td>State</td>
<td>up</td>
</tr>
<tr>
<td>Rx_Packets</td>
<td>406625</td>
</tr>
<tr>
<td>Tx_Packets</td>
<td>135553</td>
</tr>
<tr>
<td>Rx_Bytes</td>
<td>41539919</td>
</tr>
<tr>
<td>Tx_Bytes</td>
<td>30390314</td>
</tr>
<tr>
<td>Rx_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Tx_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_Dropped</td>
<td>0</td>
</tr>
<tr>
<td>Tx_Dropped</td>
<td>0</td>
</tr>
<tr>
<td>Multicast</td>
<td>236747</td>
</tr>
<tr>
<td>Collisions</td>
<td>0</td>
</tr>
<tr>
<td>Rx_Length_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_Over_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_CRC_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_Frame_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_FIFO_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_Missed_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Tx_Aborted_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Tx_Carrier_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Tx_FIFO_Errors</td>
<td>0</td>
</tr>
<tr>
<td>PHY_Media_Type</td>
<td>Copper</td>
</tr>
<tr>
<td>PHY_Idle_Errors</td>
<td>0</td>
</tr>
<tr>
<td>PHY_Receive_Errors</td>
<td>0</td>
</tr>
<tr>
<td>PHY_MDIX_Enabled</td>
<td>MDI</td>
</tr>
<tr>
<td>PHY_Local_Receiver_Status</td>
<td>OK</td>
</tr>
<tr>
<td>PHY_Remote_Receiver_Status</td>
<td>OK</td>
</tr>
</tbody>
</table>
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 because of 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>During the server bootup, press the <strong>Delete</strong> key to enter the BIOS Setup Utility.</td>
</tr>
<tr>
<td>2</td>
<td>Navigate to the Advanced menu and choose <strong>Advanced Chipset Control</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Choose <strong>ECC Error Type</strong> and change the setting to <strong>NMI</strong> (Figure A-2).</td>
</tr>
<tr>
<td>4</td>
<td>Press <strong>F10</strong> to save and exit.</td>
</tr>
</tbody>
</table>

![Figure A-2 BIOS Setup Utility—Advanced Chipset Control](image)
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 after the kernel is loaded.
- /etc/inittab—Determines the speed after the OS is loaded. Enter the following:

```
$ cat /etc/inittab | grep S0
S0:2345:respawn:/sbin/agetty ttyS0 115200 vt100
```

Note: 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 5-31. 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  172.22.97.193:9999            172.22.97.192:50343  ESTABLISHED
 tcp  0    0  172.22.97.193:9999            172.22.97.196:9999   ESTABLISHED
 tcp  0    0  172.22.97.193:9999            172.22.97.191:50950  ESTABLISHED
 tcp  0    0  172.22.97.193:9999            172.22.97.194:37543  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  172.22.97.193:9999            172.22.97.191:9999   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
```
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
Ingest Issues

- FSI Does Not Start
- Content Not Ingesting
- Asset Ingest Manager Restart Causes Endless Loop

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.

The FSI running mode should be what you set in /home/isa/bss/scripts/arroyo-site-env.sh; for example, set “FSI_DEPLOYMENT=1.”

```
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|19:04:50.048468|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
[fsid.cc:588] ERROR: FSID Port of 0 is an invalid port address
```

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 4-78 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_cserver is running. If the avs_cserver is not running, enter the rpm –qa | grep cserver command to see if it is installed.
```

- If avs_cserver is installed, enter the /arroyo/test/run command to start avs_cserver.

- If avs_cserver 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.
**Appendix A  Troubleshooting**

**Ingest Issues**

**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
RECVDFSTICALCALLBACK 2251799813686769 400 FTPProcess.cc:328: Caught exception: 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|AVSIngestMgrr1SA |0178|01024|******************** AIMd starting********************
12/12/2007|11:47:16.684145|pRunMaster       |0035|01024|Current process is the master
12/12/2007|11:47:16.745753|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[libAVSWideVine_AIM.so: cannot open shared object file: No such file or directory]
```

...
Ingest Issues

Appendix A      Troubleshooting

Ingest Issues

12/12/2007|15:55:20.324330|AIMDbManager     |0055|02051|Config change to [omeplace.here.there:8082/totalmanage/vod]{}
12/12/2007|15:55:20.325100|AIMDbManager     |0054|02051|Config change from [/totalmanage/vod][5001]
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|15:56:20.445690|AIMCache         |0316|02051|DB Tag[0004/]{}
12/12/2007|15:56:20.446060|AIMDbManager     |0054|02051|Config change from [.0.0.0:20004/]{}
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.

Action 1: Cause a failover between the master and slave Vaults.
On the master Vault, stop the statsd and Ingest Manager (AIM) services, thereby causing Vault failover. The AIM service on the new master Vault should immediately start processing ingest requests.

On the old master Vault, log in as root and restart the statsd 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. See the “CDS Content Quality Guidelines” section on page A-46 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-17.

**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:

```bash
$ 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:

1. **Step 1** Modify the `/home/isa/.arroyorc` file by adding the following line:

   ```
   cserver_opts "vault local copy count 2"
   ```

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.

```
echo 2 > /proc/calypso/tunables/vaultlocalcopycount
```

**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 4-56.

**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 `/arroyo/log/serverinfo.log.<date>` log file contains information about the GOIDs.

**Note** There is no need to identify and delete damaged or orphaned GOIDs. CServer repairs any damaged GOIDs. Orphaned GOIDs are deleted when the server reboots.
**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:

```bash
$ 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-27.

**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
==>/arroyo/log//c2k.log.01152008==>
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:igate goid d346434b982851 finished read 0 length e3 lastbytes b4 retries 0 reqlen 0/e3
15-Jan-2008 20:42:41 UTC:err:IGate::ReadClose(goid 0): ERROR: Never saw header
15-Jan-2008 20:42:41 UTC:err:IGate::ReadClose(goid 0): ERROR: Never saw EOF record
15-Jan-2008 20:42:44 UTC:out:igate goid d346434b982851 finished read 0 length e3 lastbytes b4 retries 1 reqlen 0/e3
```
15-Jan-2008 20:42:44 UTC :err:IGate::ReadClose(goid 0): ERROR: Never saw header
15-Jan-2008 20:42:44 UTC :err:IGate::ReadClose(goid 0): ERROR: Never saw EOF record
15-Jan-2008 20:42:47 UTC :out:igate goid d346434b982851 finished read 0 length e3 lastbytes b4 retries 2 reqlen 0/e3
15-Jan-2008 20:42:47 UTC :err:IGate::ReadClose(goid 0): ERROR: Never saw header
15-Jan-2008 20:42:47 UTC :err:IGate::ReadClose(goid 0): ERROR: Never saw EOF record

==gt rtsp.log ==
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|21:43:03.585957|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=20080115T204303.5862
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 4-56 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 because 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 problem reaching 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 because of the ARP timeout process the CServer is going through to reach the destination. After 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**, choose 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 5-27.

**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 protocol_timing.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 4-63.

