# Preface

Document Revision History   xvii
Audience   xviii
Objective   xviii
Document Organization   xix
Document Conventions   xix
Related Documentation   xx
Obtaining Documentation and Submitting a Service Request   xxi

# CHAPTER  1

Product Overview   1-1
Overview   1-1
VDS-TV Software   1-3
Caching Nodes   1-4
Streamer Load Balancing   1-4
CServer Functionality   1-4
Streamer Content Delivery Applications   1-4
Content Delivery   1-5
4K-HEVC/H.264 Video Support   1-6
Content Chunking   1-6
Playlist Enhancements   1-6
Digital Video Watermarking   1-9
HTTP Live Streaming   1-10
H.264/AVC Ingest   1-10
VOD Error Repair   1-11
Integrated Streamer Recorder   1-12
Media Origination Suite 2.0 VOD Support   1-13
Content Delivery System Architecture   1-15
Vault   1-16
Streamer   1-17
D5 Interface   1-17
Caching Node   1-17
Integrated Streamer-Vault   1-17
Content Delivery System Manager and Virtual Video Infrastructure Manager   1-17
### Contents

Resiliency and Redundancy  1-19  
- Vault Disk Redundancy  1-19  
- Vault Server Resiliency  1-20  
- Vault Group Redundancy  1-21  
- Streamer Disk Redundancy  1-21  
- Streamer Server Resiliency  1-21  
- Caching Node Disk Redundancy  1-21  
- Caching Node Resiliency  1-21  
- CDSM Redundancy  1-22  
- Ethernet Link Resiliency  1-22  
- Collectd Application  1-22  

Scalability  1-23  

### CHAPTER 2  

**Network Design**  2-1  

Overview  2-1  
- VDS with Vaults and Streamers  2-2  
- VDS with ISVs  2-2  
- VDS with Caching Nodes  2-2  

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

TV VVI Management  2-6  
- Centralized Management  2-7  
- Split-Domain Management  2-7  

VDS Workflow  2-7  
- Popularity-Based Caching  2-8  
- Bandwidth Manager for Thin Pipe  2-8  

Streamer Workflow  2-9  
- Setup Server  2-10  
- Control Server  2-10  
- Play Server  2-10  
- Remote Setup and Control Server  2-10  

Caching Node Workflow  2-12  

Vault Workflow  2-13  

nDVR Support for NGOD Deployments  2-13  
- Asset Metadata  2-14  
- Cache-Fill Routing  2-14  
- nDVR Architecture  2-15
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut-Through Support</td>
<td>2-15</td>
</tr>
<tr>
<td>Integration with Legacy VBOs</td>
<td>2-15</td>
</tr>
<tr>
<td>Dynamic Trick-Mode Files</td>
<td>2-15</td>
</tr>
<tr>
<td>Vault Virtualization</td>
<td>2-15</td>
</tr>
<tr>
<td>ISA Regionalization</td>
<td>2-16</td>
</tr>
<tr>
<td>Centralized Storage</td>
<td>2-16</td>
</tr>
<tr>
<td>Remote Site</td>
<td>2-16</td>
</tr>
<tr>
<td>Ingest Driver</td>
<td>2-17</td>
</tr>
<tr>
<td>Remote Ingests</td>
<td>2-18</td>
</tr>
<tr>
<td>Remote Streaming</td>
<td>2-18</td>
</tr>
<tr>
<td>Shared Content Store</td>
<td>2-19</td>
</tr>
<tr>
<td>Virtual Content Store</td>
<td>2-20</td>
</tr>
<tr>
<td>BMS Considerations for ISA Environments</td>
<td>2-21</td>
</tr>
<tr>
<td>OpenStream ISA Integration</td>
<td>2-21</td>
</tr>
<tr>
<td>Streaming Mode</td>
<td>2-22</td>
</tr>
<tr>
<td>Steering Ingests</td>
<td>2-22</td>
</tr>
<tr>
<td>Network Connections</td>
<td>2-23</td>
</tr>
<tr>
<td>Ingest Interface</td>
<td>2-26</td>
</tr>
<tr>
<td>Management Interface</td>
<td>2-27</td>
</tr>
<tr>
<td>Cache Interfaces</td>
<td>2-27</td>
</tr>
<tr>
<td>Cache/Stream Interfaces</td>
<td>2-27</td>
</tr>
<tr>
<td>Streaming Interface</td>
<td>2-27</td>
</tr>
</tbody>
</table>

**Getting Started** 3-1

- Initially Configuring the Devices 3-1
- Browser Recommendation 3-1
- Logging In to the TV CDSM 3-2
- Logging Out 3-3
- Initializing the VDS and Activating the Optional Features 3-3
- Navigating the CDSM 3-4
- Using Online Help 3-5
- Configuration Workflow 3-6
  - VDS Configuration Workflow 3-6
  - VVI Configuration Workflow 3-7
  - Central Management Configuration Workflow 3-7
  - Split-Domain Management Configuration Workflow 3-8
  - Vault Virtualization Configuration Workflow 3-9
  - ISA Regionalization Configuration Workflow 3-9
  - Virtual Content Store Configuration Workflow 3-10
CHAPTER 4
Configuring the VDS 4-1

System Level Configuration 4-1
- Configuring System Level DNS Services 4-2
- Configuring System Level NTP Services 4-3
- Configuring the Hosts Service 4-3
- Configuring the Array Name 4-4
- Configuring QAM Gateways 4-5
- ARP 4-5
- Configuring the Headend Setup 4-7
- Configuring Stream Destinations 4-9
- Configuring the Ingest Manager 4-11
- Configuring the Authentication Manager 4-14
- Configuring Ingest Tuning 4-15
- Configuring MPEG Tuning 4-17
- Configuring Shared Recorder Settings 4-20
- Configuring IP Nicknames 4-22
- Configuring the Media Importer 4-24
- Configuring Call Signs 4-25
- Configuring Input Channels 4-27
- Configuring Source Output Ports 4-30
- Configuring Multiple SOPs 4-30
- Configuring the System Level Logging 4-31
- Configuring the System Level Syslog 4-33
- Configuring System Level Error Repair 4-34

Array Level Configuration 4-35
- Configuring the Array Level DNS 4-36
- Configuring the Array Level NTP Server 4-37
- Configuring Replication Groups 4-37
- Configuring Stream Groups 4-39
- VVI with Split-Domain Management and HTTP Streamers 4-39
- Configuring D5 Interface Settings 4-41
- Locating Cache Groups 4-44
- Locating CDN Groups 4-46
- Mapping Stream Group to CDN Groups 4-48
- Configuring Vault Groups 4-49
- Configuring Ingest Steering 4-51
CHAPTER 5
System Monitoring 5-1
System Level Monitoring 5-1
Alarms Table 5-2
System Health 5-3
System Snapshot 5-5
System Failures 5-6
Monitoring Content Objects 5-17
Ingests 5-18
Viewing and Deleting Completed Ingests 5-18
Viewing Other Ingests 5-22
Viewing Ingest Percentage Status 5-22
Package Expirations 5-23
Publish Failures 5-24
Unpublished Packages 5-25
Monitoring Stream Objects 5-26
Stream Monitor 5-26
Array Level Monitoring 5-30
Array Snapshot 5-31
Barker Stream Monitor 5-31
Playout Monitor 5-31
Server Level Monitoring 5-33
Disk Monitor 5-33
S.M.A.R.T 5-35
NIC Monitor 5-35
Server Vitals 5-37
Cache/Fill Bandwidth 5-40
Services Monitor 5-42
Recommended Monitoring Schedule 5-44
Daily Tasks 5-44
Weekly Tasks 5-44
Monitoring Tasks for Streamers and Vaults 5-44
Monitoring Tasks for Vaults 5-46
Monitoring Tasks for Streamers 5-46
Monthly Tasks 5-46
Other Tasks 5-47

CHAPTER 6
System Reporting 6-1
Stream Activity 6-1
Capacity Planning 6-2
Contents

- Streams by Array  
- Streams by Time  
- Stream Play History  
- Cache/Fill Bandwidth  
- System Failures  
- Content Popularity  
- Content Activity  
- Content by Ingest Date  
- Unpublished Package Report  
- CDSM Audit Logs  
- Archived Data  
- CDSM Audit Log Archives  
- Content Reports  
- Stream Reports  
- Stream Failure Reports  
- Stream Activity Reports  

CHAPTER 7  System Maintenance  7-1

- User Access   
  - Adding Users  7-4
  - Editing User Settings  7-5
  - Deleting a User  7-6
  - Viewing User Settings  7-6
  - Changing User Default Settings  7-7
  - Configuring System Authentication Settings  7-10
    - Password Complexity Rules  7-11
    - Configuring User Authentication  7-11

- Server Maintenance  7-11
  - Restarting a Server  7-12
  - Shutting Down a Server  7-12
  - Offloading a Server  7-13
    - Server Offload—Online  7-14
    - Vault Decommissioning  7-14
  - Setting System Thresholds  7-15

- Restarting the Services  7-17
- Content Manager  7-18
- Software Maintenance  7-19
  - Viewing the Software Version and Server Information  7-19
Configuring the TV Playout Application  7-19
Importing a TV Playout Schedule  7-21
Upgrade Status of the TV Playout Application  7-21
Uploading an EPG File  7-22
Configuring the Backup Scheduling  7-23
Restoring the Configuration from Backup Files  7-26
Restoring the Content Object from Backup Files  7-26
Identifying Server IDs and Group IDs for VVI with Split-Domain Management  7-26
  Generating Server IDs and Group IDs from the VVIM  7-27
  Generating a Server ID from the Stream Manager  7-29
System Cleanup  7-30
Manuals  7-31

APPENDIX A
Troubleshooting  A-1
  General Information and Issues  A-2
    File System  A-2
    CDSM  A-2
    Vault, Streamer, Caching Node, and ISV  A-3
    Log Files  A-3
      Linux Log Files  A-4
      CServer Log Files  A-4
      RTSP Log Files  A-6
      AIM Logging System  A-7
      CDSM Log Files  A-7
    Server Configuration Files  A-8
      Description of the .arroyorc Settings  A-8
      Description of the replication_config Settings  A-11
      Description of the setupfile Settings  A-11
    Identifying the Software Versions or Releases  A-15
      Linux OS Version  A-15
      VDS-Related Releases  A-15
    Using ifstats to Monitor Traffic  A-17
    Kernel Crash  A-17
    Disk Drive Issues  A-18
      CDSM GUI Disk Monitor Page Reports a Disk Warning  A-19
    Memory Issues  A-20
    Disabling USB Ports and Password-Protecting the BIOS  A-20
    Network  A-22
      Interface Information  A-23
Startup Issues  A-24
  BIOS Settings—Operating System Hangs or Goes into KDB Mode  A-25
  Serial Console Port Settings  A-25
  Required Services Not Starting or Running Correctly  A-26
  Process Monitoring with monit  A-26

Management and Database Issues  A-27
  System Health  A-27
  Cannot Access the CDSM GUI  A-27
  CDSM GUI Does Not Register the Vaults and Streamers  A-27
  Database Monitoring  A-28

Ingest Issues  A-29
  Ingest Interface  A-29
    FSI Starts but Cannot Ingest Content  A-29
    FSI Does Not Start  A-29
    Troubleshooting collectd  A-30
    Content Not Ingesting  A-30
    Asset Ingest Manager Restart Causes Endless Loop  A-31
    Asset Ingest Manager crashing  A-33
  Asset Ingest Manager Response Codes  A-33
  Bad Content  A-33
  Network  A-33

Content Processing Issues  A-34
  Listing Content  A-34
  Orphan GOID mirroring during reboot of vaults  A-34
  Content Mirroring  A-34
  Verifying GOIDs  A-35
  Trick-Mode Issues  A-36

Cache-Fill Issues  A-36
  Tracking Cache-Fill Source  A-36
  Rules for ISV Interoperability with Vaults and Streamers  A-37
  Network  A-37
    Stream Stops Playing at the Same Place or Does Not Play at All  A-37

Streaming and Playout Issues  A-38
  Listing of Streams  A-38
  No Streaming  A-38
  Stream Not Playing  A-39
  Poor Video or Audio Quality  A-40
    No Video Displayed  A-40
    RTSP Cannot Start  A-41
Contents

Cisco VDS-TV RTSP Software Configuration Guide

APPENDIX B

Creating Bulk Configuration Files B-1

Introduction B-1

System Level Configuration Backup and Restore B-2
Using the System-Level Configuration Backup and Restore Feature B-2
Array Level Configuration Backup and Restore B-4
Using the Array-Level Configuration Backup and Restore Feature B-4
Server-Level Configuration Backup and Restore B-6
Adding a New VDS Server into an Existing System B-7

Video Stops Playing A-41
No Video Playing on the set-top A-41
VDS Is Streaming but No Video Is Playing on the set-top A-42

Session Messaging A-43
Log File Search Tips A-43
Codes A-44

Database Issues A-45
Database Replication A-46
CDSM GUI Does Not Report All the Ingested Content A-46
Errors in Log File A-46
Many Log Files A-46
Corruption Recovery A-47

Advanced Features and Applications A-48
Live Multicast Ingest A-48
Ingest with Media Scheduler A-48
Ingest without Media Scheduler A-49
Ingest Troubleshooting A-49
Ingest Troubleshooting with SSM enabled A-49

Frequently Asked Questions A-49
Reliability and Availability A-49
Serviceability and Manageability A-50
Content A-52
Other A-54

VDS Content Quality Guidelines A-55
Supported Elementary Stream Types A-55
Scrambling A-55
Transport Bit Rate A-55
Stream Length A-55
Format Restrictions A-56
Preferred Formats A-56
Replacing a VDS Server and Complete Backup and Restore  B-7
Using the Server-Level Configuration Backup and Restore Feature  B-7
Maintain Section Configuration Backup and Restore  B-10
Using the Maintain Section Configuration Backup and Restore Feature  B-10
Creating QAM Gateway Bulk Configuration Files  B-12
Creating Headend Setup Bulk Configuration Files  B-13
Creating Stream Destination Bulk Configuration Files  B-14
Creating Route Table XML Configuration Files  B-15
Creating SNMP Agent XML Configuration Files  B-16
Creating DNS Server XML Configuration Files  B-17
Creating NTP Server XML Configuration Files  B-18
Creating FSI Setup XML Configuration Files  B-19
Creating RTSP Setup XML Configuration Files  B-20
Creating Logging XML Configuration Files  B-23
Creating Syslog XML Configuration Files  B-24
Creating Server Setup XML Configuration Files  B-25
System-Level Configuration XML Schema  B-29
Array-Level Configuration XML Schema  B-52
Server-Level Configuration XML Schema  B-70
Maintain Section Configuration XML Schema  B-88

APPENDIX C
BMS Communication  C-1
OpenStream/ISA  C-1

APPENDIX D
SNMP MIB and Trap Information  D-1
Overview  D-1
SNMP Agent  D-1
SNMP Agent on a CDSM or VVIM  D-2
SNMP Management Objects and Traps  D-2
RFC Compliance  D-6

APPENDIX E
Using the VDS-TV Streamer Application Monitoring Tool  E-1
Overview  E-1
Initializing AMT on the Streamer  E-1
Logging In to AMT  E-2
AMT Statistics  E-3
Contents

Viewing Error Repair Statistics E-5
Viewing Excess Bandwidth E-7

APPENDIX F

Engineering Access Level Pages F-1

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

CDSM or VVIM Setup F-3
Deployed CServer Version F-3
Stream Failover Support F-3
Role Failover on DB Connectivity Loss F-3
Stream Steering Mode F-4
Deployment Network Config F-4
NIC Bonding F-4
Installation Type F-4
Stream Destination F-4
NAT Support F-5
Parent/Child Service Groups F-5
Asset Scale Co-Existence Support F-5
Bulk Import/Export Configuration F-5
SSV Groups F-6
Trick Mode Capture F-6
Fail Ingest Tuning F-6
Vault Groups F-7
Watermarking Support F-7
ARP Parameters F-7
Manage Recorders F-7
Future Recording Support F-8
Duplicate QAM Detection F-8
DNS Resolution Support F-8
TCP Window Scaling Support F-8
TVOD Setup F-8
Thin Pipe Management F-9
Ingest Resiliency F-9
VOD Error Repair F-9
Virtual Video Infrastructure F-10
Configuring Split-Domain Management F-10
Preface

This preface describes the audience, objective, organization and conventions of the *Cisco VDS-TV RTSP Software Configuration Guide*. It also references related documentation and describes how to obtain documentation and submit a service request.

- Audience, page xviii
- Objective, page xviii
- Document Organization, page xix
- Document Conventions, page xx
- Related Documentation, page xx
- Obtaining Documentation and Submitting a Service Request, page xxi

Document Revision History

The Document Revision History table below records technical changes to this document.
Cisco VDS-TV RTSP Software Configuration Guide

**Audience**

This guide is for the networking professional managing the Cisco TV Content Delivery System, hereafter referred to as VDS. Before using this guide, you should have experience working with 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 that you need to configure and monitor the Cisco VDS-TV. This guide provides procedures for using the commands that have been created or changed for use with the Cisco VDS-TV. It does not provide detailed information about these commands. This guide does not describe system messages that you might encounter or how to install your VDS. 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...

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
</table>
| January 2018    | • Added Configuring the enabling/disabling of ANNEX TABLE, STREAM TRICK REPORT TABLE, SESSION TABLE, MSA TABLE, PRINT CONTAINER SIZE in Appendix F Engineering Access Level Pages.  
                    • Updated Ingests section in Chapter System Monitoring and Content by Ingest Date in Chapter System Reporting. |
| April 2017      | • Added Package Scalability in Chapter Overview.  
                    • Added a new section Configuring the Backup Scheduling in Chapter System Maintenance.  
                    • Added AIM Logging System in Appendix A Troubleshooting.  
                    • Added Array Level Configuration Backup and Restore and Maintain Section Configuration Backup and Restore in Appendix B Creating Bulk Import/Export Configuration Files.  
                    • Updated System, Array, Server and Maintain-Level Configuration XML Schema in Appendix B Creating Bulk Import/Export Configuration Files.  
                    • Added Configuring Hung Stream Timeout and Configuring Transaction Delay Debug Statements in Appendix F Engineering Access Level Pages.  
                    • Added Playout Processor in Appendix F Engineering Access Level Pages. |
| September 2016  | Initial release                                                               |
the Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide or the Cisco UCS C220 M4 Server Installation and Service Guide. See the “Related Documentation” section on page xx for links to documentation online.

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

Document Organization

This document contains the following chapters and appendixes:

<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 VDS-TV.</td>
</tr>
<tr>
<td>Chapter 2, “Network Design”</td>
<td>Describes the possible network topologies for the VDS-TV.</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 VDS”</td>
<td>Describes how to configure the VDS using the CDSM web-based user interface.</td>
</tr>
<tr>
<td>Chapter 5, “System Monitoring”</td>
<td>Explains how to monitor the VDS 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 VDS, 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 D, “SNMP MIB and Trap Information”</td>
<td>Provides information on SNMP and the Cisco VDS-TV proprietary SNMP informational events and traps.</td>
</tr>
<tr>
<td>Appendix F, “Engineering Access Level Pages”</td>
<td>Describes the CDSM pages visible with the engineering access level.</td>
</tr>
<tr>
<td>Appendix H, “VDS-TV Tunables”</td>
<td>Provides information on VDS-TV Tunables.</td>
</tr>
<tr>
<td>Appendix I, “Software Licensing Information”</td>
<td>Provides information on open-source licenses and Cisco’s software licensing agreement.</td>
</tr>
</tbody>
</table>
Document Conventions

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

<table>
<thead>
<tr>
<th>Conventions</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface font</strong></td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>italic font</em></td>
<td>Arguments for which you supply values are in <em>italics</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td><strong>string</strong></td>
<td>A non quoted 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></td>
<td>Terminal sessions and information the system displays are in <strong>screen</strong> font.</td>
</tr>
<tr>
<td><strong>italic screen font</strong></td>
<td>Information you must enter is in <strong>italic screen</strong> font.</td>
</tr>
</tbody>
</table>

| **Tip** | Means the following information might help you solve a problem. |

| **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. |

Related Documentation

These documents provide complete information about the VDS, and are available at Cisco.com:
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.

- Overview, page 1-1
- Content Delivery System Architecture, page 1-15

Overview

The Cisco Videoscape Distribution Suite-TV (VDS-TV) 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 VDS-TV has a variety of mechanisms to accelerate the distribution and delivery of content. The VDS inter-operates with electronic program guides (EPGs), set-tops, and back office applications, offering an end-to-end solution for video delivery systems.

The Cisco VDS-TV functionality can be separated into five areas:

- Ingest
- Storage
- Caching
- Streaming
- Management

Each CDE in the VDS 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>
Overview

Figure 1-1 illustrates how a VDS-TV network can be deployed. A Business Management System (BMS), commonly called a back office, 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 VDS-TV: a VDS 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 VDS. The (Virtual Video Infrastructure Manager) 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 “VDS-TV and VVI Topologies” section on page 2-2. Figure 1-1 shows a high-level view of both a VDS and a VVI.

The Cisco VDS-TV 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.

---

VDS-TV Software

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

The CServer facilitates the rapid movement of content between Vaults and Streamers while keeping required bandwidth to a minimum. To accomplish this, the Cisco VDS-TV 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 VDS-TV 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 VDS-TV 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 VDS-TV. In a VDS, 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 2-12.

## 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 VDS-TV network, the Vault, TV Streamer, and CDSM are required. The TV MediaX Suite is an optional CDA. In a smaller VDS-TV 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

The VDS delivers real-time, time-shifted, and on-demand video content to set-top, personal computers, or any other device accessible through a Service Provider network.

The Cisco VVI allows service providers to support a broad range of services. For example, with the ability to distribute content from anywhere to anywhere, operators can provide user-generated and online video just as easily as any other on-demand title. The ability to deliver content with sub-second latency also lets service providers dramatically expand the video library that can be made immediately accessible to customers, allowing them to access content that resides in a different state or country virtually instantly.

Operators can also support popular real-time and time-shifted services, such as letting viewers tuning into a program in progress and restart it from the beginning, or providing network-based personal video recorder (nPVR) functions such as the ability to pause, fast forward, and rewind live TV. The Cisco VVI's centralized storage and localized streaming architecture also distributes screen-formatting processes to the network edge.

The key content delivery capabilities include the following:

- Supports multiple content formats (high-definition and standard-definition content, multiple video codec formats, multiple media file types, and so on)
- Supports ingest and streaming of real-time video services, VOD services, and Internet video.
- Supports streaming of 4K-HEVC/H.264 video content at a maximum bit rate of 40Mbps.
- Supports advertising content distribution and streaming
- Supports nPVR capabilities to provide a digital video recorder (DVR)-like experience with the network
- Provides a single content delivery network for serving set-tops, PCs, and mobile devices
- Supports content security and encryption
- Supports narrowcast service such as VOD, time-shifted TV, and switched digital video (SDV) sharing the same infrastructure
- Supports both traditional and next-generation set-tops and headends
4K-HEVC/H.264 Video Support

Starting from Release 4.2, VDS-TV support ingestion and streaming of 4K High Efficiency Video Coding (HEVC)/H.264 video content with a maximum resolution of 3840 X 2160.

Content Ingestion

The ingestion process is enhanced to support 4K-HEVC/H.264 video content. While ingesting 4K-HEVC/H.264 video content, VDS-TV generates 1x file, delta file, index files and trick files. We also support Real Time Ingestion (RTI) of 4K-HEVC/H.264 video content.

Content Streaming

VDS-TV supports streaming of 4K-HEVC/H.264 video content at a maximum resolution of 40Mbps.

Supported Deployments

- ISA and RTSP deployments that use Cisco’s IGate format for index files.
- Deployments that use ATIS index file.
- RTSP-NGOD deployments with only Cisco CDN and Cisco streamers.

Restrictions

- Tested and verified streaming of 4K-HEVC/H.264 video content encoded at a maximum bit rate of 29Mbps.
- Streaming of 4K-HEVC/H.264 video content not supported on third party CDNs and streamers.
- Testing performed with a limited set of contents.

Content Chunking

For DVD on Demand solutions and long recordings, VDS supports ingest and streaming of assets up to 120 GB in size and recordings that last longer than 12 hours. This is accomplished by dividing the asset into multiple chunks of approximately 16 GB each.

To enable content chunking, set the following tunable in all the vaults:

```
echo 2 > /proc/calypso/internal/cm_defaultGoidType
```

To disable content chunking, set the following tunable to default value 0 in all the vaults:

```
echo 0 > /proc/calypso/internal/cm_defaultGoidType
```

Also, the above mentioned command must be added in the `/arroyo/test/configrun` script of each VDS server so that the tunable is set automatically after every reboot.

Playlist Enhancements

The following playlist enhancements are supported:

- Skip Missing Playlist Element, page 1-7
- Mid-Roll Advertisement Placement Accuracy, page 1-7
- Trick-Mode Restriction, page 1-8
Skip Missing Playlist Element

If the VDS cannot locate the content referenced by a playlist element, the playlist element is skipped and streaming continues with the next element in the playlist.

Whether playing in the reverse direction or forward direction, if a playlist element references missing content, the element is skipped and streaming continues with the next element in the playlist in the same play direction. If a jump or resume command resolves the starting NPT to a location in the playlist that references missing content, streaming continues with the next playlist element in the direction indicated by the command. If there are no more elements in the play direction or in the direction indicated by the command, streaming stops.

When a playlist element is skipped, the following logging occurs:

- Log message is added to rtsp.log (Skipped playlist item: \textless Item name\textgreater).
- Log message is added to c2k log. Following are two examples:
  - cnNextContent:NOTPRESENT
  - fail stream playback with cnError:status (If the missing element is the last one in the play direction. The status code would be NOTPRESENT or READ_FAILURE.)
- SNMP counter, VDStvSkippedPlaylistElements, is updated in CISCO-VDSTV-CS-STATS-MIB.

Mid-Roll Advertisement Placement Accuracy

When playlist elements use normal play times (NPTs) for the element start and end times, the Cisco VDS-TV software converts the NPT values to file offsets for mid-roll placement of advertisements. The conversion from NPT values to file offsets is accomplished by using a straight-line rate-based computation, which is adjusted to the nearest I-Frame offset.

Release 3.0 introduces the option to use the presentation time stamp (PTS) values to convert the NPT values for mid-roll placement of advertisements, instead of using the file offsets. PTSs are included in the MPEG-TS and are used by the set-top decoder to synchronize separate elementary streams (video, audio, subtitles, and so on). Using PTS values to insert advertisement playlist elements is preferable to converting NPT values to file offsets, because PTS values more closely match the user-observed playback time.

When the file offsets are used, the NPT values are used to identify the starting and ending frames of the playlist content segment and are based on the order of the content segments in the content file.

When the PTS is used, the NPT values are used to identify the starting and ending frames of the playlist content segment and are based on the PTS, which is the display order of the content segments in the file. The display order may not be the same as the file order. Some frames have to be processed or decoded before other frames, because subsequent frame decodings depend on previously decoded frames, even though the previously decoded frames are meant to be displayed at a later time.

Configuring Conversion Mode for Playlist Ranges

By default, the VDS is configured to use the file offsets for mid-roll placement of advertisements. To use PTS values, use the Conversion Mode field on the Configure > System Level > MPEG Tuning page.
**Overview**

**Trick-Mode Restriction**

Restriction of trick-mode controls (pause, rewind, fast-forward) per playlist segment is supported. If a client issues a trick-mode command for a locked-out playlist segment or attempts to bypass a trick-mode restricted segment by jumping to the next segment, an RTSP/1.0 403 Forbidden response is sent to the set-top.

The CDSM GUI provides the ability to configure the Rewind Skip Trick-Mode Restriction on the MPEG Tuning page (Configure > System Level > MPEG Tuning).

**Relax Forward Trick-Mode Restriction After Initial Playback**

Previously, if trick-mode restriction is configured on a playlist element and a fast-forward command is issued, the restricted element ignores the fast-forward command and plays the content at normal speed. In Release 3.0, if the restricted element has been played once from beginning to end at normal speed in a specific session, then the fast-forward trick-mode restriction is relaxed for that element in that session and any further fast-forward commands on the restricted element are honored. This relaxation only applies for that session. Other sessions using the same playlist must play the restricted playlist element at least once at normal speed before the fast-forward command is honored for the restricted element.

**Enforce Trick-Mode Restriction for Jump Play Commands**

In Release 3.0, trick-mode restricted play elements are enforced and the viewer is not allowed to skip over restricted play elements by using chaptering, dragging, or jumping. Jumping and dragging playback commands move the current NPT to a new location in the forward direction.

Forward jumps are not allowed if they are initiated from within a fast-forward-restricted playlist segment. If the forward jump is initiated from within a playlist segment that permits fast-forward tricks, but jumps across, or into, one or more fast-forward-restricted segments, the jump is abbreviated to the point where the nearest (relative to the current playback position) fast-forward-restricted segment begins.

If the first playback command of a session is a for normal speed with a starting NPT other than the beginning of the content (NPT = zero), it is assumed that the session is resuming playback after previously playing through the preceding playlist elements, and therefore the fast-forward trick-mode restriction is relaxed. After the fast-forward trick-mode restriction is relaxed, the jump is allowed within the restricted segment in both the reverse and forward directions.

**Free Pass Support**

Cisco VDS-TV 3.5 release supports Free Pass feature that enables the user to jump or FF the trick restricted segments within a configurable duration, only if the user has watched an ad-break completely. The end of an ad-break is identified when the transition happens from a FF trick restricted segment to an unrestricted segment. If there are multiple FF trick restricted segments (i.e) multiple Ads, only on transition from last FF segment (last Ad) to the next unrestricted segment an ad-break is considered completed. The free pass duration starts from the time of completion of an ad-break.

**Future Recording Contents in the Playlist**

Starting from Release 3.9, Cisco VDS-TV supports future recording playlist elements in the SETUP request. The playlist elements can contain VOD (recorded data), live content and future recording data. When a STB enters time shift mode, the back-office sends a SETUP request with several playlists to the
streamer containing 8 hours of time shift content. The RTSP server validates the playlist elements and if all are valid, the RTSP server sends 200 OK to the back-office. The RTSP server also supports switch between valid playlist elements on FF, RW or 1X play.

The RTSP server stores the future recording elements in an opaque memory and plays off the VOD and live data. Once the live recording reaches the EOS then the RTSP server appends the first future element from the opaque memory to the current session. This process is repeated until all future recorded elements are played off.

The user can enable the future recording support via CDSM Setup page in CDSM GUI.

Inserting Ads to NGOD playlist

Starting from Release 3.12, VDS-TV supports transmitting advertisement details in the NGOD playlist along with the movie to the streamer. The advertisements are categorized as pre, mid and rear ads. When an advertisement is being played a new 8810 announcement message is sent by the RTSP application to the back-office. The advertisement details must have the NGOD [R|F] restriction flag that restricts rewind and fast-forward on an advertisement but pause is allowed on an advertisement.

Digital Video Watermarking

The Digital Watermarking feature, also called digital video fingerprinting, provides the ability to track the source of unauthorized content copying. A watermark is embedded into the content for each end-user. If a copy of the content is found, then the watermark can be retrieved from the copy and the source is identified. The watermark is undetectable by the person viewing the content.

At the time of ingesting the content into the Vault, the portion of the MPEG-2 Transport Stream containing the watermarked data is repeated back to back in the asset to be ingested. The asset also has a special entry in the PMT that points to a stream containing location and identification of the duplicate watermarked frames. When the Vault ingests this content, it captures all information identifying the watermarking data in a special file and removes it from the content. It also captures special metadata related to that content which is used by the Streamer to create a watermarked content that is unique to the requesting user.

When a user requests a session containing a watermarked asset, the Streamer fetches this content along with the special file identifying the location of the duplicate watermarked frames and the content metadata. The content metadata along with the client ID is provided to the watermarking library through the Watermark Application Server, which returns a decision bitmap. This bitmap is used by the Streamer to decide whether to send an original non-reference frame or its watermarked counterpart. The Streamer only sends one or the other, but never both the original and the watermarked frames.

Should a user capture this video and make it available illegally, the video can be analyzed to reverse engineer the decision bitmap and the source of the video can then be identified.

Enabling Digital Watermarking

Digital Watermarking is enabled by default. To verify the Digital Watermarking application has started, enter the `ps -ef |grep db` command. The following output line of the `ps -ef |grep db` command indicates the watermarking application has started:

```bash
isacp 6983  1  0 Sep20 ?  00:01:56 /home/isacp/bss/bin/VDSWaterMarkSvr --serverid 188 --groupid 66 --dbpath /tmp/isadb --logfile /arroyo/log/wmsvr.log --loglevel LOW
```
To enable Digital Watermarking, run the `vdsconfig` script on each Streamer and answer yes (y) to the question “Do you want to enable Watermark Server?”

Alternatively, to enable Digital Watermarking manually, log in to the Streamer as user `isa` and enter the following commands:

```
$ arroyo stop
# pgrep avsdb
# pgrep AVSRTPServer
# su -isa
$ cd /home/isa/bss/etc
$ touch wmsvr.conf
$ arroyo start wmsvr
$ service avsdb start
$ service rtsp start
```

### HTTP Live Streaming

HTTP Live Streaming is fully supported; similar to live streaming over Cache Control Protocol (CCP). The enhancements to HTTP Live Streaming consist of the following:

- Catch-Up to Live, page 1-10
- Play While Ingesting the Same Content, page 1-10

#### Catch-Up to Live

A video player can play live content close to the live point, within 2.5 seconds of the live point, without macroblocking or leaving artifacts on the screen of the player.

If play starts at 0 or some point before the live point, then the Catch-up to Live feature allows the end-user to fast-forward to the live point and resume normal play at the live point. The play point will be within 2.5 seconds of the live point.

#### Play While Ingesting the Same Content

While ingesting the content, a set-top can request the content play start at 0, at “play now,” or at any specific normal play time (NPT) value between 0 and the live point; and the content will begin playing at the requested point of play.

When a set-top sends a “play now” request, meaning the set-top is requesting that the play begin at the live point, the “play now” point is within 2.5 seconds of the live point.

### H.264/AVC Ingest

This enhancement adds the capability to ingest H.264 video files (in a CBR MPEG-2 transport stream wrapper) in an RTSP NGOD environment. This implementation is compliant with the NGOD index file specification, Comcast-SP-NGOD-CDN-OBJ-I02-101105 which includes updates to support H.264 video.
VOD Error Repair

The VOD Error Repair feature retransmits lost packets to improve the quality of the end-user video experience. The VOD Error Repair feature uses negative acknowledgement (NACK) retransmission methods to implement retransmission-based error repair.

VOD Error Repair is supported on ISA environments that use the Cisco (RTSP) setting as the LSCP Client Protocol, and RTSP environments that use the Cisco RTSP deployment type.

In addition to UDP streaming, unicast Realtime Transport Protocol (RTP) with Realtime Transport Control Protocol (RTCP) streaming, as well as Error Repair (ER) are supported.

The client dictates which streaming protocol is used by way of the RTSP SETUP message. The following streaming protocols are supported in the same system with simultaneous streams of each type:

- UDP
- RTP
- UDP with NAT traversal (Interactive Connectivity Establishment [ICE])
- RTP with NAT traversal (ICE)
- RTP with retransmission-based error repair
- RTP with NAT traversal (ICE) and retransmission-based error repair

For sessions that use UDP, aside from RTSP messages, only the media server sends packets.

For sessions that use RTP, RTCP packets may be sent from the server to the client or from the client to the server. The client must be aware of the server’s IP address and ports for receiving these packets.

For sessions that use NAT, the server sends its own IP address and ports as ICE candidates.

For sessions that do not use NAT, the transport header must include a “server ports” parameter.

For sessions that use RTP retransmission-based error repair, a client sends a second SETUP request to the VDS Control server, which requires a total of four open ports. The first SETUP message has two ports (one for RTP and one for RTCP), and the second SETUP message has two ports that carry two ICE candidates. The URLs used for the retransmission stream are appended with the “/rtx” ending.

Following is an example of the first SETUP message:

```
SETUP rtsp://192.0.2.100/movie.mpg/rtx RTSP/1.0<CRLF>
CSeq: 2 <CRLF>
Transport: RTP/AVPF/UDP; unicast; destination=54.0.1.1; client_port=8998-7123,
          MP2T/DVBC/UDP; unicast; destination=54.0.1.1; client_port=8998<CRLF>
RTSP/1.0 200 OK<CRLF>
CSeq: 2<CRLF>
Session: 12345678<CRLF>
Transport: RTP/AVPF/UDP; unicast; destination=54.0.1.1; client_port=8998-7123;
          source=101.1.2.3; server_port=50236-50237<CRLF>
```

Following is an example of the second SETUP message:

```
SETUP rtsp://192.0.2.100/movie.mpg/rtx RTSP/1.0<CRLF>
Session: 12345678 <CRLF>
CSeq: 2 <CRLF>
Transport: RTP/AVPF/UDP; unicast; destination=54.0.1.1; client_port=8999-7124<CRLF>
          <CRLF>
RTSP/1.0 200 OK<CRLF>
CSeq: 2<CRLF>
```
Retransmission-based Error Repair is only available with RTP streaming.

Background

RTP packets include sequence numbers that are used to detect missing packets and reorder out-of-order packets. RTCP is the control protocol for RTP and is used to send receiver reports from the client to the server that include monitoring information, to send sender reports from the server to the client, and to request retransmission, which is the RTCP NACK packet that includes the RTP sequence number.

The Streamer receives the retransmission RTCP NACK request. Each NACK request identifies one or more missing RTP packets. The Streamer keeps a small buffer of recently transmitted packets and the missing packets are retransmitted based on how many packets the buffer maintains.

Error Repair Client on set-top

The VOD Error Repair feature requires that the set-top have the Cisco Visual Quality Experience Client (VQE-C) software running on it. The VQE-C is the error-repair client software, which has the following capabilities:

- Receives RTP video packets
- Detects missing packets
- Requests retransmission of missing packets
- Merges retransmitted packets with original stream
- Collects statistics and counters for monitoring

The VQE-C is a software development kit (SDK) that is available for download through the open-source program. Additionally, the set-top must comply with the Cisco RTSP syntax for VOD Error Repair.

Monitoring

The play management application (PMA) log file, vqe.log, is located in the /arroyo/log directory. To check for PMA errors, enable the PMA debug flag for the vqe_cp facility on the Logging page in the CDSM.

AMT

Application Monitoring Tool (AMT) runs a web application on each Streamer and provides several troubleshooting tools. For more information, see Appendix E, “Using the VDS-TV Streamer Application Monitoring Tool.”

Integrated Streamer Recorder

Starting from Release 3.4, VDS-TV supports an Integrated Streamer Recorder (ISR) platform, a new server type based on VDS-TV architecture. ISR has multiple control interfaces that interact with external systems to provide recording, streaming, and delivery functionalities. It also has both high throughput ingress and egress data interfaces.
The ISR also supports the separation of configuration management and login network traffic from the control traffic with external systems using a separate configuration interface. By default, the configuration management traffic shares the control (management) interface with the control traffic.

In this release, the CDSM GUI is enhanced to allow for the configuration of ISR servers. An ISR server retains all of the features of a Streamer, as well as all of the features of a Recorder. When the CDSM Setup “Manage Recorders” feature is enabled, the following CDSM configuration pages will be available to allow for configuration of an ISR server:

<table>
<thead>
<tr>
<th>ISR GUI Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Level Configuration</td>
<td></td>
</tr>
<tr>
<td>Configuring MPEG Tuning</td>
<td>Configuration of Streamer settings and enabling/disabling of dynamic trick modes</td>
</tr>
<tr>
<td>Configuring Ingest Tuning</td>
<td>Setting of 1-10 trickmode speeds for dynamic trick modes</td>
</tr>
<tr>
<td>Configuring QAM Gateways</td>
<td>Configuration of QAM Gateways for Streamer group settings</td>
</tr>
<tr>
<td>Configuring Stream Destinations</td>
<td>Configuration of Stream Group settings</td>
</tr>
<tr>
<td>Configuring Shared Recorder Settings</td>
<td>Configuration of Shared Recorder settings</td>
</tr>
<tr>
<td>Array Level Configuration</td>
<td></td>
</tr>
<tr>
<td>Configuring Stream Groups</td>
<td>Configuration of Stream Groups settings</td>
</tr>
<tr>
<td>Configuring the Control and Setup IPs</td>
<td>Configuration of Control and Setup IP settings</td>
</tr>
<tr>
<td>Server Level Configuration</td>
<td></td>
</tr>
<tr>
<td>Configuring the Interfaces</td>
<td>Configuration of Streamer and Recorder settings</td>
</tr>
<tr>
<td>Configuring the Servers</td>
<td>Configuration of Streamer settings</td>
</tr>
<tr>
<td>Configuring Individual Recorder Settings</td>
<td>Configuration of Individual Recorder settings</td>
</tr>
<tr>
<td>Configuring the Route Table</td>
<td>Configuration of Streamer settings</td>
</tr>
<tr>
<td>Configuring RTSP Setup</td>
<td>Configuration of Streamer and Recorder settings</td>
</tr>
</tbody>
</table>

**Media Origination Suite 2.0 VOD Support**

The Media Origination suite (MOS) Release 2.0 introduces the following new features:

- ATIS Index File Format Support
Overview

- Cache-Control and Content Revalidation for IP nDVR Flows
- Common Copy Cloud DVR
- Multi-Language Playback for HDS, HLSv4, and HSS
- VOD Ingest and Storage (IP ABR content)
- Vault to Key Server Integration for VOD

Starting from release 3.4, VDS-TV supports IP delivery to ABR clients on VOD application from VDS-TV Vault cluster via ATIS C2. Multi-Bitrate Adaptive Transport Stream (ATS) files generated from VOD Transcoder (ex: CTM) are ingested onto Vault and the vault serves these files to VOS via ATIS C2 using HTTP 1.1 interface. CMS/VMS controls ingestion of ATS files as well as all associated metadata files.