**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. After 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 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 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=CAN6099.mpg RTSP/1.0^M CSeq: 10^M User-Agent: OpenTV VOD 1.0^M Transport: MP2T/DVBC/QAM;unicast;client=168892769.6501124101;destination=172.23.68.2;client_port=1^M
06/13/2007|20:23:33.548631|RTSPTCPLiListener.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|20:23:33.548942|StreamImpl.cc|111|Stream handle set to: = 1
06/13/2007|20:23:33.549200|StreamImpl.cc|1745|Stream setup - URL = CAN6099.mpg, downstream address = 1179649:172.23.68.2!1
06/13/2007|20:23:33.550150|QuativeSession.cc|782|SETUP Response: RTSP/1.0 200 OK^M CSeq: 10^M Session:1179649; timeout=300^M Transport: MP2T/DVBC/QAM;unicast;client=168892769.6501124101;destination=172.23.68.2;client_port=1^M
06/13/2007|20:23:33.550377|PersistenceConnection.cc|137|Repository operation successfully completed
06/13/2007|20:23:33.550553|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:23:37.313064|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:23:37.313753|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:23:37.314893|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:23:37.315025|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
```
Streaming and Playout Issues

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 CSeq: 2 User-Agent: OpenTV VOD 1 Transport: MP2T/DVBC/QAM;unicast;client=170027388.4312020202;destination=172.23.77.2;client_port=16

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|16:10:56.954832|PersistenceConnection.cc|137|Repository operation successfully completed

11/29/2007|16:10:57.195306|RTSPTCPListener.cc|298|Valid RTSP request received, port = 554
11/29/2007|16:10:57.195443|RTSPMsgHandler.cc|644|Current session count = 1
11/29/2007|16:10:57.195711|ContentManager.cc|277|Calculated content duration: = 3814142

Content-Type: application/sdp M Content-Length: 170 M v=0 M c= IN IP4 10.236.0.0 M m=video 0 udap M2T=246 423070425 M a=range:npt=0-3814.142
```

Notice:5402 Event-Date=20070613T182913.076Z "Client Session Terminated"
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 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-3 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>
</tbody>
</table>
Database Issues

This section covers the following database issues and troubleshooting methods:

- Database Replication
- Corruption Recovery

### Table A-3 \( \text{RTSP Status Codes (continued)} \)

<table>
<thead>
<tr>
<th>State</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOT_FOUND</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>
<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"     |
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

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:

```
$ grep index /arroyo/log/avsdb.log.20071106
```

```
11-06-2007 07:54:22PM:db_error DB_SECONDARY_BAD:Secondary index inconsistent with primary -30976
11-06-2007 07:54:22PM:db_error DB_SECONDARY_BAD:Secondary index inconsistent with primary -30976
11-06-2007 07:54:22PM:db_error DB_SECONDARY_BAD:Secondary index inconsistent with primary -30976
11-06-2007 07:54:22PM:db_error DB_SECONDARY_BAD:Secondary index inconsistent with primary -30976
11-06-2007 07:54:22PM:db_error DB_SECONDARY_BAD:Secondary index inconsistent with primary -30976
11-06-2007 07:54:22PM:db_error DB_SECONDARY_BAD:Secondary index inconsistent with primary -30976
```

The example output indicates that the Vault and CDSM databases are not synchronized, possibly because of the server times not being synchronized, a network connectivity issue, a server failure, or some other similar issue.

For resolution, see the “Corruption Recovery” section on page A-39.

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:

- There are many log files with a filename similar to log.00000XXXX in the /home/isa/Berkeley/DATADIR directory.
Appendix A  Troubleshooting

Database Issues

- Database could not be started. See the “Services Monitor” section on page 5-31 for more information.
- Bidirectional connections are lost between servers. See the “Required Services Not Starting or Running Correctly” section on page A-21.
- The following error message is listed in the /arroyo/log/avsdb-err.log.yyyyMMdd file:

```
tavsd: unable to allocate memory for mutex; resize mutex region
```

```
# tail -f avsdb-err.log.20081111
```

```
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
tavsd: unable to allocate memory for mutex; resize mutex region
```

- The /home/isa/Berkeley/DATADIR/REPLAY.db file increases to several GB.

```
$ ls -ltr
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002824
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002825
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002826
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002837
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002838
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002839
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002840
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002841
-rw------- 1 isa isa 10485760 Nov 11 17:46 log.0000002842
-rw-r--r-- 1 isa isa 5726769152 Nov 12 15:23 REPLAY.db
```

For resolution, see the “Corruption Recovery” section on page A-39.

Corruption Recovery

⚠️  Caution

Escape 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**
Confirm that the database is shut down.

```
#/usr/bin/db_shutdown
```

```
isa 2646 1 0 Jan09 00:14:50 /arroyo/db/avsdb
root 26088 26059 0 13:23 pts/1 00:00:00 grep avsdb
```

Make sure there is no avsdb process returned. If the avsdb 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  Confirm that the database is shut down.

        # ps -ef | grep avsdb

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.

        # su - isa
        # ps -ef | grep avsdb

Step 8  As user root, restart the CDSM database.

        # su - isa
        # ps -ef | grep avsdb

Step 9  Check the configuration on the CDSM and make sure no configuration parameters were lost.

---

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 4-23 for more information.

3.  Upload channel schedules by importing the electronic program guide (EPG). See the “Uploading an EPG File” section on page 7-10 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, choose “ON” and click **Submit**. For more information, see the “CDSM or VVIM Setup” section on page D-3.

**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).

```bash
# 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 0 172.22.97.194:9999 172.22.97.192:40207 ESTABLISHED
tcp 0 0 172.22.97.194:41815 172.22.97.192:9999 ESTABLISHED
tcp 0 0 172.22.97.194:9999 172.22.97.193:33196 ESTABLISHED
tcp 0 0 172.22.97.194:43269 172.22.97.191:9999 ESTABLISHED
```
If you can not 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/arroworc 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.

**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:

```
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.

```
# 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:

```
# /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:

```
# 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?

```
# 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:

```
kdb=off panic=1
kernel /boot/vmlinuz-2.4.32avs ro root=/dev/hda1 console=tt0 console=tt0S0,115200
```

```
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-14).

Q. How do I identify any holes in the content?
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
```

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.

```bash
# 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
```

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:

```bash
# 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 about 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:

```bash
# 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:

```bash
# su - isa
# cd ~/SDClient

Update the SDClient.cfg file with the local IP address.

# ./sdClient

Follow the SDClient menus.
```

Q. How do I view the CServer core 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.

```bash
# 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 31 maxrate 9000000 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
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 goid 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/calyxo/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 13818-1 and 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 15 GB, 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. 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. 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 are identified.

23. Content is filtered out if five seconds of null frames are identified.
Creating Bulk Configuration Files

This appendix describes the Bulk Configuration feature and consists of the following topics:

- Introduction, page B-1
- Creating QAM Gateway Bulk Configuration Files, page B-2
- Creating Stream Destination Bulk Configuration Files, page B-4
- Creating Route Table Bulk Configuration Files, page B-5
- Creating SNMP Agent Bulk Configuration Files, page B-6
- Creating DNS Server Bulk Configuration Files, page B-7
- Creating NTP Server Bulk Configuration Files, page B-8
- Creating FSI Setup Bulk Configuration Files, page B-9
- Creating RTSP Setup Bulk Configuration Files, page B-10
- Bulk Configuration XML Schema, page B-13

Introduction

Bulk Configuration provides a method of configuring common parameters for all the servers at one time by using an XML file. Following are the CDSM GUI configuration pages that offer Bulk Configuration:

- QAM Gateway
- Headend Setup
- Stream Destination
- NTP Server
- Server DNS
- SNMP Agent
- Route Tables
- RTSP Setup
- FSI Setup

Note

To enable the optional Bulk Configuration feature, see the “Bulk Configuration” section on page D-4.
Creating QAM Gateway Bulk Configuration Files

The QAM Gateway page is used to identify the QAM device (IP address), and to configure the preference settings for the Stream Groups. For Layer 2 networks, there is an option to specify the MAC address of the next hop for each Stream Group and Streamer.

Before you can use the Bulk Configuration feature to configure QAM gateways and the headend setup, all Streamers must be associated with a Stream Group. For more information on Stream Groups, see the “Configuring Stream Groups” section on page 4-28.

Table B-1 describes the Bulk Configuration file elements for QAM gateways for gigabit Ethernet streaming.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QAMLList</td>
<td>QAM</td>
<td>—</td>
<td>Marks beginning and end of QAM devices.</td>
</tr>
<tr>
<td>QAM</td>
<td>QAMStreamGroupPreference</td>
<td>IP</td>
<td>Defines a QAM device.</td>
</tr>
<tr>
<td>QAMStreamGroupPreference</td>
<td>Server</td>
<td>StreamGroupName QAMMAC Preference</td>
<td>Maps Stream Groups to the QAM device. The QAMMAC attribute is optional and is only used for Layer 2 networks.</td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID GroupID QAMMAC</td>
<td>Optional. Maps the MAC address of the QAM device to a Streamer. Only used in Layer 2 networks.</td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring QAM Gateways” section on page 4-4. The ServerID and GroupID attributes are assigned during the initial configuration of the server and are displayed as server ID and group ID on the Server Setup page. For more information, see the “Configuring the Servers” section on page 4-56.