The CMS/VMS provides the FTP Source URLs of the individual file components of the asset bundle in a single command. The VOD content is identified by a unique content identifier that is explicitly specified in the ingest command. The vault application will store all the VOD files under the unique content identifier. Additionally the vault application augments the bundle with ATIS index files and Asset Description files. When the ingest is complete the vault application returns the HTTP Access URLs of the individual file components.

The format of the URL to acquire contents from the Vault by the VOS/JITP systems is:

http://vaultip_or_fqdn/vod/ip/{CID}

The format of the URL to acquire ABR contents from the Origin server by the CDN is:

http://origin_srdn/<prefix>/<content_id>/<format_specific_suffix>

The format of the URL to acquire ABR contents from the CDN by the Clients is:

http://cdn_srdn/<prefix>/<content_id>/<format_specific_suffix>

In this release, VDS-TV supports the following MOS 2.0 VOD functionality.

Integrated Delivery function of Recording Engines to deliver the recorded content, its metadata and index resources to dedicated streamers. The Recorder supports the delivery of the recorded resources over an ATIS C2 interface as well as a HTTP 1.1 interface. The ATIS C2 interface will be used by the TV Streaming devices whereas the HTTP 1.1 interface will be used by the IP Playback functions.

Interface between the CMS and Vault application where the CMS issues a VOD Ingest command with the URLs of different components of the transcoded asset (including the CIF index and other metadata files).

For detailed information on MOS 2.0 architecture refer the following documents:

- Cisco Media Origination Suite Release 2.0 Software Installation and Configuration Guide
- Cisco Media Origination Suite Release 2.0 API Guide
- Cisco Media Origination Suite Release 2.0 Command Reference
- Cisco Media Origination Suite Release 2.0 Alarms and Error Messages Guide
- Release Notes for Cisco Media Origination Suite Release 2.0
Content Delivery System Architecture

Vaults and Streamers have different but important functions that are required for the VDS-TV 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.

<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>

Table 1-2 High-Level Description of the VDS-TV and TV VVI
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 colocated 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.

Starting from Release 3.9, VDS-TV supports 1000000 assets for RTSP environments.

The 600,000 assets supported for the RTSP environment has the following limitations:

- Maximum assets in a Vault Group is 600,000
- Maximum GOIDs (normal speed content file, index file, delta content file, trick-mode files) per Vault is 600,000
- Maximum number of assets per Vault is 65,000

Each Vault supports a maximum of 600,000 Global Object IDs (GOIDs). GOIDs are used for each asset and for each trick-mode file associated with each asset. The maximum number of assets supported on a Vault varies depending on the number of trick modes configured (the maximum number of trick modes is 12). The maximum number of assets supported in the VDS is determined by the number of trick modes configured and the number of Vaults in the system.

---

Table 1-2  *High-Level Description of the VDS-TV and TV VVI (continued)*

<table>
<thead>
<tr>
<th>Content Delivery System Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>There are two types of management:</td>
</tr>
<tr>
<td></td>
<td>• Content Delivery System Manager—Browser-based user interface</td>
</tr>
<tr>
<td></td>
<td>• SNMP agent—Network Management System (NMS) interface</td>
</tr>
<tr>
<td>Storage</td>
<td>There are four levels of storage (or cache):</td>
</tr>
<tr>
<td></td>
<td>• All content is stored on the Vault server, as well as mirrored to other Vaults.</td>
</tr>
<tr>
<td></td>
<td>• Requested content is stored on the Caching Nodes.</td>
</tr>
<tr>
<td></td>
<td>• Recently requested content, or popular content is stored on the hard drive on the Streamer.</td>
</tr>
<tr>
<td></td>
<td>• Currently requested content, or popular content, is stored in the random access memory (RAM) on the Streamer.</td>
</tr>
<tr>
<td>Event Collection</td>
<td>The Content Delivery System Manager collects logged events for reporting purposes as well as for third-party applications</td>
</tr>
<tr>
<td>Reports</td>
<td>The Content Delivery System Manager provides a reporting tool to aid performance trending and analysis of streams, popular content, bandwidth usage, and more.</td>
</tr>
</tbody>
</table>

---
Chapter 1      Product Overview

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 colocated with Vaults or distributed to remote locations. The Stream Group is responsible for the personalization and streaming of content in response to user requests.

D5 Interface

Starting from Cisco VDS-TV Release 3.5, D5 Interface (HTTP over XML) is supported between On Demand Resource Manager (ODRM) and Streaming Server component of Next Generation On Demand (NGOD) system.

This two way interface is used by Streaming Server to notify the ODRM of streaming server configuration and streaming server statistics/current resource usage and is also used by ODRM to query the streaming server status and current resource usage.

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 VDS. 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 VDS-TV or a TV VVI network.

The CDSM provides centralized management functions for the VDS-TV, 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 VDS 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.

In a VVI with CCP Streamers, similar to a VDS, 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 VDS-TV. 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.

<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>
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 VDS-TV 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 three types of mirroring:

- Local mirroring
- Mirroring within an array
- Array mirroring (from Vault Group to Vault Group)
Local Mirroring
Local mirroring defines the number of copies of each content object to maintain on the unique drives of a single Vault. Local mirroring allows resiliency for a small installation (for example one Vault). Local mirroring guards against a single drive failure, but does not protect against service interruption or potential data loss in the event of a complete server failure.

Local mirroring is not configured by default, and is generally only used when there is a single Vault in a system. Local mirroring is configured in the **Configure > Server Level > Server Setup** page with the **Vault Local Copies** field, which corresponds to the tunable “vault local copy count” in CServer. Up to four local copies are supported.

Mirroring within an Array
Mirroring within an array defines the number of copies of each content object in an array to maintain across the Vaults within that array or site. Mirroring within an array guards against a single drive failure or the failure of an entire server. The number of copies to maintain within that array is configurable in the **Configure > Server Level > Server Setup** page with the **Vault Mirror Copies** field, which corresponds to the tunable “vault mirror copies” in CServer. Up to 10 copies within an array are supported.

Array Mirroring
Array Mirroring (from Vault Group to Vault Group) specifies that each content object on all of the Vaults in one group has at least one copy on a Vault in the mirrored Vault Group. Array Mirroring is only responsible for ensuring that a single copy of each content exists in the mirrored Vault Group. If more than one copy of each content object is required within an array, Mirroring within an Array (not Array Mirroring) is responsible for this task. Array Mirroring is configured in the **Configure > Array Level > Vault Redundancy Map** page, which corresponds to the tunables “allow vault array mirroring” and “vault array mirror” in CServer. Each Vault Group can have up to 3 mirrored Vault Groups configured.

**Note**
Array Mirroring is part of the Vault Groups feature and is only available if Vault Groups is enabled on the CDSM Setup page. For more information, see the “Vault Groups” section on page F-7.

Vault Server Resiliency
The Cisco VDS-TV can handle the loss of an entire Vault server without impacting the subscriber. The communication with the back office 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 back office and handles the ingest of new content.
Chapter 1  Product Overview

Content Delivery System Architecture

Vault Group Redundancy

In addition to the Vault server redundancy, the Cisco VDS-TV offers redundancy for Vault Groups. When the VDS 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 experience. Content is mirrored among as many as four Vault Groups (one Vault Group ingests the content and up to three Vault Groups mirror the content), 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 a 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 is 30. Prior to 3.5.2 release, the maximum number of vault groups supported is 20.

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 VDS-TV 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 re-fetch of content from the Vault occurs without impacting the subscribers. For example, for a Streamer array of five Streamers with sixteen hard drives each, a lost drive only reduces the total caching capability by less than 1.25 percent. The need to replace the failed drive is not time critical in the least, making quarterly replacement of any failed Streamer drives feasible.

Streamer Server Resiliency

The Cisco VDS-TV architecture allows for failed Streamer servers as well. If any Streamer server fails, the communication to the back office is transparently handed off to another Streamer. With the VDS-TV 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 VDS-TV 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 VDS-TV architecture allows resiliency 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.
However, for RTSP-NGOD deployments, a caching node internally retries to locate the content before notifying the failure to the streamer. By default, a caching node retries twice. This retry count can be configured using a tunable

```
# cat /proc/calypso/tunables/paidretrycount
00000002
```

To set the retry count to 3, set the following tunable:

```
echo 3 > /proc/calypso/tunables/paidretrycount
```

On setting the above tunable, the cache gateway retries three time to locate the content before sending a failure response to the streamer.

### CDSM Redundancy

The Cisco VDS-TV 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 VDS servers keep track of a controller IP address in the.arroyorc file. With CDSM redundancy, both management IP addresses are specified in the.arroyorc file on each VDS 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 VDS 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. However, the VDS 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 VDS 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 VDS-TV 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.

### Collectd Application

Starting from Release 3.9, Cisco VDS-TV supports a maximum of 512 VDS replication servers hence the volume of status and statistical data received at the Controller (CDSM/VVIM) through DB replication is very high. To avoid this load, a new application collectd runs on each node/server and performs the following functionalities:

- Collects status and statistical data in each node.
- Directly uploads data from each node on to Controller (CDSM/VVIM) over a TCP connection.
The collectd application running in controller acts as a receiver and receives that data from each node via TCP. This data is stored in the memory cache and is predominantly used for real-time monitoring.

The Controller (CDSM/VVIM) which earlier connected to AVSDB to obtain the statistical and monitoring data will now connect to collectd to obtain the same data.

**Scalability**

The Cisco VDS-TV 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.

**Server Scalability**

Starting from Release 3.9, AVSDB application in VDS-TV supports 512 replication servers (including vaults, streamers, cache nodes and controllers). The CSer replication is restricted to only 512 servers. For example, the number of VDS servers supported in streaming domain (streamers + cache) is 512.

**Asset Scalability**

Starting from Release 3.9, Cisco VDS-TV is certified to support up to one million assets in the overall system.

**Package Scalability**

The existing limitation of AIM supports upto 200K packages in the 4.4 Software Release. Starting from release 4.6, VDS-TV supports upto 300K packages which is certified. The loading and start time of the AIM service is optimized upto 35 seconds, approximately.
CHAPTER 2

Network Design

This chapter describes the different network topologies for the Cisco Videoscape Distribution Suite-TV (VDS-TV), the different network connections of the VDS servers, the VDS workflow, and network configuration considerations.

- Overview, page 2-1
- VDS-TV and VVI Topologies, page 2-2
- VDS Workflow, page 2-7
- nDVR Support for NGOD Deployments, page 2-13
- Vault Virtualization, page 2-15
- BMS Considerations for ISA Environments, page 2-21
- Network Connections, page 2-23

Overview

The VDS-TV 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 set-tops. The VDS-TV solution uses a Gigabit Ethernet (GE) transport network from the headend to the distribution hub, where the HFC network terminates.

VDS-TV grows seamlessly from a single server implementation to multiple servers. As growth continues, VDS-TV 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 VDS-TV offers different configurations with regards to network topology, Business Management Systems (BMSs), and streaming modes.
VDS with Vaults and Streamers

In a VDS-TV 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 is modulated onto the HFC plant to the subscriber set-top for viewing.

VDS with ISVs

For the smallest networks, Cisco packages the VDS 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 VDS-TV with ISVs, MPEG-2 TS video is stored on the ISVs 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 set-top for viewing.

VDS with Caching Nodes

For larger networks, Cisco offers the VDS 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 set-top for viewing.

VDS-TV and VVI Topologies

The VDS-TV (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 VDS-TV 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, all VDS 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**

![Centralized Topology with Vaults and Streamers](image)

Figure 2-2 illustrates the centralized topology for ISVs.

**Figure 2-2  Centralized Topology with ISVs**

![Centralized Topology with ISVs](image)
Figure 2-3 illustrates the centralized topology for a VVI.

**Decentralized Topology**

The decentralized topology is a hub-and-spoke topology between the headend site and multiple hub sites, where the Vaults are located at the headend and the Streamers 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 Stream 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 2-4  Decentralized Topology**
Hybrid Topology

In a hybrid topology, the Vault servers and backup Streamer servers are located at the headend, with the active Streamers at a remote hub site. If the remote hub site goes down, the Streamers at the headend take over. A hybrid topology blends the advantages of centralized and decentralized topologies that is based on needs of the system implemented. Figure 2-6 illustrates the hybrid topology.
TV VVI Management

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

In a VDS, 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>
<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>
Centralized Management

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

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.

In a split-domain VVI that uses HTTP for communication between the Caching Nodes and Streamers, the databases for each domain are separate. The information stored in each database is not shared with the servers in the other domains. 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 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. The Stream Managers communicate with the VVIM by using the database replication.

Note

Split-domain management is supported in an RTSP environment, and an ISA environment with the Content Storage feature and CCP Streamers.

VDS Workflow

Content is ingested and stored in the Vault array. The Vault array can consist of two 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 back office 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

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 120 GB is supported. 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 Stream Group in response to cache-fill calls from the Streamers. Content is also distributed across the network in response to scheduled or Barker stream content fulfillment.

As Streamers need to fill content, they issue locate requests to the Vaults for the specific content. The Streamer makes a decision on which Vault to pull content from based on the responses. The process of determining where to pull content from includes memory capacity and disk capacity of the Vault, as well as network capacity.
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 2-12.

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

---

**Note**

All servers can be on different subnetworks. However, because of back office 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.

---

### Popularity-Based Caching

Popularity-based caching reduces the write rate to the storage devices on the Streamer and Caching Node while maintaining the best possible cache-hit rate on the available storage.

To control peak and average write rates to cache (flash or disk storage), the algorithm that determines when content is written to cache is changed so that only content that is likely to be accessed most often is cached. Content is only cached if it is more popular than the least popular content that is currently cached. Otherwise, the content is transmitted from the Vaults to the end-users by way of the cut-through mode, where content is temporarily stored in the Streamer and Caching Node RAM without ever writing it to disk or flash storage, and then streamed directly from the Streamer’s RAM to the end-user. When cache space is needed, the least popular content is evicted from cache first.

The write rate for caching content is determined by the rate at which previously popular content becomes less popular to the point where it no longer makes sense to keep it in cache, and previously unpopular content becomes more popular to the point where it does make sense to keep it in cache. Content popularity is measured by the time-decaying average of the number of play requests on each Global Object Identifier (GOID).

Previously, all content was written to cache (except when overloaded) and the Least Recently Used (LRU) content was evicted first.

With the Popularity-Based Caching feature, only popular content is written to cache and the least popular content is evicted first.

### Bandwidth Manager for Thin Pipe

The bandwidth manager controls the traffic leaving the site to any other site and queries all the VDS servers in the site for the thin pipe mapping configuration of each VDS server. One server in the site is elected as the bandwidth manager for all servers in the site. A site is defined by the Site Setup page, which associates groups with a site. Initially, the bandwidth manager allocates bandwidths of whatever the VDS servers have already committed, provided the committed bandwidths are within the pipe bandwidth limits; otherwise, the bandwidth manager allocates a percentage of what is committed. After the initial allocation, the bandwidth manager distributes the bandwidth equally among all the remaining VDS servers in the site.

Each VDS server in each group reports the bandwidth each one is using to the bandwidth manager every ten seconds. The bandwidth threshold for each server has an upper limit of 90 percent and a lower limit of 5 percent. If a server reaches either limit, the server reports this to the bandwidth manager.
immediately, and does not wait for the ten-second report interval. For example, if the server is given 100 Mbps and the streams that were just started uses 90 Mbps, the upper threshold limit has been reached and the server asks the bandwidth manager for more bandwidth.

A separate entry is maintained for each thin pipe with a list of servers that have the same thin pipe configuration. Servers that belong to the same thin pipe are added and removed as they become reachable or unreachable.

The bandwidth manager service runs on each server in either the primary mode or the passive mode. The one server at the site that is running the primary mode is selected through a discovery mechanism. The primary bandwidth manager maintains all the thin pipes and associated server structures. If the server running the primary bandwidth manager fails or loses connectivity, the newly elected bandwidth manager takes over and when the old primary bandwidth manager becomes available again and connectivity is restored, the thin pipe information and structures are deleted from the old primary.

All bandwidth manager messages are logged in the bwm.log file. The following logging levels are defined (default level is Information):

- Critical
- Error
- Warning
- Information
- Debug
- Debug Verbose

### 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
- Remote Setup and Control 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 back office 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 colocated with the back office server is assigned as the primary Setup server. The Setup server receives the setup request from the back office and maps the service group.

The Setup server returns the IP address of the Control server, and the set-top 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 back office, 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 set-top, 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 set-top 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.

Remote Setup and Control Server

The Remote Setup and Control Server Support feature allows the Setup and Control servers of the Streamers to be placed in a different location than the Play servers of the Streamers. All control traffic (setup and control) goes to one Streamer (Setup and Control server), and all video data traffic is served from the Streamers designated as the Play servers.

As part of this feature, there is never just one stream transmitted on a single Ethernet interface. There is always at least two active streams transmitted on an interface.

Note

The Remote Setup and Control Server Support feature is supported on a Virtual Video Infrastructure (VVI) with split-domain management in an ISA environment and Content Storage configured as either Shared or Distributed.

The VOD Error Repair feature is not supported with the Remote Setup and Control Server Support feature.
Remote Setup and Control

The setup and control traffic between the set-tops and VDS is sent to a location that is separate from the location where the video data streams originate. The Session Traversal Utilities for NAT (STUN) traffic is structured so that it is sent to the Setup server instead of the Play server. The data path through the end-user’s NAT device complies with RFC-5389.

Stream to Interface Relationship

The Remote Setup and Control Server Support feature requires at least two stream requests before sending the first data stream, and makes sure there are at least two data streams on an active Streamer interface at all times. The Control server makes sure there are at least two streams on an active Streamer, and the active Streamer makes sure there are at least two streams on an active stream interface.

If the first play request on a Play server reaches the session timeout period before a second play request is received on that Play server, the first session fails and the stream is sent back to the Control server for relocation. If there are only two sessions created on the VDS and one session is destroyed or completes, the remaining session is destroyed.

Global Source Address

The Remote Setup and Control Server Support feature introduces the Global Source Address, which is the IP address and associated port number that is used by all Play servers for transmitting stream data. The Global Source Address is defined on all Streamers (Setup, Control, and Play).

The Global Source Address is defined in the setupfile on all Streamers (Setup and Control servers, and Play servers). This address is hosted on the primary Setup server and is managed in a fault-tolerant manner; that is, it moves from interface to interface as needed if an interface fails, and it transitions to a new primary Setup server if the original primary Setup server becomes unreachable.

Each stream interface on the Streamers continues to have a unique IP address so that diagnostic packets (and cache-fill traffic if configured as a stream/cache interface) can be sent and received on those interfaces. However, all stream data packets are sent using the Global Source Address as the source.

The Control server uses the Global Source Address as the stream source address in the reply to the NAT Setup request from the set-top. This occurs whenever the Streamer Play server indicates that a remote STUN handshake is needed.

The Global Source Address has the following benefits:

- Mid-session STUN handshakes are not needed, which eliminates the overhead and associated temporary black-screens that occur on set-tops when STUN handshakes happen mid-session.
- Streams can be moved more easily for load-balancing purposes. A Streamer can move a stream from one interface to another without involving the Control server, Setup server, or set-top. A Control server can move a stream from one Play server to another without involving the Setup server or set-top.
- Address management on the Setup server and on the network is simplified. There is only one stream source address that needs to be hosted on the Setup server, and there is only one routing setup in the network configuration.

The following additional information should be considered when configuring the Remote Setup and Control Server Support feature:

- To trace the source of a stream, use the stream session ID along with the associated log files on the Streamers acting as the Play server, as well as the Streamers acting as the primary Setup server and primary Control server. Other diagnostics such as the ping command can still use the unique IP address of each stream interface.
Additional router configuration may be necessary to ensure that the Global Source Address hosted on the Setup server is used for inbound traffic and that packets sent to that address are never sent to the Play servers.

**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 Groups 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 on 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 support only CCP, while RTSP environments support only 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. 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.

**nDVR Support for NGOD Deployments**

The nDVR feature for the RTSP NGOD deployment provides the following capabilities:

- Streamers can distinguish between requests for VOD content and requests for DVR content
- Streamers route cache-fill requests for VOD content to VDS servers (Vaults, Caching Nodes, and other Streamers)
- Streamers route cache-fill requests for DVR content to third-party sources (nDVR Recorders)
- Streamers generate trick-mode files for DVR content
- Streamers generate GOIDs for DVR content and associated trick-mode and index files
- Streamers support unique copy DVR content

In previous releases, Streamers received cache-fill content from Vaults, Caching Nodes, and other Streamers by way of the Cisco Cache Control Protocol (CCP). For RTSP NGOD deployments, the Streamers received cache-fill content from Vaults, Caching Nodes, and other Streamers by way of the C2 protocol.
Streamers are able to receive cache-fill content from VDS servers (by using CCP or the C2 protocol) and third-party sources. The Streamers can route cache-fill requests to Vaults, Caching Nodes, and other Streamers for VOD content, and to third-party sources for network digital video recorder (nDVR) recordings.

The nDVR feature supports unique copy content distribution from a third-party source (for example, nDVR Recorder) to the Streamer, and from the Streamer to end-user devices, which can be an IP set-top or QAM device.

**Asset Metadata**

Each content an end-user requests from a device has a unique title ID. For each content, there are different versions based on the encoding that is compatible with the end-user device (for example, high definition [HD] or standard definition [SD] for a set-top or mobile device, as well as resolution formats), which are identified by content IDs. When a request for content is sent from the end-user device to the back office, it includes the title ID. The back office maps the title ID to the content ID for the content that is compatible with the requesting device. The back office uses the content ID when communicating with the Streamers on what content object to stream to the device.

For some CDNs, the content ID is a combination of the ADI Product ID and Asset ID (PAID), and it is used to convey both VOD and DVR content. Other CDNs send the content ID from the back office to the Streamers in a URI. For the RTSP NGOD deployment, nDVR content is identified with a URI, and VOD content is identified with a PAID.

Each unique content can have several unique data objects required for playback; such as the normal video object for standard forward playback, video objects for trick-mode content, and an index file used to map playback time offsets to corresponding data offsets within the various video files. This information can be referred to as vendor-specific content metadata, or asset metadata.

The Cisco VDS-TV software uses a global object ID (GOID) to identify the different video and index data objects for a unique content. The VDS-TV software contains an association of the content ID with the various GOIDs used to store the different objects for the content.

To support nDVR, Streamers use the third-party object identifier in cache-fill requests. The Streamer not only stores the content ID to GOID mappings, but also a GOID mapping to an external object identifier which is generated by the third-party vendor. In addition, to support cache-fill from third-party vendors, Streamers generate the GOIDs. The generated asset metadata is revalidated to ensure specifically that the PAID-to-GOID-to-external object mappings are still valid.

**Cache-Fill Routing**

Streamers are used for streaming out regular VOD content sourced from other VDS servers or DVR content sourced from the Recorders. The Streamers route the cache-fill request to the appropriate source based on the content type, which is derived from the asset name space.

A Streamer must know the origin from which the needed object is sourced when performing cache-fill. Normally, a Streamer is configured with static routes for cache-fill. The Streamer must be configured with different source routes for the different content types.

For VOD content, the content identifier is a PAID. For DVR content, the content identifier is a URI, which contains the hostname or IP address of the third-party source (nDVR Recorder).
nDVR Architecture

The C2 protocol is used for cache-fill of DVR content from the nDVR Recorders.

A request for VOD content is identified by the Provider ID and Asset ID (PAID). A request for DVR content is identified by a URI. The Setup server receives the URI or PAID over the R2 protocol in a NGOD RTSP deployment.

The R2 setup request from the back office to the Setup server sends a URI for DVR content to be played. The URI includes the routing and protocol information necessary to cache-fill the DVR content. Content is identified by a URI instead of a PAID.

Cut-Through Support

DVR content can be categorized as unique copy or common copy. Unique copy is a recording of content that belongs to a single subscriber. The Streamers perform cache-fill of unique copy recordings directly from the Recorders. Consideration is made such that any unique video content that is cached is only performed for a transitory period.

Note

Only unique copy DVR content is supported

For unique copy recordings, there is no cache gain benefit of a hierarchical caching system, as the recordings cannot be shared across subscribers; therefore, the VDS servers do not cache unique copy DVR content.

Integration with Legacy VBOs

The nDVR feature integrates with legacy video back office (VBO) systems; such as Searchange, Axiom, and Ericsson Openstream.

Dynamic Trick-Mode Files

Normally, trick-mode files are generated by the Vaults at the time of ingest. For DVR content, trick-mode files are generated dynamically by the Streamers.

Trick-mode file generation for DVR content is enabled with the Dynamic Trickmodes field on the Configure > System Level > MPEG Tuning page.

Vault Virtualization

Vault Virtualization provides the following three types of configuration:

- ISA Regionalization, page 2-16
- Shared Content Store, page 2-19
- Virtual Content Store, page 2-20
ISA Regionalization

The ISA Regionalization feature is a combination of the Virtual Video Infrastructure (VVI) and legacy Videoscape Distribution Suite-TV (VDS-TV). This feature provides the ability to centrally store content on Vaults located in a centralized storage facility and allow remote sites to have a record of inventory of this content and access it by way of the Caching Nodes or directly on the central Vaults. The remote sites still operate as independent entities with their own local Vault Group, local Content Store, and local Streamers; managed by their own CDSMs and possibly accessing their own local BMS and AMS. The Streamers at each remote site can stream both locally stored content and centrally stored content.

The ISA Regionalization feature allows the use of a centralized storage facility containing both Vaults and Caching Nodes in a Virtual Video Infrastructure (VVI), while maintaining a localized or remote VDS at each headend.

For information on configuring ISA Regionalization, see the “ISA Regionalization Configuration Workflow” section on page 3-9.

Centralized Storage

The Virtual Video Infrastructure Manager (VVIM) manages the Vaults and Caching Nodes allocated in the centralized domain. The centralized domain can be distributed across multiple geographic locations; for example, the Vaults could be located in one location and the Caching Nodes could be located in another. The VVIM typically resides in one of these locations.

Each VDS has a virtual view of the VOD content stored on the central Vaults. The centralized content is ingested once, the first time it is requested; any subsequent ingest requests for that same content increments a reference counter.

Remote Site

Each remote VDS has a local Vault Group and communicates with a local BMS and local AMS located at the headend or at another headend nearby. Each remote VDS is able to ingest local content through the local Vaults and is able to access content stored in the central storage facility by way of the Caching Nodes and Vaults in the VVI. The centrally stored content is abstracted from the BMS by means of the local Content Store providing a virtual view of that content to the BMS. Both local and central content are available to fulfill streaming requests received by the Streamers in a remote VDS.

The ISA Regionalization feature uses the existing ISA architecture, but extends the ISA content component to support new behaviors associated with where content is physically located. Each VDS operates with a local ISA Content Store, which is extended to manage both centrally and locally stored content.

Real-time asset (RTA) content is not centralized, and is stored on local Vaults in each headend. The VDS determines if content should be ingested centrally or locally based upon the type of content (VOD or RTA) that is being requested.
Note

If the local Vaults are not available because they are down or have lost connectivity, then the master Streamer in the headend automatically takes over as the Ingest Driver client. If this occurs, when the local Vaults have been recovered and regained connectivity, the Ingest Driver client must be migrated back to the local Vaults before RTA ingests can be restored.

To move the Ingest Driver client from the master Streamer back to the local Vaults, stop and restart the statsd process on the master Streamer by entering the following commands:

```
pkill statsd
/home/stats/statsd -i <server_mgmt_IP_addr> -s <subnet mask> -d <mgmt_interface_name>
```

if NIC bonding is enabled bond0 is used as management interface

Ingest Driver

The ISA Regionalization feature introduces the Ingest Driver, which has a server-side and a client-side. The Ingest Driver server is located at the central location, on the master Vault, and is responsible for managing the content ingestion and deletion requests from the Ingest Driver clients located at the remote sites.

Ingest Driver Server

The centralized Vaults run an internal Naming Service, Notification Service, and Content Store. This Content Store is not associated with a remote BMS, and acts independently of all remote sites. The Ingest Driver gets the Content Store factory from the internal Naming Service, ingests content using the createServant and provision methods, and deletes content using destroy and remove Servant.

The Ingest Driver server is started and stopped on the master Vault and is automatically restarted like other ISA processes. When the server is started, it binds to a TCP socket and waits for requests. To handle the requests quickly, there are several threads created to parse the requests and fulfill them. When the server processes the request for each content, only one request is handled; that is, other simultaneous requests for the same content are blocked.

The Ingest Driver server reads the isa.cfg file and incorporates the following Ingest Driver configuration parameters set on the CDSM GUI:

- IngestDriverEnabled=1
- IngestDriverRole=1 (for server)
- IngestDriverHost
- IngestDriverPort
- IngestDriverNoOfThreads

The Ingest Driver server logs events to the IngestDriver.log file located in the /arroyo/log directory.

Ingest Driver Client

The Ingest Driver client is used by the local Content Store to send requests to the Ingest Driver server and receive responses from the server. When a provision call from the local Content Store is received from the back office, the Ingest Driver client establishes a TCP connection with the Ingest Driver server, sends the request, and closes the connection once the response is received.

The local Content Store reads the isa.cfg file and incorporates the following Ingest Driver configuration parameters for the Ingest Driver client set on the CDSM GUI:

- IngestDriverEnabled=1
Ingest Driver Content Management

The local Content Stores at the remote sites perform content management of the content at the central facility by interfacing with the Ingest Driver. The Ingest Driver compares the requested content identifier of each content ingestion and deletion request to the VDS repository to determine if the content exists. If the content does not exist, it is ingested using FTP and the FTP URL provided by the remote site. If the content already exists, the repository is updated to maintain the reference between the requesting site and the content. The Ingest Driver returns the VDS internal representation of the content bundle and associated content information, such as file size and bit rate.

When the Ingest Driver receives a deletion request, it determines if the request is for the last reference to the content. If it is the last reference, the Ingest Driver requests that the central Content Store delete the content and associated MPEG files. If it is not the last reference for the content, the Ingest Driver just removes the reference of the requesting site for that content in the repository.

Remote Ingests

At each headend, the external ISA interfaces to the back office do not change, and call flows remain the same. The remote CDSM is extended to identify a site as part of a regionalization grouping, and specify the communication information of the Ingest Driver. Internally, the local Content Store application is modified to check for this setting. If regionalization is turned on, the local Content Store application directs VOD (provision) requests to the Ingest Driver and RTA (provisionForPush) requests are directed to the local Vaults.

The local Content Store performs the createServant call locally, thus ensuring that each remote site has its own IOR representing the content object. If the request is distributed, the local repository is updated with the content-specific information, such as the content bundle, file size, and bit rate returned by the Ingest Driver. This allows the remote site to have local representation of centrally stored content.

For RTA content, the process is same as it has always been for the VDS. The local Content Store processes the provision call (provisionForPush for RTA) and directs the local Vaults to perform the ingest of the content.

Remote Streaming

Local streaming is accomplished by way of the Cache Control Protocol (CCP) locate capability. Each remote site is configured to communicate to a specific set of storage devices which could include local Vaults, central Vaults, and Caching Nodes. The locate feature broadcasts a request for a specific content, and the system performs a cost analysis to determine which storage device can best provide service. For VOD content, if the content is not already cached on the local Streamers, it is acquired from either the central Vaults or Caching Nodes. For RTA content, if the content is not cached on the Streamers, it is acquired from the local Vaults. However, knowledge of the content type is not required as the locate capability is able to determine its location.
Shared Content Store

Shared Content Storage, also known as Shared Content Store (SCS), works with a single, centralized AMS and catcher, through which all initiation for content ingest and content deletion is sent. The SCS handles ingest and deletion requests from multiple back offices by way of the central AMS. The scenario of back offices independently ingesting and deleting content through their local AMS is not supported.

The Content Storage feature requires the Virtual Video Infrastructure feature with Caching Nodes.

Figure 2-8 shows a high-level view of the SCS and a single, centralized AMS for multiple video hub offices (VHOs). A VHO is a local deployment that includes the video back office, Streamers, application servers, QAM devices, and other headend equipment.

The DNS server typically runs on the BMS server. The Naming Service is part of the video back office (VBO). All CORBA components, including the AMS, Stream Service, and Content Store, need to register with the Naming Service. The catcher receives or “catches” new content assets from an external communication device such as a satellite transmission or FTP server. After the package is received completely by the catcher, it sends the package by way of FTP to the AMS. The package consists of video and image content assets, as well as ADI metadata.

Following are the requirements for the SCS feature:

- Single, shared DNS server with all devices registering their hostnames to it. A central, shared DNS is required to resolve multiple Naming Services belonging to the different VHOs.
- Hostnames must be unique for all devices. This is required for the Naming Service discovery.
- Each VHO has its own Naming Service to which the ISA components of the VHO register.
- AMS controls the ingest and deletion of content.
- The Vault array has one SCS.
- SCS registers with each Naming Service.
A VVI with SCS must be initialized in the following order:

1. The shared DNS server must be up and running before starting up the shared AMS, SCS, and VHO devices.
2. SCS successfully registers with the Naming Service for each VBO.
3. Each VHO Stream Service registers with its respective Naming Service.

**Ingesting Content with the Shared Content Store**

Upon receiving the content package, the AMS schedules it for ingest by informing the Package Factory in each participating VBO of the content package, and passing the pertinent information (the ADI metadata, the URL where the content package can be accessed in the AMS, and the verb `ingest`).

The SCS creates one interoperable object reference (IOR) for each content package. The IOR is returned to all VBO Package Factories that request it, including any that requested it at the time the IOR was being created.

**Deleting Content with the Shared Content Store**

To delete content that was ingested for more than one VBO, the AMS is used to send the `export package delete` request to each VBO. The content is deleted from the Vault array only when all VBOs have requested the deletion. If one or more VBOs have not requested that the content be deleted, the content remains in the Vault array.

**Virtual Content Store**

The Virtual Content Store feature in an ISA environment replaces the Shared Content Store feature. The Shared Content Store (SCS) feature is the ability of several local sites (video hub offices [VHOs]) to ingest content at a central location and share that content with the other VHOs. The SCS feature eliminated ingesting multiple copies of the same content.

Vault Virtualization replaces the SCS with the Virtual Content Store (VCS). No content is ingested at the local VHO. All ingests and deletions of content occur at the central location, and both ingests and deletions are initiated by the local BMS at each local VHO, just as they were in the SCS. However, the VHOs do not need to communicate with the super headend (SHE) as they did with the SCS feature. With VCS, communication of ingestions and deletions is handled by the Ingest Driver client residing on a Streamer in each VHO and the Ingest Driver server residing on the master Vault in the SHE. Vault Virtualization requires that Vault Groups be disabled.

The Virtual Content Store (VCS) component runs on a Streamer in the Stream Group, and if a failover occurs, the VCS fails over to another Streamer in the Stream Group.

Only one copy of the centrally located asset is ingested and shared by the system, and the asset is only deleted when all VHOs have requested the deletion.

For information on configuring Virtual Content Store, see the “Virtual Content Store Configuration Workflow” section on page 3-10.
BMS Considerations for ISA Environments

The VDS-TV 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 VDS-TV.

OpenStream ISA Integration

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

Note

Dual conditional access systems (CAS) for ISA environments, Cisco/Scientific Atlanta Power Key Encryption System (PKES) and the Motorola Offline Encryption Station (OLES), is supported. A field on the Monitor Completed Ingests page indicates whether the ingested content is encrypted or not. Both clear and encrypted content can be ingested.

For more information on the configuration parameters required to facilitate communication between the OpenStream BMS and the VDS-TV, see Appendix C, “BMS Communication.”

Figure 2-9 illustrates how the VDS-TV integrates with the OpenStream BMS.

---

**Figure 2-9  VDS-TV Integration into the OpenStream BMS**
Streaming Mode

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

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

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

Steering Ingests

The Ingest Steering feature offers the ability to have one BMS send ingest information to the master Vault, and depending on the product ID in the content name, the content is either ingested by one of the Vaults in the national Vault Groups, or it is ingested by a specific local Vault Group.

Note

For the Ingest Steering to function correctly, the content name must be in the following format: ProviderId::AssetId::contentName.

The Ingest Steering feature requires that VVI with central management and Vault Groups be enabled. Figure 2-10 shows a high-level view of Ingest Steering for a single, centralized BMS and multiple VHOs. Each VHO has a local Vault Group through which all local live content is ingested. Each Stream Group streams local live content as well as national live and VOD content. The BMS sends messages to the master Vault Group (Vault Group 1), and depending on the product ID and the ingest steering configured, the content is ingested by either the local Vault Group or the national Vault Group.

Content objects on the national Vault Groups are mirrored among each other, while the content on the local Vault Groups are copied to separate hard drives on each Vault.
Network Connections

The network connections for a VDS-TV with Vaults and Streamers, a VDS-TV with ISVs, and a TV VVI with Caching Nodes all have different network connections. Table 2-2 lists the different required interfaces for each VDS server. The interfaces are described in the following sections. Figure 2-11 illustrates a VDS-TV with Vaults and Streamers. Figure 2-12 illustrates a VDS-TV with ISVs. Figure 2-13 illustrates a TV VVI with Caching Nodes.

Table 2-2 VDS Required 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.

Note: Table 2-2 lists the mandatory interfaces for each VDS 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 4-80.
Figure 2-11 shows the different logical networks of a VDS 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 set-tops. The cache network consists of Vaults and Streamers.

Figure 2-12 shows the different logical networks of a VDS 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 set-tops.
Figure 2-12 ISV Network Connections
Figure 2-13 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 set-tops.

Figure 2-13  VVI Network Connections

Ingest Interface

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

When using Layer 2 packet forwarding, to segregate all ingest traffic through the switching fabric, we recommend the use of a port-based VLAN.
Chapter 2      Network Design

Network Connections

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.

Starting from Cisco VDS-TV Release 3.7, network interface bonding is supported on all types of VDS servers including VDS Controller. For additional information on configuring network interface bond, see the Configuring the Interfaces, page 4-80.

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 VDS servers

Note: All Cisco VDS 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 set-tops 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 Cisco Videoscape Distribution Suite-TV (VDS-TV) servers.

- Initially Configuring the Devices, page 3-1
- Browser Recommendation, page 3-1
- Logging In to the TV CDSM, page 3-2
- Initializing the VDS and Activating the Optional Features, page 3-3
- Navigating the CDSM, page 3-4
- Configuration Workflow, page 3-6

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

Initially Configuring the Devices

You must initially configure the Content Delivery Engines (CDEs) before they can participate in the VDS network. The CDE that runs the TV Content Delivery System Manager (CDSM) must be initialized first so that the CDEs running the Streamers, 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 205/220/250/420 Hardware Installation Guide, the Cisco Content Delivery Engine 110 Hardware Installation Guide Cisco UCS C220 M4 Server Installation and Service Guide, or the Cisco VDS-TV Installation, Upgrade, and Maintenance Guide, Release 4.4.

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 VDS.

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

Browser Recommendation

Cisco recommends Mozilla Firefox 36 and above as the primary browser to access the CDSM GUI. Internet Explorer 11.0 can also be used as a secondary browser to access the GUI.
Logging In to the TV CDSM

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

Step 1

Using your web browser, enter the IP address or hostname of your CDSM.

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

Note Consult your as-built documentation for the IP address of the CDSM. If you have redundant CDSMs, use the virtual IP address, not the IP addresses of the physical Ethernet interfaces.

The CDSM GUI now supports Hypertext Transport Protocol Secure (HTTPS) as a secure way to access the browser-based interface. The vdsconfig script offers the following choices to access the CDSM GUI:

- HTTP
- HTTPS
- HTTP and HTTPS

Note VVIM/CDSM uses a self-signed SSL certificate for secure access to GUI via HTTPS. As the domain name/IP address of VVIM/CDSM will vary for each installation, web browsers presents a security warning when launching the GUI. This is an expected behavior and you could either choose to ignore the warning and proceed to launching the GUI or add the certificate as a trusted certificate in the web browser.

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

Figure 3-1 System Login Page

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.
We strongly recommend that you change the built-in user password as soon as possible. See the “Editing User Settings” section on page 7-5 for more information.

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.

Tip

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

Initializing the VDS and Activating the Optional Features

Initial configuration of your VDS 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 by entering an activation key.

To initialize your VDS 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 F-3.
Step 5 To activate the Media Scheduler, scroll down to the Media Scheduler section, and click the **ON** radio button next to the **Media Scheduler** field.

- 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.

- 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 6 To activate the Ingest Manager, scroll down to the Ingest Manager section, and click the **ON** radio button next to the **Ingest Manager** field.

- In the **Activation Key** field, enter the software access key from your Right to Use Notification for the Content Delivery Application Stream Resiliency, VOD ER for Gen 1 & Gen 2 Streamers (CDATSTR2-EN) product or for the Content Delivery Application Stream Resiliency, VOD ER for Gen 3 Streamers (CDATSTR3-EN) product.

Step 7 To activate the VOD Error Repair, scroll down to the VOD Error Repair section, and click the **Enabled** radio button next to the VOD Error Repair field.

- In the **Activation Key** field, enter the software access key from your Right to Use Notification for the Content Delivery Application VOD Error Repair (CDAVER) product.

Step 8 Click **Submit**.

Step 9 Log out of the CDSM.

Navigating the CDSM

**Note**

For page navigation, Cisco strongly recommends that the user does not use the browser back or refresh buttons and instead use the CDSM GUI navigation elements.

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

Figure 3-3  CDSM User Interface

The tabs are accessible from any page in the CDSM.