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the CDS. The ALL value is case sensitive.

The Preference attribute can have a value of High or None. These values are case sensitive.

Following is an example of the Bulk Configuration file used to populate the QAM Gateway page. The example is for a Layer 2 network and uses the optional QAMMAC attribute for the QAMStreamGroupPreference and the optional Server element to specify the next hop MAC address.

```xml
<QAML xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcsl"
     <QAM IP="1.1.1.1"> <QAMStreamGroupPreference StreamGroupName="SG1" QAMMAC="00:00:00:00:00:01" Preference="High"> <Server ServerID="50" GroupID="1" QAMMAC="00:00:00:00:00:11" /> </QAMStreamGroupPreference> <QAMStreamGroupPreference StreamGroupName="SG2" QAMMAC="00:00:00:00:00:02" Preference="None"> <Server ServerID="55" GroupID="1" QAMMAC="00:00:00:00:00:11" /> </QAMStreamGroupPreference> <QAMStreamGroupPreference StreamGroupName="SG3" QAMMAC="00:00:00:00:00:03" Preference="None"/> </QAM>
```
Creating Headend Setup Bulk Configuration Files

The Bulk Configuration file for the Headend Setup page consist of service groups to Stream Groups mappings. Table B-2 defines the Bulk Configuration file elements for headend setup.

Table B-2  Bulk Configuration File Elements for Headend Setup

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headend</td>
<td>ServiceGroupToStreamGroup</td>
<td>—</td>
<td>Marks beginning and end of mapping of service groups to Stream Groups.</td>
</tr>
<tr>
<td>ServiceGroupToStreamGroup</td>
<td>—</td>
<td>ServiceGroup StreamGroup</td>
<td>Maps service groups to Stream Groups.</td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring the Headend Setup” section on page 4-7. Following is an example of the Bulk Configuration file used to populate the Headend Setup page:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Headend
    xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs">
    <ServiceGroupToStreamGroup ServiceGroup="4666669" StreamGroup="NEWTEST" />
    <ServiceGroupToStreamGroup ServiceGroup="4666668" StreamGroup="s234" />
    <ServiceGroupToStreamGroup ServiceGroup="4666664" StreamGroup="NEWTEST" />
    <ServiceGroupToStreamGroup ServiceGroup="4666663" StreamGroup="s234" />
    <ServiceGroupToStreamGroup ServiceGroup="1666669" StreamGroup="NEWTEST123" />
    <ServiceGroupToStreamGroup ServiceGroup="1666668" StreamGroup="s234" />
    <ServiceGroupToStreamGroup ServiceGroup="1666664" StreamGroup="NEWTEST" />
    <ServiceGroupToStreamGroup ServiceGroup="1666663" StreamGroup="s234" />
</Headend>
```
Creating Stream Destination Bulk Configuration Files

If the Stream Destination is set to IPTV, the Stream Destination page is displayed instead of the QAM Gateway and Headend Setup pages. For more information, see the “Stream Destination” section on page D-4. The Stream Destination page provides a way to associate subnetworks with Stream Groups. Table B-3 defines the Bulk Configuration file elements for Stream Destination.

Table B-3  Bulk Configuration File Elements for Stream Destination

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StreamDestinationList</td>
<td>StreamDestination</td>
<td>—</td>
<td>Marks beginning and end of subnets defined for IPTV.</td>
</tr>
<tr>
<td>StreamDestination</td>
<td>StreamGroupPreference</td>
<td>SubnetAddress SubnetMask</td>
<td>Defines a subnet.</td>
</tr>
<tr>
<td>StreamGroupPreference</td>
<td>—</td>
<td>StreamGroupName Preference</td>
<td>Maps Stream Groups to the subnet address.</td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring Stream Destinations” section on page 4-8.

The Preference attribute can have a value of **High** or **None**. These values are case sensitive.

Following is an example of the Bulk Configuration file used to populate the Stream Destination page.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<StreamDestinationList
 xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs">
 <StreamDestination SubnetAddress="132.2.2.0" SubnetMask="255.255.255.0">
  <StreamGroupPreference StreamGroupName="NEWTEST" Preference="High" />
  <StreamGroupPreference StreamGroupName="s234" Preference="None" />
 </StreamDestination>
 <StreamDestination SubnetAddress="130.10.10.0" SubnetMask="255.255.255.0">
  <StreamGroupPreference StreamGroupName="s234" Preference="High" />
  <StreamGroupPreference StreamGroupName="NEWTEST" Preference="None" />
 </StreamDestination>
</StreamDestinationList>
```
Creating Route Table Bulk Configuration Files

The Route Table page allows you to define multiple subnets on a server. For more information, see the “Configuring the Route Table” section on page 4-63.

Table B-4 defines the Bulk Configuration file elements for the Route Table page.

### Table B-4  Bulk Configuration File Elements for Route Tables

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RouteTableList</td>
<td>RouteTable</td>
<td>—</td>
<td>Marks beginning and end of defined routes.</td>
</tr>
<tr>
<td>RouteTable</td>
<td>Server</td>
<td>—</td>
<td>Defines a route table.</td>
</tr>
<tr>
<td></td>
<td>Route</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID</td>
<td>Identifies the CDS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GroupID</td>
<td></td>
</tr>
<tr>
<td>Route</td>
<td>—</td>
<td>Network</td>
<td>Defines a route.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SubnetMask</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RouteType</td>
<td></td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring the Route Table” section on page 4-63. The ServerID and GroupID attributes are assigned during the initial configuration of the server and are displayed as server ID and group ID on the Server Setup page. For more information, see the “Configuring the Servers” section on page 4-56.

- **Note**
  The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the CDS. The ALL value is case sensitive.

The RouteType attributes possible values are: cServer Source, cServer Destination, or Stream Control. These values are case sensitive.

Following is an example of the Bulk Configuration file used to populate the Route Table page:

```xml
<?xml version="1.0" encoding="UTF-8"?>

<RouteTableList xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
  <RouteTable>
    <Server ServerID="ALL" GroupID="ALL"/>
    <Route Network="3.2.3.0" SubnetMask="255.255.255.0" Gateway="1.1.1.10" RouteType="cServer Source" />
    <Route Network="3.2.5.0" SubnetMask="255.255.255.0" Gateway="1.1.1.1" RouteType="cServer Source" />
    <Route Network="3.2.6.0" SubnetMask="255.255.255.0" Gateway="1.1.1.10" RouteType="cServer Source" />
    <Route Network="4.2.7.0" SubnetMask="255.255.255.0" Gateway="1.1.1.10" RouteType="cServer Source" />
    <Route Network="5.2.8.0" SubnetMask="255.255.255.0" Gateway="1.1.1.10" RouteType="cServer Source" />
    <Route Network="2.2.9.0" SubnetMask="255.255.255.0" Gateway="1.1.1.10" RouteType="cServer Source" />
    <Route Network="6.2.10.0" SubnetMask="255.255.255.0" Gateway="1.1.1.10" RouteType="cServer Source" />
    <Route Network="7.2.11.0" SubnetMask="255.255.255.0" Gateway="1.1.1.10" RouteType="cServer Source" />
  </RouteTable>
  <RouteTable>
    <Server ServerID="50" GroupID="1111"/>
    <Server ServerID="51" GroupID="1111"/>
    <Server ServerID="52" GroupID="1111"/>
    <Server ServerID="53" GroupID="1111"/>
  </RouteTable>
</RouteTableList>
```
Creating SNMP Agent Bulk Configuration Files

The SNMP Agent page is used to configure SNMP communication. Table B-5 defines the Bulk Configuration file elements for the SNMP Agent page.