The tab options are used to choose 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 you are 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
Configuration Workflow

After you have completed the initial installation and configuration of the CDEs for the VDS and you have verified connectivity to the CDSM, you are ready to configure the VDS for content delivery. The configuration workflow consists of one or more of the following:

- **VDS Configuration Workflow, page 3-6**
- **VVI Configuration Workflow, page 3-7**
- **Vault Virtualization Configuration Workflow, page 3-9**
- **TV MediaX Configuration Workflow, page 3-10**
- **TV Playout Configuration Workflow, page 3-11**

**VDS Configuration Workflow**

Table 3-1 lists the basic tasks, in the recommended order, for configuring the VDS 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 administrator password</td>
<td>Change the administrator password for the CDSM.</td>
<td>Editing User Settings, page 7-5</td>
</tr>
<tr>
<td>Interface setup</td>
<td>Configure the different interfaces on the VDS servers.</td>
<td>Configuring the Interfaces, page 4-80</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 4-85</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 4-93</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 4-39</td>
</tr>
<tr>
<td>Control and setup IPs</td>
<td>Configure the Control server and Setup server IP address for the Stream Groups.</td>
<td>Configuring the Control and Setup IPs, page 4-64</td>
</tr>
<tr>
<td>QAM gateways(^1)</td>
<td>Configure the QAM Gateways for the VDS.</td>
<td>Configuring QAM Gateways, page 4-5</td>
</tr>
</tbody>
</table>

(\(^1\)) A QAM gateway is used to connect to a QAM device.
The other configuration settings, barker streams, parent/child service groups, DNS settings, and so on, can be configured in any order.

VVI Configuration Workflow

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

Central Management Configuration 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>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headend setup</td>
<td>Configure service groups for Gigabit Ethernet streaming, ASI streaming, and barker streams.</td>
<td>Configuring the Headend Setup, page 4-7</td>
</tr>
<tr>
<td>Ingest tuning</td>
<td>Configure the trick-mode speeds for ingested content.</td>
<td>Configuring Ingest Tuning, page 4-15</td>
</tr>
</tbody>
</table>

1. If the Stream Destination feature is set to IPTV, the QAM Gateway page and Headend Setup page are replaced with the Stream Destination page. A setting of Mixed for Stream Destination displays all three pages. For more information, see the “Configuring Stream Destinations” section on page 4-9.

The other configuration settings, barker streams, parent/child service groups, DNS settings, and so on, can be configured in any order.

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</td>
<td>Change the administrator password for the CDSM.</td>
<td>Editing User Settings, page 7-5</td>
</tr>
<tr>
<td>Interface setup</td>
<td>Configure the different interfaces on the VDS servers.</td>
<td>Configuring the Interfaces, page 4-80</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 4-85</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 4-93</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 Cache Groups, page 4-55</td>
</tr>
<tr>
<td>Control and Setup IP addresses</td>
<td>Configure the Control server and Setup server IP address for the Stream Groups.</td>
<td>Configuring the Control and Setup IPs, page 4-64</td>
</tr>
<tr>
<td>Cache Groups setup</td>
<td>A Cache Group consists of one or more Caching Nodes.</td>
<td>Configuring Cache Groups, page 4-55</td>
</tr>
<tr>
<td>Stream to Cache map</td>
<td>Cache Groups are mapped to Stream Groups and given a preference.</td>
<td>Mapping Stream Groups to Cache-Fill Sources, page 4-59</td>
</tr>
</tbody>
</table>
Split-Domain Management Configuration 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 Chapter 2, “Network Design,” and the “CDSM or VVIM Setup” section on page F-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 7-5</td>
</tr>
<tr>
<td>Interface setup</td>
<td>VVIM and Stream Manager</td>
<td>Configure the different interfaces on the VDS servers.</td>
<td>Configuring the Interfaces, page 4-80</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 QoS.</td>
<td>Configuring the Servers, page 4-85</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 4-93</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 4-39</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 4-64</td>
</tr>
<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 4-55</td>
</tr>
<tr>
<td>Stream to cache mapping</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 4-59</td>
</tr>
<tr>
<td>QAM gateways (^1)</td>
<td>Stream Manager</td>
<td>Configure the QAM Gateways for the VDS.</td>
<td>Configuring QAM Gateways, page 4-5</td>
</tr>
</tbody>
</table>

1. If the Stream Destination feature is set to IPTV, the QAM Gateway page and Headend Setup page are replaced with the Stream Destination page. A setting of Mixed for Stream Destination displays all three pages. For more information, see the “Configuring Stream Destinations” section on page 4-9.
Chapter 3      Getting Started

Configuration Workflow

Note

Before configuring the VHO ISA Settings on the Stream Manager, resubmit the Shared ISA settings on the VVIM. If the CDSM or VVIM GUI pages are not updated with respect to the ISA settings, resubmit the Shared ISA Settings page on the VVIM and the VHO ISA Setup page on the Stream Manager.

The other configuration settings, Vault Groups, Master Vault Group, Vault Redundancy Map, barker streams, parent/child service groups, DNS settings, and so on, can be configured in any order.

Vault Virtualization Configuration Workflow

The Vault Virtualization can be configured as follows:

- ISA Regionalization (with local Vaults in headend)
- Virtual Content Store (without local Vaults in headend)
- Shared Content Store (pre-Release 2.5.2 version of Virtual Content Store)

This section consists of the configuration workflow for the following:

- ISA Regionalization Configuration Workflow, page 3-9
- Virtual Content Store Configuration Workflow, page 3-10

ISA Regionalization Configuration Workflow

In addition to the configuration workflow for split-domain management, Table 3-4 lists the basic tasks, in the recommended order, for configuring ISA Regionalization with references to the associated sections in each chapter. For more information, see the “ISA Regionalization” section on page 2-16 and the “CDSM or VVIM Setup” section on page F-3.

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>Headend setup¹</td>
<td>Stream Manager</td>
<td>Configure service groups for Gigabit Ethernet streaming, ASI streaming, and barker streams.</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, page 4-15</td>
</tr>
</tbody>
</table>

¹ If the Stream Destination feature is set to IPTV, the QAM Gateway page and Headend Setup page are replaced with the Stream Destination page. A setting of Mixed for Stream Destination displays all three pages. For more information, see the “Configuring Stream Destinations” section on page 4-9.

Table 3-4  ISA Regionalization 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>CDSM Setup</td>
<td>Stream Manager (CDSM)</td>
<td>Configure each Stream Manager for ISA Regionalization.</td>
<td>Configuring ISA Regionalization, page F-11</td>
</tr>
<tr>
<td>VVIM Setup</td>
<td>VVIM</td>
<td>Configure the VVIM for ISA Regionalization</td>
<td>Configuring ISA Regionalization, page F-11</td>
</tr>
<tr>
<td>Vault groups</td>
<td>Stream Manager</td>
<td>Assign local Vault Groups, configure Vault redundancy, and assign the master Vault.</td>
<td>Configuring Vault Groups, page 4-49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mapping Vault Groups for Redundancy, page 4-61</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuring the Master Vault Group, page 4-63</td>
</tr>
</tbody>
</table>
Trick-mode settings on the VVIM and Stream Managers must be the same. To configure trick-mode settings in the CDSM GUI, choose \textit{Configure > System Level > Ingest Tuning}.

### Virtual Content Store Configuration Workflow

In addition to the configuration workflow for split-domain management, Table 3-5 lists the basic tasks, in the recommended order, for configuring Virtual Content Store with references to the associated sections in each chapter. For more information, see the “Virtual Content Store” section on page 2-20 and the “CDSM or VVIM Setup” section on page F-3.

#### Table 3-5 Virtual Content Store 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>CDSM Setup</td>
<td>Stream Manager (CDSM)</td>
<td>Configure each Stream Manager for Virtual Content Store.</td>
<td>Configuring Virtual Content Store, page F-11</td>
</tr>
<tr>
<td>VVIM Setup</td>
<td>VVIM</td>
<td>Configure the VVIM for Virtual Content Store.</td>
<td>Configuring Virtual Content Store, page F-11</td>
</tr>
</tbody>
</table>

When Content Storage is set to \textbf{Distributed} and the VVI is set to centralized management (VVI & Stream Manager), the following configuration pages are affected:

- Configure > System Level > Distributed ISA Setup page
- Configure > Array Level > VHO ISA Settings page

Both the above pages require configuration.

### TV MediaX Configuration Workflow

Table 3-6 lists the basic tasks for configuring the TV MediaX Suite CDA with references to the associated sections in each chapter.

#### Table 3-6 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 Call Signs, page 4-25</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, page 4-27</td>
</tr>
</tbody>
</table>

TV MediaX is an optional feature and requires a software activation key to enable it. For more information, see the “Initializing the VDS and Activating the Optional Features” section on page 3-3.
Table 3-6  TV MediaX Configuration Workflow (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload an EPG file. During the upload process, the EPG file is</td>
<td>Uploading an EPG File,</td>
</tr>
<tr>
<td>parsed into database records that in turn populates the Media</td>
<td>page 7-22</td>
</tr>
<tr>
<td>Scheduler.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></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</td>
<td></td>
</tr>
<tr>
<td>from the Input Channels page, and the ADI metadata XML file is</td>
<td></td>
</tr>
<tr>
<td>created.</td>
<td></td>
</tr>
<tr>
<td>2. The database records are marked according to the Media</td>
<td></td>
</tr>
<tr>
<td>Scheduler settings (scheduled, unscheduled, marked for</td>
<td></td>
</tr>
<tr>
<td>scheduling, and so on).</td>
<td></td>
</tr>
<tr>
<td>3. The ADI metadata is published to the back office.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>TV Playout Configuration Workflow</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-7 lists the basic tasks for configuring the TV Playout CDA with references to the associated sections in each chapter.

TV Playout is an optional feature and is only displayed if the TV Playout feature is enabled. For more information, see the “Playout Scheduler” section on page F-15.

Table 3-7  TV Playout Configuration Workflow

<table>
<thead>
<tr>
<th>Task</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the streaming mode (active-active or active-standby) for</td>
<td>“Configuring the TV Playout Application” section on</td>
</tr>
<tr>
<td>the Barker Stream/Playlist and Playout Scheduler.</td>
<td>page 7-19</td>
</tr>
<tr>
<td>Map each channel to a multicast group IP address and port, and</td>
<td>“Configuring Input Channels” section on page 4-27</td>
</tr>
<tr>
<td>specify the settings for every program in the channel.</td>
<td></td>
</tr>
<tr>
<td>Upload an TV Playout file. During the upload process, the file</td>
<td>Importing a TV Playout Schedule, page 7-21</td>
</tr>
<tr>
<td>is parsed into database records that in turn populates the TV</td>
<td></td>
</tr>
<tr>
<td>Playout Scheduler.</td>
<td></td>
</tr>
</tbody>
</table>

The following CDSM pages are part of TV Playout CDA:

- Configure > System Level > Output Channels
- Configure > Array Level > Manual Ingest
- Configure > Array Level > Barker Stream/Playlist
- Configure > Array Level > Playout Scheduler
- Configure > Array Level > Playout Exporter
- Configure > Array Level > EPG Exporter
• Monitor > Array Level > Barker Monitor
• Monitor > Array Level > Playout Monitor
• Reports > System Level > Playout/Barker Reports (Only report available for TV Playout)
• Maintain > Users > User Default Settings
• Maintain > Services > Content Manager
• Maintain > Software > Application Configuration
• Maintain > Software > Playout Importer
• Maintain > Software > Playout Upgrade Status
Configuring the VDS

This chapter provides information on configuring the Cisco Videoscape Distribution Suite-TV (VDS-TV) servers.

- System Level Configuration, page 4-1
- Array Level Configuration, page 4-35
- Server Level Configuration, page 4-80
- Command Line Non-GUI Configuration, page 4-114

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 F-10.

System Level Configuration

The System Level tab has the following configuration options:

- Configuring System Level DNS Services, page 4-2
- Configuring System Level NTP Services, page 4-3
- Configuring the Hosts Service, page 4-3
- Configuring the Array Name, page 4-4
- Configuring QAM Gateways, page 4-5
- Configuring the Headend Setup, page 4-7
- Configuring Stream Destinations, page 4-9
- Configuring the Ingest Manager, page 4-11
- Configuring the Authentication Manager, page 4-14
- Configuring Ingest Tuning, page 4-15
- Configuring MPEG Tuning, page 4-17
- Configuring Shared Recorder Settings, page 4-20
- Configuring IP Nicknames, page 4-22
Configuring System Level 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 Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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.

**Step 3** Click Submit.

To clear the fields and start over, click Reset.

<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 sub domain consistent with what OpenStream is using, for example, bms.n2bb.com. Accordingly, unqualified host names 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>
Configuring System Level NTP Services

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

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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 VDS server or configuring NTP on a CDSM or VVIM, see “Other NTP Configurations” section on page 4-101.

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 > System Level > Host Service. The host names currently configured are listed at the bottom of the page.

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.
To configure the host service settings, do the following:

**Step 1** Choose **Configure > System Level > 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**.

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 1-15.

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

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

**Note** If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure an array name setting, do the following:

---

**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 host names 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>
Chapter 4 Configuring the VDS

System Level Configuration

Step 1 Choose Configure > System Level > 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 F-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 VDS 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 that 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 4-93.
To view the current configuration for a QAM gateway, choose **Configure > System Level > 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 > System Level > 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 Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating QAM Gateway Bulk Configuration Files” section on page B-12.

**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 Subnet</td>
<td>To enter QAM subnet, check the QAM Subnet check box.</td>
</tr>
<tr>
<td>QAM IP/QAM Subnet IP</td>
<td>IP address of the QAM gateway or Subnet IP address of the QAM gateway if QAM Subnet check box is selected.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet Mask 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 4-93.</td>
</tr>
</tbody>
</table>

Stream Group Preferences

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Group Preferences</td>
<td>Choose the preference for each Stream Group. The preferences are:</td>
</tr>
<tr>
<td></td>
<td>• High—First preference of Streamer or Stream Group to stream to this QAM.</td>
</tr>
<tr>
<td></td>
<td>• 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 4-39.</td>
</tr>
</tbody>
</table>

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 F-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 F-20.
You must first configure the Stream Groups before you can configure the headend setup for a specific service group. See the “Configuring Stream Groups” section on page 4-39.

To configure the headend setup, do the following:

**Step 1** Choose Configure > System Level > 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 Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating Headend Setup Bulk Configuration Files” section on page B-13.

**Figure 4-2  Headend Setup Page**

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 4-39.

Step 5 Click Submit.

To delete a service group, choose it from the Select Service Group drop-down list and click Delete.
Chapter 4  Configuring the VDS

System Level Configuration

## 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 F-4.

To configure the Stream Destination, do the following:

### Step 1

Choose **Configure > System Level > 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 Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Configuration file for QAM Gateways, see the “Creating Stream Destination Bulk Configuration Files” section on page B-14.

### 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 set-tops, be sure the IP subnet reflects the public, routeable IP address for the NAT device, not the internal private IP address of the set-top.

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 VDS 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 4-39.

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**.
Chapter 4  Configuring the VDS

System Level Configuration

## Configuring the Ingest Manager

The Ingest Manager takes care of provisioned content objects by collecting the metadata and sending messages to the appropriate subsystem to ingest the content. When the content expiration period has ended, the Ingest Manager deletes the content after the additional license window has expired. The additional license window is the license window end time plus the Additional Package Window.

**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. For information on enabling the Ingest Manager feature, see the “Ingest Manager” section on page F-16.

**Note**

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure the Ingest Manager, do the following:

**Step 1**  Choose Configure > System Level > Ingest Manager. The Ingest Manager page is displayed.

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

### Table 4-4  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>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><strong>Use Asset ID</strong></td>
<td>Choose Yes to use the Asset ID for the content name, otherwise choose No. The recommended setting is No. If set to No, the Ingest Manager uses the *.mpg as the content name when used in combination with the Media Scheduler. For Media Scheduler, Use Asset ID must be No; otherwise, the recording does not succeed.</td>
</tr>
<tr>
<td>Manage CORBA Services</td>
<td>ISA only field. Choose Yes to have the VDS manage the CORBA services, otherwise choose No.</td>
</tr>
</tbody>
</table>
Chapter 4  Configuring the VDS

System Level Configuration

Table 4-4  Ingest Manager Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Notify Service</td>
<td>ISA only field. Choose <strong>Yes</strong> to have the VDS require the use of the Notify Service, otherwise choose <strong>No</strong>.</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 is typically the FTP server on CDSM itself. The example for this FTP server to publish packages by Ingest Manager is: ftp://aimmgr:aim123@192.168.16.25:21/</td>
</tr>
<tr>
<td>Meta Publish URL #2</td>
<td>URL of the backup server where the metadata is published.</td>
</tr>
</tbody>
</table>

**Ingest Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 back office. 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 back office. 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>
<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 back office. 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>
</tbody>
</table>
Table 4-4  Ingest Manager Fields (continued)

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

**Back Office 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 back office. 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. If the <strong>Retry Interval</strong> is set to zero, the Ingest Manager retries once every 6000 seconds (100 minutes).</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>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 4-27 for more information.</td>
</tr>
<tr>
<td>Backoffice Timeout</td>
<td>Amount of time (in seconds) to wait for the back office 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 back office support, otherwise choose <strong>Disable</strong> to disable back office support.</td>
</tr>
<tr>
<td>Backoffice URL</td>
<td>Location of the TotalManage back office.</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>

**Encryption Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Choose <strong>Verimatrix</strong>, or <strong>Widevine</strong> to use encryption. Choose <strong>Disable</strong> 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

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. For information on enabling the Authentication Manager feature, see the “NoteProvider::contentOne.mpg is an example of a Content ID. CNTSWP is a unique identifier that distinguishes the content swap URL” section on page F-19.

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

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure the Authentication Manager, do the following:

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

**Note** Depending on the Authentication Manager protocol selected (either Cisco or EventIS), the Authentication Manager displays different fields.

---

**Figure 4-4** Authentication Manager Page—Cisco

<table>
<thead>
<tr>
<th>Authentication Manager IP: 10.74.17.45</th>
<th>Port: 7104</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Server SOAP Interface:</td>
<td></td>
</tr>
<tr>
<td>HTTP: 10.74.17.50:30090</td>
<td></td>
</tr>
<tr>
<td>Authentication Timeouts: 10 seconds</td>
<td></td>
</tr>
<tr>
<td>Notification Retry Interval: 0 seconds</td>
<td></td>
</tr>
<tr>
<td>Debug Level: HIGH</td>
<td></td>
</tr>
</tbody>
</table>

Note: Depending on the Authentication Manager protocol selected (either Cisco or EventIS), the Authentication Manager displays different fields.
Enter the Authentication Manager settings as appropriate. See Table 4-5 for descriptions of the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Manager IP</td>
<td>Authentication Manager resides on the master Streamer. Typically, the Authentication Manager IP address is the same as that of the master Streamer.</td>
<td>EventIS Cisco</td>
</tr>
<tr>
<td>Authentication Manager Port</td>
<td>Authentication Manager port number default is 7794. 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>
<td>EventIS Cisco</td>
</tr>
<tr>
<td>EventIS Hostname</td>
<td>Hostname or IP address of the EventIS server.</td>
<td>EventIS Cisco</td>
</tr>
<tr>
<td>EventIS Port</td>
<td>Port number on the EventIS server used to receive authentication requests.</td>
<td>EventIS Cisco</td>
</tr>
<tr>
<td>Authentication Server SOAP Interface</td>
<td>IP address, port, and logical partition on the authentication server in the following format: http://&lt;ip_address&gt;:&lt;port&gt;/&lt;path&gt;, which is used to receive authentication requests (such as IsAuthorizedRequest, SETUP and TEARDOWN SessionNotification).</td>
<td>Cisco</td>
</tr>
<tr>
<td>Authentication Timeout</td>
<td>Time to wait, in seconds, for the authentication server to respond. The range is from 1 to 10.</td>
<td>EventIS Cisco</td>
</tr>
<tr>
<td>Notification Retry Interval</td>
<td>Time to wait, in seconds, before attempting to connect to the authentication server again. The range is from 1 to 60.</td>
<td>Cisco</td>
</tr>
</tbody>
</table>

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

Click Submit.

Configuring Ingest Tuning

The Ingest Tuning page allows you to set the speeds of the trick-mode files created for each ingested content and configure the ingest error detection settings in the Fail Ingest Settings section.

For NGOD deployments, if Dynamic Trickmodes is enabled on the MPEG Tuning page, then the Ingest Tuning page displays on the Stream Manager and is used to set the trick-mode speeds that the Streamer uses to generate trick-mode files.

The Fail Ingest Settings section is only displayed if the Fail Ingest Tuning feature is enabled. The Fail Ingest Tuning feature is enabled by default. For more information, see the “Fail Ingest Tuning” section on page F-6.

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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.
To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To view the current ingest tuning settings, choose **Configure > System Level > Ingest Tuning**. To configure the ingest tuning, do the following:

**Step 1**  
Choose **Configure > System Level > Ingest Tuning**. The Ingest Tuning page is displayed.

**Step 2**  
Enter the ingest tuning settings as appropriate. See Table 4-6 for descriptions of the fields.

<table>
<thead>
<tr>
<th>Table 4-6</th>
<th>Ingest Tuning Fields</th>
</tr>
</thead>
</table>

<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–Speed 10</td>
<td>You can set ten different trick-mode speeds for each ingested content. A trick-mode file, either fast-forward or rewind (–X), is created for each selected speed. Choose the trick-mode speed from the drop-down list and click <strong>Submit</strong>. To reset the values and start over, click <strong>Reset</strong>.</td>
</tr>
<tr>
<td><strong>Fail Ingest Settings</strong></td>
<td></td>
</tr>
<tr>
<td>PSI Errors</td>
<td>When program specific information (PSI) errors setting is enabled and the VDS software cannot find the PAT and PMT, the ingest fails. The default for <strong>PSI Errors</strong> is Disabled.</td>
</tr>
<tr>
<td>Bit Rate Errors</td>
<td>If <strong>Bit Rate Errors</strong> is enabled, and the VDS cannot determine the bit rate, cannot find the Program Clock Reference (PCR), or determine the PCR PID; the ingest fails. If the VDS software cannot determine the bit rate, it tries the bit rate of 3.75 Mbps, which may be correct and allows the ingest to continue. This parameter is not applicable when using the nABLE back office. The default setting is Disabled.</td>
</tr>
</tbody>
</table>
| Error Count Method     | If **Error Count Method** is enabled, the errors are counted every \( n \) minutes, where \( n \) is specified in the **Number of Minutes** field. The error count applies to the following thresholds:  
  - Discontinuity Rate  
  - Number of Picture Gaps  
  - Picture Gap Duration  
  - Continuity Counter Errors  
  - Number of Sync Loss Errors  
  - Sync Loss Duration.  
  If a threshold is reached, the ingest fails. The default setting is Disabled. |
| Number of Minutes      | **Number of Minutes** applies to the **Error Count Method**. The default setting is 30. If a threshold is reached within the specified minutes, the ingest fails. |
Configuring MPEG Tuning

The MPEG Tuning page allows you to configure the settings for various aspects of MPEG tuning.

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

To configure the settings, do the following:

Step 1 Choose Configure > System Level > MPEG Tuning. The MPEG Tuning page is displayed.

Note

Table 4-6 Ingest Tuning Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discontinuity Rate</td>
<td><strong>Discontinuity Rate</strong> threshold sets the number of discontinuities that constitutes a failure. Discontinuities may appear if content is spliced together before ingest, also many discontinuities appear near the beginning of a sample; therefore, the default setting is <strong>Ignore</strong>.</td>
</tr>
<tr>
<td>Number of Picture Gaps</td>
<td>Picture gap is when two pictures appear more than one second apart in a transport stream. The <strong>Number of Picture Gaps</strong> threshold sets the number of picture gaps that constitutes a failure. The default is 3.</td>
</tr>
<tr>
<td>Picture Gap Duration</td>
<td><strong>Picture Gap Duration</strong> allows you to specify the maximum time that defines a picture gap. A picture gap occurs whenever two pictures are more than one second apart. Even if they are 15 minutes apart, it is still only counted as one picture gap. If a picture gap exceeds the <strong>Picture Gap Duration</strong>, the ingest fails. The default is 5 seconds.</td>
</tr>
<tr>
<td>Continuity Counter Errors</td>
<td>Sets the <strong>Continuity Counter Errors</strong> threshold. The default is Ignore. Each transport-stream packet header has a 4-bit continuity counter, which increments for each transport-stream packet with the same PID. The continuity counter wraps around to zero when it reaches its maximum value of F (hexadecimal). It is used to determine if any packets are lost, repeated, or out of sequence. The MPEG-2 specification allows the continuity counter to be discontinuous in order to accommodate local insertion of data packets and splicing. As a consequence, the continuity counter can be discontinuous even in an error-free transmission.</td>
</tr>
</tbody>
</table>

Step 3 Click Submit. To clear the fields and start over, click Reset.
Step 2  Enter the settings as appropriate. See Table 4-7 for descriptions of the fields.

### Table 4-7  MPEG Tuning Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ingest MPEG Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Program ID Standardization    | 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 is 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. |
| PSI                           | 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. |
| Sequence End Remove           | 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. |
| Rate Standardize              | 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. |
| MPEG File Index Format        | Specifies the index file format for the content.                                                                                                                                                           |
| Playlist Trick-Mode Restrictions | **Rewind Skip** is enabled, if a rewind trick-mode command is issued and a rewind-restricted segment is encountered, it is skipped and rewinding continues on the next segment.  
When Rewind Skip is disabled (default setting), if a rewind trick-mode command is issued and a rewind-restricted segment is encountered from an unrestricted segment, the rewinding stops and the unrestricted segment is played at normal play speed.  
As an example, Segment 2 is unrestricted and Segment 1 has the rewind trick-mode speed restricted. If a rewind command is issued during the playing of Segment 2, rewinding of Segment 2 occurs until the end of Segment 1 is encountered where the rewind trick-mode is restricted. Rewinding stops and the unrestricted Segment 2 begins to play at normal speed. |
Forward Jump

If forward-trick restrictions are enabled AND forward-jump restrictions are enabled, forward jumps will be disallowed if the jump begins on an forward-trick-restricted playlist segment.

Starting from Cisco VDS-TV Release 3.12, jump restriction can be enabled/disabled on a per session basis rather than enabling/disabling globally for all streams. If a parameter for jump restriction is received in the Require header of the SETUP request, then the jump restriction is applied for that session regardless of the configuration of Forward Jump.

Skipping Stone Mode

If forward-jump restrictions are enabled, the Skipping-Stone Mode parameter controls the behavior of forward-jump restrictions when the jump begins in an unrestricted playlist segment, but there is one or more forward-trick-restricted playlist segments between the beginning and end of the jump.

When Skipping-Stone Mode is enabled, the jump will skip to the beginning of an intervening forward-trick-restricted playlist segment, switch to 1x playback for the duration of the segment, and jump to the jump's original end or the beginning of the next forward-trick-restricted segment, whichever comes first.

When Skipping Stone Mode is disabled, a jump will switch to 1x playback at the beginning of the first intervening forward-restricted segment and will remain at 1x until a new play command is received.

Free Pass Jump

If Free Pass Jump is enabled and a jump over a trick restricted segments is attempted the jump is allowed only if the command is issued within the free pass duration.

Free Pass Fast Forward

If Free Pass Fast Forward is enabled and FF of a trick restricted segments is attempted the FF is allowed only if the command is issued within the free pass duration.

Delayed Jump Ahead

Delayed Jump Ahead requires the Free Pass Jump to be enabled. Whenever an issued jump has been denied because it attempted to jump over a FF trick requested segment the original requested NPT is saved. If a jump is issued while playing in a FF trick restricted segment the command is canceled and this configuration has no effect. Once an ad-break is watched the play will continue from the NPT that is saved. However if the user issues any valid play command before the ad-break could finish that play will finally prevail and play doesn't resume from the saved NPT.

Free Pass Time

The amount of time during which the user will be allowed to jump over or FF a trick restricted segment. After which the free pass will expire and the restrictions will be in force.

The default value for Free Pass Time is 120 seconds.

Pre-VOD Ad. Once

When Pre-VOD Ad Once is enabled, the pre-VOD AD is played only once.

When Pre-VOD Ad Once is disabled (default setting), the pre-VOD AD is played repeatedly.

Forward Skip

When Forward Skip is disabled, if a fast forward trick-mode command is issued and a fast forward-restricted segment is encountered, it is skipped and fast forwarding continues on the next segment.

When Forward Skip is enabled (default setting), if a fast forward trick-mode command is issued and a fast forward-restricted segment is encountered from an unrestricted segment, the fast forwarding stops and the fast-forward restricted segment is played at normal play speed.

Library Timeout

A network partition could cause the Setup server to wait forever for the remote Stream Groups to respond to the application for setup requests. The Library Timeout sets the time interval (in microseconds) that the SetStreamInfo API should wait before considering the remote Stream Group unavailable.

The range is from 1000 to 5000. The default is 2000 (2 seconds).
Configuring Shared Recorder Settings

The Shared Recorder Settings page is used to configure the Recorders in an nDVR system. For more information, see the “nDVR Support for NGOD Deployments” section on page 2-13.

The settings on the Shared Recorder Settings page are applied to all Recorders in the VDS. The Shared Recorder Settings page is used to configure large numbers of Recorders quickly and with less errors than manual configuration. Individual settings made on the Recorder Setup page override any Shared Recorder Settings.

Any changes to the Shared Recorder Settings page are propagated to all Recorders, except the settings of Recorders that have individual settings. Any Recorder settings that were modified with the Recorder Setup page (that is, different settings than the Shared Recorder Settings page) are not overwritten by the Shared Recorder Settings page.

All configuration changes to the Recorder require the Recorder be restarted. To restart the Recorder, log in to Linux operating system of the Recorder, shut down the database (the `db_shutdown` command) and enter the `reboot` command.
If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure the shared Recorder settings, do the following:

**Step 1**  
Login to the CDSM GUI, and choose **Configure > System Level > Shared Recorder Settings**. The Shared Recorder Settings page is displayed.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Recorder Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Recorder Manager</td>
<td>The IP address of the Recorder Manager. The Recorder Manager port is port number 80.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>The IP address of the NTP server.</td>
</tr>
<tr>
<td>Heartbeat Interval</td>
<td>The amount of time (in seconds) to wait between sending heartbeat messages to the Recorder Manager. The range is from 2 to 30. The default is 5.</td>
</tr>
<tr>
<td>Recorder Location</td>
<td>Name of the location of the Recorder. The name can be from 1 to 128 characters in length.</td>
</tr>
<tr>
<td>Recording Modify</td>
<td>The time window (in seconds) before a recording starts in which an operator cannot modify recording parameters. The end time can be modified even after the configured time window has passed. If the change to the end time specifies a time that is before the current time, the Recorder stops the recording. The range is from 1 to 60. The default is 5.</td>
</tr>
<tr>
<td>SCTE-35 Ad Markers</td>
<td>Choose either to <strong>Retain</strong> or <strong>Discard</strong> the SCTE-35 Ad markers. If SCTE-35 markers are discarded, both the PID in the PMT and the data are removed. If the SCTE-35 markers are preserved, the Recorder places the SCTE-35 Ad markers in the index file.</td>
</tr>
<tr>
<td>Recorder Port</td>
<td>The port number on the Recorder used for management communications with the Recorder Manager. The range is from 50005 to 65535. The default is 50005.</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>Read-only field. The communication protocol version of the Recorder Manager and the Recorder interface. The default is 1.</td>
</tr>
<tr>
<td>Threadpool Size</td>
<td>Read-only field. The number of message processing threads of the Recorder. The default is 16.</td>
</tr>
<tr>
<td>Status Report Interval</td>
<td>Read-only field. How often (in seconds) the Recorder reports status information to the Recorder Manager. The default is 60 seconds.</td>
</tr>
</tbody>
</table>
Table 4-8  Shared Recorder Settings Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Request Timeout</td>
<td>Read-only field. The time that the Recorder application waits for an HTTP request after it is signaled. The default is 5 seconds.</td>
</tr>
<tr>
<td>HTTP Response Timeout</td>
<td>Read-only field. The time that the Recorder application waits for an HTTP response. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

**Manager Notify Thresholds**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Bandwidth</td>
<td>Threshold, as a percentage, for recording bandwidth. If this threshold is exceeded (that is, if the bandwidth used for ingesting recordings exceeds the configured percentage), the Recorder sends a notification to the Recorder Manager. The range is from 1 to 100. The default is 1.</td>
</tr>
<tr>
<td>Delivery Bandwidth</td>
<td>Threshold, as a percentage, for delivery bandwidth. If threshold is exceeded (that is, if the bandwidth used for delivering recordings exceeds the configured percentage), the Recorder sends a notification to the Recorder Manager. The range is from 1 to 100. The default is 1.</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>Threshold, as a percentage, for storage capacity. If threshold is exceeded (that is, if the disk storage used on the Recorder exceeds the configured percentage), the Recorder sends a notification to the Recorder Manager. The range is from 1 to 100. The default is 1.</td>
</tr>
</tbody>
</table>

**Location Virtual IP**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Virtual IP</td>
<td>IP address the Recorders use 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 in the “Product Overview” chapter of the Cisco VDS-TV RTSP Software Configuration Guide, Release 4.4.</td>
</tr>
<tr>
<td>Location Subnet Mask</td>
<td>Subnet mask for the Location Virtual IP.</td>
</tr>
</tbody>
</table>

**IP Packet Priority**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP DSCP</td>
<td>DSCP value for the transmitted HTTP IP packet. The range is from 0 to 63 and the default value is 36.</td>
</tr>
</tbody>
</table>

**Step 3**  
Click **Submit** to save the settings.

---

**Configuring IP Nicknames**

The IP nicknames are used as an alternative for the IP address in the CDSM drop-down lists.

**Note**  
If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.
For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure an IP nickname for a VDS server or QAM gateway, do the following:

Step 1
Choose **Configure > System Level > IP Nickname**. The IP Nicknames page is displayed(Figure 4-5).

![Figure 4-5 IP Nicknames Page](image)

**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

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

There are two ways to import an EPG file, one is to manually upload the file by using the EPG Upload page (Uploading an EPG File, page 7-22), the other is to automatically import the EPG file using the Media Importer page.

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 of the EPG files from an FTP server.

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure the Media Importer, do the following:

**Step 1** Choose Configure > System Level > Media Importer. The Media Importer page is displayed.

**Step 2** Enter the settings as appropriate. See Table 4-9 for descriptions of the fields.

<table>
<thead>
<tr>
<th>Table 4-9</th>
<th>Media Importer Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td><strong>Media Importer Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Importer Type</td>
<td>To upload the EPG using the CDSM, set the Importer Type to host. For information on uploading an EGP file, see the “Uploading an EPG File” section on page 7-22.</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 Enable Auto Import 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>
<tr>
<td>FTP Path</td>
<td>Directory path of the location of the EPG files on the FTP server. Enter the relative or absolute path according to the configuration of the FTP server. Mismatching the configuration could result in failure of Auto Import function.</td>
</tr>
<tr>
<td>Username</td>
<td>Username, if required, to access the FTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password, if required, to access the FTP server.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Number of times to retry connecting to the FTP server, if the connection fails.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>Number of seconds to wait before retrying the connection to the FTP server.</td>
</tr>
</tbody>
</table>
Table 4-9  Media Importer Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Import Schedule</td>
<td></td>
</tr>
<tr>
<td>Daily</td>
<td>If daily is chosen (the default setting), enter the time of day the EPG file should be imported using the 24-hour clock format.</td>
</tr>
<tr>
<td>Weekly</td>
<td>If weekly is chosen, choose the days of the week and the time of day (24-hour clock format) when the EPG file should be imported.</td>
</tr>
</tbody>
</table>

Note: If the Media Importer is importing, any configuration changes to the Auto Import feature take effect after current auto import is complete.

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

Configuring Call Signs

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

Note: The CallSign Setup is part of the Real Time Capture Type (non-Media Scheduler) optional feature.

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.

Starting from Cisco VDS-TV Release 3.5.2, Source Specific Multicast (SSM) feature is supported that enables VDS-TV to specify the source IP to receive the multicast feed from. The user can specify the source IP and backup source IP for a given multicast feed in CallSign setup page.

SSM feature is supported only for EventIS (off vpath) RTSP deployment.

Note: If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure a CallSign, do the following:

Step 1  Choose Configure > System Level > CallSign Setup. The CallSign Setup page is displayed(Figure 4-6).
Step 2  Enter the call sign 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>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</td>
</tr>
<tr>
<td></td>
<td>(SPTS).</td>
</tr>
<tr>
<td>Port</td>
<td>Port associated with the CallSign.</td>
</tr>
<tr>
<td>Primary Source</td>
<td>Optional field. IP address of the primary source of multicast feed.</td>
</tr>
<tr>
<td>Backup Source</td>
<td>Optional field. IP address of the backup source of multicast feed.</td>
</tr>
</tbody>
</table>

Note: This field is applicable only if RTSP deployment is configured as EventIS (off vpath)

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.
Chapter 4      Configuring the VDS

Configuring Input Channels

Note

The Input Channels page is part of the Media Scheduler 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 7-22.

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.

Note

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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 4-7).
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.

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

Step 4  In the Port field, enter the port number the Vault should listen to for ingesting content.

Step 5  Enter the channel settings as appropriate. See Table 4-11 for descriptions of the fields.

### Table 4-11  Input Channels 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>
</tbody>
</table>
Table 4-11  Input Channels Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 Yes. Otherwise, choose No.</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 back office. 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**  
In OCN deployment using MediaX, you cannot delete a channel that has future scheduled events but the channel gets deleted after start of the recording.

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

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 F-16.

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 VDS, 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. 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 4-93.

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 the event of a transport network failure. If a stream interface fails, another stream interface in the same SOP takes over.

Note
If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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 should not span more than one Stream Group.
A logical SOP, which is an SOP virtual IP address and domain name, can span multiple source subnets.

To configure the Multiple SOP feature, do the following:

1. Choose Configure > System Level > Source Output Port. The Source Output Port page is displayed.
2. In the SOP Name field, enter the domain name of this Streamer for identification purposes to the On Demand Resource Manager (ODRM).
3. In the Virtual IP field, enter the virtual IP address for this SOP.
4. Click Submit.
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 4-93.

Configuring the System Level Logging

All logs are located in the /arroyo/log directory. The log files are rotated at least once a day and time stamps are added to the filenames. Some log files that grow rapidly are rotated more frequently (determined by file size); this rotation may happen up to once an hour. Most log files have the following suffix: .log.<YYYYMMDD.> The time zone for log rotation and filename suffixes is coordinated universal time (UTC). As part of the new log entry format, the log level and facility are included.

All log entries have the following changes:
- Stream handle is represented in decimal format
- IP addresses are represented in dotted-decimal format
- Clear identification of where a stream is going rather than a MAC address
- Time is represented in UTC
- Global Object ID (GOID) is represented in hexadecimal

Stream Trace
Log messages currently in the streamevent.log file are converted to a structured message and assigned the “stream trace” facility number. Other messages that record stream creation, routing, or playout are converted to a structured message and assigned the “stream trace” facility number. This enhancement, along with configuring syslog-ng to direct all “stream trace” facility messages to a single, centralized log server, provides a coherent set of log messages that describe stream history.

Facility Information, and Associated Log File and Debug Flags
For information on each facility and associated log file and debug flags, use the loginfo tool. The loginfo tool can run on any VDS server, including the CDSM. Start a Telnet or SSH session, log in to the VDS server, and enter the loginfo command without any arguments. Information on each facility is listed.
Configuring Logging Levels

All logging is configured at the System Level or Server Level. The configuration of the logging levels at the Server Level overrides the System Level settings.

**Note**

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To set a log level for a facility at the System Level, do the following:

**Step 1** Choose **Configure > System Level > Logging**. The Log page is displayed.

**Step 2** From the **Facility Name** drop-down list, select a facility and click **Display**. The Log Level fields are displayed.

The facilities list is based on the configuration of the system.

**Step 3** Enter the Log Level settings as appropriate. See Table 4-12 for descriptions of the fields.

<table>
<thead>
<tr>
<th><strong>Table 4-12 Log Level Fields</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Local Log Level</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

A log level setting includes all the more urgent levels. For example, if the log level is set to Error (3), then Alert (2), Critical (1), and Emergency (0) log entries are included as well as Error (3).
Step 4  Click Submit.

To clear the fields and start over, click Reset.

To delete the log level settings for a facility, select the facility from the drop-down list and click Delete.

### Configuring the System Level Syslog

The Syslog configuration page at the System Level and Server Level is used to configure the IP address and port of the server that is to receive remote logging. The configuration of the syslog server at the Server Level overrides the System Level settings. For remote logging information to be sent for a facility, the Remote Log Level must be set on the Logging page. See the “Configuring the System Level Logging” section on page 4-31 for more information.

**Note**

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure the remote logging server, do the following:

#### Step 1
Choose Configure > System Level > Syslog. The Syslog page is displayed.

#### Step 2
Check the Enable Remote Logging check box.

#### Step 3
In the IP Address field, enter the IP address of the remote server that is to receive syslog messages.

#### Step 4
In the Port field, enter the port of the remote server that is to receive syslog messages.
To delete the remote server settings, click **Delete**.

### Configuring System Level Error Repair

The VOD Error Repair settings can be configured on the System Level, Array Level, and the Server Level. Settings configured at the Array Level take precedence over System Level settings, and settings at the Server Level take precedence over Array Level or System Level settings.

**Note**

VOD Error Repair is a licensed feature. VOD Error Repair requires the LSCP Client Protocol be set to Cisco (RTSP) and the set-top have the Cisco Visual Quality Experience Client (VQE-C) software running on it. For more information, see the **“VOD Error Repair”** section on page F-9.

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the **“Bulk Import/Export Configuration”** section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, **“Creating Bulk Configuration Files.”**

To configure error repair at the System Level, do the following:

**Step 1**

Choose **Configure > System Level > Error Repair**. The Error Repair page is displayed.

**Step 2**

Enter the Error Repair settings as appropriate. See **Table 4-13** for descriptions of the fields.

**Table 4-13  VOD Error Repair Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error Repair Mode</strong></td>
<td></td>
</tr>
<tr>
<td>ER Enable</td>
<td>To enable Error Repair, check the <strong>ER Enable</strong> check box.</td>
</tr>
<tr>
<td>RTP Encapsulation Enable</td>
<td>To enable RTP encapsulation, check the <strong>RTP Encapsulation Enable</strong> check box. VDS-TV supports both UDP and RTP encapsulation. If the RTP Encapsulation Enable check box is not checked, the VDS is configured to only handle UDP encapsulation.</td>
</tr>
<tr>
<td><strong>Repair Packets DSCP</strong></td>
<td></td>
</tr>
<tr>
<td>DSCP of Repair Packets Sent</td>
<td>DSCP value for the transmitted RTP and RTCP packets sent for error repair. The range is from 0 to 63. The default is 0.</td>
</tr>
<tr>
<td><strong>RTCP Report Exporting</strong></td>
<td></td>
</tr>
</tbody>
</table>
To monitor the VOD Error Repair feature, use the Application Monitoring Tool (AMT). For more information, see Appendix E, “Using the VDS-TV Streamer Application Monitoring Tool.”

Array Level Configuration

The Array Level tab has the following configuration options:

- Configuring the Array Level DNS, page 4-36
- Configuring the Array Level NTP Server, page 4-37
- Configuring Replication Groups, page 4-37
- Configuring Stream Groups, page 4-39
- Configuring D5 Interface Settings, page 4-41
- Locating Cache Groups, page 4-44
- Locating CDN Groups, page 4-46
- Mapping Stream Group to CDN Groups, page 4-48
- Configuring Vault Groups, page 4-49
- Configuring Ingest Steering, page 4-51
- Configuring SSV Groups, page 4-54
- Configuring Cache Groups, page 4-55
- Mapping Vault Groups to Cache Groups, page 4-57
- Mapping Cache Groups to Cache Groups, page 4-58
- Mapping Stream Groups to Cache-Fill Sources, page 4-59
- Mapping Vault Groups for Redundancy, page 4-61
- Configuring the Master Vault Group, page 4-63
- Configuring the Control and Setup IPs, page 4-64

### Table 4-13  VOD Error Repair Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exporting</td>
<td>Click the Enabled radio button to enable exporting of the RTCP reports. The RTCP reports can be exported to a third-party analysis application.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address or the domain name of the server hosting the analysis application.</td>
</tr>
<tr>
<td>TCP Ports</td>
<td>Enter the TCP port number that is used to receive the reports on the server hosting the analysis application.</td>
</tr>
</tbody>
</table>
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 Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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 4-14** 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>
<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>
Chapter 4  Configuring the VDS

Array Level Configuration

Configuring the Array Level NTP Server

The Array NTP Server page is used to configure up to 16 NTP servers.

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.

Note

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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 VDS server or configuring NTP on a CDSM or VVIM, see “Other NTP Configurations” section on page 4-101.

Configuring Replication Groups

Starting from Release 3.9, AVSDB application in VDS-TV supports 512 replication servers (including vaults, streamers, cache nodes and controllers). To scale to 512 devices, AVSDB is enhanced to use hierarchical replication. A large replication domain is logically split into smaller replication groups. In each replication group, a node is selected as a replication master, referred to as replication group master.

Note

CServer replication is limited to only 512 servers. For example, the number of VDS servers supported in streaming domain (streamers + cache) is 512.

A Replication group master acts as a receiver for data replicated from other groups and forwards them to nodes in its group over separate replication sessions. Each node in a group replicates data to other nodes within its group, controller and to replication master of the other replication groups. A controller replicates data only to replication group master.

A server can never be a member of more than one replication group.

When grouping servers, you should consider network costs, bandwidth usage, and geographic locations of Vaults, Caching Nodes, and Streamers.
To configure a Replication Group, do the following:

**Step 1** Choose **Configure > Array Level > Replication Groups Setup**.

**Step 2** Select the Replicate Group type.

**Step 3** From the **Select Replication Group to View/Edit** drop-down list, choose **Add New Replication Group** and click **Display**.

**Step 4** Enter settings as appropriate. See **Table 4-15** for description of fields.

**Table 4-15**  **New Replication Group Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Vault/Cache/Streamer Replicate Group Name</td>
<td>Specify the name of the Replicate Group. Use only alphanumeric characters (0–9, a–z, A–Z), the dash (-), and the underscore (_) to create a Replicate Group name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specify the IP address of the replicate group.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify the subnet mask of the replicate group.</td>
</tr>
</tbody>
</table>

**Step 5** To edit a Replication Group, choose the Replication Group from the drop-down list and click **Display**.

**Step 6** Add the servers (vaults/streamers/cache node) to the Replication Group depending on the Replication Group Type.

The unassigned servers are listed along with a drop down-list for each that offers the options described in **Table 4-16**.

**Table 4-16**  **Server Options**

<table>
<thead>
<tr>
<th>Server Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Change</td>
<td>Do not make any changes to the Replication Group assignment. Applicable only to servers assigned to the selected Replication Group.</td>
</tr>
<tr>
<td>Replication Group Name</td>
<td>Add/Modify this server (vault/streamer/cache node) to this Replication Group. Applicable only for unassigned servers.</td>
</tr>
<tr>
<td>None</td>
<td>Remove this server from this Replication Group. Applicable only to servers assigned to the selected Replication Group.</td>
</tr>
<tr>
<td>Don’t Change</td>
<td>Do not assign this server to this Replication Group. Applicable only for unassigned servers.</td>
</tr>
</tbody>
</table>

**Step 6** Click **Submit** to save the settings.

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

To view the members of a Replication Group, choose the Replication Group from the drop-down list and click **Display**.
To delete a Replication Group, remove all vault/streamer/cache node from the group, then click **Delete Group**.

**Configuring Stream Groups**

A Stream Group consists of one or more Streamers. Streamers within a Stream Group work as a team with regard to content caching, load distribution, and bandwidth usage. Stream Groups interact with other Stream Groups by passing streams among each other based on performance qualification and cost considerations. If a Stream Group must give up a stream to another group, Stream Group preferences set on the QAM Gateway page are followed. Stream Groups relate to QAM gateways or destination subnetwork by the Stream Group preference. For more information about Stream Group and QAM gateway associations, see the “Configuring QAM Gateways” section on page 4-5. For more information about destination subnetworks and Stream Groups, see the “Configuring Stream Destinations” section on page 4-9.

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.

Starting with VDS-TV Release 3.4, ISR Stream groups are also configured via Stream Groups page.

**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 7-26.

For more information about the VVI settings on the CDSM Setup page, see the “Virtual Video Infrastructure” section on page F-10.

---

**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.
If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure a Stream Group, do the following:

**Step 1** Choose **Configure > Array Level > Stream Groups Setup**. The Stream Groups page is displayed (Figure 4-8).

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

**Note**

For ISR Stream Group, the user is provided an option to enable or disable **Fade Frame Support**.

---

**Figure 4-8 Stream Groups Page**

---

**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 4-17.
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.

<table>
<thead>
<tr>
<th><strong>Table 4-17 Unassigned Streamer Options</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unassigned Streamer Option</strong></td>
</tr>
<tr>
<td>No Change</td>
</tr>
<tr>
<td>Stream Group Name</td>
</tr>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

**Configuring D5 Interface Settings**

To configure D5 settings for a Stream Group, do the following:

**Note**
The D5 Setup page is visible if D5 Support is enabled in the **Maintain > Software > CDSM Setup** page.

**Note**
If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”
Step 1 Choose **Configure > Array Level > D5 Setup**. The D5 Setup page is displayed (Figure 4-9).

**D5 Setup**

From the **Stream Groups** drop-down list, choose a group to be configured and click **Display**. The D5 Interface settings for the specified streaming group is displayed.

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

Enter the D5 Interface settings as appropriate. See **Table 4-18** for the descriptions of the fields.

**Table 4-18 D5 Interface Settings Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Streaming IP</td>
<td>Read only field. The IP address of the Master Streamer.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This field can be configured in Control/Setup IP field available in Control/Setup IP page under Configure &gt; Array Level &gt; Control/Setup IP.</td>
</tr>
<tr>
<td>Port</td>
<td>Read only field. The TCP port number the RTSP server is listening to for communication with the streamer.</td>
</tr>
<tr>
<td>Component Name</td>
<td>Read only field. Name of the master Streamer registered with the DNS server. This is a critical communication component and must match the table entry in the DNS server.</td>
</tr>
<tr>
<td>Model Name</td>
<td>Optional. Manufacturer and Model Number of the device. The suggested format is Manufacturer + &quot;:&quot; + Model.</td>
</tr>
</tbody>
</table>
Chapter 4  Configuring the VDS

Array Level Configuration

Table 4-18  D5 Interface Settings Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Delivery Protocol      | The content delivery protocol supported by the streaming server. The supported delivery protocols are:  
  - UDP  
  - HTTP  
  - PGM  
  - RTP.  
  The default value is UDP. |
| Significant Resource Usage | Mandatory field. If the available bandwidth or stream bandwidth exceeds the configured Significant Resource Usage percentage of maximum bandwidth within the configured notify interval then the streamer posts the Streaming Status Message to ODRM. The default is 10 and range is 5 - 50. For example, if maximum bandwidth is 10 Gbps and Significant Resource Usage is 10 then when the D5 service detects change in Available BW or Streaming BW for any of SOPS by 1 Gbps [10% of 10 Gbps) a Streaming Status message is sent to ODRM to notify of the change. |
| Specify Policies       | Optional field. The Streaming Server policies which are considered by the ODRM during Streaming server selection. The supported policies are:  
  - VOD  
  - nDVR. |
| ODRM URL               | Mandatory field. The fully qualified domain name (FQDN) or IP Address, port of the ODRM. |
| Notify Interval        | Mandatory field. Time to wait, in seconds before attempting to send the Streaming Server Status message to ODRM. The default is 60 seconds and range is from 60 - 600 seconds. |

Source Output Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOP Name</td>
<td>The SOPs are auto populated for Streaming Group and displayed to help in configuring corresponding router loop back address connected, which are to be advertised as part of SOP configuration to ODRM, in status messages sent for D5 interface.</td>
</tr>
<tr>
<td>Router Loopback Address</td>
<td>The loopback address of the router to which the server port is connected.</td>
</tr>
</tbody>
</table>

Step 2  Click Submit.  
To reset the fields, click Reset.  
Step 3  Enter the following command and press Enter to restart rtsp.  

```
# service rtsp restart
```

Step 4  Enter the following command and press Enter to start d5.
# service d5 start

## 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.

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 F-10.

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 F-10 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 7-26.

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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.

To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”
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 4-10).

**Figure 4-10  Cache Group Locator Page**

To add Cache Group Locations, select “Add Cache Group Locations” from the select box below.

- Configured Cache Locations:
  - Add Cache Group Locations

  ![Cache Group Locator Page](image)

- VVIM IP: 172.32.97.165
- 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**.

### Locating CDN Groups

The CDN Group Locator page is used by the Stream Manager in a VVI with split-domain management to identify and locate the CDN 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 CDN Group Locator page is visible if the Third Party CDN Support is enabled in the **Maintain > Software > CDSM Setup** page. |

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

- Import
- Upload
- Manually

The **Import** option uses an HTTP GET request to communicate with the VVIM in retrieving the CDN 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 F-10 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 7-26.

| Note | If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**. |

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To identify and locate the CDN Groups, do the following:

| Step 1 | Choose **Configure > Array Level > CDN Group Locator**. |
| Step 2 | From the **Configured CDN Locations** drop-down list, choose **Add CDN 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 CDN Group Locator page, it is displayed in the **VVIM IP** field.

**b. Click Import CDN Groups.**

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

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

- **a.** Get the CDNGroupsConfig.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 CDNGroupsConfig.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 CDN Groups File Location field.
- **d.** Click **Upload**.

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

---

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

**Step 1** Choose **Configure > Array Level > CDN Group Locator**. The CDN Group Locator page is displayed.

**Step 2** From the **Configured CDN Locations** drop-down list, choose a CDN Group Location. The page refreshes and the CDN Group information is displayed. The Location Virtual IP and Location Subnet fields are informational only.

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

**Step 4** To delete a CDN Group location, click **Delete**.

---

To add Third Party CDN Groups Location, do the following:

**Step 1** Choose **Configure > Array Level > CDN Group Locator**. The CDN Group Locator page is displayed.

**Step 2** From the **Configured CDN Locations** drop-down list, choose a CDN Group Locations Manually. The page refreshes and the CDN Group information fields are displayed.

**Step 3** Enter the **CDN Group Name**, **Location Virtual IP**, **Location Port**, **Location Subnet Mask** for the corresponding Third Party CDN Group.

**Step 4** CDN groups can be added to a particular Volume Name. To add a new Volume Name, enter the volume name in the **New Volume Name** field and click **Add**. The new volume name will be added to the list of unassigned volumes. The unassigned volume names can be moved to assigned volume names by clicking on right arrow button and the assigned volume names can be moved to unassigned volume names by clicking on the right arrow button.

**Step 5** Click **Submit** to save changes. To reset the fields, click **Reset**.

**Step 6** To delete a CDN Group location, click **Delete**.
Note: The New Volume Name field is visible if Volume Name Based Support is enabled in the Maintain > Software > CDSM Setup page.

Mapping Stream Group to CDN Groups

The Stream Group to CDN Map is used by the Stream Manager in a VVI with split-domain management to map the CDN Groups to a particular Volume.

Note: The CDN Group Locator page is available when Third Party CDN is enabled in the Maintain > Software > CDSM Setup page.

Note: If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To map Stream Group to CDN, do the following:

Step 1 Choose Configure > Array Level > Stream To CDN Map.

Step 2 From the Stream Groups drop-down list, choose a Stream Group. From the Volume drop-down list, choose a Volume click Select. Available CDN groups mapped with the particular Volume are listed.

Step 3 Choose the CDN preference by selecting High, Medium, Low, None. Hence a particular groups priority is set.

Step 4 To rename the CDN Group Location, enter a new name in the CDN Location Name and click Submit. To reset the field, click Reset.

Step 5 To delete a CDN Group location, click Delete.

To select a default CDN group if a Volume route fails, do the following:

Step 1 From the CDN Groups drop-down list, choose a CDN Group.

Step 2 All the available CDN Groups are listed, Choose the desired CDN Group and click Submit. To reset the field, click Reset.
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 4-61.

---

**Note**

The Vault Groups Setup page is part of the Vault Groups feature and is displayed only if Vault Groups is enabled. For more information, see the “Vault Groups” section on page F-7. 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 F-10.

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**

The maximum number of Vault Groups is 30. Prior to 3.5.2 release, the maximum number of vault groups supported is 20.

---

**Note**

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”
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 4-11).

**Figure 4-11 Vault Groups Setup Page**

To add a new Vault Group, select “Add New Vault Group” from the select box below and click **Display**. To add members to a group, select the group, then select any “Unassigned Vault Servers” to be added to the group and click **Submit**. To move members from one Vault Group to another Vault Group, select the member’s current group from the list below and click **Display**. Once the group members are displayed you may use the “New Group” select box to choose a new Vault Group to assign each member to. Alternatively, you may choose none from the “New Group” select box to remove a member from its current group and leave it unassigned.

**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** Enter settings as appropriate. See Table 4-19 for description of fields.

**Table 4-19 New Vault Group Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Vault Group Name</td>
<td>Specify the name of the Vault Group. Use only alphanumeric characters (0–9, a–z, A–Z), the dash (–), and the underscore (__) to create a Vault Group name.</td>
</tr>
<tr>
<td>Location Virtual IP</td>
<td>Specify the virtual IP address of the vault group used for locate port service. This virtual IP address is bound to the locate IP and port. <strong>Note</strong>: This field is applicable only for RTSP deployment using HTTP protocol.</td>
</tr>
<tr>
<td>Location Subnet Mask</td>
<td>Specify the subnet mask of the location Virtual IP address <strong>Note</strong>: This field is applicable only for RTSP deployment using HTTP protocol.</td>
</tr>
</tbody>
</table>
Step 4  For a VVI that uses HTTP for communication between the Vault and Streamers, do the following:

- Enter the IP address this Vault Group uses as the virtual IP address for the Locate Port service in the Location Virtual IP field. 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 2-12.

- Enter the Subnet Mask for the Location IP address in the Location Subnet Mask field.

Step 5  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 4-20.

Table 4-20  Unassigned Vault Options

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

Step 6  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 Ingest Steering

The Ingest Steering page allows you to have specific Vault Groups ingest content with specified Product IDs. For example, if you have a Vault Group that you want to be responsible for ingesting all the live ingests, you can use the Product ID to direct that content to that Vault Group.

The back office uses the Ingest Manager to ingest packages, including content. As specified in the ADI 1.1 Specification, there is an ADI XML file for each package and the Product ID is one attribute in this ADI XML file.

Every Product ID maps to only one Vault Group. The Product ID is included in the ADI.XML for FTP pull content, additionally, the Product ID can be configured in the Input Channels page for MediaX live content. Ingestion with such Product ID information is correctly dispatched to the Vault Group mapped in Ingest Steering.

For more information, see the “Steering Ingests” section on page 2-22.

Note  The Ingest Steering page is not available if the Ingest Steering feature is not enabled. The Ingest Steering feature requires Vault Groups to be enabled.
Enabling or disabling Ingest Steering requires restarting the FSI process on all Vaults. If Ingest Steering has been enabled and has taken effect, the changes to the Ingest Steering configuration do not take effect immediately.

- If there is ingest activity, wait two hours for FSI to reload the new configuration.
- If there is no ingest activity, restarting the FSI process on all Vaults could make the changes take effect immediately.

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure Ingest Steering, do the following:

**Step 1** Choose Configure > Array Level > Ingest Steering. The Ingest Steering page is displayed (Figure 4-12).
Step 2  In the **New Product ID** field, enter the product ID and click **Add**. The product ID is listed in the Unassigned Products text box. Repeat for each product ID.

Step 3  From the **Select Vault Group to assign products** drop-down list, choose a Vault Group and click **Display**.

Step 4  To assign the product IDs to the selected Vault Group, click the product ID to highlight it and click the > button.
To assign all product IDs, click the >> button.
To remove all product IDs from the Assigned Products text box, click the << button.
To remove one product ID from the Assigned Products text box, click the product ID to highlight it and click the < button.
To delete a group of product IDs, click the first product ID, then hold the Ctrl key and click the remaining product IDs, then click **Delete**.
To delete one product ID, click the product ID to highlight it and click **Delete**.

Step 5  When you have finished assigning the product IDs for the Vault Group displayed, click **Submit**.
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.

Note

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 F-6. 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 4-61. 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 4-66.

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

Note

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.

Note

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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 4-21.
Step 5

Click **Submit**.

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

To view the members of an SSV Group, choose the SSV Group from the drop-down list and click **Display**.

To delete an SSV Group, first remove all SSVs from the group, then click **Delete Group**.

### 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.

---

**Note**

The Cache Groups Setup page is part of the VVI feature and is displayed only on VVIMs.

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.

---

**Note**

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

---

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 4-13).
Figure 4-13 Cache Groups Setup Page—HTTP Streamers

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.

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 2-12.

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 4-22.

Table 4-22 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 4-55 and the “Configuring Vault Groups” section on page 4-49.

#### Note

The Cache To Vault Map page only displays on the VVIM and is available only when Vault Groups and VVI are both enabled. For more information, see the “Vault Groups” section on page F-7 and the “Virtual Video Infrastructure” section on page F-10.

#### Note

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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 4-55 or the “Configuring Vault Groups” section on page 4-49. 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 Cache Groups to Cache Groups

The Cache To Cache Map page is used to map Cache Groups to Cache Groups in a VVI. Before you can map Cache Groups to Cache Groups, you must create them. For more information, see the “Configuring Cache Groups” section on page 4-55.

The Cache To Cache Map page only displays on the VVIM. For more information, see the “Virtual Video Infrastructure” section on page F-10.

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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

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

Step 2 From the Cache Group drop-down list, choose a Cache Group and click Select. All available Cache Groups are displayed.

Step 3 Choose the preference setting for each Cache 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 Cache 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 Cache Group, choose the Cache Group from the drop-down list and click Select.
To delete a Cache Group, see the “Configuring Cache Groups” section on page 4-55. When a Cache Group is deleted, the mapping for the Cache Group is also deleted, and any other mappings to the Cache Group are 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 4-39 and the “Configuring Cache Groups” section on page 4-55 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 4-44 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 F-10.

---

Streamers can be used as cache-fill sources when **Streamer is Cache** is enabled on the Server Setup page (“Configuring the Servers,” page 4-85). 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.

---

**Note**

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

---

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 4-14).
### Figure 4-14  Stream To Cache Map Page

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

<table>
<thead>
<tr>
<th>Cache Group Preferences</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>CacheGrp1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CacheGrp2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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**.

---

**Note**

The Stream to Cache Map page is associated with the configuration file FillSourceConfig in /arroyo/test directory. After submitting the Stream to Cache Map page, the FillSourceConfig file is updated.

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 4-39 or “Configuring Cache Groups” section on page 4-55. 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 4-49 for more information.

Note

The Vault Redundancy Map page is part of the Vault Groups feature and is displayed only if Vault Groups 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 F-10 and the “Vault Groups” section on page F-7.

Note

The maximum number of Vault Groups is 30. Prior to 3.5.2 Release, the maximum number of vault groups supported is 20.

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 1-21.

Note

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

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 4-15).
**Figure 4-15  Vault Redundancy Map Page**

![Vault Redundancy Map Diagram]

**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. You can select up to three Vault Groups to which to mirror content.

  **Note**  The **Vault Mirror Copies** field in the Server Setup page determines the number of mirrored copies kept in the VDS for the content stored on the specified Vault. See the “Configuring the Servers” section on page 4-85 for more information. The Vault Redundancy Map page specifies which Vault Groups participate in the content mirroring.

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

**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 4-49. When a Vault Group is deleted, the mapping for the Vault Group is also deleted.
Configuring the Master Vault Group

The Master Vault Group page allows you to select the Vault Group that has the master Vault and the master IP address. One of the Vaults in the Master Vault Group is designated the master Vault. If the master Vault fails, another Vault in the Master Vault Group takes over as the master Vault.

**Note**

All Vaults in the Master Vault Group must be in the same network; otherwise, the master Vault failover fails.

The master IP address is set as part of the initial configuration (vdsconfig script) and the information is added to the statsd line in the rc.local file.

To locate the master Vault in the Master Vault Group, go to the System Health page (Monitor > System Health).

**Note**

The Master Vault Group page is part of the Vault Groups feature and is displayed only if Vault Groups is enabled. If VVI is enabled, The Master Vault Group page is displayed only on the VVIM. For more information, see the “Virtual Video Infrastructure” section on page F-10 and the “Vault Groups” section on page F-7.

**Note**

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure the Master Vault Group, do the following:

**Step 1** Choose Configure > Array Level > Master Vault Group. The Master Vault Group is displayed.

**Step 2** Check the Master Vault Group check box associated with the Vault Group.

**Step 3** Click Submit.

**Note**

After you have submitted the settings the first time, if you change the Master Vault Group, you must restart all the Vaults in the old Master Vault Group and the new Master Vault Group for the changes to take effect. See the “Restarting a Server” section on page 7-12 for more information.
Configuring the Control and Setup IPs

A Streamer designated as the Setup server interfaces with the back office 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 7-26.

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 18,000 sessions. You must configure a Control server for each group of up to 18,000 sessions. For instance, if you have 19,000 sessions, 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 2-9.

Starting with VDS-TV Release 3.4, Control and Setup IPs are also configured for ISR Stream Groups.

---

**Note**

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”
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 4-16).

**Figure 4-16 Control/Setup IP Page**

<table>
<thead>
<tr>
<th>Stream Group</th>
<th>Control/Setup IP</th>
<th>Subnet Mask</th>
<th>IP Type</th>
<th>Setup ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR Group1</td>
<td>172.23.37.142</td>
<td>255.255.255.0</td>
<td>Control/Setup IP</td>
<td>3</td>
</tr>
<tr>
<td>SR Group2</td>
<td>172.23.103.169</td>
<td>255.255.255.0</td>
<td>Control/Setup IP</td>
<td>4</td>
</tr>
</tbody>
</table>

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

**Step 3**
From the **IP Type** drop-down list, choose an IP type. See Table 4-23 for descriptions of the types.

**Table 4-23 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 Sites**

The Site Setup page allows you to create sites and assign Stream Groups, Cache Groups, and Vault Groups to them for configuring thin pipe maps. To configure thin pipe maps, you must first configure the sites.
If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure a site, do the following:

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

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

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

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

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

**Step 4** Add the appropriate Stream Groups, Vault Groups, and Cache Groups to the site.

The unassigned groups are listed along with a drop down-list for each that offers the options described in Table 4-22.

<table>
<thead>
<tr>
<th>Group Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Change</td>
<td>Do not make any changes to the site assignment.</td>
</tr>
<tr>
<td>Site Name</td>
<td>Add this group to this site.</td>
</tr>
<tr>
<td>None</td>
<td>Remove this group from this site. Applicable only to groups assigned to the selected site.</td>
</tr>
<tr>
<td>Don’t Change</td>
<td>Do not assign this group to this site.</td>
</tr>
</tbody>
</table>

**Step 5** Click Submit.

To reset the field, click Reset.

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

To delete a site, first remove all groups from the site, then click Delete Site.

### Configuring Cache-Fill Bandwidth Using Thin Pipe Mapping

The Thin Pipe Map page allows you to configure low-bandwidth connections between local and remote sites. A local site consists of groups of servers in the same site, for example, all the Streamers in a Stream Group are considered part of the same site, or local site. A remote site consists of groups of servers in other Stream Groups, Cache Groups, and Vault Groups. Before you can configure thin pipes, you must define the sites. For more information, see the “Configuring Sites” section on page 4-65.
There can be multiple thin pipes configured for each local site. 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 site with a Stream Group. The thin pipes are completely independent of each other. Additionally, thin pipes can be created among servers at the same site by selecting the same site for Local Site and Available Remote Site.

The Thin Pipe Map page also allows for the configuration of thin pipes in a hierarchy, where a remote site 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.

---

**Note**
The Thin Pipe Map page is displayed only if Thin Pipe Management is enabled. See the “Thin Pipe Management” section on page F-9 for more information.

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

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

---

**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 VDS server. See the “Configuring the Servers” section on page 4-85 for more information.

As an example, Figure 4-17 shows the maximum bandwidth available for the various groups in a Virtual Video Infrastructure (VVI) system with two super headends (SHEs) and three caching sites.

---

**Note**
If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”
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, Super Headend 1 (SHE1) to Super Headend 2 (SHE2) and Cache Site 3 share a 3 Gbps link on the route between SHE1 and the other two sites, then another thin pipe must be configured to specify this 3-Gbps restriction.

Table 4-25 lists the thin pipe mappings that would be configured for the different Vault Groups illustrated in Figure 4-17.

### Table 4-25 Thin Pipe Mappings for Thin Pipe Example

<table>
<thead>
<tr>
<th>Thin Pipe Map</th>
<th>Remote Site</th>
<th>Bandwidth (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Super Headend 1 (SHE1)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHE1toAll</td>
<td>SHE2, Cache Site 1, Cache Site 2, Cache Site 3</td>
<td>5</td>
</tr>
<tr>
<td>SHE1toSHE2</td>
<td>SHE2</td>
<td>4</td>
</tr>
<tr>
<td>SHE1toCS1</td>
<td>Cache Site 1</td>
<td>2</td>
</tr>
<tr>
<td>SHE1toCS2</td>
<td>Cache Site 2</td>
<td>2</td>
</tr>
<tr>
<td>SHE1toCS3</td>
<td>Cache Site 3</td>
<td>2</td>
</tr>
<tr>
<td><strong>Super Headend 2 (SHE2)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHE2toAll</td>
<td>SHE1, Cache Site 1, Cache Site 2, Cache Site 3</td>
<td>4</td>
</tr>
<tr>
<td>SHE2toCS1</td>
<td>Cache Site 1</td>
<td>2</td>
</tr>
<tr>
<td>SHE2toCS2</td>
<td>Cache Site 2</td>
<td>2</td>
</tr>
<tr>
<td>SHE2toCS3</td>
<td>Cache Site 3</td>
<td>2</td>
</tr>
<tr>
<td><strong>Cache Site 1 (CS1)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS1toAll</td>
<td>SHE1, SHE2, Cache Site 2, Cache Site 3</td>
<td></td>
</tr>
</tbody>
</table>
The thin pipes configured in Table 4-25 ensure that the bandwidth for SHE1 never exceeds the maximum bandwidth available for SHE1, which is 5 Gbps. This means that even if all remote groups were requesting cache fills from SHE1, which would be a maximum throughput of 9 Gbps, the actual maximum bandwidth of cache-fill traffic coming from SHE1 would never exceed 5 Gbps.

One server in the site is elected as the bandwidth manager for all servers in the site. The bandwidth manager controls the traffic leaving the site to any other site and queries all the VDS servers in the site for the thin pipe mapping configuration of each VDS server. For more information about the bandwidth manager, see the “Bandwidth Manager for Thin Pipe” section on page 2-8.

Before you can configure thin pipes, you must define the sites. For more information, see the “Configuring Sites” section on page 4-65.

To configure a Thin Pipe Map, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Configure &gt; Array Level &gt; Thin Pipe Map</strong>. The Thin Pipe Map page is displayed.</td>
</tr>
<tr>
<td>2</td>
<td>From the <strong>Configured Pipes</strong> drop-down list, choose <strong>Create New Pipe</strong> and click <strong>Select</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>From the <strong>Local Site</strong> drop-down list, choose the site that you want to use as the local site for this thin pipe map.</td>
</tr>
<tr>
<td>4</td>
<td>In the <strong>Pipe Name</strong> field, enter the name for the pipe map.</td>
</tr>
<tr>
<td>5</td>
<td>In the <strong>Max Transmit Bandwidth</strong> field and the <strong>Max Receive Bandwidth</strong> field, enter the maximum transmit and receive megabits per second (Mbps) for this pipe.</td>
</tr>
</tbody>
</table>

The Max Bandwidth fields represent the throughput for the pipe, which is defined per site (Stream Group, Cache Group, and so on); not each server. For all existing thin pipes, only the **Max Transmit Bandwidth** and **Max Receive Bandwidth** fields are allowed to be edited. All other fields are read only.

If Site 1 has 2 Vault Groups with 2 Vaults each and Site 2 has 1 Cache Group with 2 Caching Nodes, and the network design and physical link were such that it could support 500 Mbps throughput (that is, 500 Mbps transmit and 500 Mbps receive), then the maximum of the **Transmit Max Bandwidth** cannot exceed 500 Mbps and the maximum of the **Receive Max Bandwidth** cannot exceed 500 Mbps. Further, 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.

### Table 4-25 Thin Pipe Mappings for Thin Pipe Example (continued)

<table>
<thead>
<tr>
<th>Thin Pipe Map</th>
<th>Remote Site</th>
<th>Bandwidth (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Site 2 (CS2)</td>
<td>SHE1, SHE2, Cache Site 1, Cache Site 3</td>
<td>2</td>
</tr>
<tr>
<td>Cache Site 3 (CS3)</td>
<td>SHE1, SHE2, Cache Site 1, Cache Site 2</td>
<td>2</td>
</tr>
</tbody>
</table>

Note
Step 6 In the Available Remote Sites area, check the check box next to each remote site that you want to use this maximum bandwidth restriction.

Step 7 Check the Limit traffic to all HTTP subnets check box if this thin pipe with the Max Bandwidth settings configured is created to limit the bandwidth between the selected Local Site and the HTTP Streamers in a VVI represented by the selected remote sites.

Note This field is only applicable if HTTP is the cache-fill protocol. HTTP as the cache-fill protocol is only supported in RTSP environments.

Step 8 Alternatively, to apply the thin pipe settings to specific HTTP Streamer subnets, uncheck the Limit traffic to all HTTP subnets check box and specify the subnets in the Subnet Configuration section. Enter the Network and Subnet Mask for each subnet. To add more HTTP Streamer subnets, click the plus icon in the Subnet Configuration section.

Note This field is only applicable if HTTP is the cache-fill protocol.

Step 9 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 7-22 and the “Configuring Input Channels” section on page 4-27 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 4-18).

**Figure 4-18 Media Scheduler Page—User Preferences**

<table>
<thead>
<tr>
<th>User Preferences</th>
<th>Preference Editors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hide On Return</td>
</tr>
<tr>
<td></td>
<td>Show On Return</td>
</tr>
</tbody>
</table>

Action on Recurring Schedules (Only for user generated schedules)

- Preserve Existing Schedules
- Overwrite Existing Schedules

Package Name Preferences

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

- Auto generate
- Don’t auto generate

Channels To Schedule

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

**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 7-7.
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 4-75.

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.

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**.

Check the check boxes for the channels that you want to schedule.

**Note**  To create new channels, see the “Configuring Input Channels” section on page 4-27.

Click **Save** to save the settings. The calendar is displayed (Figure 4-19).

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

---

**Scheduling Content for Ingest**

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

Choose **Configure > Array Level > Media Scheduler**. If Hide On Return was selected in the User Preferences, the Media Scheduler calendar is displayed (Figure 4-19). If Show On Return was selected in the User Preferences, the User Preferences are displayed (Figure 4-18).

From the calendar, click the day that you want to schedule. If the month that 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 4-20).

![Figure 4-20 Media Scheduler Page—Schedule](image)

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, hover your mouse cursor over a cell. A pop-up displays the program information (Figure 4-21).

![Figure 4-21 Media Scheduler Page—Program Information](image)

**Step 3**
Click each cell for each program that 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 4-75.

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.
Package Metadata Editor

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

To use the Package Metadata Editor, do the following:

**Step 1**
To enter new metadata for any unused timeslot, click the unused timeslot. To edit existing metadata, double-click the scheduled timeslot. A new window opens and the Package Metadata Editor is displayed (Figure 4-22).

**Figure 4-22 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 4-23).

Figure 4-23  
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 4-26 for descriptions of the 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 4-71 for more information.

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

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.

Starting from Release 3.9, the media scheduler conflict reporting is enhanced to support different conflict scenarios. The table below describes the different conflict scenarios and the corresponding action taken by VDS-TV.

### Table 4-27 Media Scheduler Conflict Reporting

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Conflict Scenario</th>
<th>VDS-TV Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Re-ingesting the same tribune feed.</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Schedule with a change in the Title</td>
<td>Report Conflict.</td>
</tr>
<tr>
<td>3</td>
<td>Schedule with a change in the TV Rating</td>
<td>Overwrite the existing schedule.</td>
</tr>
<tr>
<td>4</td>
<td>Schedule with a change in the Genre</td>
<td>Overwrite the existing schedule.</td>
</tr>
<tr>
<td>5</td>
<td>Schedule with a change in the Series ID</td>
<td>Report Conflict</td>
</tr>
<tr>
<td>6</td>
<td>Schedule with a change in the Original Air Date</td>
<td>Overwrite the existing schedule.</td>
</tr>
<tr>
<td>7</td>
<td>Schedule with a change in the event start time</td>
<td>Report Conflict</td>
</tr>
<tr>
<td>8</td>
<td>Schedule with a change in the event end time</td>
<td>Report Conflict</td>
</tr>
<tr>
<td>9</td>
<td>Schedule with a change in both the event start time and the end time</td>
<td>Report Conflict</td>
</tr>
</tbody>
</table>

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 4-24).

To go to the main Media Scheduler page, click **Go To Scheduler**.
Step 2
To fix a scheduling conflict, check the corresponding schedules and click either Overwrite or Retain or Discard. On clicking Overwrite, the old schedule is replaced with the new schedule and is marked scheduled for recording. On clicking Retain, the old schedule is retained and is marked scheduled for recording. On clicking Discard, the schedules are discarded and the slot is made empty.

Note
While resolving conflicts, if any overlap event is found, then overwrite/retain of the event should be done for the complete overlap event occurrence. Partial overwrite/retain may lose some event details. For example, if an event is scheduled from 9AM to 10AM and in successive EPG uploads, if there are two events scheduled from 9AM to 9:30AM and 9:30AM to 10AM, the GUI reports two conflicts. The user must resolve both the conflicts in a single attempt by either clicking Overwrite or Retain.

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 4-22). 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.
Configuring Array Level Error Repair

The VOD Error Repair settings can be configured on the System Level, Array Level, and the Server Level. Settings configured at the Array Level take precedence over System Level settings, and settings at the Server Level take precedence over Array Level or System Level settings.

**Note**

VOD Error Repair is a licensed feature. VOD Error Repair requires the LSCP Client Protocol be set to Cisco (RTSP) and the set-top have the Cisco Visual Quality Experience Client (VQE-C) software running on it. For more information, see the “VOD Error Repair” section on page F-9.

To configure error repair at the Array Level, do the following:

**Step 1** Choose **Configure > Array Level > Error Repair**. The Error Repair page is displayed.

**Step 2** From the Select **Stream Group to View/Edit**, select a Stream Group and click **Display**.

**Step 3** Enter the Error Repair settings as appropriate. See Table 4-28 for descriptions of the fields.

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

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

To return the settings to the factory default values, click **Factory**.

To monitor the VOD Error Repair feature, use the Application Monitoring Tool (AMT). For more information, see Appendix E, “Using the VDS-TV Streamer Application Monitoring Tool.”

---

**Table 4-28 VOD Error Repair Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error Repair Mode</strong></td>
<td></td>
</tr>
<tr>
<td>ER Enable</td>
<td>To enable Error Repair, check the <strong>ER Enable</strong> check box.</td>
</tr>
<tr>
<td>RTP Encapsulation Enable</td>
<td>To enable RTP encapsulation, check the <strong>RTP Encapsulation Enable</strong> check box. VDS-TV supports both UDP and RTP encapsulation. If the RTP Encapsulation Enable check box is not checked, the VDS is configured to only handle UDP encapsulation.</td>
</tr>
<tr>
<td><strong>Repair Packets DSCP</strong></td>
<td></td>
</tr>
<tr>
<td>DSCP of Repair Packets Sent</td>
<td>DSCP value for the transmitted RTP and RTCP packets sent for error repair. The range is from 0 to 63. The default is 0.</td>
</tr>
<tr>
<td><strong>RTCP Report Exporting</strong></td>
<td></td>
</tr>
<tr>
<td>Exporting</td>
<td>Click the <strong>Enabled</strong> radio button to enable exporting of the RTCP reports. The RTCP reports can be exported to a third-party analysis application.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address or the domain name of the server hosting the analysis application.</td>
</tr>
<tr>
<td>TCP Ports</td>
<td>Enter the TCP port number that is used to receive the reports on the server hosting the analysis application.</td>
</tr>
</tbody>
</table>
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, page 4-80
- Configuring the Servers, page 4-85
- Configuring Individual Recorder Settings, page 4-91
- Configuring the Route Table, page 4-93
- Configuring the SNMP Agent, page 4-95
- Configuring the Server Level DNS, page 4-99
- Configuring the Server Level NTP, page 4-100
- Configuring RTSP Setup, page 4-103
- Configuring FSI Setup, page 4-109
- Configuring the Server Level Logging, page 4-110
- Configuring the Server Level Syslog, page 4-113
- Configuring Server Level Error Repair, page 4-114

Configuring the Interfaces

The Interface Setup page is used to configure the different interfaces on the VDS servers. The functionality of the Ethernet interfaces on the VDS servers is configurable. However, there is an optimal configuration for each server. The interface functions are described in Table 4-30.

Starting from Cisco VDS-TV Release 3.7, network interface bonding is supported on all types of VDS servers such as vaults, cache, streamers and VDS Controllers. Only Linux controlled ports can support NIC bonding. CServer controlled ports cannot be used for NIC bonding. The Linux interfaces that supports bonding for different VDS-TV hardwares are listed below:

<table>
<thead>
<tr>
<th>VDS-TV Hardware</th>
<th>Linux interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDE 460</td>
<td>eth0, eth1, eth2 and eth3</td>
</tr>
<tr>
<td>CDE 470</td>
<td>eth0, eth1, eth2 and eth3</td>
</tr>
<tr>
<td>CDE 110</td>
<td>eth0, eth1, eth2 and eth3</td>
</tr>
<tr>
<td>CDE 100</td>
<td>eth0, eth1, eth2 and eth3</td>
</tr>
<tr>
<td>CDE 250</td>
<td>eth0 and eth1</td>
</tr>
<tr>
<td>CDE 220</td>
<td>eth0 and eth1</td>
</tr>
<tr>
<td>CDE 420</td>
<td>eth0 and eth1</td>
</tr>
<tr>
<td>UCSC-220M4-2U1</td>
<td>eth0 and eth1</td>
</tr>
<tr>
<td>CDE 280</td>
<td>eth0 and eth1</td>
</tr>
</tbody>
</table>
To create a bonding interface, user must specify two Ethernet interfaces of same type (GigE or 10GigE). When bonding is enabled, the current management IP address is assigned to the bonded interface and the corresponding port is selected as a member. An interface can be assigned to only one bonded interface. A minimum of two slave interfaces and a maximum of four interfaces can be bonded at a time. Only interfaces configured as Management, General and Not Used can be bonded and at least one of the interfaces must be a management interface.

**Warning** If the interface to be bonded is used for a different purpose such as ingest then re-configuration of interfaces is required and it also may require re-cabling. For example, if eth1 is used as an ingest interface then the ingest interface should be moved to a different port before enabling bonding on eth1. The bonded interface LAN wires should be in the same subnet switch/switches.

<table>
<thead>
<tr>
<th>Table 4-30 VDS Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>General</td>
</tr>
<tr>
<td>Management</td>
</tr>
<tr>
<td>Ingest</td>
</tr>
<tr>
<td>Cache</td>
</tr>
<tr>
<td>Stream/Cache</td>
</tr>
<tr>
<td>Stream</td>
</tr>
<tr>
<td>Stream Control</td>
</tr>
<tr>
<td>Locate</td>
</tr>
</tbody>
</table>
Table 4-30  VDS Interfaces (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Control</td>
<td>This interface is used when the user requires a separate interface for control traffic that is delivered on a network not reachable from management interface (eth0). The Default Control interface can be configured only on a single interface, it cannot be configured for multiple interfaces. Although not restricted, ideally the “Default Control” interface should be configured on a 1GigE interface, and not a 10GigE.</td>
</tr>
<tr>
<td>Ingest/Stream/Cache</td>
<td>This interface can be used for ingest, streaming, and caching.</td>
</tr>
<tr>
<td>Ingest/Cache</td>
<td>This interface is used on a Streamer-Recorder for ingest and caching traffic.</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

Note

For UCSC-220M4-2U1 hardware use eth0 as management.