Table B-5  Bulk Configuration File Elements for SNMP Agent

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPAgentList</td>
<td>SNMPAgent</td>
<td>—</td>
<td>Marks beginning and end of defined SNMP agents.</td>
</tr>
<tr>
<td>SNMPAgent</td>
<td>Server</td>
<td>Contact</td>
<td>Defines an SNMP agent.</td>
</tr>
<tr>
<td></td>
<td>SNMPCommunity</td>
<td>GroupID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMPTrapStation</td>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID</td>
<td>Identifies the CDS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GroupID</td>
<td></td>
</tr>
<tr>
<td>SNMPCommunity</td>
<td>—</td>
<td>Name</td>
<td>Defines the community for the SNMP agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Permissions</td>
<td></td>
</tr>
<tr>
<td>SNMPTrapStation</td>
<td>—</td>
<td>TrapStation</td>
<td>Defines the trap station for the SNMP agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version</td>
<td></td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring the SNMP Agent” section on page 4-67. The ServerID and GroupID attributes are assigned during the initial configuration of the server and are displayed as server ID and group ID on the Server Setup page. For more information, see the “Configuring the Servers” section on page 4-56.

The ServerID and GroupID attributes can have the value **ALL** if the configuration applies to all servers in the CDS. The **ALL** value is case sensitive.

Following is an example of the Bulk Configuration file used to populate the SNMP Agent page:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<SNMPAgentList
  xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
  <SNMPAgent Contact="TestContact" Location="TestLocation">
    <Server ServerID="ALL" GroupID="ALL"/>
    <SNMPCommunity Name="public" Permissions="Read-Only"/>
    <SNMPCommunity Name="public2" Permissions="Read-Only"/>
  </SNMPAgent>
</SNMPAgentList>
```
Creating DNS Server Bulk Configuration Files

The Server DNS page is used to configure the DNS servers. Table B-6 defines the Bulk Configuration file elements for the Server DNS page.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSList</td>
<td>DNS</td>
<td>—</td>
<td>Marks the beginning and ending of the DNS settings</td>
</tr>
<tr>
<td>DNS</td>
<td>Server</td>
<td>—</td>
<td>Defines the DNS server settings.</td>
</tr>
<tr>
<td></td>
<td>DomainSuffix</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNSServer</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID</td>
<td>Identifies the CDS server.</td>
</tr>
<tr>
<td></td>
<td>—</td>
<td>GroupID</td>
<td></td>
</tr>
<tr>
<td>DomainSuffix</td>
<td>—</td>
<td>—</td>
<td>Defines the domain suffix.</td>
</tr>
<tr>
<td>DNSServer</td>
<td>—</td>
<td>—</td>
<td>Defines the DNS server.</td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring the Server Level DNS” section on page 4-69. The ServerID and GroupID attributes are assigned during the initial configuration of the server and are displayed as server ID and group ID on the Server Setup page. For more information, see the “Configuring the Servers” section on page 4-56.

Note

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the CDS. The ALL value is case sensitive. The Permission attribute can have the value of Read-Only or Read-Write.

Following is an example of the Bulk Configuration file used to populate the Server DNS page:

```
<?xml version="1.0" encoding="UTF-8"?>

<DNSList
    xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs">
    <DNS>
```

---

<SNMPTrapStation TrapStation="77.77.77.77" Version="v1"/>

<SNMPTrapStation TrapStation="177.77.77.77" Version="v2"/>

</SNMPAgent>

<SNMPAgent Contact="XXXX" Location="YYYY">
    <Server ServerID="71" GroupID="1111" />
    <Server ServerID="72" GroupID="1111" />
    <Server ServerID="73" GroupID="1111" />
    <Server ServerID="74" GroupID="1111" />
    <Server ServerID="75" GroupID="1111" />

    <SNMPCommunity Name="XXXX" Permissions="Read-Only"/>
    <SNMPCommunity Name="YYYY" Permissions="Read-Only"/>

    <SNMPTrapStation TrapStation="5.99.99.9" Version="v1"/>
    <SNMPTrapStation TrapStation="55.77.77.77" Version="v2"/>

</SNMPAgent>

</SNMPAgentList>
Creating NTP Server Bulk Configuration Files

The NTP Server page is used to configure the NTP servers. Table B-7 defines the Bulk Configuration file elements for the NTP Server page.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTPServerList</td>
<td>NTPServer</td>
<td>—</td>
<td>Marks the beginning and ending of the NTP settings.</td>
</tr>
<tr>
<td>NTPServer</td>
<td>Server</td>
<td>NTPServerIP</td>
<td>Defines the NTP settings.</td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID</td>
<td>Identifies the CDS server.</td>
</tr>
<tr>
<td></td>
<td>—</td>
<td>GroupID</td>
<td></td>
</tr>
<tr>
<td>NTPServerIP</td>
<td>—</td>
<td>—</td>
<td>Defines the NTP server.</td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring the Server Level NTP” section on page 4-70. The ServerID and GroupID attributes are assigned during the initial configuration of the server and are displayed as server ID and group ID on the Server Setup page. For more information, see the “Configuring the Servers” section on page 4-56.

**Note**

The ServerID and GroupID attributes can have the value **ALL** if the configuration applies to all servers in the CDS. The **ALL** value is case sensitive.

Following is an example of the Bulk Configuration file used to populate the NTP Server page:

```xml
<?xml version="1.0" encoding="UTF-8"?>

<NTPServerList
    xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
    <NTPServer>
        <Server ServerID="ALL" GroupID="ALL"/>
        <NTPServerIP>198.168.1.10</NTPServerIP>
        <NTPServerIP>172.31.2.11</NTPServerIP>
    </NTPServer>
</NTPServerList>
```
Creating FSI Setup Bulk Configuration Files

The FSI Setup page is used to configure the FSI. Table B-8 defines the Bulk Configuration file elements for the FSI Setup page.

Table B-8  Bulk Configuration File Elements for FSI Setup

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSISetupList</td>
<td>FSISetup</td>
<td>—</td>
<td>Marks the beginning and ending of the FSI settings.</td>
</tr>
<tr>
<td>FSISetup</td>
<td>Server</td>
<td>IPAddress, ServerPort, FTPClientPort, FTPOutServerPort, FTPOutLoginTTL, LogLevel, ContentRootPath, AsyncCallbackURL</td>
<td>Defines the FSI settings.</td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID, GroupID</td>
<td>Identifies the CDS server.</td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring FSI Setup” section on page 4-78. The ServerID and GroupID attributes are assigned during the initial configuration of the server and are displayed as server ID and group ID on the Server Setup page. For more information, see the “Configuring the Servers” section on page 4-56.

Note

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the CDS. The ALL value is case sensitive. The LogLevel attribute can have the value of High, Low, or Off.

Following is an example of the Bulk Configuration file used to populate the FSI Setup page:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<FSISetupList
    xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
    <FSISetup IPAddress="171.1.1.1"
        ServerPort="333"
        FTPClientPort="555"
        FTPOutServerPort="5001"
        FTPOutLoginTTL="64"
        LogLevel="Off"
        ContentRootPath="/videcontent/"
        AsyncCallbackURL="http://1.1.1.1/test.php" >
        <Server ServerID="61" GroupID="1111"/>
    </FSISetup>
</FSISetupList>
```
Creating RTSP Setup Bulk Configuration Files

The RTSP Setup page is used to configure the RTSP. Table B-9 defines the Bulk Configuration file elements for the RTSP Setup page.