To configure the interface settings, do the following:

Step 1  Choose Configure > Server Level > Interface Setup. The Interface Setup page is displayed (Figure 4-25).

Note

If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To export the configuration of this page for all VDS servers in the system, click Export. To import a Bulk Configuration XML file, click Browse to locate the file, then click 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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the Server Setup page and Interface Setup page, see Appendix B, “Creating Bulk Configuration Files.”

Step 2  From the Server IP drop-down list, choose the IP address or nickname of the server and click Display.
Step 3 To enable Network Interface Bonding for a server, check the **Enable NIC Bonding** check box and select the slave interfaces for the management interface bond.

**Note** The **Enable NIC Bonding** check-box is displayed only of NIC Bonding is enabled in **Maintain > Server > CDSM/VVIM Setup** page

Step 4 Enter the interface settings as appropriate. See Table 4-31 for descriptions of the fields.
### Table 4-31 Interface Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bond Interface Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Slave Interfaces</td>
<td>Select the slave interfaces for management interface bond.</td>
</tr>
<tr>
<td><strong>Interface Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Choose each interface setting as appropriate. See Table 4-30 for descriptions of the different interface types.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address for this interface. The IP address set for this interface overrides the default Source IP setting.</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>
</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>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask for this interface.</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>
</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>
</tr>
</tbody>
</table>

**Note** The Auto Populate IPs check box is available when the first applicable interface (for example, the first stream interface) is configured with an IP address. If the Setting has been selected for each of the remaining interfaces, checking the Auto Populate IPs check box and clicking Auto Populate Now automatically enters the next consecutive IP address as the IP Address for the next interface, and continues to populate all IP Address fields until they are all filled. Any preexisting IP addresses in the IP Address fields are overwritten.

**Step 5** Click Submit to save the settings.

To clear the fields and start over, click Reset.
Starting with VDS-TV Release 3.4, the Server Setup page is also used to configure the ISR.

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.

*Note*  If Bulk Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To export the configuration of this page for all VDS servers in the system, click **Export**. To import a Bulk Configuration XML file, click **Browse** to locate the file, then click **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 Import/Export Configuration**” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the Server Setup page and Interface Setup page, see Appendix B, “Creating Bulk Configuration Files.”

**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, ISR and ISV server. The ISV server setup page has a combination of the Vault and Streamer fields. See **Table 4-33** for descriptions of the fields and to which server they apply.

**Table 4-32** lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

---

**Table 4-32**  **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>
<tr>
<td>Vault Group ID on the Server Setup</td>
<td>arrayid</td>
</tr>
<tr>
<td>Stream Group ID on the Configuration Generator page</td>
<td>arrayid</td>
</tr>
</tbody>
</table>
### Table 4-33  Server Setup Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</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 that 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, ISR</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 Null Streaming drop-down list, choose Enabled to allow the streaming of null MPEG files, or Disabled to prevent the streaming of null MPEG files.</td>
<td>Streamer, ISV, ISR</td>
</tr>
<tr>
<td>Live Playback</td>
<td>Determines if the play for a session should start from LIVE point or 0 if play from NOW is sussted. This is applicable only for the first play command after session setup.</td>
<td>Streamer, ISR</td>
</tr>
<tr>
<td>Playlist Trick-mode Restriction</td>
<td>Informational only. Displays the settings for the Playlist Trick-mode Restrictions. For information on setting this field, see the “Configuring MPEG Tuning” section on page 4-17.</td>
<td>Streamer, ISV, ISR</td>
</tr>
<tr>
<td>Dynamic Trickmodes</td>
<td>Informational only. Displays the settings for the Dynamic Trickmodes. For information on setting this field, see the “Configuring MPEG Tuning” section on page 4-17.</td>
<td>Streamer, ISV, ISR</td>
</tr>
<tr>
<td>Playlist Range Conversion Mode</td>
<td>Informational only. Displays the settings for the Playlist Range Conversion Mode. For information on setting this field, see the “Configuring MPEG Tuning” section on page 4-17.</td>
<td>Streamer, ISV, ISR</td>
</tr>
<tr>
<td>STUN Play Error Delay</td>
<td>Session Traversal Utilities for NAT (STUN) Play Error Delay field is available when NAT is enabled through the CDSM Setup page. The NAT feature is part of the Stream Destination feature. NAT is available only for RTSP environments with the Cisco RTSP Deployment Type. See the “NAT Support” section on page F-5 for more information. The STUN Play Error Delay is the time allowed to complete the connectivity handshake between each callback to the control application by the CServer. The range is from 1 to 2999 milliseconds. The default is 1000.</td>
<td>Streamer, ISV</td>
</tr>
<tr>
<td>STUN Play Timeout</td>
<td>Session Traversal Utilities for NAT (STUN) Play Timeout field is available when NAT is enabled through the CDSM Setup page. The NAT feature is part of the Stream Destination feature. The STUN Play Timeout is the total time the CServer waits before the connectivity check fails. The range is from 1 to 299 seconds. The default is 10.</td>
<td>Streamer, ISV</td>
</tr>
</tbody>
</table>

### Default Stream/Cache Settings

<table>
<thead>
<tr>
<th>Default Stream/Cache Settings</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<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, ISR</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, ISR</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>
</tbody>
</table>
### Table 4-33  Server Setup Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ingest MPEG Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PID Standardization</td>
<td>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 4-15.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td>Sequence End Remove</td>
<td>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 4-15.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td>Rate Standardize</td>
<td>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 4-15.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td><strong>Fail Ingest Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fail Ingest Settings Status</td>
<td>Informational only. If the server settings are out of synchronization with the Fail Ingest configuration settings, a warning message to resubmit the Ingest Tuning page is displayed.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td><strong>Stream Group Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stream Group Stream Group ID</td>
<td>These fields display the Stream Group and Stream Group ID that 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 4-39.</td>
<td>Streamer, ISV, ISR</td>
</tr>
<tr>
<td>Streamer Is Cache</td>
<td>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 Streamers 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 4-59.</td>
<td>Streamer, ISV, ISR</td>
</tr>
<tr>
<td><strong>Cache Group Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cache Group 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 4-55.</td>
<td>Caching Node</td>
</tr>
<tr>
<td><strong>Vault Group Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vault Group 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 4-49.</td>
<td>Vault, ISV</td>
</tr>
<tr>
<td><strong>Jumbo Frames Support</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stream Jumbo Frames</td>
<td>By default, jumbo frames are disabled on stream interfaces. In this case, stream traffic adheres to standard frames, which 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, ISR</td>
</tr>
</tbody>
</table>
Cache Jumbo Frames

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.

Server Offload

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. For more information, see the “Offloading a Server” section on page 7-13.

Vault Mirror Copies

From the drop-down list, choose the number of copies of content to store in the Vaults in the array or site. **Vault Mirror Copies** defines the number of copies that should be maintained within the array. The range is from 0 to 10.

Vault Local Copies

From the drop-down list, choose the number of copies of content that are stored on this server. The range is from 1 to 4.

DSCP Marking Method

From the **DSCP Marking Method** drop-down list, select one of the following options:

- Simple
- AutoAF1x, AutoAF2x, AutoAF3x, or AutoAF4x
- Custom

For more information about the options and associated fields, see the “Configuring QoS Settings” section on page 4-89.

**Note**  DSCP can also be set for HTTP Streamers when HTTP is selected as the cache-fill protocol for VVI on the CDSM Setup page.

FTP Out Settings

**FTP Out Interface**

Choose either the **Management** interface or the **Ingest** interface as the FTP out interface. This setting is overridden by the interface the remote FTP client uses to send requests. The response to the FTP client request always uses the same interface the request came in on.

**FTP Out Bandwidth**

Enter the maximum bandwidth (in Mbps) allowed for FTP functionality. Valid entries are 0 to 1000 for 1-GigE FTP Out interfaces and 0 - 10000 for 10-GigE FTP Out interfaces.

**FTP Out Sessions**

Enter the maximum number of FTP out sessions allowed. The range is from 1 to 32.

Network Settings

**Gateway Device**

Choose one of the interfaces as default gateway device to the network. This configuration is reflected in `/etc/sysconfig/network` file.

**Note**  bond0 is listed as one of the interfaces if NIC bonding is enabled and management NIC bonding bond0 is configured.

**Gateway**

IP address of the gateway to the network.
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

The DSCP Marking Method field allows you to set one of the following marking methods:

- **Simple**
- **AF Class**
- **Custom**

#### Simple
The Simple DSCP Marking Method option allows you to set the DSCP for each of the following types of traffic:

- Control DSCP
- Data DSCP
- Stream DSCP

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. Control, data, or stream 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. DSCP is set separately for control, data, and stream traffic.

#### Custom
The Custom DSCP Marking Method option allows you to set the DSCP for each of the following types of traffic:

- Control Traffic
- Stream Traffic
- Highest Priority Retransmit Traffic
- Committed Rate Lost Packet Recovery
- Committed Rate Traffic
- Mirroring Lost Packet Recovery (Vault only)
- Mirroring Live Ingest Traffic
- Drive Failure Repair Traffic (Vault only)
- Mirroring Traffic (Vault only)
- Lowest Priority Data Smoothing Traffic (Vault only)

**AF Class**

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).

DSCP can also be set for HTTP Streamers when HTTP is selected as the cache-fill protocol for VVI on the CDSM Setup page.

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 4-34 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 4-34  **AF Class Drop Probability Configured on Each VDS Server**

<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 Individual Recorder Settings

The Shared Recorder Settings page is used to configure the Recorders in an nDVR system. For more information, see the “nDVR Support for NGOD Deployments” section on page 2-13.

Starting with VDS-TV Release 3.4, Recorder Setup page is used to configure the recording settings for an ISR.

The Recorder Setup page is used to set individual settings on a Recorder or a ISR and consists of parameters specific to each Recorder (for example, host name, gateway, component name, and model name), and shared parameters that can be individualized (for example, Recorder Manager IP address and port, communication intervals, and thresholds).

When a new Recorder is added to the VDS, the shared Recorder settings are applied to the new Recorder when the new Recorder is selected on the Recorder Setup page. To apply the shared Recorder settings to a new Recorder, choose Configure > Server Level > Recorder Setup, from the Recorder IP drop-down list, select the IP address of the Recorder, and click Display. When the process is complete, a message displays in the left-panel stating that the Shared Recorder Settings have been applied.

To configure individual settings on a Recorder, do the following:

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

**Note** If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To export the configuration of this page for all VDS servers in the system, click Export. To import a Bulk Configuration XML file, click Browse to locate the file, then click 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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file, see Appendix B, “Creating Bulk Configuration Files.”

**Step 2** From the Recorder IP drop-down list, choose the IP address or host name of the server and click Display. The Recorder Setup fields current settings are displayed with the shared settings displayed where applicable.

**Note** If you change the "Current Setting" for fields marked with a “*” those values will over-ride the Shared Recorder Settings (“Shared Settings” below) set on the Configure > System Level > Shared Recorder Settings page. To overwrite this Recorder’s current values with the Shared Recorder Settings click the Sync button below.

**Step 3** Enter the settings as appropriate. See Table 4-35 for descriptions of the fields.

<table>
<thead>
<tr>
<th><strong>Table 4-35</strong> Recorder Setup Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Recorder Management</td>
</tr>
<tr>
<td>Host Name</td>
</tr>
<tr>
<td>Gateway</td>
</tr>
</tbody>
</table>
Table 4-35  Recorder Setup Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP DSCP</td>
<td>DSCP value for the transmitted HTTP IP packet. The range is from 0 to 63 and</td>
</tr>
<tr>
<td></td>
<td>the default value is 36.</td>
</tr>
<tr>
<td>Recorder Status</td>
<td>Read-only field. Recorder status is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Operational</td>
</tr>
<tr>
<td></td>
<td>• Offline</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td>C2 HTTP Index Setting</td>
<td>Informational only. The C2 HTTP index is enabled or disabled.</td>
</tr>
<tr>
<td>Dynamic Trickmodes</td>
<td>Informational only. Displays the settings for the Dynamic Trickmodes.</td>
</tr>
<tr>
<td></td>
<td>For more information on setting this field, see the “Configuring MPEG</td>
</tr>
<tr>
<td></td>
<td>Tuning” section in the “Configuring the VDS” chapter of the Cisco</td>
</tr>
<tr>
<td>Recorder Behavior</td>
<td></td>
</tr>
<tr>
<td>Component Name</td>
<td>Read-only field. The system name given to this Recorder.</td>
</tr>
<tr>
<td>Model Name</td>
<td>Read-only field. The CDE model of this Recorder.</td>
</tr>
<tr>
<td>Recorder Manager</td>
<td>IP address of the Recorder Manager. The Recorder Manager port is port</td>
</tr>
<tr>
<td></td>
<td>number 80.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>IP address of NTP server.</td>
</tr>
<tr>
<td>Heartbeat Interval</td>
<td>Amount of time (in seconds) to wait between sending heartbeat messages</td>
</tr>
<tr>
<td></td>
<td>to the Recorder Manager. The range is from 2 to 30. The default is 5.</td>
</tr>
<tr>
<td>Recorder Location</td>
<td>Name of the location of the Recorder. The name can be from 1 to 128</td>
</tr>
<tr>
<td></td>
<td>characters in length.</td>
</tr>
<tr>
<td>Recording Modify</td>
<td>Time window (in seconds) before a recording starts in which an operator</td>
</tr>
<tr>
<td></td>
<td>can modify recording parameters; after which, any changes will be</td>
</tr>
<tr>
<td></td>
<td>rejected (except end time). The end time can be modified even after the</td>
</tr>
<tr>
<td></td>
<td>configured time window has passed.</td>
</tr>
<tr>
<td></td>
<td>If the change to the end time specifies a time that is before the current</td>
</tr>
<tr>
<td></td>
<td>time, the Recorder stops the recording.</td>
</tr>
<tr>
<td></td>
<td>The range is from 1 to 60. The default is 5.</td>
</tr>
<tr>
<td>SCTE-35 Ad Markers</td>
<td>Choose either to Retain or Discard the SCTE-35 Ad markers. If SCTE-35</td>
</tr>
<tr>
<td></td>
<td>markers are discarded, both the PID in the PMT and the data</td>
</tr>
<tr>
<td></td>
<td>are removed. If the SCTE-35 markers are preserved, the Recorder places</td>
</tr>
<tr>
<td></td>
<td>the SCTE-35 Ad markers in the index file.</td>
</tr>
<tr>
<td>Recorder Port</td>
<td>Port number on the Recorder used for management communications</td>
</tr>
<tr>
<td></td>
<td>with the Recorder Manager. The range is from 50005 to 65535. The default</td>
</tr>
<tr>
<td></td>
<td>is 50005.</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>Read-only field. Communication protocol version of the Recorder Manager</td>
</tr>
<tr>
<td></td>
<td>and the Recorder interface. The default is 1.</td>
</tr>
<tr>
<td>Threadpool Size</td>
<td>Read-only field. Number of message processing threads of the Recorder. The</td>
</tr>
<tr>
<td></td>
<td>default is 16.</td>
</tr>
<tr>
<td>Status Report Interval</td>
<td>Read-only field. How often (in seconds) the Recorder reports status</td>
</tr>
<tr>
<td></td>
<td>information to the Recorder Manager. The default is 60.</td>
</tr>
</tbody>
</table>
## Configuring the Route Table

The Route Table provides the ability to define multiple subnets on a server that apply 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 four different route types:

- **CServer Source** (written to the SubnetTable file)
- **CServer Destination** (written to the RoutingTable file)
- **Linux Destination**
- **Linux Source**

### Table 4-35  Recorder Setup Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Request Timeout</td>
<td>Read-only field. Time that the Recorder application waits for an HTTP request after it is signaled. The default is 5 seconds.</td>
</tr>
<tr>
<td>HTTP Response Timeout</td>
<td>Read-only field. Time that the Recorder application waits for an HTTP response. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

### Manager Notify Thresholds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Bandwidth</td>
<td>Threshold, as a percentage, for recording bandwidth. If this threshold is exceeded (that is, if the bandwidth used for ingesting recordings exceeds the configured percentage), the Recorder sends a notification to the Recorder Manager. The range is from 1 to 100. The default is 1.</td>
</tr>
<tr>
<td>Delivery Bandwidth</td>
<td>Threshold, as a percentage, for delivery bandwidth. If threshold is exceeded (that is, if the bandwidth used for delivering recordings exceeds the configured percentage), the Recorder sends a notification to the Recorder Manager. The range is from 1 to 100. The default is 1.</td>
</tr>
<tr>
<td>Storage Capacity</td>
<td>Threshold, as a percentage, for storage capacity. If threshold is exceeded (that is, if the disk storage used on the Recorder exceeds the configured percentage), the Recorder sends a notification to the Recorder Manager. The range is from 1 to 100. The default is 1.</td>
</tr>
</tbody>
</table>

### Location Virtual IP

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Virtual IP</td>
<td>IP address the Recorders use 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 in the “Product Overview” chapter of the <em>Cisco VDS-TV RTSP Software Configuration Guide, Release 4.4</em>.</td>
</tr>
<tr>
<td>Location Subnet Mask</td>
<td>Subnet mask for the Location Virtual IP.</td>
</tr>
</tbody>
</table>

**Step 4** Click **Submit** to save the settings.
Each route type has a different function, and each route type is written to a different file on the VDS server.

**Note**
Starting with VDS-TV Release 3.4, Stream Control Route type has been replaced with more general procedure of creating Linux Source and Linux Destination routes for Stream Control interface.

**Note**
You cannot have intersecting subnets for any defined routes for CServer Source or CServer Destination. Similarly, you cannot have intersecting subnets for any defined routes for Linux Source and Linux Destination subnets.

### 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 4-80), and IP addresses for the interfaces are set on the Server Setup page ("Configuring the Servers," page 4-85). **Figure 4-26** shows an example of interfaces configured for multiple subnets on a Streamer.

**Figure 4-26**  **Subnet Configuration Example on Streamer**

Table 4-36 shows the possible configuration settings to use to define the subnets described in Figure 4-26.

<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 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.
Chapter 4      Configuring the VDS

Server Level Configuration

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.

Linux Destination Route Type

Linux Destination Route is generalization of previously existing Stream Control Route and can be created independently of an interface. When Linux Destination is selected from the Route Type drop-down list, a corresponding Linux Source Route should also be created containing the IP’s of one of the interfaces (for example, a stream control interface, ethX) defined in the interface setup page, as well as containing the Linux Destination Route Gateway IP. The Linux Destination route is then written to the file route-ethX, which is used to add routes to the routing table when the system reboots.

Note: For Linux Destination, if a corresponding Linux Source route and/or corresponding interface is not present, a special route will not be created in the system and Default Gateway will be used. No route-ethX file will be written for such a Linux Destination route.

Linux Source Route Type

When Linux Source is selected from the Route Type drop-down list, a gateway for a Default Control interface whose IP address is contained in this network is defined. So, for a Default Control interface ethX with IP <ip3>, a Linux Source route should be defined that contains <ip3>. This route then gets written to the shared_intf_setp. A Linux Destination route is not necessary for the Default Control interface.

Configuring the SNMP Agent

The SNMP Agent sets up SNMP on the VDS. SNMP management features on the servers include:

- SNMPv1, SNMPv2c, and SNMPv3
- Standard MIBs

SNMPv3 adds support for user-password-based authentication and access control. SNMPv3 also optionally allows encryption of all SNMP communications, including objects contained in a response to a GET or inside traps (notifications or INFORMs).

While SNMPv3 provides multiple ways of implementing authentication, access control, and encryption, the VDS-TV software has the following implementation:

- User-Based Security Model, page 4-96
- View-Based Access Control Model, page 4-96

For more information about SNMP on the VDS, see Appendix D, “SNMP MIB and Trap Information.”
User-Based Security Model

The User-based Security Model (USM), which provides SNMP message-level security, is implemented as follows:

- Users are created (configured) in the SNMP agent on a VDS server through the CDSM GUI, as well as on the Network Management Station (NMS).
- Password-based authentication is optional, and if enabled, the user must have an associated authentication key (password) of a minimum length of eight characters, and an authentication protocol of either HMAC-MD5 or HMAC-SHA1.
- Encryption is optional, if enabled, an encryption key (a minimum of eight characters) is required, and an encryption protocol of DES or AES.

View-Based Access Control Model

The View-based Access Control Model (VACM) is used for controlling access to management information. The VDS-TV software implements VACM by allowing configuration of each management object (OID) or group of OIDs on a VDS server through the CDSM GUI to be exposed with read-only or read-write access to a configured user.

Note

The SNMPv2c security model that uses community strings for read-only or read-write access is still supported. SNMPv3 USM and VACM are optional.

Trap Community Enhancements

The configuration of a per-trap-sink community string or a default community string is supported. The supported notifications are: SNMPv1 TRAPs, SNMPv2 NOTIFICATIONS, and SNMPv2-inform INFORM. Each trap sink, associated with a different trap station, can have optional default community strings that are used when sending traps. Alternatively, a default trap community string can be configured, which is used if the per-station community string is not configured.

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.

*Note*  
If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To export the configuration of this page for all VDS servers in the system, click Export. To import a Bulk Configuration XML file, click Browse to locate the file, then click 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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the SNMP settings, see Appendix B, “Creating Bulk Configuration Files.”

**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 4-37.
Table 4-37  

<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>Default Trap Community</td>
<td>Default trap community string shared between this SNMP agent and a network management system that might receive traps.</td>
</tr>
</tbody>
</table>

### Community Authentication

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 that you are adding, read/write privileges are applied.</td>
</tr>
</tbody>
</table>

### User-based Security Model

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of a user defined in this SNMP agent (also known as SNMP engine). The same name is defined and used in a network management station (NMS).</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Protocol used for user authentication is either MD5 or SHA-1. Both are used in conjunction with HMAC. The default is MD5.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Password used for user authentication; the minimum length is eight characters.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Protocol used for encryption is either DES or AES. Note Encryption is not enabled unless Encryption is selected in the VACM Authentication drop-down list.</td>
</tr>
<tr>
<td>Encryption Password</td>
<td>Password used for encryption; the minimum length is eight characters.</td>
</tr>
</tbody>
</table>

### View-based Access-Control Model

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of user granted access to the specified object or OID sub-tree.</td>
</tr>
<tr>
<td>Access</td>
<td>Permissions granted to this user for this object or OID sub-tree is either read-only (GET) or read-write (GET/SET). Note Currently, VDS-TV objects support only GET requests.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication types available are the following:</td>
</tr>
<tr>
<td></td>
<td>• None—Only user name is matched, no passwords.</td>
</tr>
<tr>
<td></td>
<td>• Authentication—Password-based user authentication is used. Both username and password must match to get access.</td>
</tr>
<tr>
<td></td>
<td>• Encryption—Password-based user-authentication is used; additionally, SNMP traffic is encrypted.</td>
</tr>
<tr>
<td>OID</td>
<td>Specific object or OID sub-tree the user is able to access.</td>
</tr>
<tr>
<td>Note</td>
<td>If OID field is left blank, it means all OIDs are accepted.</td>
</tr>
</tbody>
</table>
To clear the fields and start over, click **Reset**.

### Configuration Rules and Guidelines for USM and VACM

The following rules and guidelines apply to configuring USM and VACM entries:

- There is a one-to-one relationship between a USM entry and a VACM entry.
- For every username in VACM, there must be a matching username in USM.
- All usernames must be unique for both USM and VACM entries.
- Only one OID per VACM username is allowed.
- If the VACM entry has an Authentication setting of **None**, then the USM password is not verified, which means the user is not required to enter the authentication password when accessing the OID associated with the corresponding VACM entry.
- If the VACM OID field is left blank, it means the user can access all OIDs.

---

**Note**

The Cisco VDS-TV MIBs, as well as the supporting Cisco 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 configure up to 16 domain suffixes and 16 DNS servers. 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 4-27).

*Note* If Bulk Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To export the configuration of this page for all VDS servers in the system, click Export. To import a Bulk Configuration XML file, click Browse to locate the file, then click 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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the DNS servers, see Appendix B, “Creating Bulk Configuration Files.”

**Figure 4-27 Server DNS Page**

To add a new Domain Name Suffix or DNS Server complete either of the fields below and click the Submit button. You may enter a max of 16 Domain or DNS entries. To remove a configured Domain Name Suffix or DNS Server check the box next to that entry and click the Delete Entry button at the bottom of the page. Any servers on this Cisco CSM that do not have an Array Level or Server Level DNS entry will use System Level DNS values. System or Array Level DNS values have been saved. You may override them by entering additional values below.

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

**Step 3** Enter the DNS Server Level settings as appropriate. See Table 4-38 for descriptions of the DNS fields.
Configuring the Server Level NTP

The NTP Server page is used to configure up to 16 NTP servers. The clocks on all VDS servers (Vault, Streamer, and Caching Node) and the CDSM and VVIM in a VDS must be synchronized 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**, **Import**, and **Export** buttons. To export the configuration of this page for all VDS servers in the system, click **Export**. To import a Bulk Configuration XML file, click **Browse** to locate the file, then click **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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the NTP servers, see Appendix B, “Creating Bulk Configuration Files.”

**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**.

---

**Table 4-38 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>
Other NTP Configurations

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

Setting the Time Zone on a VDS Server

To set the time zone on a VDS server, log in to the VDS 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:

**Step 1**
Log in to the CDSM or VVIM as root.

**Step 2**
Set the run levels for the NTP service.

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

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 VDS. Table 4-39 describes each type of deployment.

<table>
<thead>
<tr>
<th>Environment</th>
<th>RTSP Deployment Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorola</td>
<td>RTSP</td>
<td>Streamer acts as the RTSP client and the back office 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 back office 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 set-top communicates with the back office to create a VOD session. Upon completion, the set-top creates an RTSP session with the Streamers. The Streamer acts as an RTSP server and is responsible for accepting the request from the set-top.</td>
</tr>
<tr>
<td>EventIS</td>
<td>EventIS</td>
<td>The set-top communicates with the back office to initiate a purchase transaction and generate an entitlement ID. The set-top then initiates an RTSP session with the Streamer. The Streamer authenticates the entitlement ID with the back office 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 set-top. The EventIS deployment with “off vpath” is selected when control messages go through the back office before reaching the RTSP server, while the stream control messages go directly to the RTSP server.</td>
</tr>
<tr>
<td>Cable and IPTV</td>
<td>Cisco</td>
<td>Cisco RTSP defined protocol that supports both IPTV and cable set-tops. Uses “on vpath” communication.</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**, **Import**, and **Export** buttons. To export the configuration of this page for all VDS servers in the system, click **Export**. To import a Bulk Configuration XML file, click **Browse** to locate the file, then click **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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the RTSP settings, see Appendix B, “Creating Bulk Configuration Files.”

**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 4-28).

**Figure 4-28  RTSP Setup Page for RTSP Deployment**

<table>
<thead>
<tr>
<th>RTSP Setup configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a streamer IP from the list and click <strong>Display</strong> to view/edit the RTSP settings for that machine. Once displayed you may edit the settings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RTSP deployment: RTSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Looping Session Timeout: 0 milliseconds</td>
</tr>
<tr>
<td>Session Inactivity Timeout: 300000 milliseconds</td>
</tr>
<tr>
<td>Back-office Timeout: 0 milliseconds</td>
</tr>
<tr>
<td>RTSP Server IP: 16.1.2.34.118</td>
</tr>
<tr>
<td>RTSP Server Port: 554</td>
</tr>
<tr>
<td>Reconnect IP: 6.8.0.8</td>
</tr>
<tr>
<td>Reconnect Port:</td>
</tr>
<tr>
<td>Max History:</td>
</tr>
<tr>
<td>Log Level: high</td>
</tr>
<tr>
<td>Maintenance Mode: off</td>
</tr>
</tbody>
</table>

**Step 3**  Enter the RTSP settings as appropriate. Table 4-40 describes each field and lists the associated RTSP deployment.

*Note*  If you change any of the RTSP Setup settings, you must resubmit the Control/Setup IP page. For more information, see the “Configuring the Control and Setup IPs” section on page 4-64.
### Table 4-40  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 4-64.</td>
<td>All</td>
</tr>
<tr>
<td>Looping Session Timeout</td>
<td>Activity timeout value for looping streams (carousels). If a GET_PARAMETER request (heartbeat) is received from the back office 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, NGOD, IPTV, Quative, EventIS, Cisco</td>
</tr>
<tr>
<td>Session Inactivity Timeout</td>
<td>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, Cisco</td>
</tr>
<tr>
<td>Session Pause Timeout</td>
<td>The interval set for the repeatable pause timer. On expiry of the pause timer, the NGOD streaming server sends an <strong>ANNOUNCE code 2105 - Pause Timeout Reached</strong> over R2 and C1 interface anytime between the configured Session Pause Timeout and Session Pause Timeout + 30 seconds. The default value is 900000 milliseconds (15 minutes). The range is 0 to 3600000 milliseconds. Note: If the session pause timeout value is set between 1 to 30000 milliseconds, the session pause timeout value is considered internally as 30000 milliseconds. That is, ANNOUNCE code 2105 is sent on expiry of 30000 milliseconds, for values set between 1 and 30000 milliseconds. Note: If the session pause timeout value is set to 0, the pause timeout announce feature is disabled, that is, ANNOUNCE code 2105 is not sent on expiry of the session pause timer. Note: Restart RTSP service by executing <code>service rtsp restart</code> if the session pause timeout value is modified.</td>
<td>NGOD</td>
</tr>
<tr>
<td>Database Connect Size</td>
<td>Size of the database connection for the RTSP Servers/streamers. The default value is 2.</td>
<td>All</td>
</tr>
<tr>
<td>UDP Packet Size</td>
<td>Size of the UDP Packet can send/receive by the RTSP Server/streamer. The default value is 1400.</td>
<td>All</td>
</tr>
<tr>
<td>Threadpool Size</td>
<td>Maximum number of threads in the pool for RTSP Server/streamer. The default value is 32.</td>
<td>All</td>
</tr>
<tr>
<td>Max Sessions</td>
<td>Maximum number of stream sessions handled parallel by RTSP Server/Streamer. The default value is 3000.</td>
<td>All</td>
</tr>
</tbody>
</table>
### Table 4-40  RTSP Fields for All Deployment (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>RTSP Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Callback Server IP</td>
<td>IP address of the callback server. The VDS 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 (set-top initiated) and abnormal (timeout) terminations.</td>
<td>Quative</td>
</tr>
<tr>
<td>Callback Server Port</td>
<td>UDP port number of the callback server.</td>
<td>Quative</td>
</tr>
<tr>
<td>Backoffice Timeout</td>
<td>Timeout value for closing a connection to the back office. If a message is not received from the back office 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, Cisco</td>
</tr>
<tr>
<td>RTSP Server IP</td>
<td>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>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>Authentication Manager resides on the master Streamer. Typically, the Authentication Manager IP address is the same as that of the master Streamer. This field is only informational. To modify this field, see the “Configuring the Authentication Manager” section on page 4-14. The default is 7792.</td>
<td>EventIS, Cisco</td>
</tr>
<tr>
<td>Authentication Manager Port&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Authentication Manager port number is determined by the properties specifications of the Authentication Manager. If you need to change the port number, contact Cisco technical support. This field is only informational. If you must modify this field, see the “Configuring the Authentication Manager” section on page 4-14. The default is 7792.</td>
<td>EventIS, Cisco</td>
</tr>
</tbody>
</table>
| Bandwidth Manager IP<sup>1</sup> | Bandwidth Manager resides on the master Streamer. Typically, the Bandwidth Manager IP address is the same as that of the master Streamer.  
**Note** The Bandwidth Manager for the EventIS on vpath FSI Setup is not the same as the Bandwidth Manager for Thin Pipe Mapping. | EventIS on vpath                                                             |
| Bandwidth Manager Port<sup>1</sup> | Bandwidth Manager port number default is 7791. This port number is determined by the configuration settings in the Bandwidth Manager.                                                                 | EventIS on vpath                                                             |
| Backup Bandwidth Manager IP<sup>1</sup> | IP address of the network interface card (NIC) that you want the Bandwidth Manager to bind to in the event that the primary Bandwidth Manager IP and port fail.                                                                 | EventIS on vpath                                                             |
| Backup Bandwidth Manager Port<sup>1</sup> | 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. | EventIS on vpath                                                             |
### Table 4-40  RTSP Fields for All Deployment (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>RTSP Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Resource Manager IP</td>
<td>IP address used by the back office or Session Resource Manager (SRM) for communication of session control requests to the VDS RTSP server.</td>
<td>EventIS off vpath, Cisco</td>
</tr>
<tr>
<td>Session Resource Manager Port</td>
<td>Port number used by the back office or SRM for communication of session control requests to the VDS RTSP server.</td>
<td>EventIS off vpath, Cisco</td>
</tr>
<tr>
<td>Backup Session Resource Manager IP</td>
<td>IP address of the network interface card (NIC) that you want the SRM to bind to in the event that the primary SRM IP and port fail.</td>
<td>Cisco</td>
</tr>
<tr>
<td>Backup Session Resource Manager Port</td>
<td>Port number that you want the SRM to use in the event that the primary SRM IP and port fail.</td>
<td>Cisco</td>
</tr>
<tr>
<td>Stream Control IP</td>
<td>IP address used by the set-top for communication of trick-mode requests to the VDS 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>Port number used by the set-top for communication of trick-mode requests to the VDS 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 back office server. After a connection has been established with the back office for RTSP communication, sometimes the back office 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>IP address on the Streamer used to receive LSCP requests.</td>
<td>DSM-CC, NGOD</td>
</tr>
<tr>
<td>LSCP Listener Port</td>
<td>TCP port number on the Streamer that is listening for LSCP commands from the set-top. 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>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>
</tbody>
</table>
Step 4  Configure the clients that will communicate with the Streamer. The clients consist of the set-tops, which typically require only one client definition.

The client configuration is displayed in a delimited string format:

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

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

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

Table 4-41 describes the fields for the client definitions.

<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 and Cisco always use TCP transport.</td>
</tr>
</tbody>
</table>
Table 4-41  \textit{Client Configuration Fields (continued)}

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Client model type to use for communication with the client. The types are:</td>
</tr>
<tr>
<td></td>
<td>- nCUBE</td>
</tr>
<tr>
<td></td>
<td>- Digeo</td>
</tr>
<tr>
<td></td>
<td>- NGOD</td>
</tr>
<tr>
<td></td>
<td>- Myrio</td>
</tr>
<tr>
<td></td>
<td>- Quative</td>
</tr>
<tr>
<td></td>
<td>- EventIS</td>
</tr>
<tr>
<td></td>
<td>- Cisco</td>
</tr>
<tr>
<td></td>
<td>A client model of nCUBE means the client uses RTSP with nCUBE syntax.</td>
</tr>
<tr>
<td></td>
<td>A Digeo client model uses Digeo syntax, and so on.</td>
</tr>
</tbody>
</table>

Note If you change any of the RTSP Setup settings, you must resubmit the Control/Setup IP page. For more information, see the “Configuring the Control and Setup IPs” section on page 4-64.

Step 5  Click \textbf{Submit}.

To clear the fields and start over, click \textbf{Reset}.

---

**Configuring FSI Setup**

The File Service Interface (FSI) allows the back office 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 \textbf{Configure > Server Level > FSI Setup}. The FSI Setup page is displayed.

Note If Bulk Configuration is enabled, the \textbf{Configuration File Location} field is displayed, along with the \textbf{Browse}, \textbf{Import}, and \textbf{Export} buttons. To export the configuration of this page for all VDS servers in the system, click \textbf{Export}. To import a Bulk Configuration XML file, click \textbf{Browse} to locate the file, then click \textbf{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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the FSI settings, see Appendix B, “Creating Bulk Configuration Files.”
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.

Step 3  Enter the FSI settings as appropriate. See Table 4-42 for descriptions of the fields.

### Table 4-42  FSI Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSI IP Address</td>
<td>IP address of the Vault used in FSI communications with the back office. 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>Port number on the Vault used in FSI communications with the back office. The default is 20004.</td>
</tr>
<tr>
<td>FTP Client Port</td>
<td>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>Port used by FSI communications for egress (FTP out pulls) from the Vault. We recommend setting the FTP Out Server Port to 5500.</td>
</tr>
<tr>
<td>FTP Out Login TTL</td>
<td>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>FSI Content Root Path</td>
<td>Root directory used to store MPEG content files on the Vault. This field is used in both nABLE and NGOD RTSP deployments. The default is /files.</td>
</tr>
<tr>
<td>Note</td>
<td>The FSI Content Root Path must be set to /files; otherwise, the FSI process does not function correctly.</td>
</tr>
<tr>
<td>Async. Callback URL</td>
<td>For IPTV deployments only. The asynchronous callback URL is where the recording completion notification is sent when a scheduled recording completes its capture. This URL is basically used to tell the client the recording is completed.</td>
</tr>
</tbody>
</table>

Step 4  Click Submit.

To clear the fields and start over, click Reset.

---

### Configuring the Server Level Logging

All logs are located in the /arroyo/log directory. The log files are rotated at least once a day and time stamps are added to the filenames. Some log files that grow rapidly are rotated more frequently (determined by file size); this rotation may happen up to once an hour. Most log files have the following suffix: .log.<YYYYMMDD>. The time zone for log rotation and filename suffixes is coordinated universal time (UTC). As part of the new log entry format, the log level and facility are included.

All log entries have the following changes:

- Stream handle is represented in decimal format
- IP addresses are represented in dotted-decimal format
- Clear identification of where a stream is going rather than a MAC address
- Time is represented in UTC
- Global Object ID (GOID) is represented in hexadecimal

**Stream Trace**
Log messages currently in the streamevent.log file are converted to a structured message and assigned the “stream trace” facility number. Other messages that record stream creation, routing, or playout are converted to a structured message and assigned the “stream trace” facility number. This enhancement, along with configuring syslog-ng to direct all “stream trace” facility messages to a single, centralized log server, provides a coherent set of log messages that describe stream history.

**Facility Information, and Associated Log File and Debug Flags**
For information on each facility and associated log file and debug flags, use the `loginfo` tool. The `loginfo` tool can run on any VDS server, including the CDSM. Start a Telnet or SSH session, log in to the VDS server, and enter the `loginfo` command without any arguments. Information on each facility is listed.

**Configuring Logging Levels**
All logging is configured at the System Level or Server Level. The configuration of the logging levels at the Server Level overrides the System Level settings.

To set a log level for a facility at the Server Level, do the following:

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

**Note** If Bulk Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To export the configuration of this page for all VDS servers in the system, click **Export**. To import a Bulk Configuration XML file, click **Browse** to locate the file, then click **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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the Logging settings, see Appendix B, “Creating Bulk Configuration Files.”

**Step 2** From the **Server IP** drop-down list, select an IP address.

**Step 3** From the **Facility Name** drop-down list, select a facility and click **Display**. The Log Level fields are displayed.

The facilities list is based on the configuration of the system.
### Step 4
Enter the Log Level settings as appropriate. See Table 4-12 for descriptions of the fields.

#### Table 43 Log Level Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Local Log Level** | The Local Log Level drop-down list has the following options:  
  - Emergency (0)  
  - Alert (1)  
  - Critical (2)  
  - Error (3)  
  - Warning (4)  
  - Notice (5)  
  - Informational (6)  
  
  A log level setting includes all the more urgent levels. For example, if the log level is set to Error (3), then Alert (2), Critical (1), and Emergency (0) log entries are included as well as Error (3). |
| **Remote Log Level** | To enable remote logging for the selected facility, select the appropriate log level from the Remote Log Level drop-down list. The default setting is disable. |
| **Debug Flags** | Debug messages, if applicable, are configured by setting one or more debug flags. To select or unselect debug flags, you have the following options:  
  - To select one debug flag, click the flag.  
  - To select multiple debug flags, hold down the Ctrl key and click each flag, or hold down the Shift key and click the beginning flag and ending flag.  
  - To unselect a debug flag when a group of debug flags are selected, hold down the Ctrl key and click the flag. |

### Step 5
Click Submit.

To clear the fields and start over, click Reset.

To delete the log level settings for a facility, select the facility from the drop-down list and click Delete.
Chapter 4  Configuring the VDS

Server Level Configuration

Configuring the Server Level Syslog

The Syslog configuration page at the System Level and Server Level is used to configure the IP address and port of the server that is to receive remote logging. The configuration of the syslog server at the Server Level overrides the System Level settings. For remote logging information to be sent for a facility, the **Remote Log Level** must be set on the Logging page. See the “Configuring the Server Level Logging” section on page 4-110 for more information.

To configure the remote logging server, do the following:

---

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

---

**Note**  If Bulk Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To export the configuration of this page for all VDS servers in the system, click **Export**. To import a Bulk Configuration XML file, click **Browse** to locate the file, then click **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 Import/Export Configuration” section on page F-5. For information about the Bulk Configuration feature and creating a Bulk Configuration file for the Syslog settings, see Appendix B, “Creating Bulk Configuration Files.”

**Step 2**  From the **Server IP** drop-down list, select an IP address.

**Step 3**  Check the **Enable Remote Logging** check box.

**Step 4**  In the **IP Address** field, enter the IP address of the remote server that is to receive syslog messages.

**Step 5**  In the **Port** filed, enter the port of the remote server that is to receive syslog messages.

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

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

To delete the remote server settings, click **Delete**.
Configuring Server Level Error Repair

The VOD Error Repair settings can be configured on the System Level, Array Level, and the Server Level. Settings configured at the Array Level take precedence over System Level settings, and settings at the Server Level take precedence over Array Level or System Level settings.

Note

VOD Error Repair is a licensed feature. VOD Error Repair requires the LSCP Client Protocol be set to Cisco (RTSP) and the set-top have the Cisco Visual Quality Experience Client (VQE-C) software running on it. For more information, see the “VOD Error Repair” section on page F-9.

To configure error repair at the Server Level, do the following:

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

Step 2
From the Server IP drop-down list, select an IP address and click Display.

Step 3
Enter the Error Repair settings as appropriate. See Table 4-44 for descriptions of the fields.

Step 4
Click Submit.

To clear the fields and start over, click Reset.

To return the settings to the factory default values, click Factory.

To delete the settings, click Delete.

To monitor the VOD Error Repair feature, use the Application Monitoring Tool (AMT). For more information, see Appendix E, “Using the VDS-TV Streamer Application Monitoring Tool.”

Table 4-44 VOD Error Repair Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repair Packets DSCP</td>
<td>DSCP value for the transmitted RTP and RTCP packets sent for error repair.</td>
</tr>
<tr>
<td></td>
<td>The range is from 0 to 63. The default is 0.</td>
</tr>
<tr>
<td>RTCP Report Exporting</td>
<td>Click the Enabled radio button to enable exporting of the RTCP reports.</td>
</tr>
<tr>
<td></td>
<td>The RTCP reports can be exported to a third-party analysis application.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address or the domain name of the server hosting the analysis</td>
</tr>
<tr>
<td></td>
<td>application.</td>
</tr>
<tr>
<td>TCP Ports</td>
<td>Enter the TCP port number that is used to receive the reports on the server</td>
</tr>
<tr>
<td></td>
<td>hosting the analysis application.</td>
</tr>
</tbody>
</table>

Command Line Non-GUI Configuration

This section explains the following command line configuration:
Configuring Graceful End of Stream

When a user jumps over the end of stream, streaming is continued for a configurable number of seconds (grace period) before reaching end of stream. On reaching EOS, streamer plays from NPT calculated as (EOS - grace period)

To enable graceful end of stream, do the following:

1. Add a line `GRACE_EOS=5` in `/home/isa/bss/etc/rtsp.conf` file. (here 5 is an example value)
2. Restart RTSP application.
System Monitoring

The CDSM provides tools that can be used for system monitoring and system diagnostics.

- System Level Monitoring, page 5-1
- Monitoring Content Objects, page 5-17
- Monitoring Stream Objects, page 5-26
- Array Level Monitoring, page 5-30
- Server Level Monitoring, page 5-33
- Recommended Monitoring Schedule, page 5-44

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 F-10.

System Level Monitoring

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

- System Health, page 5-3
- System Snapshot, page 5-5
- System Failures, page 5-6

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.
Alarms Table

Any time there is an alarmed event, an alarm is displayed in the CDSM banner. The Alarms table is displayed when you roll your mouse over the alarm icon. See Figure 5-1. Clicking the alarmed event in the Alarm table 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

The following errors and situations are monitored and registered in the Alarms table if found, and linked to the System Cleanup page:

- Orphaned server IDs
- Multiple or duplicate Cache Locate IP addresses
- Out of range Group IDs
- ServerMap and StatMap inconsistencies
- Extra or incorrect SERVERMAP15 entries

See the “System Cleanup” section on page 7-30 for more information.

In addition to the System Cleanup page links, the following situations are monitored and registered in the Alarms table:

- System clock is out of synchronization
- MSA events exist for the current CDSM day
- Incorrect IDs on the Stream Manager (for ISA environments only)
- Missing or incorrect initial IDs (Group, Server, and Setup)
- Primary VDS server (Vault, Setup, Control) fails over to another VDS server.
- Primary CDSM fails and secondary CDSM becomes the primary
- Primary and secondary CDSM port failures
- Primary and secondary CDSM Linux file system threshold exceeded

System Clock Not Synchronized

If a VDS server system clock is off from that of the CDSM (VVIM or Stream Manager) by more than two minutes, an alert is added to the Alarms table. Clicking the alert takes you to the Configure > System Level > System NTP Server page.

MSA Events

If MSA events exist (System Failures) for the current CDSM day, an alert is added to the Alarms table. Clicking the alert takes you to the Monitor > System Level > System Failures page.
Incorrect IDs on Stream Manager in ISA environment

If VVI is enabled in an ISA environment and you logged in to the Stream Manager, and if there are errors associated with the IDs; an alert is added to the Alarms table. Clicking the alert takes you to the Maintain > Software > ID Manager page.

Missing or Incorrect Initial IDs

If the CDSM is initially configured incorrectly as a legacy VDS or VVI with central management, then reconfigured or reinstalled for a VVIM or Stream Manager, the starting IDs for group IDs, server IDs, and setup IDs need to be changed from the old system to the new system. An alert is added to the Alarms table to inform you of the situation. Clicking the alert takes you to the Maintain > Software ID Management page to correct the situation.

System Health

The System Health page provides a top-level view of the overall health of each group in the VDS and each server in each group.

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

The colored boxes for each group on the System Health Monitor page have the following meaning:

- Green—All servers in the group are operating.
- Yellow—One or more servers are not operational, but have not reached any thresholds.
- Red—One or more servers are not operational and have reached a threshold.

To view the VDS servers for each group, click the plus sign (+) for the group. The VDS servers for the group are displayed, along with the IP address or hostname, software version, and server role of each VDS server. If a server is currently acting as one of the following server roles, an icon is displayed next to that server indicating the specific role:

- Stream Setup
- Stream Control
- Setup/Control
• Vault Master
• Primary CDSM/VVIM
• Backup CDSM/VVIM

The Server Role legend is displayed in the left-panel.

The colored boxes for each server on the System Health Monitor page have the following meaning:

• Green—All components are operating.
• Yellow—Some components are not operational, but have not reached a threshold.
• Red—Some components are not operational and have reached a threshold.

The servers can have the following states:

• Online —Server is operational.
• Down—Server is down or database is down.
• No Ingest—Vault is offline for ingest (still accepting cache-fill traffic)
• Offline—Vault is offline for all traffic (ingest and cache-fill), Streamer or Caching Node is offline.

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 5-35 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 5-33 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 5-42 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 5-37 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 F-20.

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 VDS. A summary of the state of all streams, content ingests, and disk usage is displayed. See Figure 5-3. **System Snapshot Page**

![System Snapshot Page](image)

In a VVI, the Stream Manager only displays the stream-related date and the VVIM only displays the bandwidth and content-related data.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Refresh Rate</td>
<td>How often the information is refreshed. The default is 30 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 VDS is currently streaming.</td>
</tr>
<tr>
<td>HD Streams</td>
<td>Total number of high-definition stream objects the VDS is currently streaming.</td>
</tr>
<tr>
<td>SD Streams</td>
<td>Total number of standard-definition stream objects the VDS is currently streaming.</td>
</tr>
</tbody>
</table>
To view the details of system failures, do the following:

**Step 1** Choose Monitor > System Level > System Failures. The System Failures page is displayed.

Each system failure is listed by date and time, followed by the session ID.

**Note** Stream Failure monitoring displays only the system failures for the current day. To view past system failures, see the “System Failures” section on page 6-25.

**Step 2** From the System Failures drop-down list, choose the time stamp and session ID of the stream object and click Display. The system failure details are displayed. See Figure 5-4.

To delete a system failure, display the object and click Delete.
Table 5-2 describes the stream failure details.

**Table 5-2  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. To view the IP address associated with the Server ID, see the “Configuring the Servers” section on page 4-85.</td>
</tr>
<tr>
<td>Group ID</td>
<td>All servers that are part of the same VDS system (managed by one CDSM) have the same Group ID. This Group ID corresponds to the CDSM GUI array ID and should be unique across an enterprise. Table 5-3 describes the ID mapping 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>
</tbody>
</table>
Table 5-3 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and \texttt{.arroyorc} files.

<table>
<thead>
<tr>
<th>CDSM GUI ID Name</th>
<th>Description</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>

Table 5-3 lists the Managed Services Architecture (MSA) error codes. Some MSA monitored events are monitored for the VDS as well, and are prefaced by “AVS_” instead of “MSA_.” They are denoted with a footnote in the table. Some MSA monitored events are not errors, but rather information about an event. Not all MSA events trigger an SNMP trap.

Table 5-4 lists the Managed Services Architecture (MSA) error codes. Some MSA monitored events are monitored for the VDS as well, and are prefaced by “AVS_” instead of “MSA_.” They are denoted with a footnote in the table. Some MSA monitored events are not errors, but rather information about an event. Not all MSA events trigger an SNMP trap.

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5001</td>
<td>MSA_INT_ERR$^1$</td>
<td>There is an internal error. INT_ERR has a subset of error codes that specifically describe where the error occurred. See Table 5-5.</td>
</tr>
<tr>
<td>5002</td>
<td>MSA_FLOW$^1$</td>
<td>Entry or exit of a measured or tracked flow, or some other important check point, and is recorded as non-realtime.</td>
</tr>
<tr>
<td>5003</td>
<td>MSA_CMPT_NOT_EXIST$^1$</td>
<td>Component does not exist.</td>
</tr>
<tr>
<td>5004</td>
<td>MSA_REQ_TIMEOUT$^1$</td>
<td>Client timed out waiting for a response to a request.</td>
</tr>
</tbody>
</table>
### Table 5-4  MSA Error Codes (continued)

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5005</td>
<td>MSA_CMPT_OUT_OF_SVC1</td>
<td>Component is unavailable.</td>
</tr>
<tr>
<td>5006</td>
<td>MSA_REQ_NOT_IMPL1</td>
<td>Requested item is not implemented.</td>
</tr>
<tr>
<td>5007</td>
<td>MSA_RES_INVALID1</td>
<td>Resource is invalid.</td>
</tr>
<tr>
<td>5008</td>
<td>MSA_RES_DUP1</td>
<td>Duplicate resource is being added to the session.</td>
</tr>
<tr>
<td>5009</td>
<td>MSA_CMPT_DUP</td>
<td>It was determined that a component that was being added has the same name as a previously created component.</td>
</tr>
<tr>
<td>5010</td>
<td>MSA_REQ_CREATE</td>
<td>Attempt to create a request failed.</td>
</tr>
<tr>
<td>5011</td>
<td>MSA_UNKNOWN</td>
<td>Unclassified or undetermined error occurred.</td>
</tr>
<tr>
<td>5012</td>
<td>MSA_REAP</td>
<td>Component is destroyed outside of the normal expected flows.</td>
</tr>
<tr>
<td>5013</td>
<td>MSA_VS_LSC_TIMEOUT</td>
<td>Video server timed out waiting for the client to issue a resume or play command after the initial creation of the stream.</td>
</tr>
<tr>
<td>5014</td>
<td>MSA_SVC_GROUP_MISSING</td>
<td>Request contains a missing service group.</td>
</tr>
<tr>
<td>5015</td>
<td>MSA_RES_NO_CAPACITY</td>
<td>Resource is currently out of capacity and cannot satisfy the request.</td>
</tr>
<tr>
<td>5016</td>
<td>MSA_RES_NO_BANDWIDTH</td>
<td>Resource does not have the bandwidth to deliver the stream.</td>
</tr>
<tr>
<td>5017</td>
<td>MSA_REQ_FAIL</td>
<td>Request failed.</td>
</tr>
<tr>
<td>5018</td>
<td>MSA_RES_UNAVAIL</td>
<td>Response is not available.</td>
</tr>
<tr>
<td>5019</td>
<td>MSA_FLOW_RT</td>
<td>Entry or exit of a measured or tracked flow, and is recorded in real-time.</td>
</tr>
<tr>
<td>5020</td>
<td>MSA_LSC_SERVER_FAILURE</td>
<td>LSC response; server failed.</td>
</tr>
<tr>
<td>5021</td>
<td>MSA_LSC_NO_MEMORY</td>
<td>LSC response; dynamic memory allocation failure.</td>
</tr>
<tr>
<td>5022</td>
<td>MSA_LSC_IMPL_LIMIT</td>
<td>LSC response; implementation limit exceeded.</td>
</tr>
<tr>
<td>5023</td>
<td>MSA_LSC_NO_RESOURCES</td>
<td>LSC response; no resources.</td>
</tr>
<tr>
<td>5024</td>
<td>MSA_LSC_SERVER_ERROR</td>
<td>LSC response; server error.</td>
</tr>
<tr>
<td>5025</td>
<td>MSA_LSC_MPEG_DELIVERY</td>
<td>LSC response; unable to deliver MPEG stream.</td>
</tr>
<tr>
<td>5026</td>
<td>MSA_LSC_ERR</td>
<td>Generic DSM-CC error event.</td>
</tr>
<tr>
<td>5027</td>
<td>MSA_LSC_BAD_REQUEST</td>
<td>LSC response; invalid request.</td>
</tr>
<tr>
<td>5028</td>
<td>MSA_LSC_BAD_STREAM</td>
<td>LSC response; invalid stream handle.</td>
</tr>
<tr>
<td>5029</td>
<td>MSA_LSC_WRONG_STATE</td>
<td>LSC response; wrong state.</td>
</tr>
<tr>
<td>5030</td>
<td>MSA_LSC_UNKNOWN</td>
<td>LSC response; unknown error.</td>
</tr>
<tr>
<td>5031</td>
<td>MSA_LSC_NO_PERMISSION</td>
<td>LSC response; client does not have permission for the request.</td>
</tr>
<tr>
<td>5032</td>
<td>MSA_LSC_BAD_PARAM</td>
<td>LSC response; invalid parameter.</td>
</tr>
<tr>
<td>5033</td>
<td>MSA_LSC_NO_IMPL</td>
<td>LSC response; not implemented.</td>
</tr>
<tr>
<td>5034</td>
<td>MSA_LSC_TRANSIENT</td>
<td>LSC response; transient error.</td>
</tr>
<tr>
<td>5035</td>
<td>MSA_LSC_BAD_SCALE</td>
<td>LSC response; incorrect scale value.</td>
</tr>
<tr>
<td>5036</td>
<td>MSA_LSC_BAD_START</td>
<td>LSC response; stream start time does not exist.</td>
</tr>
<tr>
<td>5037</td>
<td>MSA_LSC_BAD_STOP</td>
<td>LSC response; stream stop time does not exist.</td>
</tr>
<tr>
<td>9001</td>
<td>MSA_INGEST_INIT</td>
<td>FSI not able to ingest due to FTP init error.</td>
</tr>
</tbody>
</table>
Table 5-5 lists the error codes for internal errors and external errors. Internal errors are errors that occurred in the VDS and specifically describe where the error occurred. External errors are errors that occurred in the network or network components, which includes the ContentStore, StreamService, and so on. The error codes listed in Table 5-5 provide more detail to the MSA_INT_ERR or AVS_INT_ERR error code.

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9002</td>
<td>MSA_CONTENT_ALREADY</td>
<td>FSI denies ingest request as there is already an active ingest for the same content.</td>
</tr>
<tr>
<td>9004</td>
<td>MSA_INGEST_CANCELED</td>
<td>FTP transfer canceled.</td>
</tr>
<tr>
<td>9005</td>
<td>MSA_UNKNOWN_ERROR</td>
<td>Unknown error. This could be due to content not found in database or other failures.</td>
</tr>
<tr>
<td>9006</td>
<td>MSA_ALLOC_ERROR</td>
<td>FSI not able to ingest due to memory allocation failure.</td>
</tr>
<tr>
<td>9007</td>
<td>MSA_FILLCB_FAILED</td>
<td>FSI not able to ingest as Cserver not able to fill data from FTP.</td>
</tr>
<tr>
<td>9008</td>
<td>MSA_ICONTENT_FAILED</td>
<td>FSI not able to ingest due to Cserver content array length out of bound error.</td>
</tr>
<tr>
<td>9009</td>
<td>MSA_INGEST_FAILED</td>
<td>General ingest failure.</td>
</tr>
<tr>
<td>9010</td>
<td>MSA_INGEST_DIST_ERROR</td>
<td>FSI unable to talk to FSI in other vaults. Check connections between vaults.</td>
</tr>
</tbody>
</table>

1. This event is monitored by the VDS as well as MSA, and is displayed with the prefix “AVS_” instead of “MSA_.

Table 5-5 MSA Error Codes (continued)

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>INGEST_THREADS_NOT_RUNNING</td>
<td>Cache server threads are not running.</td>
</tr>
<tr>
<td>1002</td>
<td>INGEST_NIC_DOWN</td>
<td>Ingest interface is disabled.</td>
</tr>
<tr>
<td>1003</td>
<td>INGEST_DATA_BLOCKAGE</td>
<td>Ingest data read is backlogged, causing data socket blockage.</td>
</tr>
<tr>
<td>1004</td>
<td>BAD_CONTENT</td>
<td>Content data is not recoverable.</td>
</tr>
<tr>
<td>1005</td>
<td>NOT_ENOUGH_NIC_BANDWIDTH</td>
<td>Not enough bandwidth left over on NICs to perform the operation.</td>
</tr>
<tr>
<td>1006</td>
<td>NOT_ENOUGH_SYSTEM_RESOURCES</td>
<td>Not enough system resources left to perform the operation.</td>
</tr>
<tr>
<td>1007</td>
<td>NOT_ENOUGH_DISK_SPACE_AVAILABLE</td>
<td>Not enough disk space available.</td>
</tr>
<tr>
<td>1008</td>
<td>STREAMER_MAX_SLOTS_LIMIT_EXCEEDED</td>
<td>No stream slot available to allocate the stream.</td>
</tr>
<tr>
<td>1009</td>
<td>REMOTE_VAULT_DOWN</td>
<td>Remote Vault is not responding.</td>
</tr>
<tr>
<td>1010</td>
<td>REMOTE_STREAMER_DOWN</td>
<td>Remote Streamer is down.</td>
</tr>
<tr>
<td>1011</td>
<td>VAULT_DISK_BAD</td>
<td>Disk is bad on a Vault.</td>
</tr>
</tbody>
</table>
### Chapter 5      System Monitoring

#### System Level Monitoring

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1012</td>
<td>STREAMER_DISK_BAD</td>
<td>Disk is bad on a Streamer.</td>
</tr>
<tr>
<td>1013</td>
<td>CONTENT_LOCATE_FAILED</td>
<td>Cannot locate the content on any Vault.</td>
</tr>
<tr>
<td>1014</td>
<td>CONTENT_FILL_FAILED</td>
<td>Cannot push content to the Streamer from Vault.</td>
</tr>
<tr>
<td>1015</td>
<td>NOT_ENOUGH_FILL_BANDWIDTH</td>
<td>Not enough fill bandwidth available.</td>
</tr>
<tr>
<td>1016</td>
<td>FILL_LINKS_DOWN</td>
<td>Fill links are down.</td>
</tr>
<tr>
<td>1017</td>
<td>STREAMING_LINKS_DOWN</td>
<td>Stream links are down.</td>
</tr>
<tr>
<td>1018</td>
<td>VAULT_MIRRORING_SITE_DOWN</td>
<td>Mirroring site of the Vault array is down.</td>
</tr>
<tr>
<td>1019</td>
<td>SET_CONTENT.Bundle_FAILED</td>
<td>Set content bundle descriptor array failed.</td>
</tr>
<tr>
<td>1020</td>
<td>SET_DESTINATION_FAILED</td>
<td>Set destination of stream failed.</td>
</tr>
<tr>
<td>1021</td>
<td>DESTROY_STREAM_FAILED</td>
<td>Destroy stream failed.</td>
</tr>
<tr>
<td>1022</td>
<td>PLAY_STREAM_FAILED</td>
<td>Play stream failed.</td>
</tr>
<tr>
<td>1023</td>
<td>FILLCB_FAILED</td>
<td>Fill CB failed.</td>
</tr>
<tr>
<td>1024</td>
<td>WAIT_FOR_FTP_DATA_DONE_FAILED</td>
<td>Wait for FTP data done failed.</td>
</tr>
<tr>
<td>1025</td>
<td>GET_CURRENT_NPT FAILED</td>
<td>Get current NPT for LSCP status failed.</td>
</tr>
<tr>
<td>2001</td>
<td>CAN_NOT_CONNECT_TO_NAME_SERVICE</td>
<td>Cisco ISA cannot connect to the BMS Naming Server.</td>
</tr>
<tr>
<td>2002</td>
<td>CAN_NOT_CONNECT_TO_NOTIFY_SERVICE</td>
<td>Cisco ISA cannot connect to the Notify Server.</td>
</tr>
<tr>
<td>2003</td>
<td>CAN_NOT_CREATE_EVENT_CHANNELS</td>
<td>Cisco ISA cannot create event channels.</td>
</tr>
<tr>
<td>2004</td>
<td>NO_CONTENT_EVENT_CHANNEL_FOUND</td>
<td>Naming server does not have content event channel.</td>
</tr>
<tr>
<td>2005</td>
<td>NO_STREAM_EVENT_CHANNEL_FOUND</td>
<td>Naming server does not have stream event channel.</td>
</tr>
<tr>
<td>2006</td>
<td>EVENT_CHANNEL_OBJECT_NOT_EXISTS</td>
<td>Event channel object does not exist in Notify Server.</td>
</tr>
<tr>
<td>2007</td>
<td>CORBA_CONNECTION_FAILED</td>
<td>CORBA System exception while connecting to other entity.</td>
</tr>
<tr>
<td>2008</td>
<td>CORBA_BROKEN_PIPE</td>
<td>CORBA system exception with broken pipe with other entity.</td>
</tr>
<tr>
<td>2009</td>
<td>CORBA_CONTENT_STORE_BIND_FAILED</td>
<td>CORBA bind exception while starting Cisco ContentStoreFactory.</td>
</tr>
<tr>
<td>2010</td>
<td>CORBA_STREAM_SERVICE_BIND_FAILED</td>
<td>CORBA bind exception while starting Cisco StreamService.</td>
</tr>
<tr>
<td>2011</td>
<td>CORBA_SYSTEM_ERROR</td>
<td>CORBA system exception while connecting to the servant.</td>
</tr>
<tr>
<td>2012</td>
<td>CORBA_TRANSIENT_ERROR</td>
<td>CORBA system exception with object being transient.</td>
</tr>
<tr>
<td>2013</td>
<td>CORBA_TIMEOUT_ERROR</td>
<td>CORBA timeout exception.</td>
</tr>
<tr>
<td>2014</td>
<td>CORBA IOR NIL</td>
<td>Orb object is nil.</td>
</tr>
<tr>
<td>2015</td>
<td>CORBA IOR NIL AFTER_NARROW</td>
<td>Orb object is nil after narrow.</td>
</tr>
<tr>
<td>2021</td>
<td>SERVICE_GROUP_NOT_SUPPORTED</td>
<td>Service group is not supported.</td>
</tr>
<tr>
<td>2022</td>
<td>REMOTE_CONTENT_STORE_FACTORY_DOWN</td>
<td>Remote Cisco ContentStoreFactory is down.</td>
</tr>
<tr>
<td>Numeric Error Code</td>
<td>Error Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>2023</td>
<td>VAULT_HAS_FULL_LOAD</td>
<td>Vault is running with full load.</td>
</tr>
<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>2028</td>
<td>NO_LSCP_SET_TOP_CONNECTION</td>
<td>LSCP server to set-top connection is down.</td>
</tr>
<tr>
<td>2029</td>
<td>LSCP_SERVER_BIND_FAILED</td>
<td>LSCP server cannot bind to the running port.</td>
</tr>
<tr>
<td>2030</td>
<td>LSCP_PROXY_BIND_FAILED</td>
<td>LSCP proxy cannot bind to the running port.</td>
</tr>
<tr>
<td>2031</td>
<td>STREAMER_GROUP_MAX_LIMIT_EXCEEDED</td>
<td>Stream count is exceeding the limit for the Streamer group.</td>
</tr>
<tr>
<td>2032</td>
<td>STREAMER_MAX_LIMIT_EXCEEDED</td>
<td>Stream count is exceeding the limit for a Streamer.</td>
</tr>
<tr>
<td>2033</td>
<td>REMOTE_STREAMER_NOT_RESPONDING</td>
<td>Remote Streamer is down.</td>
</tr>
<tr>
<td>2034</td>
<td>NOT_ENOUGH_MQAM_BANDWIDTH</td>
<td>Not enough MQAM bandwidth.</td>
</tr>
<tr>
<td>2035</td>
<td>NO_QAM_FOR_SERVER_ID</td>
<td>Server is not connected to any QAM.</td>
</tr>
<tr>
<td>2036</td>
<td>NOT_ENOUGH_QAM_BANDWIDTH</td>
<td>Not enough QAM bandwidth.</td>
</tr>
<tr>
<td>2037</td>
<td>STREAMER_IS_NOT_IN_THE_SERVICE_GROUP</td>
<td>Streamer is not in the service group.</td>
</tr>
<tr>
<td>2038</td>
<td>STREAMER_HAS_FULL_LOAD</td>
<td>Streamer is running with full load.</td>
</tr>
<tr>
<td>2039</td>
<td>STREAMER_IS_NOT_CONNECTED_THAT_QAM</td>
<td>Server is not connected to the QAM.</td>
</tr>
<tr>
<td>2040</td>
<td>INVALID_SERVICE_GROUP</td>
<td>Service group is not returned by session gateway.</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>2042</td>
<td>CONTENT_OBJECT_NOT_YET_PROVISIONED</td>
<td>Content object is not yet provisioned.</td>
</tr>
<tr>
<td>2043</td>
<td>STREAM_OBJECT_NOT_YET_PROVISIONED</td>
<td>Stream object is not yet provisioned.</td>
</tr>
<tr>
<td>2044</td>
<td>STREAM_OBJECT_IS_OUT_OF_SERVICE</td>
<td>Stream object is out of service.</td>
</tr>
<tr>
<td>2045</td>
<td>STREAM_OBJECT_IS_ALREADY_PROVISIONED</td>
<td>Stream object is already in service.</td>
</tr>
<tr>
<td>2046</td>
<td>CONTENT_OBJECT_IS_ALREADY_PROVISIONED</td>
<td>Content object is already in service.</td>
</tr>
<tr>
<td>2047</td>
<td>STREAM_SERVANT_OBJECT_NOT_EXIST</td>
<td>Remote streamer does not have a servant for stream object.</td>
</tr>
<tr>
<td>2048</td>
<td>NO_DESTINATION_QAM_IP_FOUND</td>
<td>No QAM IP Address is received for the stream destination.</td>
</tr>
<tr>
<td>2049</td>
<td>NO_DESTINATION_QAM_PORT_FOUND</td>
<td>No QAM port is received for the stream destination.</td>
</tr>
<tr>
<td>2050</td>
<td>FAILED_TO_SET_STREAM_DESTINATION</td>
<td>Some error occurred while setting the stream destination.</td>
</tr>
<tr>
<td>2051</td>
<td>UNABLE_TO_ACCEPT_CONNECTION</td>
<td>Cannot accept more TCP connections.</td>
</tr>
<tr>
<td>2052</td>
<td>UNABLE_TO_REGISTER_EVENT_HANDLER</td>
<td>Cannot register event handle to serve the TCP connection.</td>
</tr>
<tr>
<td>2053</td>
<td>CAN_NOT_LOCATE_QAM_IP_FOR_TSID_IN</td>
<td>Cannot locate the QAM IP addresses associated with TSID IN.</td>
</tr>
</tbody>
</table>
Table 5-6 lists the error codes for errors that could occur during ingest or during trick-mode file creation, which cause system failures.

### INT_ERR Error Codes (continued)

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2099</td>
<td>NS_LOG_MONITOR_ERROR</td>
<td>Ns_log file is not updating. Restart the ISA service.</td>
</tr>
<tr>
<td>2100</td>
<td>AVS_ISA_GENERIC_ERROR</td>
<td>Some unknown error occurred during execution of the operation.</td>
</tr>
<tr>
<td>3001</td>
<td>CACHE2APP_INITIALIZER_ERROR</td>
<td>Failed to initialize Cache2App library.</td>
</tr>
<tr>
<td>3002</td>
<td>FILLCB_FAILED</td>
<td>FillCB failed during content ingest.</td>
</tr>
<tr>
<td>3003</td>
<td>DESTROYCB_FAILED</td>
<td>Failed while destroying the content bundle descriptor.</td>
</tr>
<tr>
<td>3004</td>
<td>WAIT_FOR_FTP_DATA_DONE_FAILED</td>
<td>API wait for FTP data done has returned an error.</td>
</tr>
<tr>
<td>3005</td>
<td>SET_CONTENT_BUNDLE_DESCRIPTOR_FAILED</td>
<td>Failed while setting content bundle descriptor for a stream.</td>
</tr>
<tr>
<td>3006</td>
<td>SET_DESTINATION_FAILED</td>
<td>Failed while setting destination of the stream.</td>
</tr>
<tr>
<td>3007</td>
<td>SET_ENCRYPTION_KEY_FAILED</td>
<td>Failed while setting ECM keys for the stream.</td>
</tr>
<tr>
<td>3008</td>
<td>CREATE_STREAM_FAILED</td>
<td>AVS cache server cannot allocate the stream handle.</td>
</tr>
<tr>
<td>3009</td>
<td>DESTROY_STREAM_FAILED</td>
<td>AVS cache server cannot tear down the stream.</td>
</tr>
<tr>
<td>3010</td>
<td>DESTROY_REMOTE_STREAM_FAILED</td>
<td>AVS cache server cannot tear down stream on remote server.</td>
</tr>
<tr>
<td>3011</td>
<td>PLAY_STREAM_FAILED</td>
<td>AVS cache server cannot play the stream.</td>
</tr>
<tr>
<td>4001</td>
<td>DATABASE_DOWN</td>
<td>Database is down.</td>
</tr>
<tr>
<td>4002</td>
<td>DATABASE_SYNCHRONIZING_REPLICATION_Q</td>
<td>Database is synchronizing with replication queue.</td>
</tr>
<tr>
<td>4003</td>
<td>DATA_IS_NOT_IN_SYNC</td>
<td>Database is not in sync with master.</td>
</tr>
<tr>
<td>4004</td>
<td>DATABASE_RETURNED_ERROR</td>
<td>Database has returned an error; maybe because there is no record found.</td>
</tr>
<tr>
<td>4005</td>
<td>DATABASE_RECORD_NOT_FOUND</td>
<td>Record is not found in the database.</td>
</tr>
<tr>
<td>4006</td>
<td>DATABASE_CAN_NOT_INSERT_RECORD</td>
<td>Record cannot be inserted into the database.</td>
</tr>
<tr>
<td>4007</td>
<td>DATABASE_CAN_NOT_DELETE_RECORD</td>
<td>Record cannot be deleted from the database.</td>
</tr>
<tr>
<td>4008</td>
<td>DATABASE_CAN_NOT_UPDATE_RECORD</td>
<td>Record cannot be updated.</td>
</tr>
<tr>
<td>4009</td>
<td>DATABASE_QUERY_SEND_ERROR</td>
<td>Failed to make a query to the database.</td>
</tr>
</tbody>
</table>

### 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>
</tbody>
</table>
## Table 5-6  MPEG Error Codes (continued)

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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_CDN_AVC_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 or check interface bandwidth limits.</td>
</tr>
<tr>
<td>8021</td>
<td>TRICK_INGEST_FIRST_PTS_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_CANCELLED</td>
<td>PIDs could not be standardized. Check ingest feed.</td>
</tr>
<tr>
<td>8026</td>
<td>TRICK_INGEST_OVERFLOW</td>
<td>Ingest fails because of ring buffer overflow. Check ingest feed.</td>
</tr>
</tbody>
</table>
### Chapter 5      System Monitoring

#### System Level Monitoring

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 configuration 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>
<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>
</tbody>
</table>
### Table 5-6 MPEG Error Codes (continued)

<table>
<thead>
<tr>
<th>Numeric Error Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 5-7 lists the Managed Services Architecture (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>Request for content was bad. Check the target back office URL.</td>
</tr>
<tr>
<td>7002</td>
<td>MSA_UNKNOWN_HOST</td>
<td>Host is unknown. Check the target back office 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 back office did not respond within the allowed time interval.</td>
</tr>
<tr>
<td>7005</td>
<td>MSA_UNKNOWN</td>
<td>Unknown error occurred. Check the /home/isa/bss/log/aim.log.</td>
</tr>
<tr>
<td>7006</td>
<td>MSA_FAILED_POST</td>
<td>Ingest Manager failed to post the ADI to the back office.</td>
</tr>
<tr>
<td>7007</td>
<td>MSA_PKG_EXPIRED</td>
<td>Package has expired and the retry record is removed.</td>
</tr>
<tr>
<td>7008</td>
<td>MSA_STORE_FAILED</td>
<td>Ingest Failed because AIM had a problem with the storage server or vault(s) not available for recording.</td>
</tr>
<tr>
<td>7009</td>
<td>MSA_ENCRYPT_FAILED</td>
<td>Ingest Failed because AIM was unable to encrypt the content</td>
</tr>
<tr>
<td>7010</td>
<td>MSA_BACKOFFICE_FAILED</td>
<td>Ingest failed because AIM was unable to contact the back office.</td>
</tr>
<tr>
<td>7011</td>
<td>MSA_INVALID_URL</td>
<td>The URL provided for the ingest is invalid.</td>
</tr>
<tr>
<td>9011</td>
<td>VAULT_NOT_AVAILABLE_FOR_RECORDING</td>
<td>Vault(s) not available for recording. Check if vault(s) are available for recording and is online.</td>
</tr>
<tr>
<td>10003</td>
<td>OUTOFDISKSPACE_INGEST_FAILURE</td>
<td>Ingest failed due to insufficient disk space.</td>
</tr>
</tbody>
</table>

Monitoring Content Objects

The content objects links on the Monitor System Level page provides information on the status of content ingests. The following different ingest states are monitored:

<table>
<thead>
<tr>
<th>Ingest State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed Ingests</td>
<td>Lists content objects that have been fully ingested.</td>
</tr>
<tr>
<td>Active Ingests</td>
<td>Lists content objects that are in the process of being ingested.</td>
</tr>
<tr>
<td>Provisioned Ingests</td>
<td>Lists content objects that have been requested for ingestion, by way of the BMS administrator creating an entry, but have not yet begun active ingestion.</td>
</tr>
<tr>
<td>Unprovisioned Ingests</td>
<td>Lists content objects that were terminated by the BMS administrator or have been created but do not yet contain any information (in other words, they are blank shells).</td>
</tr>
<tr>
<td>Failed Ingests</td>
<td>Lists content objects that failed to complete the ingest process. All failed ingests are reported back to the OpenStream system.</td>
</tr>
</tbody>
</table>
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 time of the ingested content. 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 and Deleting Completed Ingests, page 5-18
- Viewing Other Ingests, page 5-22
- Viewing Ingest Percentage Status, page 5-22

#### Viewing and Deleting 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 10 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.

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 5-5** shows an example of the 100 most recent RTI (live recordings) and FTP (VOD Contents) Completed Ingests list. The content name, file size, duration, and date the object was ingested are displayed.

<table>
<thead>
<tr>
<th>Package Expiration</th>
<th>Lists Package Expiration information, including expiration dates and all associated metadata. Allows for package expiration adjustments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish Failures</td>
<td>Lists the packages that were not able to be published to the back office and provides a mechanism to republish the package.</td>
</tr>
<tr>
<td>Unpublished Packages</td>
<td>Provides a list of unpublished packages and their corresponding VOD Market Site(s) and retry counts</td>
</tr>
</tbody>
</table>
Starting from Release 4.8, Cisco VDSTV displays the 100 most recent completed RTI Ingests and FTP Ingests. It is applicable for RTSP EventIS deployment only.

### Step 3
To view the details of a content object, click the content name. The Ingest Details are displayed (Figure 5-6).

<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>
Table 5-9 describes the content object details that are displayed for each type of ingest.
Table 5-9  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>Asset Name</td>
<td>Name of the asset. An asset has three basic components: metadata, content, other assets are hierarchically arranged to have a parent-child relationship.</td>
</tr>
<tr>
<td>Ingest IP</td>
<td>IP address for 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></td>
<td>• Live</td>
</tr>
<tr>
<td>Encrypted</td>
<td>Whether the content object is encrypted or not; Yes means encrypted and No means not encrypted.</td>
</tr>
<tr>
<td>Get GOID Info</td>
<td>Click Get Goid Info to retrieve and display the current GOID information from the database.</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>• GOID—Global object identifier. An internal identifier used by the VDS.</td>
</tr>
<tr>
<td></td>
<td>• Speed/Direction—Trick-mode speed and direction (play, fast forward, rewind, iGate, redo). The iGate value references offsets in the MPEG file, where there are iframes for smoother trick-mode transitions. The redo value indicates the copy of the content when ingested may have changed slightly and is being redone.</td>
</tr>
<tr>
<td></td>
<td>• Server ID—Server ID where the copy is stored.</td>
</tr>
<tr>
<td></td>
<td>• Status—Status of the stored content.</td>
</tr>
<tr>
<td></td>
<td>• Status Date/Time—Date and time the content copy status was collected.</td>
</tr>
</tbody>
</table>
To delete the completed ingest, click **Delete**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Content ID</td>
<td>Full identification of this content object.</td>
</tr>
<tr>
<td>URL</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>
</tbody>
</table>

### Viewing Other Ingests

To view the details of active, provisioned, unprovisioned, and failed ingests, do the following:

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

- Active Ingests
- Provisioned Ingests
- Unprovisioned Ingests
- Failed Ingests

**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 5-20** 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 5-9 on page 5-21** describes the content object details that are displayed for each type of ingest.

**Note** The Unprovisioned Ingests page displays only the content name and the date the content object was considered unprovisioned.

### Viewing Ingest Percentage Status

Starting from Cisco VDSTV Release 3.5, the user can view the ingest percentage status in XML Response instead of **Callback Pending** response. To view the ingest percentage status:

1. Add a line INGEST_STATUS=1 in /home/isa/bss/etc/aim.conf file.
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 enabled in your deployment.

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

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

**Step 2** In the **Available Packages** field, begin typing the package name, then select the package name from the list provided.

**Step 3** Click **Display**.

Figure 5-7 shows an example of the Package Expiration details.

![Figure 5-7 Package Expiration Page](image)

**Table 5-10 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 Date</td>
<td>Date the package expires in the format MM-DD-YYYY</td>
</tr>
</tbody>
</table>
To adjust the license expiration date, 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.

In the Asset Details section, to view the metadata associated with the package expiration, click the details hyperlink next to the metadata you want to view.

To delete a package, choose the package from the Available Packages list by typing the characters of the package name, click Display, and then click Delete in the Package Expiration Details section.

**Publish Failures**

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 back office and provides a mechanism to republish the package.

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

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.
Table 5-11 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>
<tr>
<td>Module Type</td>
<td>Internal identifier for what failed. In the example in Figure 5-8, the</td>
</tr>
<tr>
<td></td>
<td>publishing of the package failed.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Date the database record was created for this failure.</td>
</tr>
</tbody>
</table>

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

To restart the publishing process and set the creation date to today, click Publish.

To delete an unpublished package, click Delete.

Unpublished Packages

The Unpublished Packages page provides a list of all unpublished packages and their corresponding VOD Market Site(s) and the retry counts.

To view a list of all unpublished packages, do the following:
Monitoring Stream Objects

The monitored stream objects consist of the Stream Monitor page.

Stream Monitor

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

| Step 1 | Choose Monitor > System Level > 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 ID 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. |
|        |   • Search by Specific Field—You can perform a text string search by selecting the field you want to search on, entering the complete text string (for example, the full IP address) in the Search field, and clicking Search. A list of stream objects that match the text string in the field you selected are listed. Click the linked field (session ID 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 the Quick List methods, a list is displayed. The list of stream objects can span several pages. To view the next page, click the page number.

The stream object list is generated by entering a specific value for the selected field (for example, Destination IP) in the Quick List box. The stream object list displays the session ID, stream start time, Destination IP and port (or subnet address if Stream Destination is enabled), service group, and the TSID in and out if applicable.
Figure 5-9 shows an example of the stream object list generated by clicking Most Recent 100 or All Streams. The Session handles and the stream start time are displayed.

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

Figure 5-10 shows an example of the stream object details.
Table 5-12 describes the stream details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream ID</td>
<td>Internal unique identifier assigned to the stream session by the Streamer.</td>
</tr>
<tr>
<td>Content ID</td>
<td>Content identifier of the stream object.</td>
</tr>
<tr>
<td>LSCP IP</td>
<td>Source IP address of the LSCP transaction (set-top).</td>
</tr>
<tr>
<td>Session ID</td>
<td>Session ID of the stream object.</td>
</tr>
<tr>
<td>Create Time</td>
<td>Date and time the stream object was created.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Date and time the stream object was last modified.</td>
</tr>
<tr>
<td>TSID out</td>
<td>The output transport stream identification on the associated MQAM device. <strong>Note</strong>: This field is applicable only when Streaming Mode is set to ASI.</td>
</tr>
<tr>
<td>Service Group</td>
<td>Service group that the stream object is transmitting on.</td>
</tr>
</tbody>
</table>
Table 5-12  Stream Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QAM IP</td>
<td>IP address of the QAM device delivering this stream object.</td>
</tr>
<tr>
<td>Note</td>
<td>If Stream Destination is enabled, this field displays the subnet address.</td>
</tr>
<tr>
<td>QAM Port</td>
<td>Port the QAM device is using to receive the stream object.</td>
</tr>
<tr>
<td>Note</td>
<td>If Stream Destination is enabled, this field does not display.</td>
</tr>
<tr>
<td>Program Number</td>
<td>This field is applicable only when Streaming Mode is set to ASI.</td>
</tr>
<tr>
<td></td>
<td>The numerical MPEG program number for this stream object.</td>
</tr>
<tr>
<td>Bandwidth Used</td>
<td>Transport stream bandwidth, in bytes, required for this stream object.</td>
</tr>
<tr>
<td>Op State</td>
<td>Operational State indicates the state of the object. The possible states are:</td>
</tr>
<tr>
<td></td>
<td>- InService—Stream object is functioning.</td>
</tr>
<tr>
<td></td>
<td>- OutOfService—Occurs when the entity using the object wants to temporarily stop the object.</td>
</tr>
<tr>
<td></td>
<td>- Created—Stream object not yet provisioned.</td>
</tr>
<tr>
<td></td>
<td>- Destroyed—Stream object is destroyed.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Administrative state of this stream object. The possible administrative states are:</td>
</tr>
<tr>
<td></td>
<td>- Unprovisioned—Stream is loading.</td>
</tr>
<tr>
<td></td>
<td>- InService—Stream is available for streaming.</td>
</tr>
<tr>
<td></td>
<td>- OutOfService—Stream is not available for streaming.</td>
</tr>
<tr>
<td>Stream State</td>
<td>Stream state originates from the LSCP server and has the following modes:</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 normal play time (NPT). When at start NPT, it enters 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 searching for start NPT. When at start NPT, it enters transport pause mode.</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>
</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 F-6.