Table B-9  Bulk Configuration File Elements for RTSP Setup

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTSPSetupList</td>
<td>RTSPSetup</td>
<td>—</td>
<td>Marks the beginning and ending of the RTSP settings.</td>
</tr>
<tr>
<td>RTSPSetup</td>
<td>Server</td>
<td></td>
<td>See the RTSP Setup Fields table for a description of</td>
</tr>
<tr>
<td></td>
<td>RTSPClientList</td>
<td></td>
<td>the values and the applicable fields for your RTSP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>deployment.</td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID</td>
<td>Identifies the CDS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GroupID</td>
<td></td>
</tr>
<tr>
<td>RTSPClientList</td>
<td>RTSPClient</td>
<td>—</td>
<td>Marks the beginning and ending of the RTSP clients.</td>
</tr>
<tr>
<td>RTSPClient</td>
<td>—</td>
<td>ReceivePort</td>
<td>Defines the RTSP client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SendPOrt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReceiveBuffer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Model</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transport</td>
<td></td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring RTSP Setup” section on page 4-73. The ServerID and GroupID attributes are assigned during the initial configuration of the server and are displayed as server ID and group ID on the Server Setup page. For more information, see the “Configuring the Servers” section on page 4-56.

Note

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the CDS. The ALL value is case sensitive.

Following are examples of the Bulk Configuration file used to populate the RTSP Setup page for the different RTSP deployment types:

**DSM-CC RTSP Deployment**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
 xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
 <RTSPSetup MasterStreamingIP="1.1.1.1"
 BackofficeTimeout="3000"
 RTSPServerIP="121.1.1.2"
 LSCPAddress="1.1.1.1"
 LSCPPort="1111"
 LSCPResponsePadding="on"
 RTSPServerPort="5000"
 LogLevel="Off"
 MaintenanceMode="on">
 <Server ServerID="5" GroupID="111"/>
 <RTSPClient ReceivePort="111" SendPort="222" ReceiveBuffer="65535" Model="nCube" Transport="TCP" />
```
<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
    xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
    <RTSPSetup MasterStreamingIP="121.1.1.1"
        LoopingSessionTimeout="11000"
        SessionInactivityTimeout="22000"
        BackofficeTimeout="33000"
        RTSPServerIP="171.1.1.2"
        RTSPServerPort="15000"
        ReconnectIP="12.1.1.3"
        ReconnectPort="9000"
        MaxHistory="5"
        LogLevel="high"
        MaintenanceMode="off">
        <Server ServerID="2" GroupID="1111"/>
        <RTSPClient ReceivePort="3111" SendPort="9222" ReceiveBuffer="65535" Model="nCube" Transport="TCP" />
        <RTSPClient ReceivePort="3999" SendPort="8888" ReceiveBuffer="65535" Model="Diego" Transport="TCP" />
    </RTSPSetup>
</RTSPSetupList>

<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
    xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
    <RTSPSetup MasterStreamingIP="1.1.1.1"
        BackofficeTimeout="3000"
        SessionInactivityTimeout="22000"
        RTSPServerIP="121.1.1.2"
        RTSPServerPort="5000"
        LSCPAddress="1.1.1.1"
        LSCPPort="1111"
        LSCPResponsePadding="on"
        ComponentName="xyz"
        LogLevel="low"
        MaintenanceMode="on">
        <Server ServerID="2" GroupID="1111"/>
        <RTSPClient ReceivePort="111" SendPort="222" ReceiveBuffer="65535" Model="nCube" Transport="TCP" />
        <RTSPClient ReceivePort="999" SendPort="888" ReceiveBuffer="65535" Model="Diego" Transport="TCP" />
    </RTSPSetup>
</RTSPSetupList>

<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
    xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
    <RTSPSetup MasterStreamingIP="1.1.1.1"
        SessionInactivityTimeout="22000"
        LogLevel="high"
        MaintenanceMode="on">
        <Server ServerID="2" GroupID="1111"/>
    </RTSPSetup>
</RTSPSetupList>
Appendix B      Creating Bulk Configuration Files

Creating RTSP Setup Bulk Configuration Files

<EventIS on-vpath RTSP Deployment>
<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
<RTSPSetup MasterStreamingIP="172.1.1.1" 
 BackofficeTimeout="3000"
 SessionInactivityTimeout="22000"
 AuthenticationManagerIP="121.1.1.2"
 AuthenticationManagerPort="5000"
 BandwidthManagerIP="121.1.1.2"
 BandwidthManagerPort="5000"
 BackupBandwidthManagerIP="1.1.1.1"
 BackupBandwidthManagerPort="1111"
 LogLevel="high"
 MaintenanceMode="off">
<Server ServerID="2" GroupID="1111"/>
<RTSPClient ReceivePort="111" SendPort="222" ReceiveBuffer="65535" Model="nCube" Transport="TCP" />
<RTSPClient ReceivePort="999" SendPort="888" ReceiveBuffer="65535" Model="Diego" Transport="TCP" />
</RTSPSetup>
</RTSPSetupList>

<EventIS off-vpath RTSP Deployment>
<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
<RTSPSetup MasterStreamingIP="172.1.1.1" 
 SessionInactivityTimeout="2000"
 AuthenticationManagerIP="121.1.1.2"
 AuthenticationManagerPort="5000"
 ServerIP="10.1.1.1"
 ServerPort="5555"
 StreamControlIP="191.1.1.2"
 StreamControlPort="9000"
 LogLevel="high"
 MaintenanceMode="off">
<Server ServerID="2" GroupID="1111"/>
<RTSPClient ReceivePort="111" SendPort="222" ReceiveBuffer="65535" Model="nCube" Transport="TCP" />
<RTSPClient ReceivePort="999" SendPort="888" ReceiveBuffer="65535" Model="Diego" Transport="TCP" />
</RTSPSetup>
</RTSPSetupList>

<Quative RTSP Deployment>
<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList xmlns="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs" >
<RTSPSetup MasterStreamingIP="172.1.1.1" 
 SessionInactivityTimeout="2000"
 CallbackServerIP="129.1.1.2"
 CallbackServerPort="4000"
 LogLevel="low"
 MaintenanceMode="on"
<Server ServerID="2" GroupID="1111"/>
<RTSPClient ReceivePort="111" SendPort="222" ReceiveBuffer="65535" Model="nCube" Transport="TCP"/>
<RTSPClient ReceivePort="999" SendPort="888" ReceiveBuffer="65535" Model="Diego" Transport="TCP"/>
</RTSPSetup>
</RTSPSetupList>

## Bulk Configuration XML Schema

The XML Schema file describes and dictates the content of the XML file. The BulkConfiguration.xsd file contains the XML schema.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ws="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs"
targetNamespace="http://www.cisco.com/schemas/VCPBU/CDS-TV/R0/ciscowebsvcs">
    <!-- Configure/Server/ elements -->
    <xs:element name="Server">
        <xs:complexType>
            <xs:attribute name="ServerID" type="xs:string" use="required"/>
            <xs:attribute name="GroupID" type="xs:string" use="required"/>
            <xs:attribute name="QAMMAC" type="xs:string"/>
        </xs:complexType>
    </xs:element>
    <!-- Configure/System/QAMGateway/ elements -->
    <xs:element name="QAMStreamGroupPreference">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded"/>
                <xs:attribute name="StreamGroupName" type="xs:string"/>
                <xs:attribute name="QAMMAC" type="xs:string"/>
                <xs:attribute name="Preference" type="xs:string"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="TSIDOutLink">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ws:TSIDOutLink" minOccurs="0" maxOccurs="unbounded"/>
                <xs:attribute name="Index" type="xs:nonNegativeInteger"/>
                <xs:attribute name="TSIDOut" type="xs:string"/>
                <xs:attribute name="TSIDOutLinkStatus" type="xs:string"/>
                <xs:attribute name="ServiceGroup" type="xs:string"/>
                <xs:attribute name="RFNumber" type="xs:string"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="QAMASILink">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ws:TSIDOutLink" minOccurs="0" maxOccurs="unbounded"/>
                <xs:attribute name="Number" type="xs:string"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```
<xs:attribute name="TSIDIn" type="xs:string"/>
<xs:attribute name="TSIDInLinkStatus" type="xs:string"/>
</xs:complexType>
</xs:element>

<xs:element name="QAMLink">
<xs:complexType>
<xs:attribute name="Status" type="xs:string"/>
<xs:attribute name="ServiceGroup" type="xs:string"/>
<xs:attribute name="RFNumber" type="xs:string"/>
</xs:complexType>
</xs:element>

<xs:element name="GQAMLink">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:TSIDOutLink" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
<xs:attribute name="ServiceGroup" type="xs:string"/>
<xs:attribute name="RFNumber" type="xs:string"/>
</xs:complexType>
</xs:element>

<xs:element name="QAM">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:QAMStreamGroupPreference" minOccurs="0" maxOccurs="unbounded"/>
<xs:element ref="ws:QAMLink" minOccurs="0" maxOccurs="unbounded"/>
<xs:element ref="ws:QAMASILink" minOccurs="0" maxOccurs="unbounded"/>
<xs:element ref="ws:GQAMLink" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
<xs:attribute name="IP" type="xs:string"/>
<xs:attribute name="Type" type="xs:string"/>
<xs:attribute name="GQAMPort" type="xs:positiveInteger"/>
</xs:complexType>
</xs:element>

<xs:element name="QAMList">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:QAM" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>

<!-- Configure/System/StreamDestination/ elements -->

<xs:element name="StreamGroupPreference">
<xs:complexType>
<xs:attribute name="StreamGroupName" type="xs:string"/>
<xs:attribute name="Preference" type="xs:string"/>
</xs:complexType>
</xs:element>
</xs:element>

<xs:element name="StreamDestination">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamGroupPreference"
        minOccurs="0"
        maxOccurs="unbounded"/>
      <xs:attribute name="SubnetAddress" type="xs:string"/>
      <xs:attribute name="SubnetMask" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="StreamDestinationList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamDestination"
        minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Headend/ elements -->

<xs:element name="ServiceGroupToStreamGroup">
  <xs:complexType>
    <xs:attribute name="ServiceGroup" type="xs:string"/>
    <xs:attribute name="StreamGroup" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="Headend">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:QAM" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:ServiceGroupToStreamGroup" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Server/RouteTables/ elements -->

<xs:element name="Route">
  <xs:complexType>
    <xs:attribute name="Network" type="xs:string"/>
    <xs:attribute name="SubnetMask" type="xs:string"/>
    <xs:attribute name="Gateway" type="xs:string"/>
    <xs:attribute name="RouteType" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="RouteTable">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:Route"
<xs:element name="RouteTableList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:RouteTable" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Server/SNMP/ elements -->

<xs:element name="SNMPCommunity">
  <xs:complexType>
    <xs:attribute name="Name" type="xs:string"/>
    <xs:attribute name="Permissions" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="SNMPTrapStation">
  <xs:complexType>
    <xs:attribute name="TrapStation" type="xs:string"/>
    <xs:attribute name="Version" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="SNMPAgent">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:SNMPCommunity" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:SNMPTrapStation" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="Contact" type="xs:string"/>
    <xs:attribute name="Location" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="SNMPAgentList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SNMPAgent" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Server/RTSP/ elements -->

<xs:element name="RTSPClient">
  <xs:complexType>
<xs:element name="RTSPSetup">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:RTSPClient" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="MasterStreamingIP" type="xs:string"/>
    <xs:attribute name="LoopingSessionTimeout" type="xs:positiveInteger"/>
    <xs:attribute name="SessionInactivityTimeout" type="xs:positiveInteger"/>
    <xs:attribute name="BackofficeTimeout" type="xs:positiveInteger"/>
    <xs:attribute name="RTSPServerIP" type="xs:string"/>
    <xs:attribute name="RTSPServerPort" type="xs:positiveInteger"/>
    <xs:attribute name="ReconnectIP" type="xs:string"/>
    <xs:attribute name="ReconnectPort" type="xs:positiveInteger"/>
    <xs:attribute name="MaxHistory" type="xs:nonNegativeInteger"/>
    <xs:attribute name="LogLevel" type="xs:string"/>
    <xs:attribute name="MaintenanceMode" type="xs:string"/>
    <xs:attribute name="LSCPAddress" type="xs:string"/>
    <xs:attribute name="LSCPPort" type="xs:positiveInteger"/>
    <xs:attribute name="LSCPResponsePadding" type="xs:string"/>
    <xs:attribute name="ComponentName" type="xs:string"/>
    <xs:attribute name="BandwidthManagerIP" type="xs:string"/>
    <xs:attribute name="BandwidthManagerPort" type="xs:positiveInteger"/>
    <xs:attribute name="AuthenticationManagerIP" type="xs:string"/>