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

### Array Level Monitoring

The Array Level Monitoring pages provide an overall view of the health and activity of an specified array, monitoring and deletion of barker streams, and a display of the Playout Schedule if the Playout Scheduler is enabled. The Array Level links are:

- **Array Snapshot**
- **Barker Stream Monitor**

### Table 5-12 Stream Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed Direction</td>
<td>Speed direction is as follows:</td>
</tr>
<tr>
<td></td>
<td>• Play</td>
</tr>
<tr>
<td></td>
<td>• Not playing (Pause)</td>
</tr>
<tr>
<td></td>
<td>• (n) fast-forward, where (n) means (n) times fast-forward</td>
</tr>
<tr>
<td></td>
<td>• (-n) rewind, where (n) means (n) times rewind</td>
</tr>
<tr>
<td>Provision Multiple</td>
<td>Provision Multiple is enabled if this field is “yes” and disabled if this field is “no.”</td>
</tr>
</tbody>
</table>
**Array Snapshot**

The Array Snapshot page provides an overview of the current activity for the specified array of servers on the VDS. 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 5-5.

**Barker Stream Monitor**

The Barker Stream feature is optional and is not listed on the Array Level left-panel menu if it is not included in your deployment. The Barker Stream feature is also not available if the Stream Destination is set to IPTV. For more information, see the “Stream Destination” section on page F-4.

The Barker Stream Monitor page lists the Barker streams currently configured. Figure 5-12 shows an example of Barker streams. To delete a Barker stream configuration, click **Delete**.

![Figure 5-12 Barker Stream Monitor Page](image)

**Playout Monitor**

The Playout Monitor page displays the Playout Schedule that is currently configured for the selected day and channels.

The Playout Monitor page is part of the TV Playout feature and is displayed only if TV Playout feature is enabled. For more information, see the “Playout Scheduler” section on page F-15.

To view the Playout Schedule, do the following:
**Array Level Monitoring**

**Chapter 5  System Monitoring**

**Step 1** Choose Monitor > Array Level > Playout Monitor. The Playout Monitor page displays the calendar. (Figure 5-13).

**Figure 5-13  Playout Monitor Page—Calendar**

![Playout Monitor Page](image)

**Step 2** To view the days that have scheduled content for a channel, from the Channel drop-down list, select a channel. The days that have been scheduled for the selected channel are highlighted in the calendar.

For example, in Figure 5-13, CHAN-31 has been selected and October 10, 11, and 12 are highlighted, indicating those days have been scheduled content for CHAN-31.

**Step 3** 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.

If you selected a channel from the Channel drop-down list, then only that channel is displayed in the Playout Monitor.

The schedule for the day you selected is displayed.

---

**Note** The Playout Monitor page displays the delivery service mode for the Playout Scheduler application. To change the delivery service mode (active-active or active-standby), see the “Configuring the TV Playout Application” section on page 7-19.

The timeslots have different colors depending on the status of the scheduled content and the type of content. The Playout Scheduler page displays a legend describing the different colors for the timeslots 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.
Server Level Monitoring

The Server Level Monitoring pages provide detail information on the health and activity of a VDS server or the CDSM (or VVIM).

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 5-14 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 30 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.

---

**Note** If the disk is either sick, abandoned or reported sick then a red disk warning is displayed on the GUI but a solid blue LED is illuminated on the disk.
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 5-14, the hda2 partition has an alarm indicator because the usage has exceeded the user-defined threshold of 40 percent. There is also an alarm icon for partitions that have changed to read-only. For information on setting thresholds, see the “Setting System Thresholds” section on page 7-15.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Temp</td>
<td>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.) will display “Suspended” for a suspended drive.</td>
</tr>
</tbody>
</table>
S.M.A.R.T

The VDS 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 5-15 shows an example of the Disk Activity graph.

**Figure 5-15 Disk Monitor—Streamer Disk Activity Graph**

The Disk Activity graph displays an average calculation of the amount of data read (in megabytes per second) and data writes over a five-second period.

**NIC Monitor**

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

To view the current status of a NIC on a server, 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 5-16** shows an example of the eth4 interface on 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 for a VDS server and 30 seconds for a CDSM (or VVIM). 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 5-13 Disk Status Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
Table 5-14 describes the information displayed for a NIC port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Speed</td>
<td>Speed of the interface in megabits per second (Mbps).</td>
</tr>
<tr>
<td>Admin State</td>
<td>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>Operational state of the port interface. The operational state is either up or down. If the port is not connected to the network or is malfunctioning, the operational state displayed is down.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Physical conduit of the interface. The physical type is either copper or fiber optic.</td>
</tr>
<tr>
<td>Poll Interval</td>
<td>Number of seconds between each disk polling.</td>
</tr>
<tr>
<td>Transmit</td>
<td>Total number of bytes transmitted since this port has been operational and configured as administratively up.</td>
</tr>
<tr>
<td>Received</td>
<td>Total number of bytes received since this port has been operational and configured as administratively up.</td>
</tr>
</tbody>
</table>

To view the average transmit and receive activity that has occurred in the last two seconds for each port on this server, click **Graph Ports**. Figure 5-17 shows an example of the Port Activity graph.
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).

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 for a VDS server and 30 seconds for a CDSM (or VVIM). 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 5-20 shows an example of the Server Vitals page for a Vault (CDE250).
### Server Vitals Page for CDE 250

#### Temperatures

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU1 Temp</td>
<td>Low</td>
<td>Ok</td>
</tr>
<tr>
<td>CPU2 Temp</td>
<td>Low</td>
<td>Ok</td>
</tr>
<tr>
<td>System Temp</td>
<td>No reading</td>
<td>No status</td>
</tr>
</tbody>
</table>

#### Fan Speed

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan1</td>
<td>5522 RPM</td>
<td>Ok</td>
</tr>
<tr>
<td>Fan2</td>
<td>5522 RPM</td>
<td>Ok</td>
</tr>
<tr>
<td>Fan3</td>
<td>No reading</td>
<td>No status</td>
</tr>
<tr>
<td>Fan4</td>
<td>No reading</td>
<td>No status</td>
</tr>
<tr>
<td>Fan5</td>
<td>No reading</td>
<td>No status</td>
</tr>
<tr>
<td>Fan6</td>
<td>No reading</td>
<td>No status</td>
</tr>
<tr>
<td>Fan7</td>
<td>No reading</td>
<td>No status</td>
</tr>
<tr>
<td>Fan8</td>
<td>No reading</td>
<td>No status</td>
</tr>
</tbody>
</table>

#### Voltages

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Vcore</td>
<td>1.84V with</td>
<td>Ok</td>
</tr>
<tr>
<td>CPU2 Vcore</td>
<td>1.84V with</td>
<td>Ok</td>
</tr>
<tr>
<td>+5V</td>
<td>5.42V with</td>
<td>Ok</td>
</tr>
<tr>
<td>+12V</td>
<td>12.1W with</td>
<td>Ok</td>
</tr>
<tr>
<td>+3.3V</td>
<td>3.33V with</td>
<td>Ok</td>
</tr>
<tr>
<td>+15V</td>
<td>15.15V with</td>
<td>Ok</td>
</tr>
<tr>
<td>5VUSB</td>
<td>5.22V with</td>
<td>Ok</td>
</tr>
<tr>
<td>3.3V</td>
<td>3.33V with</td>
<td>Ok</td>
</tr>
</tbody>
</table>

#### Power Supply

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>PD Status</td>
<td>Good</td>
</tr>
</tbody>
</table>
## Chapter 5  System Monitoring

### Server Level Monitoring

Figure 5-19  Server Vitals Page for CDE 460

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU1 Temp</td>
<td>30C</td>
<td>Ok</td>
</tr>
<tr>
<td>CPU2 Temp</td>
<td>30C</td>
<td>Ok</td>
</tr>
<tr>
<td>System Temp</td>
<td>30C</td>
<td>Ok</td>
</tr>
<tr>
<td>Peripheral Temp</td>
<td>30C</td>
<td>Ok</td>
</tr>
<tr>
<td>PCH Temp</td>
<td>5C</td>
<td>Ok</td>
</tr>
</tbody>
</table>

### Fan Speed

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAN1</td>
<td>725 RPM</td>
<td>Ok</td>
</tr>
<tr>
<td>FAN2</td>
<td>895 RPM</td>
<td>Ok</td>
</tr>
<tr>
<td>FAN3</td>
<td>759 RPM</td>
<td>Ok</td>
</tr>
<tr>
<td>FAN4</td>
<td>no seeing</td>
<td>No status</td>
</tr>
<tr>
<td>FAN5</td>
<td>no seeing</td>
<td>No status</td>
</tr>
<tr>
<td>FAN6</td>
<td>no seeing</td>
<td>No status</td>
</tr>
</tbody>
</table>

### Voltages

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU1 Voltage</td>
<td>0V</td>
<td>Ok</td>
</tr>
<tr>
<td>CPU2 Voltage</td>
<td>12V</td>
<td>Ok</td>
</tr>
<tr>
<td>3.3V</td>
<td>3.33 Volts</td>
<td>Ok</td>
</tr>
<tr>
<td>48VDC</td>
<td>48VDC</td>
<td>Ok</td>
</tr>
<tr>
<td>5V</td>
<td>5.26 Volts</td>
<td>Ok</td>
</tr>
<tr>
<td>12V</td>
<td>11.80 Volts</td>
<td>Ok</td>
</tr>
<tr>
<td>5VSB</td>
<td>5.32 Volts</td>
<td>Ok</td>
</tr>
</tbody>
</table>

### Power Supply

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS2 Status</td>
<td>Good</td>
<td></td>
</tr>
</tbody>
</table>
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 5-21 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 for a VDS server and 30 seconds for a CDSM (or VVIM). 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.

The values in the Cache/Fill Bandwidth page are only accurate if the clocks on the VDS servers are synchronized with the CDSM. If the clocks on the VDS servers are out of sync with the CDSM by more than two minutes, no values are displayed.

### 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>Number of active streams on this Streamer.</td>
</tr>
<tr>
<td>Active Stream Bandwidth</td>
<td>Bandwidth (in Mbps) used for streaming on this Streamer.</td>
</tr>
<tr>
<td>Unique Stream Count</td>
<td>Number of unique streams on this Streamer.</td>
</tr>
<tr>
<td>Unique Stream Bandwidth</td>
<td>Bandwidth (in Mbps) used for serving unique streams on this Streamer.</td>
</tr>
<tr>
<td>Fill Receive Stream Count</td>
<td>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>Bandwidth (in Mbps) used on this Streamer for retrieving content from the Vault.</td>
</tr>
<tr>
<td>Disk Read Stream Count</td>
<td>Number of streams on this Streamer sending content that was retrieved from the hard drives on the Streamer.</td>
</tr>
<tr>
<td>Disk Read Bandwidth</td>
<td>Bandwidth (in Mbps) used on this Streamer for retrieving locally stored content (content on the Streamer hard drives).</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 5-22 shows an example of a Streamer server.

**Figure 5-22 Services Monitor Page—Streamer**

<table>
<thead>
<tr>
<th>Service</th>
<th>Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Cache Server</td>
<td>All</td>
<td>Cache server runs on all servers. The Cache server is responsible for the core functions of the VDS.</td>
</tr>
<tr>
<td>Cisco Content Store Master</td>
<td>Vault</td>
<td>Content Store Master process is running if you are looking at a master Vault server. The Content Store Master serves as the master Vault process for accepting inbound OpenStream connections.</td>
</tr>
<tr>
<td>Cisco Content Store Slave</td>
<td>Vault</td>
<td>Content Store Slave process is running if you are looking at either a master or a slave Vault server. The Content Store Slave handles requests proxied by the Content Store Master.</td>
</tr>
<tr>
<td>Cisco Stream Service Master</td>
<td>Streamer</td>
<td>Streamer Service Master process is running if you are looking at a master Streamer server. The Stream Service Master serves as the master Streamer process for accepting inbound OpenStream connections.</td>
</tr>
</tbody>
</table>

Table 5-16 describes the services listed on the Services Monitor page. All services described in Table 5-16 may not be listed on the Services Monitor page. The services listed are determined by the type of VDS deployment.
Chapter 5  System Monitoring

Server Level Monitoring

Cisco VDS-TV RTSP Software Configuration Guide

Table 5-16  VDS Services (continued)

<table>
<thead>
<tr>
<th>Service</th>
<th>Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Primary Stream Setup Service</td>
<td>Streamer</td>
<td>Primary Setup Service is running if you are looking at the Streamer server designated as the primary Setup server. The Setup server handles setting up stream sessions.</td>
</tr>
<tr>
<td>Cisco Stream Control Service</td>
<td>Streamer</td>
<td>Stream Control Service accepts set-top play stream commands, for example, LSCP.</td>
</tr>
<tr>
<td>Cisco Resource Manager</td>
<td>Streamer</td>
<td>Resource Manager runs on a Streamer server. The Resource Manager handles orphaned streams.</td>
</tr>
<tr>
<td>Cisco AVS Launcher</td>
<td>Streamers</td>
<td>AVS Launcher is responsible for communicating setup and control IP address movement with CServer for the streaming components.</td>
</tr>
<tr>
<td>Cisco DB Server</td>
<td>All</td>
<td>DB (database) server runs on all servers and is responsible for keeping track of all data objects in the VDS.</td>
</tr>
<tr>
<td>Cisco DB Synchronization Status</td>
<td>All</td>
<td>Displays the status of the database synchronization among all servers. The states are “OK” and “not OK.”</td>
</tr>
<tr>
<td>Cisco SNMP Server</td>
<td>All</td>
<td>SNMP server shows as running when the SNMP agent is running.</td>
</tr>
<tr>
<td>Cisco System Manager</td>
<td>All</td>
<td>System Manager runs on each server and facilitates communication with the CDSM.</td>
</tr>
<tr>
<td>Cisco Error Repair Server</td>
<td>Streamer</td>
<td>VOD Error Repair server runs on Streamer that has the Application Monitoring Tool (AMT) enabled.</td>
</tr>
<tr>
<td>Cisco Ingest Manager</td>
<td>Vault</td>
<td>Ingest Manager process is running if you are looking at a master Vault server and the optional Ingest Manager feature is part of your deployment.</td>
</tr>
<tr>
<td>Cisco CDSM Web Server</td>
<td>CDSM</td>
<td>The Apache web server on the CDSM.</td>
</tr>
<tr>
<td>Cisco CDSM Importer Server</td>
<td>CDSM</td>
<td>The importer server on the CDSM.</td>
</tr>
<tr>
<td>Cisco CDSM Exporter Server</td>
<td>CDSM</td>
<td>The exporter server on the CDSM.</td>
</tr>
<tr>
<td>Cisco collectd Server</td>
<td>All</td>
<td>The cisco collect server collects the status and statistical data of each server and upload the data of each server on to the Controller (CDSM/VVIM) via TCP connection.</td>
</tr>
</tbody>
</table>
Recommended Monitoring Schedule

This monitoring schedule is recommended to ensure that the VDS 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 VDS, the Linux operating system, and 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 5-3 for more information.

- Choose **Monitor > System Level > Failed Ingests** to check for any failed ingests. See the “Ingests” section on page 5-18 for more information.

- Choose **Monitor > System Level > System Failures** to check for any system failures. See the “System Failures” section on page 5-6 for more information. It is also possible to run a report for the previous day. See the “System Failures” section on page 6-25 for more information.

Weekly Tasks

The following tasks should be performed weekly:

- Monitoring Tasks for Streamers and Vaults, page 5-44
- Monitoring Tasks for Vaults, page 5-46
- Monitoring Tasks for Streamers, page 5-46

Note

All commands require that you log into each 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:

```bash
df -h
```

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

Chapter 5      System Monitoring

Recommended Monitoring Schedule

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:

```
vdsServices status
```  

**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 4-85). The number of GOIDs is also dependent on the trick speeds you configured (see the “Configuring Ingest Tuning” section on page 4-15). 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 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:

   ```bash
   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/ContentStore/server/ContentStore.log` for ingest errors on each Vault. The master Vault has an additional log.

### 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. In an ISA environment, look for any errors in the `/Streaming/lscp_server/LSCPService.log` on the primary Control server, and `/Streaming/master/StreamService.log` on the primary Setup server.

2. Look at the streaming log.

   ```bash
   tail -f /arroyo/log/streamevent.log.<date>
   ``

### 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 VDS 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 VDS.
Chapter 5  System Monitoring

Recommended Monitoring Schedule
System Reporting

The CDSM provides tools that can be used for system monitoring and system diagnostics.

- Stream Activity, page 6-1
- Content Activity, page 6-33
- CDSM Audit Logs, page 6-36
- Archived Data, page 6-39

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 F-10.

Stream Activity

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

- Capacity Planning, page 6-2
- Streams by Array, page 6-7
- Streams by Time, page 6-13
- Stream Play History, page 6-16
- Cache/Fill Bandwidth, page 6-22
- System Failures, page 6-25
- Content Popularity, page 6-29

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

The Capacity Planning report provides information on high usage of bandwidth and streams for the selected date range and modifier.

Step 1

From the Available Reports drop-down list, choose Capacity Planning (Figure 6-1).

Figure 6-1 Available Reports for Stream Activity

Note

If Trick Mode Capture is disabled, the data for the Capacity Planning report is not available. For information on enabling the Trick Mode Capture, see the “Trick Mode Capture” section on page F-6.
Choose a modifier. See Table 6-1 for a description of each modifier.

### Table 6-1 Capacity Planning Modifiers

<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>Service Group</td>
<td>Filters the report by the service group you choose in a later step.</td>
</tr>
<tr>
<td>Streamer</td>
<td>Filters the report by the Streamer or ISV¹ you specify in a later step.</td>
</tr>
</tbody>
</table>

1. ISV = Integrated Streamer-Vault.

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

Choose a time breakdown. See Table 6-2 for a description of each time breakdown.

### Table 6-2 Time Breakdown Options

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per hour</td>
<td>Peak usage of bandwidth and streams per hour within the specified date range.</td>
</tr>
<tr>
<td>Per day</td>
<td>Peak usage of bandwidth and streams per day within the specified date range.</td>
</tr>
</tbody>
</table>
Stream Activity

Chapter 6  System Reporting

Table 6-2  Time Breakdown Options (continued)

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per week</td>
<td>Peak usage of bandwidth and streams per week within the specified date range. Incomplete weeks are not returned. The start date determines the first day of the week. For example, if you specify Tuesday, the 2nd of November 2010 as the start date, the first week is calculated as spanning from Tuesday, the 2nd of November 2010 to Monday, the 8th of November 2010. The second week is calculated as spanning from Tuesday, the 9th of November 2010 to Monday, the 15th of November 2010.</td>
</tr>
<tr>
<td>Daily per min</td>
<td>Peak usage of bandwidth and streams per minute for each standard week within the specified date range.</td>
</tr>
<tr>
<td>Daily per 5 min</td>
<td>Peak usage of bandwidth and streams per five minute intervals for each standard week within the specified date range.</td>
</tr>
<tr>
<td>Daily per 15 min</td>
<td>Peak usage of bandwidth and streams per fifteen minute intervals for each standard week within the specified date range.</td>
</tr>
<tr>
<td>Daily per hour</td>
<td>Peak usage of bandwidth and streams per hour for each standard week within the specified date range.</td>
</tr>
</tbody>
</table>

**Step 5**  If you selected a modifier that requires a value, choose or specify the value.

**Step 6**  Click **Display**.

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

Figure 6-3 shows an example of the Capacity Planning report in a chart view displaying peak usage of bandwidth and streams daily covering a 23-day period with no optional modifiers selected.
The report displays:

- Report type (for example, Capacity Planning Report displaying daily peak values)
- From and to dates
- Peak stream count for each time breakdown within the time period selected
- Peak bandwidth in Mbps for each time breakdown within the time period selected

Hover your cursor over a data point to view the time breakdown, peak stream count, and peak bandwidth associated with the data point.

Click the Grid button to view the chart information in a table (Figure 6-4).
Click the **Chart** button to return to the chart view.

Click **New Report** to return to the report selection page.

**Step 7**

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 Array

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

**Step 1**  
From the **Available Reports** drop-down list, choose **Streams By Array**. Figure 6-5 shows the selection fields for the Streams by Array report.

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

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

**Table 6-3  Streams by Array Modifiers**

<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>

**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
Stream Activity

- 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 6-6* shows an example of the Streams by Array report in a chart view displaying daily stream activity covering a six-day period with no optional modifiers selected.

*Figure 6-6  Streams by Array Report*

The report displays:

- Report type (for example, Daily Stream Activity Report for streams by array)
- From and to dates
- Number of high-definition (HD) streams, number of standard definition (SD) streams, and total number of streams for each time breakdown within the time period selected

Hover your cursor over a data point to view the time breakdown, number of HD streams, number of SD streams, and total number of streams associated with the data point.

Click the **Grid** button to view the chart information in a table. Click the **Chart** button to return to the chart view.

Click **Previous Report** to return to the report selection page.
To see more detail, click a bar in the chart. For example, in Figure 6-6, click the bar representing the number of streams transmitted on Apr 26, 2011. The Session ID Summary is displayed for this date (Figure 6-7).

**Figure 6-7 Session ID Summary**

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

If a content object is associated with a session, do the following to view stream history information:

**a.** Click a session ID to see the stream play history of a specific session(Figure 6-8).

**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 F-6.
The report opens in a chart view and displays:

- Session ID
- Set-top MAC address
- Termination reason
- Date and time of each play or trick mode action
- Server ID of the Play server that served the trick mode
- Elapsed time of each action

At the bottom of each Stream Play History report is a legend mapping the action to a color. Hover your cursor over a data point to view detailed action information, including start date and time, status, start of normal play time (nptstart), end of normal play time (nptend), and duration.

Click the Grid button to view the chart information in a table. Click the Chart button to return to the chart view.

Click Previous Report to return to the previous page.

b. To see details about the stream associated with this session, click Show Stream Data (Figure 6-9).
The Stream Data displays:
- Details about the stream (QAM IP address, QAM port, and, if applicable, service group)
- Details about the content (content name, ingest information, server ID of the server storing the content, and so on)

Click Hide Stream Data to hide stream data.

Click Previous Report to return to the previous page.

c. 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.
Step 10 If a playlist is associated with a session, do the following to view stream history information:

a. Click the Session ID to see the playlist history for the session (Figure 6-10).

Figure 6-10 Session Playlist History

The report opens in a chart view and displays:
- Session ID
- Start time of each playlist
- Elapsed time of each playlist in minutes

Each content segment in the playlist is represented by a different color. In the example presented in Figure 6-10, the selected playlist began at 18:18:33, it was 240 minutes in duration, and it consisted of four content segments.

Hover your cursor over a content segment to view detailed segment information, including start date and time, segment number, segment duration, and playlist duration.

Click Previous Report to return to the previous page.

b. To see the stream play history for a specific playlist, click a bar in the chart representing a playlist.
Note

If Trick Mode Capture is disabled, clicking a bar in the chart does not link to the stream play history. For information on enabling the Trick Mode Capture, see the “Trick Mode Capture” section on page F-6.

Click Previous Report to return to the previous page.

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

Click Hide Stream Data to hide the stream data.

Click Previous Report to return to the previous page.

to
d. 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 SD and HD 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 6-11 shows the selection fields for the Streams by Time report.

**Figure 6-11  Streams by Time Report Selection Fields**

- **Step 2** Using the drop-down lists provided, or the calendars, choose a **From Date** and **To Date** for the report.
- **Step 3** Choose a time breakdown of per hour, per half hour, per 15 minute, or per minute.
- **Step 4** Click **Display**.

To clear the fields and start over, click **Reset**.
Figure 6-12 shows an example of the Streams by Time report in a chart view with the **Per Hour** time breakdown selected.

**Figure 6-12   Streams by Time Report**

The report displays:

- Report type (for example, Stream Activity Report for streams by time)
- From and to dates
- Number of HD streams, number of SD streams, and total number of streams for each time breakdown within the time period selected

Hover your cursor over a data point to view the time breakdown, number of HD streams, number of SD streams, and total number of streams associated with the data point.

Click the **Grid** button to view the chart information in a table. Click the **Chart** button to return to the chart view.

Click **Previous Report** to return to the previous page.
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 6-13 Stream Play History Report Selection Fields](image)

**Step 2** Choose a modifier. See Table 6-4 for a description of each modifier.

---

**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:

- 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.

- 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.
Table 6-4  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.

**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.

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

**Step 6** If a content object is associated with a session, do the following to view stream history information:

a. To see the stream play history of a specific session, click a session ID (Figure 6-15).

**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 F-6.
The report opens in a chart view and displays:

- Session ID
- Set-top 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

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

Hover your cursor over a data point to view detailed action information, including start date and time, status, nptstart, nptend, and duration.

Click the **Grid** button to view the chart information in a table. Click the **Chart** button to return to the chart view.

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

b. To see details about the stream associated with this session, click **Show Stream Data** (Figure 6-16).
The Stream Data displays:

- Details about the stream (QAM IP address, QAM port, and, if applicable, service group)
- Details about the content (content name, ingest information, server ID of the server storing the content, and so on)

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.

c. 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.

**Step 7** If a playlist is associated with a session, do the following to view stream history information:

a. Click the Session ID to see the playlist history for the session (Figure 6-17).

![Figure 6-17 Session Playlist History](image)

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

b. To see the stream play history for a specific playlist, click a bar in the chart representing a playlist.

**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 F-6.

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

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

Click **Hide Stream Data** to hide the stream data.
Click Previous Report to return to the previous page.

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

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:

---

**Figure 6-18 Cache/Fill Bandwidth Report Selection Fields**

![Cache/Fill Bandwidth Report Selection Fields](image)

- **Step 1** From the Available Reports drop-down list, choose Cache/Fill Bandwidth. Figure 6-18 shows the selection fields for the Cache/Fill Bandwidth report.

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

- **Step 3** Using the drop-down lists provided, or the calendar, choose a Start Date for the report.

  **Note** The report displays bandwidth used from 12:00 am to 11:59 pm on the day specified as the start date.

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

- **Step 5** Click Display.

To clear the fields and start over, click Reset.
Figure 6-19 shows an example of the Cache/Fill Bandwidth report in a chart view.

**Figure 6-19  Cache/Fill Bandwidth Report**

The report displays the minimum, average, and maximum bandwidth used for each timeslot for the selected Streamer. Hover your cursor over a data point to view the same information in a summary view. Click the **Grid** button to view the chart information in a table. Click the **Chart** button to return to the chart view.

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.

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.
System Failures

The System Failures report lists the number of system failures.

To view the System Failures report, do the following:

**Step 1**

From the **Available Reports** drop-down list, choose **System Failures**. Figure 6-20 shows the selection fields for the System Failures report.

![Figure 6-20 System Failures Report Selection Fields](image)

**Step 2**

Choose an error code, if applicable. See Table 5-2 in the “System Failures” section on page 5-6 for descriptions of possible error codes.

**Step 3**

Choose a modifier. See Table 6-5 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

Note The time breakdown Monthly is not available when you choose Service Group or Server ID as a modifier or when you choose an error code.

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 6-21 shows an example of the System Failures report in a chart view.

**Figure 6-21  System Failures Report**

The report displays:
- Report type
- From and to dates
- Number of HD failures, number of SD failures, and total number of failures for each time breakdown

Hover your cursor over a data point to view the time breakdown, number of HD failures, number of SD failures, and total number of failures associated with the data point.

Click the **Grid** button to view the chart information in a table. Click the **Chart** button to return to the chart view.

Click Previous Report to return to the previous page.

---

**Step 8**  
To see more detail, click a bar in the chart. For example, in Figure 6-21, click the bar representing the stream failures occurring on May 4th, 2011. The Stream Failure Details report is displayed (Figure 6-22).
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

**Step 9** If a content object is associated with a session, do the following to view stream history information:

a. 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 F-6.

b. 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.
Chapter 6  System Reporting

Stream Activity

**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.

c. 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.

**Step 10**  If a playlist is associated with a session, do the following to view stream history information:

a. Click the Session ID to see the playlist history for the session.

b. To see the stream play history for a specific playlist, click a bar in the chart representing a playlist.

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

Click Previous Report to return to the previous page.

d. 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 6-23 shows the selection fields for the Content Popularity report.
**Step 2**
Using the drop-down lists provided, or the calendars, choose a **Start Time** and **End Time** for the report. The end time must be within 24 hours of the start time.

**Step 3**
Click **Display**.
To clear the fields and start over, click **Reset**.
Figure 6-24 shows an example of the Content Popularity report in a chart view.

**Figure 6-24  Content Popularity Report**

The report displays:

- Report type
- From and to dates
- Content filenames
- Number of times each content was streamed within the time period selected

Hover your cursor over a data point to view the content object name and the number of streams associated with the data point.

Click the Grid button to view the chart information in a table. Click the Chart button to return to the chart view.
**Step 4**  To view content details, click the content object name in a chart view. The Content Detail report is displayed (Figure 6-25).

---

**Figure 6-25**  Content Popularity Details

![Content Detail](image)

Click **Close** to close this window.

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

**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 reports lists all content stored on all Vaults in the specified group and all unpublished packages. The available reports for content activity 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** Choose **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 6-26).

**Step 3** From the **Array** drop-down list, choose an array.

**Step 4** From the **Ingest Type** drop-down list, choose one of the following:

- RTI—To view the **Live recordings** reports
- FTP—To view the **VOD contents** reports
- Both—To view both the **Live recordings and VOD contents** reports.

**Note** It is applicable for RTSP EventIS deployment only.

**Step 5** Using the drop-down lists provided, or the calendars, choose a **From Date** and **To Date** for the report.

**Step 6** Choose **Include Deleted** to include content that has been deleted from the array; otherwise, choose **Exclude Deleted**.

**Step 7** Click **Display**.
To clear the fields and start over, click **Reset**.

**Figure 6-27** shows an example of the Content Activity report.

**Figure 6-27**  Content Activity Report

The report displays:

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

**Step 8** To view the details of an in-service content object, click the content filename link (**Figure 6-28**).

**Figure 6-28**  Content Detail

Click **Close** to close this window.

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

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

The Unpublished Package report is part of the optional Ingest Manager feature. This option is only listed in the Content Activity Available Reports drop-down list if the Ingest Manager is included in your deployment.

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 6-29).

**Figure 6-29 Unpublished Package Selection Fields**

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 6-30* shows an example of the Unpublished Package report.

### Figure 6-30  Unpublished Package Report

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Create Time</th>
<th>Source URL</th>
<th>Target URL</th>
<th>Assets</th>
</tr>
</thead>
</table>

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 6-31* shows the selection fields for the CDSM Audit logs.
Using the **Top Level Filter** drop-down list provided, choose a top-level filter from the options presented in Table 6-6.

**Table 6-6 Top-level Filters**

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Sections</td>
<td>Filter on date only.</td>
</tr>
<tr>
<td>Configure</td>
<td>Filters the log by actions taken using the Configure tab of the CDSM or VVIM.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Filters the log by actions taken using the Monitor tab of the CDSM or VVIM.</td>
</tr>
<tr>
<td>Maintain</td>
<td>Filters the log by actions taken using the Maintain tab of the CDSM or VVIM.</td>
</tr>
<tr>
<td>Auto System Cleanup</td>
<td>Filters the log by the automatic system cleanup process of the CDSM or VVIM.</td>
</tr>
<tr>
<td>All Other</td>
<td>Filters the log by all other actions that do not relate to the Configure, Monitor, or Maintain tabs of the CDSM or VVIM, or to the automatic system cleanup process.</td>
</tr>
</tbody>
</table>

Using the **Sub Level Filter** drop-down list provided, choose a second-level filter from the options presented in Table 6-7.

**Table 6-7 Sub-level Filters**

<table>
<thead>
<tr>
<th>Top-level Filter</th>
<th>Low-Level Filter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure</td>
<td>If the log is filtered by the Configure tab, choose to filter the log further by the actions taken using the System Level, Array Level, or Server Level pages of the Configure tab.</td>
</tr>
<tr>
<td>Monitor</td>
<td>If the log is filtered by the Monitor tab, choose to filter the log further by the actions taken using the System Level, Array Level, or Server Level pages of the Monitor tab.</td>
</tr>
</tbody>
</table>
Table 6-7 Sub-level Filters (continued)

<table>
<thead>
<tr>
<th>Top-level Filter</th>
<th>Low-Level Filter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain</td>
<td>If the log is filtered by the Maintain tab, choose to filter the log further by the actions taken using the Users, Servers, Services, or Software pages of the Maintain tab.</td>
</tr>
<tr>
<td>All Sections, Auto System Cleanup, and All Other</td>
<td>To apply a top-level filter only, choose All Sub Sections from the Sub Level Filter drop-down list.</td>
</tr>
</tbody>
</table>

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

Step 5 Click Display.

To clear the fields and start over, click Reset.

Figure 6-32 shows an example of the CDSM Audit log.

Figure 6-32 CDSM Audit Log

The log displays:
- Top-level (Top category) and secondary-level (Sub Category) filters applied to the log
- From and to dates
- Action taken (Section Descriptor)
- User who took the action
- System used
- Date the action occurred

Step 6 Use the Top Category and Sub Category filters to filter the contents of the CDMS Audit Log within the specified date range.

Step 7 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 8 To download the report to a comma-separated value (CSV) file, do one of the following:
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 6-8 describes the different archived data.

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

To download an archived data report, do the following:

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

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

**Step 3** Right-click the HTTP link of the report that 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.

**Figure 6-33** Save As Dialog Box

**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 6-36.

Content Reports

Table 6-9 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 VDS 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>Operational state is not used and is always 2 (In Service).</td>
</tr>
<tr>
<td>mAdminState</td>
<td>Administrative state is not used and is always 2 (In Service).</td>
</tr>
<tr>
<td>mProvisionForPush</td>
<td>Type of FTP provisioned. Values are:</td>
</tr>
<tr>
<td></td>
<td>• 0—FTP pull</td>
</tr>
<tr>
<td></td>
<td>• 1—FTP push</td>
</tr>
<tr>
<td></td>
<td>• 3—Live recording</td>
</tr>
<tr>
<td>mURL</td>
<td>URL of the content file. This field is applicable only for FTP pull.</td>
</tr>
<tr>
<td>mIngestIpAddress</td>
<td>IP address of the ingest interface on the Vault used to download the content file.</td>
</tr>
<tr>
<td>mIngestFileSize</td>
<td>Content file size, in bytes.</td>
</tr>
<tr>
<td>mCreateTime</td>
<td>Time and date this content file was created. The time and date is represented in seconds since the start of Unix epoch time.¹</td>
</tr>
<tr>
<td>mLastModifiedTime</td>
<td>Time and date this content file was last modified. The time and date is represented in seconds since the start of Unix epoch time.¹</td>
</tr>
<tr>
<td>mDeleteTime</td>
<td>Time and date this content file was deleted. The time and date is represented in seconds since the start of Unix epoch time¹.</td>
</tr>
<tr>
<td>mServerId</td>
<td>Server ID of the Vault server that is the primary source for this content file.</td>
</tr>
<tr>
<td>mAssetName</td>
<td>Asset name of the content, if populated.</td>
</tr>
<tr>
<td>mEncrypted</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mRate</td>
<td>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 6-10 describes the fields in the Stream Report CSV files.

**Table 6-10 Stream Report Archive Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mSessionId</td>
<td>Session ID of the stream.</td>
</tr>
<tr>
<td>mGoid</td>
<td>Global object identifier. Used by the VDS 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></td>
<td>The transport stream bandwidth, in bytes, required for this stream object.</td>
</tr>
<tr>
<td>mQAMIp</td>
<td>IP address of the QAM device that participated in transmitting the stream.</td>
</tr>
<tr>
<td></td>
<td>The IP address is represented as an integer. For example, 3232235818 decimal</td>
</tr>
<tr>
<td></td>
<td>converts to C0A8012A hexadecimal, which translates to 192.168.1.42.</td>
</tr>
<tr>
<td>mQAMPort</td>
<td>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>Timestamp when the stream was created. The timestamp is represented in</td>
</tr>
<tr>
<td></td>
<td>seconds since the start of Unix epoch time. (^1)</td>
</tr>
<tr>
<td>mEndTime</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>mName</td>
<td>Name of the asset.</td>
</tr>
</tbody>
</table>

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

Stream Failure Reports

Table 6-11 describes the fields in the Stream Failure Report CSV files.

**Table 6-11 Stream Failure Report Archive Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mSessionId</td>
<td>Session ID of the failed stream.</td>
</tr>
<tr>
<td>mKey</td>
<td>VDS database key for this record.</td>
</tr>
<tr>
<td>mServerId</td>
<td>Server ID of the Streamer that participated in transmitting the stream.</td>
</tr>
<tr>
<td>mGroupId</td>
<td>Array ID the Streamer is associated with.</td>
</tr>
<tr>
<td>mServiceGroup</td>
<td>Service group that participated in transmitting the stream.</td>
</tr>
<tr>
<td>mQAMIp</td>
<td>IP address of the QAM device that participated in transmitting the stream.</td>
</tr>
<tr>
<td></td>
<td>The IP address is represented as an integer. For example, 3232235818 decimal</td>
</tr>
<tr>
<td></td>
<td>converts to C0A8012A hexadecimal, which translates to 192.168.1.42.</td>
</tr>
</tbody>
</table>
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 6-12 describes the fields that are exported to the CSV file.

**Table 6-12 Stream Activity Report Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mSessionId</td>
<td>Session ID of the stream.</td>
</tr>
<tr>
<td>mActionTime</td>
<td>Timestamp when the stream activity occurred. The timestamp is represented in seconds since the start of Unix epoch time.</td>
</tr>
<tr>
<td>mServerId</td>
<td>Server ID of the Streamer that is providing the stream.</td>
</tr>
<tr>
<td>mOpState</td>
<td>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>
</tbody>
</table>

1. Unix epoch time is 1970-01-01T00:00:00Z
Table 6-12 Stream Activity Report Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mNptOffset</td>
<td>Current point in time (milliseconds) where the stream is on the set-top, based on from NPT and to NPT.</td>
</tr>
</tbody>
</table>
| mDestroyedReason | This field is only populated if the stream is destroyed by the VDS orphan stream handler. The VDS orphan stream handler only destroys a stream for one of the following two reasons:  
  • Orphan session is detected  
  • LSCP timeout maximum has been reached |

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.

- User Access, page 7-2
- Server Maintenance, page 7-11
- Restarting the Services, page 7-17
- Software Maintenance, page 7-19
- Manuals, page 7-31

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 F-10.

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 VDS server. Rebooting a Vault server does not interrupt stream services, but causes current ingests to fail. If your VDS 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

Login authentication is used to control user access and configuration rights to the CDSM. Login authentication is the process by which the CDSM verifies whether the person who is attempting to log in to the CDSM has a valid username and password. If the local database is used, the person logging in must have a user account created on the CDSM. If an external server is used, the user account information is stored in an authentication database, and the CDSM must be configured to access the particular authentication server (or servers) where the database is kept.

Each user is assigned an access level. The VDS provides the following levels of user configuration rights:

- **Read only** access provides access to the monitoring capabilities, reports, and user manuals.
- **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 VDS.
- **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 VDS at the time of installation and for VDS diagnostics. After your VDS 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.

Caution

If you are using RADIUS or TACACS+ for login authentication, make sure the configuration is correct and the server is operating correctly. If RADIUS or TACACS+ is not configured correctly, or if the RADIUS or TACACS+ server is not online, then the users may be unable to log in to the CDSM.

Local Database User Password Encryption

Passwords are not stored as clear text in the local database. They are stored using Secure Hash Algorithm (SHA), which includes a salt that is randomly generated for increased security. When a user logs in to the CDSM, SHA-1 is used to generate the hashed version of the user password, including the randomly generated salt, which is then sent for authentication. If the hashed version stored in the database matches what the user entered, the user is allowed access to CDSM; otherwise, access is denied.
CDSM User Login Checks

System checks are performed on the CDSM during the user login process and during access to the CDSM GUI. If any one of the checks does not pass, access to the CDSM is denied and an error message is displayed with information on which check failed.

Table 7-1 describes the system checks that are performed during the user login process and during user access to the CDSM.

<table>
<thead>
<tr>
<th>Check</th>
<th>Description</th>
<th>Additional Information</th>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Space</td>
<td>Verify that all drives have not exceeded 95 percent storage capacity.</td>
<td>Disk space is checked every time an HTTP request is received by the CDSM. If any drive exceeds the threshold, the CDSM access is denied and the user is navigated to the login window where an error message is displayed. The drive names and threshold values can be configured in CDSM.ini file in the /arroyo/www/htdocs/CDSM/VDSTV/conf directory. [disk-partition] drive.names = /arroyo,/arroyo/db drive.threshold = 95</td>
<td>CDSM is running out of disk space (/arroyo). Contact the System Administrator for further assistance.</td>
</tr>
<tr>
<td>User Account Locked</td>
<td>Verify that the user attempting to log in does not have this attribute enabled on the account.</td>
<td>The User Account Locked check box is checked on the Edit User page for the account. Only a user with Master-level access can check or un check the User Account Locked check box.</td>
<td>User account is locked. Contact the System Administrator for further assistance.</td>
</tr>
<tr>
<td>Max. Concurrent User Sessions</td>
<td>Verify that the number of concurrent user sessions has not been exceeded.</td>
<td>The Max. Concurrent User Sessions field is set on the Edit User page for the account. If the number of sessions the user is concurrently logged in to does not exceed the setting, access is allowed; otherwise, access is denied until the user logs out of one of the other sessions.</td>
<td>Maximum number of concurrent sessions reached. Try again later.</td>
</tr>
<tr>
<td>Password Expiration Interval</td>
<td>Verify that the password has not expired.</td>
<td>The Password Expiration Interval field is set on the System Authentication page. If this field is set, and the password has expired, the user is denied access to the CDSM.</td>
<td>Password has expired. Contact the System Administrator for further assistance.</td>
</tr>
</tbody>
</table>

If the checks described in Table 7-1 all pass, the user is authenticated and if authentication is successful, the following checks are performed:

1. If the **Force Password Change** check box is checked for the user account, then the user is navigated to the Edit User page and the user is forced to change the password.