    <xs:attribute name="AuthenticationManagerPort" type="xs:positiveInteger"/>
    <xs:attribute name="BackupBandwidthManagerIP" type="xs:string"/>
    <xs:attribute name="BackupBandwidthManagerPort" type="xs:positiveInteger"/>
    <xs:attribute name="CallbackServerIP" type="xs:string"/>
    <xs:attribute name="CallbackServerPort" type="xs:positiveInteger"/>
    <xs:attribute name="ServerIP" type="xs:string"/>
    <xs:attribute name="ServerPort" type="xs:positiveInteger"/>
    <xs:attribute name="StreamControlIP" type="xs:string"/>
    <xs:attribute name="StreamControlPort" type="xs:positiveInteger"/>
  </xs:complexType>
</xs:element>

<xs:element name="RTSPSetupList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:RTSPSetup" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Server/FSI/ elements -->

<xs:element name="FSISetup">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
Bulk Configuration XML Schema

<xs:complexType name="ws:Server">
    <xs:sequence>
        <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
        <xs:element ref="ws:DomainSuffix" minOccurs="0" maxOccurs="unbounded" />
        <xs:element ref="ws:DNSServer" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>

<xs:element name="DNSList">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:DNS" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Configure/Server/NTPServer elements -->
<xs:element name="NTPServerIP" type="xs:string"/>
<xs:element name="NTPServer">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="DNSList">  
    <xs:complexType> 
        <xs:sequence> 
            <xs:element ref="ws:DNS" minOccurs="0" maxOccurs="unbounded" /> 
        </xs:sequence> 
    </xs:complexType> 
</xs:element>  

<!-- Configure/Server/DNS elements -->
<xs:element name="DomainSuffix" type="xs:string"/>
<xs:element name="DNSServer" type="xs:string"/>
<xs:element name="DNS">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:DomainSuffix" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:DNSServer" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="FSISetupList">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:FSISetup" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="DomainSuffix" type="xs:string"/>
<xs:element name="DNSServer" type="xs:string"/>
<xs:element name="DNS">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:DomainSuffix" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:DNSServer" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Configure/Server/DNS elements -->
<xs:element name="DomainSuffix" type="xs:string"/>
<xs:element name="DNSServer" type="xs:string"/>
<xs:element name="DNS">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:DomainSuffix" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:DNSServer" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Configure/Server/NTPServer elements -->
<xs:element name="NTPServerIP" type="xs:string"/>
<xs:element name="NTPServer">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Configure/Server/DNS elements -->
<xs:element name="DomainSuffix" type="xs:string"/>
<xs:element name="DNSServer" type="xs:string"/>
<xs:element name="DNS">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:DomainSuffix" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:DNSServer" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Configure/Server/NTPServer elements -->
<xs:element name="NTPServerIP" type="xs:string"/>
<xs:element name="NTPServer">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:complexType name="NTPServerList">
  <xs:sequence>
    <xs:element ref="ws:NTPServer" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
</xs:element>
</xs:element>
</xs:schema>
APPENDIX

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 C-1
- SNMP Management Objects and Traps, page C-2
- RFC Compliance, page C-5

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 4-67.

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 SNMP agent on the server uses certain variables that are included in a Cisco 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/sbin/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) file 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 C-5.

The CISCO-CDS-TV-MIB.txt MIB file is available through the CDSM, and is dependent on the following MIBs distributed on Cisco.com:


You can download the MIBs by doing the following:

**Step 1** Choose Configure > Server Level > SNMP Agent. The SNMP Agent page is displayed with a list of the MIB files at the bottom of the page.

**Step 2** To save the file locally, right-click the MIB filename, and choose Save As, Save Target As, or a similar save command.

To view the file, click the MIB filename.

The CISCO-CDS-TV-MIB.txt file has the following MIB nodes:

- cdstvConfigObjects—Configuration of servers
- cdstvMonitorObjects—Monitoring of cache-fill, streaming, disk states, and services running
- cdstvNotifyObjects—Objects specific to traps (notifications), for example, Managed Services Architecture (MSA) event objects

Table C-1 describes the traps in the CISCO-CDS-TV-MIB.

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdstvDiskHealthUp</td>
<td>Signifies that the previously inactive disk is now active and ready, that is, the disk has returned to the OK (0) state.</td>
</tr>
<tr>
<td>cdstvDiskHealthDown</td>
<td>Signifies that the active disk is now inactive, that is, it has left the OK (0) state.</td>
</tr>
<tr>
<td>cdstvMSAEvent</td>
<td>Signifies that an MSA event (error) has occurred.</td>
</tr>
<tr>
<td>cdstvServiceUp</td>
<td>Signifies that a previously stopped service is now running, that is, it has left the not running state. The cdstvServiceName object, which contains the name of the service, is sent with the trap.</td>
</tr>
<tr>
<td>cdstvServiceDown</td>
<td>Signifies that the previously running service is now stopped, that is, it has left the running state. The cdstvServiceName object, which contains the name of the service, is sent with the trap.</td>
</tr>
</tbody>
</table>
SNMP Management Objects and Traps

**Table C-1 Cisco TV CDS Traps (continued)**

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdstvDiskUsageHigh</td>
<td>Signifies that the disk usage on the system has crossed the maximum usage threshold. The cdstvDiskUsagePercent object, which contains the percentage of the disk that is used, is sent with the trap. This trap corresponds to the Disk Capacity Notify field on the System Threshold page. For more information, see the “Setting System Thresholds” section on page 7-7. When the disk usage exceeds the threshold set for the Disk Capacity Notify field, the cdstvDiskUsageHigh trap is sent.</td>
</tr>
<tr>
<td>cdstvDiskUsageNormal</td>
<td>Signifies that the disk usage on the system has returned to a value within the usage threshold. The cdstvDiskUsagePercent object, which contains the percentage of the disk that is used, is sent with the trap.</td>
</tr>
<tr>
<td>cdstvLinuxFSUsageHigh</td>
<td>Signifies that the Linux file system (FS) usage on the server has crossed the maximum usage threshold. The cdstvLinuxFSMountPoint and cdstvLinuxFSUsagePercent objects, which contain the mount point and the percentage used, are sent with the trap.</td>
</tr>
<tr>
<td>cdstvLinuxFSUsageNormal</td>
<td>Signifies that the Linux file system (FS) usage on the server has returned to a value within the usage threshold. The cdstvLinuxFSMountPoint and cdstvLinuxFSUsagePercent objects, which contain the mount point and the percentage used, are sent with the trap.</td>
</tr>
<tr>
<td>cdstvPortLossHigh</td>
<td>Signifies that the port loss on the system has crossed the maximum threshold. The cdstvPortLossPercent object, which contains port loss percentage, is sent with the trap.</td>
</tr>
<tr>
<td>cdstvPortLossNormal</td>
<td>Signifies that the port loss on the system has returned to a value within the threshold. The cdstvPortLossPercent object, which contains port loss percentage, is sent with the trap.</td>
</tr>
<tr>
<td>cdstvSysHealthUp</td>
<td>Signifies that a previously abnormal system health parameter is now normal; that is, it has left the not OK state. See Table C-2 on page C-4 for the descriptions of the objects sent with this trap.</td>
</tr>
<tr>
<td>cdstvSysHealthDown</td>
<td>Signifies that a previously normal system health parameter is now abnormal; that is, it has left the OK state. See Table C-2 on page C-4 for the descriptions of the objects sent with this trap.</td>
</tr>
</tbody>
</table>

Monitored Services SNMP Traps

The services reported as up or down in SNMP correspond to the services on the Service Monitor page. For more information on the monitored services, see the “Services Monitor” section on page 5-31.

For the cdstvServiceUp and cdstvServiceDown traps, if the database shuts down, a cdstvServiceDown trap is sent for the Cisco DB server, but no other services can be monitored without the database running. No SNMP traps are sent for services until the database is functional again.

If the SNMP agent itself is down, the CDSM shows the Cisco SNMP Server as “Not Running” but no SNMP trap can be sent for this service because the SNMP agent itself is down.

If the CDS server is shut down cleanly, there may be a cdstvServiceDown trap sent for the Cisco SNMP Server before the entire server shuts down. No traps can be sent until the SNMP agent is running.
System Health Threshold Crossing Alerts
The temperature, fans, and power are monitored on the CDS servers and the states and thresholds are displayed on the Server Vitals page. See the “Server Vitals” section on page 5-28. If a threshold is exceeded, an alarmed event is registered on the CDSM and the cdstvSysHealthDown trap is sent with information about the threshold crossing alert (TCA).

Note
The Server Vitals page is displayed only if the CDSM Health Monitor feature is enabled. For more information, see the “CDSM or VVIM Health Monitoring” section on page D-8.

Table C-2 describes the objects that are sent with the cdstvSysHealthUp and cdstvSysHealthDown traps.

Table C-2 System Health SNMP Trap Objects

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Possible values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdstvSysHealthName</td>
<td>String</td>
<td>Name of the system health monitoring parameter, for example, VBAT Voltage.</td>
</tr>
<tr>
<td>cdstvSysHealthType</td>
<td>1—Fan-speed</td>
<td>Type of the system health monitoring parameter.</td>
</tr>
<tr>
<td></td>
<td>2—Voltage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3—Temperature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4—Chassis intrusion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5—Power supply failure</td>
<td></td>
</tr>
<tr>
<td>cdstvSysHealthReading</td>
<td>Integer</td>
<td>Current reading (value) of the system health parameter; for example, fan speed, voltage, or temperature. Fan speed is expressed in rpm, voltage in mV and temperature in degree Celsius. For chassis intrusion and power-supply failure, 1 denotes an error condition, and 0 denotes normal condition.</td>
</tr>
<tr>
<td>cdstvSysHealthHighLimit</td>
<td>Integer</td>
<td>Higher limit (threshold) of the system health parameter. Voltage is expressed in mV and temperature in degree Celsius. Not applicable for other parameters such as fan speed.</td>
</tr>
<tr>
<td>cdstvSysHealthLowLimit</td>
<td>Integer</td>
<td>Lower limit (threshold) of the system health parameter. Fan speed is expressed in rpm and voltage in mV. Not applicable for other parameters such as temperature.</td>
</tr>
<tr>
<td>cdstvSysHealthStatus</td>
<td>1—Normal</td>
<td>Current status of the system health parameter. The not-ok value applies to power supply failure and chassis intrusion, because high and low limits do not apply to these parameters.</td>
</tr>
<tr>
<td></td>
<td>2—Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3—High</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4—Not-OK</td>
<td></td>
</tr>
</tbody>
</table>
### RFC Compliance

Table C-3 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 C-3  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>
APPENDIX

Engineering Access Level Pages

This appendix describes the VVIM or CDSM pages available through the Engineering access level. The Engineering access level provides the following pages:

- CDSM or VVIM Diagnostics, page D-2
- CDSM or VVIM Setup, page D-3
- System Configs, page D-9

The Engineering access level is primarily used for initializing the CDS at the time of installation and for system diagnostics. After your system 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.

When you configure the CDSM for Virtual Video Infrastructure (VVI), all references to CDSM are changed to Virtual Video Infrastructure Manager (VVIM) for the Vault and Caching Node manager. For example, the CDSM Audit Logs available through the Report > System Level left-panel menu is changed to the VVIM Audit Logs when VVI is configured on the CDSM Setup page, which changes to the VVIM Setup page.
CDSM or VVIM Diagnostics

To access the CDSM or VVIM Diagnostics page, choose **Maintain > Software > CDSM Diagnostics** or **VVIM Diagnostics**. The first section of this page provides configuration information that is useful in diagnosing a problem. The following remaining sections of the CDSM or VVIM 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 or VVIM 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 or VVIM Setup

The CDSM or VVIM Setup page is used to initially configure the CDS. After you have set the CDSM or VVIM Setup fields for your system, click **Submit**. Configuration and start up messages are displayed in the left panel.

Deployed CServer Version

For Release 2.1, this field is always set to 2.1.x.

Stream Failover Support

Stream failover support is available for both the ISA and RTSP environments. 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 (Silo site steering)
- Multi-site

Single-site steering uses only one Stream Group to serve streams to all QAM devices. Multi-site steering can use more than one Stream Group to serve streams to the QAM devices. The QAM Gateway page reflects whether single-site or multi-site steering is enabled, by the number of preference levels available. Multi-site steering offers four preference levels (high, medium, low, and none). Single-site steering offers two preference levels (high and none).

**Note**

Multi-site steering is available only 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 2.1 are **ISA 2.1** and **RTSP 2.1**.
Stream Destination

The possible settings for Stream Destination are **Cable** and **IPTV**.

The cable setting is the existing configuration with the QAM Gateway page and Headend Setup page, which allows you to map Stream Groups to QAM devices and service groups if applicable.

The IPTV setting provides the Stream Destination page in place of the QAM Gateway page and Headend Setup page. The Stream Destination page allows you to map the Stream Groups to specified subnets, which is useful in IPTV networks where each end-user has an IP address.

An option for ISA environments using the IPTV setting for the Stream Destination is the NAT option. The NAT Traversal feature allows streaming to client devices that are behind a NAT device.

**Note**

The Stream Destination feature is available only for single-site steering.

Parent/Child Service Groups

Parent/Child Service Groups is an optional feature and is only for ISA environments that use ASI streaming. The Parent/Child Service Groups page allows finer granularity of the service groups.

Bulk Configuration

Bulk Configuration provides a method of configuring common configuration parameters for all the servers at one time by means of an XML file. Following are the CDSM GUI configuration pages that offer bulk configuration:

- QAM Gateway
- Headend Setup
- Stream Destination
- NTP Server
- Server DNS
- SNMP Agent
- Route Tables
- RTSP Setup
- FSI Setup
SSV Groups

When SSV Groups is enabled, Stream Groups, Vault Groups, and Cache Groups are disabled. The SSV Group optional feature is for a CDS that uses only ISVs. The Thin Pipe Map page and Vault Redundancy Map page are also displayed when SSV Groups is enabled. The Vault Redundancy Map page allows mapping of ISVs for mirrored content, and the Thin Pipe Map page allows creation of low-bandwidth connections between local and remote groups.

Note

The term SSV used in the CDSM GUI is the same as the ISV. The terms are interchangeable.

When SSV Groups is enabled, all pages referring to Vaults or Streamers display as SSV instead. These pages include the Stream Destination page, the QAM Gateway page, the Headend Setup page, the Control/Setup IP page, and the Vault Redundancy Map page.

Trick Mode Capture

In Release 2.2, Trick Mode Capture is an optional feature. When Trick Mode Capture is enabled, the applicable Stream Activity reports can drill down to the Stream Play History Drilldown, which displays the trick modes for a session ID. Additionally, the Graph Stream button is displayed on the Stream Monitor page. The Stream Activity reports that can drill down to the Stream Play History Drilldown are the following:

- Stream Play History
- Streams by Array
- Streams per STM-MAC
- Bandwidth per Service Group
- Stream Failures

When Trick Mode Capture is disabled, the session ID in the Stream Activity reports no longer links to the Stream Play History Drilldown and the Graph Stream button is removed from the Stream Monitor page.

Vault Redundancy

When Vault Redundancy is enabled and at least two Vault Groups are configured and mapped to each other, at least one copy of each content within a group is mirrored to the configured peer group. The Vault Redundancy adds the Vault Groups and Vault Redundancy Mapping configuration pages to the Array Level.

Note

In Release 2.1, the maximum number of Vault Groups is two.

RS DVR

This feature is not activated in this release.
Thin Pipe Management

Thin Pipe Management allows you to configure low-bandwidth connections between local and remote groups. A local group consists of servers in the same group (Stream Group, Cache Group, Vault Group). A remote group consists of servers in other Stream Groups, Cache Groups, and Vault Groups. Use the Thin Pipe Map page to configure this feature.

Shared Content Store

Shared Content Store is an optional feature for the ISA environment. The Shared Content Store allows one instance of a Content Store to be shared with many instances of Stream Services, each located in its own video hub office (VHO) with its own video backoffice (VBO).

Virtual Video Infrastructure

The Virtual Video Infrastructure (VVI) provides management of the Caching Nodes in a central management configuration or a split-domain management configuration.

When you enable VVI, you need to choose the Management System Role of the CDSM. The Management System Role has the following options:

- VVI and Stream Manager—Central management of all Vaults, Caching Nodes, and Streamers
- VVI (Vault/Cache) Manager—Management of only the Vaults and Caching Nodes
- Stream Manager—Management of only the Streamers

The Cache Fill Protocol options are for selecting the type of data communication that is used between Caching Nodes and Streamers. Cache Control Protocol (CCP) is used for communication among the Vaults, Caching Nodes, and Streamers. For more information about CCP Streamers and HTTP Streamers, see the “Caching Node Workflow” section on page 2-9.

Note
ISA environments only support CCP, while RTSP environments only support HTTP for VVI.

The split-domain management is made up of the VVI (Vault/Cache) Manager and the Stream Manager. For the Stream Manager to be able to communicate with the VVI Manager, you need to enter the IP address of the VVI Manager in the VVI (Vault/Cache) Manager VVIM IP field.

If CCP is used as the cache-fill protocol, you must provide a name for the Stream Manager in the Stream Domain Name field so that the VVIM can identify it from other Stream Managers. Communication between the VVI Manager and the Stream Manager is accomplished through database replication when using CCP.

If you choose HTTP, communication between the VVI Manager and the Stream Manager uses port 80. If port 80 is not open for communication, you can enter the data manually (used for Stream Group IDs), or upload an XML file (used for Cache Group Locator information), depending on the information required.

Note
When you configure the CDSM for Virtual Video Infrastructure (VVI), all references to CDSM are changed to Virtual Video Infrastructure Manager (VVIM) for the Vault and Caching Node manager.
The VVIM and Stream Managers display different configuration, monitoring, reports, and maintenance pages based on the servers they manage. For example, when CCP is the cache-fill protocol, the VVIM displays the Configuration Generator page in the Maintenance > Software left-panel menu. The Configuration Generator page is used to generate the group IDs and server IDs for the Stream Managers to use in their domains.

### Configuring Split-Domain Management

To configure a VVIM that uses split-domain management, set the VVI fields as follows:

- **VVI Options**—Enabled
- **Management System Role**—VVI (Vault/Cache) Manager
- **Cache Fill Protocol**—HTTP or CCP (Must be configured the same as the Stream Manager.)

To configure a Stream Manager that uses split-domain management, set the VVI fields as follows:

- **VVI Options**—Enabled
- **Management System Role**—Stream Manager
- **Cache Fill Protocol**—HTTP
- **VVI (Vault/Cache) Manager VVIM IP**—IP address of the VVIM
- **Stream Domain Name**—Domain name for the Stream Domain (If CCP is the Cache Fill Protocol)

### 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.

### 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 a 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 applicable only to RTSP environments. The options are the following:

- DSM-CC
- RTSP
- NGOD
- IPTV
- 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). 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 or VVIM NAV Setup

The CDSM NAV Setup changes what displays in the CDSM GUI.

CDSM or VVIM Health Monitoring

The CDSM Health Monitoring optional feature displays the Server Level monitor page, Server Vitals page and a Vitals column in the System Health Monitor page. The Server Vitals page displays the current values, as well as thresholds, for monitored system components on the server. Server components are monitored and when a threshold is exceeded, the System Health Monitor page and Server Vitals page report the event and an SNMP trap is sent.
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 after 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-22, 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.
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 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 PARTYALTERS, 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