2. If the **Password Expiration Reminder** interval has started, the user is navigated to the Edit User page and notified that the password is about to expire. The user can, however, ignore the reminder and continue without changing the password.
Adding Users

The VDS 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 7-2.

Step 3
Click Add User to add this user.

To clear the fields and start over, click Reset.

### Table 7-2 Add User Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New User Login ID</td>
<td>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>Password associated with the user login name. The password must be at least 5 characters. The maximum is 20.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password entered in the Password field.</td>
</tr>
<tr>
<td>Override Password Check</td>
<td>Passwords are validated for complexity; To override the password complexity validation, check the Override Password Check check box. The Override Password Check is not available when the user password is changed for the currently logged in user.</td>
</tr>
<tr>
<td>Access</td>
<td>Choose the appropriate access level from the drop-down list. See the beginning of the “User Access” section on page 7-2, for descriptions of the access levels.</td>
</tr>
</tbody>
</table>

**Add User—Force Password Change**

When a new user is added, the Force Password Change attribute for the user is checked. When the user logs in to the CDSM for the first time, the Edit User page is displayed and the user is forced to change the password.

**Note**
When changing the password, browser-saved passwords may be requested to be changed.

During a password change, the new password is validated for complexity based on the Password Complexity Rules set on the System Authentication page. The password complexity check can be overridden if the change password is performed by a user with Master-level access and the Override Password Check check box is checked. The Override Password Check check box is available on the Add Users page and the Edit Users page if the user has Master-level access.
Editing User Settings

The Edit User page is used to update the user settings.

**Note**

Only users with Master-level access can change the access level, delete a user, and configure the user-level account settings.

To edit the user settings, 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 one of the following:

- Change Password
- Change Access
- Manage User Account

**Step 3**
From the **User Name** drop-down list, choose a user name.

**Step 4**
The fields that are available are based on the Action selected. **Table 7-3** describes the fields associated with each Action.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Password</td>
<td>Password associated with the user login name. The range is 5 to 20 characters.</td>
<td>Change Password</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password entered in the <strong>Password</strong> field.</td>
<td>Change Password</td>
</tr>
<tr>
<td>Override Password</td>
<td>Passwords are validated for complexity; To override the password complexity validation, check the <strong>Override Password Check</strong> check box. The Override Password Check is not available when the user password is changed for the currently logged in user.</td>
<td>Change Password</td>
</tr>
<tr>
<td>Access</td>
<td>Choose the appropriate access level from the drop-down list. See the beginning of the “<strong>User Access</strong>” section on page 7-2, for descriptions of the access levels.</td>
<td>Manage User Account</td>
</tr>
<tr>
<td>Lock Account on Failed Login</td>
<td>When the <strong>Lock Account on Failed Login</strong> check box is checked, the user is locked out of the CDSM GUI if the number of failed login attempts exceeds the allowed number of failed attempts configured in the System Authentication page. This setting overrides the Lock Account on Unsuccessful Login setting on the System Authentication page.</td>
<td>Manage User Account</td>
</tr>
<tr>
<td>User Account Locked</td>
<td>To lock a user out of the CDSM GUI, check the <strong>User Account Locked</strong> check box.</td>
<td>Manage User Account</td>
</tr>
</tbody>
</table>
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 7-8).

**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.

*Table 7-4* describes the user fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login ID</td>
<td>Name of the user account</td>
<td></td>
</tr>
<tr>
<td>Access Level</td>
<td>Access level of the particular user</td>
<td></td>
</tr>
<tr>
<td>Last Update</td>
<td>Date on which the user updated their password.</td>
<td></td>
</tr>
<tr>
<td>Last Login Time</td>
<td>Date and time on which the user last logged into CDSM.</td>
<td></td>
</tr>
<tr>
<td>Max. Sessions</td>
<td>Maximum number of concurrent sessions configured for the particular user.</td>
<td>Manage User Account</td>
</tr>
</tbody>
</table>
Changing User Default Settings

The User Default Settings page allows you to specify your settings for the Media Scheduler or Playout Scheduler pages 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 4-70.

To change the default settings for a user, do the following:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Maintain</strong> &gt; <strong>Users</strong> &gt; <strong>User Default Settings</strong>. The User Default Settings page is displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the <strong>Select User</strong> drop-down list, choose a user. The User Default Settings page refreshes and displays the user settings (Figure 7-1).</td>
</tr>
</tbody>
</table>

### Table 7-4 View User Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curr. Sessions</td>
<td>Total number of concurrent sessions (stale and active sessions) for the particular user.</td>
</tr>
<tr>
<td>Action</td>
<td><strong>Clear</strong>. As a user with master access level, click <strong>Clear</strong> for clearing any stale sessions and log out the active sessions for the corresponding user account. Starting from Release 4.4, VDS-TV displays <strong>Clear</strong> button irrespective of Max. Concurrent User Session being set or not.</td>
</tr>
</tbody>
</table>

**Note**

The **Clear** button is not displayed for the current logged in user and when the user account has 0 concurrent sessions.
Enter the settings as appropriate. See Table 7-5 for descriptions of the fields.

<table>
<thead>
<tr>
<th>Table 7-5</th>
<th>User Default Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td><strong>Media Scheduler</strong></td>
<td></td>
</tr>
<tr>
<td>Action on Recurring Schedules</td>
<td>Choose either <strong>Preserve Existing Schedules</strong> or <strong>Overwrite Existing Schedules</strong>. This option is only for user-generated schedules; this option is not for uploaded electronic program guide (EPG) data. <strong>Preserving Existing Schedules</strong> keeps any content that is currently scheduled for the day and channel you selected and only fills in the empty timeslots. <strong>Overwrite Existing Schedules</strong> overwrites any content that is currently scheduled for the day and channel you selected.</td>
</tr>
<tr>
<td>Package Name Auto-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>
<tr>
<td><strong>Playout Scheduler</strong></td>
<td></td>
</tr>
<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; this option is not for imported playout schedules. <strong>Preserving Existing Schedules</strong> keeps any content that is currently scheduled for the day and channel you selected and only fills in the empty timeslots. <strong>Overwrite Existing Schedules</strong> overwrites any content that is currently scheduled for the day and channel you selected.</td>
</tr>
</tbody>
</table>
Step 4 In the Input Channels Displayed 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.

---

### Table 7-5 User Default Preferences (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Selection</td>
<td>Choose either the Use Suggester option or the Use Select Box option. Use Suggester displays a text box for selecting content, and Use Select Box displays a drop-down list. If there are a large number of content objects, the Use Suggester is the preferred choice.</td>
</tr>
</tbody>
</table>
|                   | - If Use Suggester is selected, as you type in the text box, content matching the text is displayed in a list. If you click Search, The Content List window is displayed with the following options:  
|                   |  - Quick Lists—Click Most Recent Ingests, and the 25 most recently ingested content objects are listed.  
|                   |  - Browse Content—Click a character in the Browse Content section, and all content objects beginning with that letter are listed.  
|                   |  - Content List—Displays the results of the Search, the Quick List, or the Browse Content selection. The content name and ingest time are listed.  
|                   |  You can select a content object from the Content List, or select Close in the upper-right corner of the window and start your search again.  
|                   | - If Use Select Box is selected, use the down arrow of the drop-down list to display the list and select the content object. |
| Output Channels Displayed | Check the check boxes for the channels you want displayed, or check the Select All check box to chose all channels. |

### Manual Ingest FTP Preferences

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP username</td>
<td>The username to log into the FTP server.</td>
</tr>
<tr>
<td>FTP password</td>
<td>The password to log into the FTP server.</td>
</tr>
<tr>
<td>FTP host</td>
<td>The IP address or fully qualified domain name (FQDN) of the FTP server.</td>
</tr>
<tr>
<td>FTP Directory</td>
<td>The directory path where the content files are located. This can be an absolute or virtual path, depending on how the FTP server is configured. Make sure you begin the FTP path with a forward slash (/). The search includes all subdirectories.</td>
</tr>
<tr>
<td>File Extensions</td>
<td>The extensions of the types of content file you want retrieve. Separate multiple file extensions with a semicolon (;), and begin each file extension with a period (.). For example, to retrieve all MPEGs with a .mpg extension and transport streams with a .ts extension, you would enter the following: .mpg;.ts.</td>
</tr>
</tbody>
</table>
Configuring System Authentication Settings

The System Authentication page is only visible to users with Master-level access. The System Authentication fields apply system wide to all users of the CDSM GUI. Table 7-6 describes the System Authentication fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Account on Unsuccessful Login</td>
<td>If the Lock Account on Unsuccessful Login check box is checked, a user account is locked after the number of Unsuccessful Login Attempt Count has been reached within the Unsuccessful Login Attempt Period. For example, if the Unsuccessful Login Attempt Count is set to 3, the Unsuccessful Login Attempt Period is set to 1 day, and Lock Account on Unsuccessful Login is checked; then after 3 unsuccessful attempts within 1 day, the user account is locked.</td>
</tr>
<tr>
<td>Unsuccessful Login Attempt Count</td>
<td>Number of login attempts to allow the user before the account is locked. If the account is locked, the master-level user can unlock the account by unchecking the User Account Locked check box on the Edit Users page.</td>
</tr>
<tr>
<td>Unsuccessful Login Attempt Period</td>
<td>Time interval for which the number of unsuccessful login attempt count is persisted. When the time interval lapses, and if the account is not locked, the Unsuccessful Login Attempt Count is reset to 0.</td>
</tr>
<tr>
<td>Enable Password History</td>
<td>The history of user passwords is stored in the database if the Enable Password History check box is checked. During a password change, if the Enable Password History check box is checked, the new password is compared with the history of the user’s passwords, and the password change is only successful if the new password is different than the passwords that were previously used.</td>
</tr>
<tr>
<td>Password History Size</td>
<td>Specify the number of old passwords to store for each user in the database. The default is 2.</td>
</tr>
<tr>
<td>Password Change Interval</td>
<td>Minimum interval between non-administrative password changes for a given user. The default is 24 hours.</td>
</tr>
<tr>
<td>Password Expiration Interval</td>
<td>Maximum lifetime of the password. If the password has not been changed within the Password Expiration Interval, then the user account is automatically disabled.</td>
</tr>
<tr>
<td>Password Expiration Reminder</td>
<td>Interval prior to the password expiration that the user is notified about the password expiration.</td>
</tr>
<tr>
<td>Idle Session Timeout Interval</td>
<td>Maximum time a session can be idle. If the time lapse between user requests exceeds the Idle Session Timeout Interval setting, the user is redirected to the Login page.</td>
</tr>
</tbody>
</table>

As an example, if the Password Expiration Interval is set to 6 months (180 days) and the Password Expiration Reminder is set to 15 days; then 15 days before the password expires, the user is taken to the Edit Users page where a message is displayed stating the password is soon to expire. The message also includes the number of days the current password is active before it expires. The user has the option to change the password or continue without changing the password.
If the password expires, the user cannot log in to the CDSM. A Master-level user can change the user password and unlock the user account. Anytime the user password is changed by the Master-level user, the **Force Password Change** check box is checked and the next time the user logs in to the CDSM, the user is taken to the Edit Users page and is forced to change the password. The user is not able to access any of the other CDSM GUI pages until a password change has occurred.

**Password Complexity Rules**

Password Complexity Rules apply to any password change performed by the user. These rules can be overridden by Master-level users when the **Override Password Check** check box is checked on the Add Users page or the Edit Users page.

**Configuring User Authentication**

The VDS-TV software offers the following database options for maintaining user authentication data:

- Local database (located on the CDSM)
- RADIUS server (external database)
- TACACS+ server (external database)

The User Authentication page displays the configuration settings of the Authentication Protocol, which is configured through the `vdsconfig` script. The user authentication settings consist of choosing an external access server (TACACS+ or RADIUS) or the internal (local) CDSM authentication database for user access management, and setting the challenge key and timeout. The default is to use the local database for authentication. The `vdsconfig` script prompts you for the primary and backup external access server configuration. If the CDSM does not get a response from the primary server within the timeout period, the backup server is contacted.

---

**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, page 7-12
- Shutting Down a Server, page 7-12
- Offloading a Server, page 7-13
- Setting System Thresholds, page 7-15
Restarting a Server

⚠️ Caution
Restarting a Vault or Streamer server while there are still active ingests and streams causes the current ingests and streams to fail.

Restarting a server briefly shuts down the unit, then restarts it using the installed version software image. This action does not power off the unit.

To restart a server, do the following:

- **Step 1** Choose Maintain > Servers > Server Restart. The Server Restart page is displayed.
- **Step 2** From the Server IP/Name 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 Restart drop-down list, choose Yes and click Submit.

Shutting Down a Server

⚠️ Caution
Shutting down a Vault or Streamer server while there are still active 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/Name 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 set a server to **Online** or **Offline**. When a server is offline, the server is configured to reject new provisioning; that is, new ingests are not allowed on a Vault and new streams are not allowed on a Streamer and existing streams are moved to another Streamer gracefully.

### Caching Nodes and Streamers

If HTTP is used as the cache-fill protocol between Caching Nodes and Streamers and the Caching Node hosting the locate port is set to Offline, then a backup or available Caching Node in the same Cache Group becomes the primary host of the locate port. If a backup or available Caching Node is set to Offline, the state is changed from backup or available to not usable. This failover scenario is similar to the Setup and Control server failover scenario for Streamers, in that all servers in the same group advertise their availability to act as the primary with a backup taking over as primary if the primary becomes unavailable because of offline status, losing connectivity, or failure.

### Vaults

The Vault or ISV has two options for setting a server to offline:

- **Offline (No Ingest)**
- **Offline (No Ingest & Fill)**

The **Offline (No Ingest)** option enables the Vault or ISV to continue handling cache-fill requests and mirroring activities, but the server does not participate in any new content ingests. The **Offline (No Ingest & Fill)** option stops all cache-fill requests and any new content ingests, but the server still participates in mirroring activities.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The protocoltiming log file only displays the “WARNING: Server is going OFFLINE” message when the <strong>Offline (No Ingest &amp; Fill)</strong> option is selected for Vaults. The <strong>Offline (No Ingest)</strong> option for Vaults does not take the Vault completely offline, the Vault still participates in mirroring and cache-fill traffic; therefore, the server going offline message is not displayed in the protocoltiming log. The TRICKLE_DOWN file is used to determine the state of the Vault for the <strong>Offline (No Ingest)</strong> option.</td>
</tr>
</tbody>
</table>

To set a server to offline, do the following:

**Step 1** Choose **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

**Step 2** To offload by server, click the **Server** radio button.

**Step 3** From the **Server IP/Name** drop-down list, choose the IP address or nickname of the server and click **Display**. The server type, server ID, array ID, and current status of the server are displayed.

**Step 4** In the New Server Status drop-down list, select the appropriate setting and click **Submit**.

**Step 5** To offload by stream group, click the **Group** radio button.

**Step 6** From the **Group Name** drop-down list, choose the stream group and click **Display**. The server ID, group ID, Part No. and current status of the server are displayed. To change the offload status of this group of server, click the desired status and click **Submit**.

After setting a server to offline, current traffic activity can be monitored, and when the server offline is complete, the software can be updated. To view activity on a Vault server, see the “Monitoring Content Objects” section on page 5-17. To view activity on a Streamer, see the “Monitoring Stream Objects” section on page 5-26. 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 Status setting is persistent through a system reboot.

Server Offload—Online

After the software upgrade or maintenance is complete, you need to set the server to online so that the server can again participate in the system.

To set a server to online, do the following:

---

**Step 1** Choose **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

**Step 2** From the **Server IP/Name** 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** In the New Server Status drop-down list, select **Online** and click **Submit**.

Vault Decommissioning

The Server Offload page offers the ability to gracefully decommission a Vault from the system. Content on the Vault is moved to other Vaults during the decommission process so that no content is lost.

The process of decommissioning a Vault requires that the Vault first be put into Offline (No Ingest & Fill) mode. After the Vault is offline the option to decommission is listed in the Server Offload page.

To decommission a Vault, 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, select the IP address or nickname of the Vault and click **Display**.

**Step 3** From the **New Server Status** drop-down list, select **Offline (No Ingest & Fill)**.

**Step 4** Click **Submit**. The Current Server Status displays “Offline For Ingest & Fill.”

Note
Before continuing, make sure the Vault has been offloaded by checking the protocol timing log.

**Step 5** From the **New Server Status** drop-down list, select **Decommission**. The Decommission option is only displayed when the Vault is in the “Offline For Ingest & Fill” state.

**Step 6** Click **Submit**. The Current Server Status displays “Decommission (Inactive).” After the decommissioning starts the Current Server Status displays “Decommission (Active).” When the decommissioning is complete the Current Server Status displays “Decommission (Completed)” and the **Shutdown** button is displayed.

**Step 7** Click **Shutdown** to shut down the services running within CServer and completely isolate the Vault from the VDS.
After the decommission is complete, the Vault is isolated from the VDS. If the Vault is rebooted, it has the state of “Offline (No Ingest & Fill). The Vault entries in the database and .arroyorc remain intact. To remove the Vault entries from the database and .arroyorc file, the avsdb and statsd processes must be restarted, which impacts the serviceability of the system. Removal of a Vault from the database and .arroyorc file should be performed during a maintenance window.

**Setting System Thresholds**

The System Thresholds page allows you to set thresholds for loss and usage of the VDS resources, as well as enable or disable monitoring of the VDS 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 5-42. Table 7-7 lists each threshold in the Performance Parameters section, and where each threshold is monitored.

---

**Table 7-7   Performance Thresholds**

<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 5-3.</td>
</tr>
<tr>
<td>Disk Loss</td>
<td>The Disk indicator box on the “System Health” section on page 5-3.</td>
</tr>
<tr>
<td>Disk Capacity Notify</td>
<td>The “Disk Monitor” section on page 5-33.</td>
</tr>
<tr>
<td>Disk Capacity Warning</td>
<td>The “Disk Monitor” section on page 5-33.</td>
</tr>
<tr>
<td>Linux File System Usage</td>
<td>The “Disk Monitor” section on page 5-33.</td>
</tr>
</tbody>
</table>
To set the system thresholds and enable or disable the system services, do the following:

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

**Figure 7-2 System Thresholds Page**

<table>
<thead>
<tr>
<th>Performance Parameters</th>
<th>Current Value</th>
<th>Default Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Loss %</td>
<td>10</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Disk Loss %</td>
<td>25</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Disk Capacity Notify %</td>
<td>75</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Disk Capacity Warning %</td>
<td>89</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>Linux File System Usage %</td>
<td>90</td>
<td>90</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS Settings</th>
<th>Current Value</th>
<th>Default Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempt(s)</td>
<td>2</td>
<td>2</td>
<td>1-3</td>
</tr>
<tr>
<td>Timeout</td>
<td>5, 10</td>
<td>5</td>
<td>1-30</td>
</tr>
</tbody>
</table>

**System Services**

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Monitored</th>
<th>Current Value</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Content Store Master</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco Content Store Slave</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco Resource Manager</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco Cache Server</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco DDI Server</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco SNMP Server</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco System Manager</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco Asset Manager</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco Loggrd Manager</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco AVS Launcher</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
<tr>
<td>Cisco VDSM Web Server</td>
<td>Yes</td>
<td>Monitored</td>
<td>Monitored</td>
</tr>
</tbody>
</table>

**Step 2** Enter the threshold settings and enable or disable the services as appropriate.

**Step 3** Enter the Attempt(s) and Timeout parameters for DNS settings.

**Note** The DNS settings will be reflected into /etc/resolv.conf file only after clicking **Push Config** in System DNS/Array DNS/ Server DNS page.

**Step 4** 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 VDS. 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 7-8 describes the different services.

### Table 7-8  Restart Services Options

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reload Service Groups</td>
<td>Any time there are changes (adding, editing, or deleting) to the QAM Gateway or Headend Setup configuration, it is necessary to reload the service groups. If the Content Storage feature is enabled, the Reload Service Group option is not available. It is not necessary to reload the service groups if the Content Storage feature is enabled.</td>
</tr>
<tr>
<td>ISA/OpenStream</td>
<td>Any time there are changes to the Streamer BMS or Vault BMS pages, it is necessary to restart the ISA/OpenStream service. If the Content Storage feature is enabled, it is not necessary to reload the ISA/OpenStream service, and therefore the option is not available.</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>
<tr>
<td>AIM</td>
<td>Any time there are changes to ingest manager configurations and there is a need to recover from AIM hang issue, it is necessary to restart the AIM service. Also, specify the time in seconds to wait before restarting AIM. The default value is 120 seconds and range is 30 to 600 seconds. <strong>Note</strong> Restarting AIM option is available only for master vault.</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/Name** 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 fields and start over, click **Reset**.
Content Manager

The Content Manager page allows deletion of multiple content objects.

---

**Note**

The Content Manager page is part of the TV Playout feature and is displayed only if TV Playout feature is enabled. For more information, see the “Playout Scheduler” section on page F-15.

---

To delete multiple content objects, do the following:

**Step 1**

Choose **Maintain > Services > Content Manager**. The Content Manager page is displayed with the 100 most recent ingests listed.

The first text box and **Display** button provide access to the details of a completed ingest object and takes you to the **Monitor > System Level > Completed Ingests** page. 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 10 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**. After you click **Display**, the Completed Ingest page is displayed with the details of the selected content object.

**Step 2**

To display a list of content objects, use one of the following methods:

- 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.

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. The content name, file size, duration, and date the object was ingested are displayed.

**Step 3**

Check the Delete check box next to each content object you want to delete, and click **Delete**.

---

**Note**

It takes approximately four seconds to ensure the content is deleted from the entire system and the CDSM GUI displays the change before the next delete task is triggered. If a large number of content objects are selected for deletion, the time to complete the operation increases.
Software Maintenance

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

- Viewing the Software Version and Server Information
- Configuring the TV Playout Application
- Importing a TV Playout Schedule
- Upgrade Status of the TV Playout Application
- Uploading an EPG File
- Configuring the Backup Scheduling
- Identifying Server IDs and Group IDs for VVI with Split-Domain Management
- System Cleanup

Viewing the Software Version and Server Information

To view the VDS-TV software version and server information, choose Maintain > Software > Software Version. The Software Version page is displayed. From the Server IP drop-down list, choose a server IP address or nickname 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)

Configuring the TV Playout Application

The Application Configuration page allows you to choose the Streamers participating in streaming content for the TV Playout application, and to choose how the Streamers participate. The following applications are configurable:

- Barker Stream/Playlists
- Playout Scheduler

The Application Configuration page is part of the TV Playout feature and is displayed only if TV Playout feature is enabled. For more information, see the “Playout Scheduler” section on page F-15.

The Streamers, or ISVs, chosen for the TV Playout application participate in an **active-standby** relationship, or an **active-active** relationship.
In an **active-standby** relationship, one server acts as the authority and all streams initiate from this server. The other servers participating in streaming for the TV Playout application only take over when the active server goes offline.

In an **active-active** relationship, all servers participating in the TV Playout application, stream the content at the same time.

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

To configure the Barker Stream and Playout Schedule applications, do the following:

---

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

**Figure 7-3 Application Configuration Page**

Choose the **Stream Delivery Mode**.

**Active-Standby**—All streams initiate from one server (active). The other servers (standby) only take over when the active server goes offline.

**Active-Active**—All servers stream the content at the same time.

---

**Step 2** Check the check box next to each server participating in each application.

---

**Step 3** For **Active-Active**, check the check box next to each server participating in each application.
**Step 4**  Click **Submit** to save the settings.

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

---

### Importing a TV Playout Schedule

The Playout Importer page can be used to upload a Playout file, containing the Playout Scheduler data from another VDS, into the Playout Scheduler of this VDS. The Playout file is an XML file.

**Note**

The Playout Importer page is part of the TV Playout feature and is displayed only if TV Playout feature is enabled. For more information, see the “Playout Scheduler” section on page F-15.

To import a Playout file, do the following:

**Step 1**  Choose **Maintain > Software > Playout Importer**. The Playout Importer page is displayed.

**Step 2**  In the **Playout Export Location** text box, enter the full path and filename, or click **Browse** to locate the file using the Browse window.

**Step 3**  When importing a Playout file, each channel is checked for an existing playout schedule, if there are conflicts, the setting in the **Action on Import** field is used to decide how to handle the conflict. Select **Preserve existing schedules**, to preserve the existing playout schedule when a conflict is identified. Select **Overwrite existing schedules**, to overwrite the existing playout schedule.

**Step 4**  Click **Import**.

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

---

### Upgrade Status of the TV Playout Application

After upgrading the VDS-TV software from Release 1.5.4.6, there are some steps that must be followed before any configuration changes can occur. The Playout Upgrade Status page tracks the status of these steps. Clicking the Status of each step takes the user to the page that needs to be modified. (For the link to work on the first one, the user needs to have Engineering-level access.)

Additionally, the Alarms table displays an alarm stating the playout upgrade is incomplete.

**Note**

The Playout Upgrade Status page is part of the TV Playout feature and is displayed only if TV Playout feature is enabled. For more information, see the “Playout Scheduler” section on page F-15.
Uploading an EPG File

The EPG File Upload page can be used to upload an electronic program guide (EPG) file into the VDS for use with the Media Scheduler. The EPG file is an XML file.

Note

The EPG File Upload page is part of the Media Scheduler feature. For more information, see the “Media Scheduler” section on page F-14.

Before you can upload an EPG file, you need to enter the channel information. See the “Configuring Input Channels” section on page 4-27 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**.
Configuring the Backup Scheduling

To configure the backup scheduler to take backup of configuration and content object table entries, perform the following:

**Step 1** Choose **Maintain > Software > Backup Scheduler MAINTAIN page.** The Backup Scheduler MAINTAIN page appears (Figure 7-4).

*Figure 7-4 Backup Scheduler MAINTAIN page*
Cisco recommends you to schedule both configuration and content table backup during less traffic hours (suggested 6 a.m. local time on week days). High traffic hours are usually 5 p.m. to 12 a.m. on week days and 8 a.m. to 12 a.m. on weekends.

To clear the scheduled auto-backup, uncheck the **Enable Auto-backup** checkbox and click **Submit**.

On success or failure of the backup configuration or content table entries, the alarm is sent to the user.

Step 2 Enter the settings as appropriate. See Table 7-9 for description of the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Auto-backup</td>
<td>Check the <strong>Enable Auto-backup</strong> check box to automatically take backup of the Configuration and Content object table entries and store it in Local and/or Remote server. The backup scheduler fields appears.</td>
</tr>
<tr>
<td>Backup Destination</td>
<td></td>
</tr>
<tr>
<td>Local Server</td>
<td>Check the <strong>Local server</strong> check box to store the backup files on your local server.</td>
</tr>
<tr>
<td>Remote Server</td>
<td>Check the <strong>Remote server</strong> check box to store the backup files on the remote server.</td>
</tr>
<tr>
<td>Server IP</td>
<td>IP address of the <strong>Remote</strong> server.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Click the method to store the backup files to either <strong>SCP</strong> or <strong>FTP</strong> on remote server.</td>
</tr>
<tr>
<td>Username</td>
<td>Username of the remote server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the remote server.</td>
</tr>
<tr>
<td>Backup Configuration</td>
<td>Check the <strong>Backup Configuration</strong> check box to automatically take backup of the Configuration and store it in Local and/or Remote server.</td>
</tr>
<tr>
<td>Destination Path(s)</td>
<td></td>
</tr>
<tr>
<td>Local server - backup path</td>
<td>Specifies the destination path on <strong>local server</strong>.</td>
</tr>
<tr>
<td>Remote server - backup path</td>
<td>Specifies the destination path on <strong>remote server</strong>.</td>
</tr>
<tr>
<td>Retention Count</td>
<td>Specifies the recent number of Configuration backup files to be maintained in the backup location.</td>
</tr>
<tr>
<td></td>
<td>The default value is 5.</td>
</tr>
</tbody>
</table>
Step 3  Click **Submit** to save the settings.
To reset the Backup Scheduler MAINTAIN page, click **Reset**.

---

**Restoring the Configuration from Backup Files**

To restore the Configuration from the backup files, you must un-tar the configuration backup file in the configured backup path and then perform either one of the following:

- Choose **Maintain > Software > Backup & Restore page**, you can restore the configuration levels by uploading the appropriate XML files under Configure sections and click **Restore**. You can ensure the success or failure on the GUI.

- Using API, you can add the backup files on CLI, restore the configuration using API request to import. The API response contains the success or failure message.

**Restoring the Content Object from Backup Files**

To restore the Content Object table entries from the backup file, perform the following:

**Step 1** Log into the Controller as root.

**Step 2** Go to `/arroyo/db/avsdbutil`, run the following command:

```
./avsdb_util.py –s avsdb_tabletemplate.s –i <path/csv file> –o <output_path>
```

- Option `-i` for the backup file as input
- Option `-s` for the table template of avsdb
- Option `-o` for the output wis saved in the specified path

You can verify the status of the content object restore file in the `<output_path>/avsdb_util_output.csv` path.

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

When using CCP Streamers in a VVI with split-domain management, it is mandatory that all group IDs and server IDs be unique for each server in the system. To assure this, 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 7-10** lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

**Table 7-10  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>
</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 vdsconfig 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 vdsconfig 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
- CDN 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 or CDNGroupConfig.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.

**Note**

If Bulk Import/Export Configuration is enabled, the **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”
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 7-5).

### Figure 7-5 Configuration Generator Page

Click **Download** link below to save the Cache Groups Configuration File. To save it to the local disk, right-click on the **Download** link and select the option to save the target file.

[Click Download link...]

A new range start for Stream Group IDs and Server IDs may be generated and issued to the Streamer Domain CSM administrator in order to add Streamers to a Streamer Domain and Start configuring Stream Groups. Click **Generate New IDs** button below to generate a new ID.

**Stream Domain Name:**

**Stream Manager IP:**

**Stream Domain Name:**

**Stream Manager IP:**

**Generate New IDs**

<table>
<thead>
<tr>
<th>Stream Domain Name</th>
<th>Stream Manager IP</th>
<th>Stream Group ID Range</th>
<th>Server ID Range</th>
<th>Setup ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>StreamDomain1</td>
<td>172.22.00.00</td>
<td>[0000 - 20000]</td>
<td>1001 - 1250</td>
<td>5 - 1</td>
</tr>
<tr>
<td>StreamGroup2E</td>
<td>[Not Generated]</td>
<td>[0000 - 20000]</td>
<td>1314 - 1755</td>
<td>7 - 1</td>
</tr>
<tr>
<td>testdomain</td>
<td>[Not Generated]</td>
<td>[0000 - 50000]</td>
<td>1271 - 20000</td>
<td>13 - 10</td>
</tr>
<tr>
<td>testdomain</td>
<td>172.22.00.00</td>
<td>[0000 - 20000]</td>
<td>2018 - 2250</td>
<td>15 - 16</td>
</tr>
<tr>
<td>[Not Generated]</td>
<td>172.22.00.00</td>
<td>[0000 - 20000]</td>
<td>1214 - 1500</td>
<td>22 - 20</td>
</tr>
<tr>
<td>[Not Generated]</td>
<td>172.22.00.00</td>
<td>[0000 - 50000]</td>
<td>1214 - 1500</td>
<td>5 - 1</td>
</tr>
<tr>
<td>[Not Generated]</td>
<td>[0000 - 20000]</td>
<td>[0000 - 15700]</td>
<td>5 - 1</td>
<td></td>
</tr>
</tbody>
</table>

**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**.

### Configuration Generator Table

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).

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 4-64 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.

Generating a Server ID from the Stream Manager

The Server ID Generator page is used to generate a server ID for a Streamer that is being added to the VVI, but is unable to communicate with the Stream Manager. During the initial configuration, the Streamer contacts the Stream Manager and requests a server ID. If the Streamer is unable to contact the Stream Manager, the vdsconfig script displays a prompt to contact the Stream Manager administrator for a server ID. The Stream Manager administrator would then go to the Server ID Generator page to generate a server ID for the Streamer.

Note

The Server ID Generator page is available only on the Stream Manager when VVI and Content Storage are enabled in an ISA environment. For more information, see the “Content Storage” section on page F-12 and the “Virtual Video Infrastructure” section on page F-10.

There is a range of server IDs, 1 to 1000, that are reserved for Vaults and Caching Nodes. It is the responsibility of the VVIM administrator to make sure the server IDs are unique among all Vaults and Caching Nodes in the VVI. The VVIM reserves a group of 250 server IDs for each Stream Domain (for example, 1001-1250, 1251-1500, and so on).

Note

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”
To generate a server ID for a Streamer, do the following:

**Step 1** Choose **Maintain > Software > ID Management**. The Server ID Generator page is displayed; including the System ID Settings, which consist of the following:

- Group ID Range Start—Beginning ID for the Stream Groups, Vault Groups, and Cache Groups
- Server ID Range Start—Beginning ID for the VDS servers in the system
- Setup ID Range Start—Beginning ID for the Streamer Setup server

**Step 2** Click **Generate New ID**. The new server ID is displayed in the Server ID field.

---

**System Cleanup**

The System Cleanup page allows you to clean up any errors that may have accumulated on your system. When errors occur, they are added to the Alarms table. See the “Alarms Table” section on page 5-2 for more information and other alarms and alerts that link to other CDSM pages.

The following errors and situations are monitored and registered in the Alarms table if found and linked to the System Cleanup page:

- Orphaned server IDs
- Multiple or duplicate Cache Locate IP addresses
- Out of range Group IDs
- ServerMap and StatMap inconsistencies
- Extra or incorrect SERVERMAP15 entries

The System Cleanup page displays a **Fix All** option if there are no errors found for the Cache Locate IP addresses (either Multiple or Duplicate). If Multiple or Duplicate Cache Locate IP addresses errors are found, then the **Fix All** option is not displayed until these are resolved, because they require user input as to which entry to keep and which entry to remove.

**Orphaned Server IDs**

Orphaned Server IDs occur when servers are removed from the CDSM without first removing them from the groups they belong to (for example, Vault Group or Stream Group). This leaves a reference in the groupmap table to the server ID that is no longer valid, which means the group can no longer be edited through the CDSM GUI.

**Multiple or Duplicate Cache Locate IP Addresses**

The CDSM GUI checks and validates user input to prevent multiple locate entries in the VDS server setupfile files; this is an additional check for multiple or duplicate Locate IP addresses. The Locate IP address is used in VVIM systems with HTTP as the cache-fill protocol. The procedures are different between multiple and duplicate Locate IP addresses:

- **Duplicate Locate IP Addresses**—Two or more identical entries in the control IP map table for a single Cache Group, having the same group ID, locate IP, and locate subnet IP. If this has occurred, select any one of the entries for removal, and the CDSM automatically reduces the number of entries to one.

- **Multiple Locate IP Addresses**—More than the required single-entry for a Cache Group, and the entries are not identical in that they have differing IP addresses or subnets. If this has occurred, select the entries you want removed.
Out of Range Group IDs

Sometimes the CDSM is configured as a legacy system with Stream Groups and Vault Groups, only later to find that it was incorrectly configured and needs to be changed to a VVIM or Stream Manager. This creates Stream Group map table entries that use the incorrect group ID range with no method of removing them from the CDSM GUI because the configuration pages for groups correctly filters out the incorrect group IDs from the drop-down lists. The Out of Range Group IDs check cleans up these groups.

SERVERMAP and STATMAP Inconsistencies

When adding a large number of VDS servers to a CDSM, mistakes can be made with regard to the .arroyorc file found on each VDS server (for example, incorrect group ID [array ID] or IP address). This can lead to incorrect entries in the server STATMAP table. Additionally, servers that are not removed correctly can also leave an incorrect entry in the server STATMAP table. The server STATMAP table is used to generate the System Monitor content and errors in it can lead to display issues and incorrect states being displayed.

Extra or Incorrect SERVERMAP Entries

If the CDSM is reconfigured or reinstalled for a different type of VDS (legacy or VVI) and the CDSM is not properly wiped clean, there could be residual entries in the SERVERMAP15 table and STATMAP table that do not apply to the current configuration.

Manuals

To view the manual, choose Maintain > 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 Cisco Videoscape Distribution Suite-TV (VDS-TV) by showing the symptoms, probable causes, and recommended actions for a variety of issues.

- General Information and Issues, page A-2
- Startup Issues, page A-24
- Management and Database Issues, page A-27
- Ingest Issues, page A-29
- Content Processing Issues, page A-34
- Cache-Fill Issues, page A-36
- Streaming and Playout Issues, page A-38
- Session Messaging, page A-43
- Database Issues, page A-45
- Advanced Features and Applications, page A-48
- Frequently Asked Questions, page A-49
- VDS Content Quality Guidelines, page A-55

There are a variety of possible combinations of VDS topologies, back office 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 VDS, 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 Information and Issues

This section describes the VDS 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
- Disabling USB Ports and Password-Protecting the BIOS
- Network

File System

The CDSM file system differs from the file system on the VDS servers (Vault, Streamer, Caching Node, 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 6-39.

- `/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 VDS 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 files.
Appendix A      Troubleshooting

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, Caching Node, and ISV

The VDS servers (Vault, Streamer, Caching Node, and ISV) have the following directory structures:

- /arroyo/db
- /arroyo/log
- /arroyo/test/
- /arroyo/archive
- /home/isa

In addition to the above directories, the VDS servers 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/run—Contains process ID (PID) files for running the application
- /home/isa/bss/scripts—Contains general scripts

Log Files

There are four types of log files in an RTSP environment:

- Linux Log Files
- CServer Log Files
- RTSP Log Files
- AIM Logging System

The log files are rotated at least once a day and time stamps are added to the filenames. Some log files that grow rapidly are rotated more frequently (determined by file size); this rotation may happen up to once an hour. Most log files have the following suffix: .log.<YYYYMMDD.> The time zone for log rotation and filename suffixes is coordinated universal time (UTC).

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 /arroyo/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.
To change the log level or set the debug flags for the log files, use the **Configure > System Level > Logging** and **Configure > Server Level > Logging** pages. For more information, see the “Configuring the System Level Logging” section on page 4-31 and the “Configuring the Server Level Logging” section on page 4-110.

The following log tools are available:

- **loginfo**—Provides information on each facility, associated log file, and debug flags. The `loginfo` tool can be run on any VDS server, including the CDSM. To view help on `loginfo`, enter the `loginfo -h` -v command.

- **logconfig**—Provides log configuration on CDSM. To view help on `logconfig`, enter the `logconfig -h` -v command.

### 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 VDS 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 yyyyymmdd (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/collectd.log.<date>`—Provides logs for monitoring and statistical data collection.
- `/arroyo/log/stresstest.log.<date>`—Provides CPU uptime information.
- `/arroyo/log/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>`
Appendix A      Troubleshooting

General Information and Issues

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>
</tbody>
</table>
Table A-1 Protocoltiming Warning Messages (continued)

<table>
<thead>
<tr>
<th>Warning Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 can no longer 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 `isa` is the owner of the application files in an RTSP environment. To change from the root, use the `su – isa` command.

All application log files are located in `/arroyo/log` directory. When a log file reaches around 50 MB in size, it is archived and moved to the archive directory. When the RTSP or FSI is restarted, all current log files are archived and moved to the archive directory. The latest archived log files remain uncompressed, while the rest are gzipped. The archive directory always maintains the ten latest archives of each log file. The older log files are deleted.

If the RTSP application or the FSI application does not start, check the following files for possible reasons:

- `rtsp.err`
- `rtspmonitor.log`
- `fsi.err`
- `fsi.out`

These files are located in the `/arroyo/log/` directory.

The VDS RTSP environment has the following useful log files:

- `/arroyo/log/fsi.log`
- `/arroyo/log/rtspmonitor.log`
- `/arroyo/log/aim.log`
- `/arroyo/log/library.log`—Logs the cache2app library information

Log File—rtspmonitor.log

The rtspmonitor.log log file stores the processing state and associated session ID of each thread.
The thread state logging is controlled by the THREAD_MON_FREQ in the arroyo-env.sh script in the /home/isa/bss/scripts directory. The THREAD_MON_FREQ parameter is used as a time interval to print the thread state and the corresponding value, which could range from 0 to 65535. The default value for the THREAD_MON_FREQ parameter is 30. The logging can be turned off by setting THREAD_MON_FREQ to 0.

The THREAD_MON_FREQ parameter can be enabled from the CDSM. For more information about enabling the parameter, see Configuring the Server Level Logging section.

### AIM Logging System

Table A-2 lists the AIM logs, level and their values.

<table>
<thead>
<tr>
<th>AIM LOGS</th>
<th>LOG LEVEL</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>LOG_EMERG</td>
<td>0</td>
</tr>
<tr>
<td>—</td>
<td>LOG_ALERT</td>
<td>1</td>
</tr>
<tr>
<td>—</td>
<td>LOG_CRIT</td>
<td>2</td>
</tr>
<tr>
<td>ERR(msg)</td>
<td>LOG_ERR</td>
<td>3</td>
</tr>
<tr>
<td>LOG(msg)</td>
<td>LOG_WARNING</td>
<td>4</td>
</tr>
<tr>
<td>DEBUG(msg)</td>
<td>LOG_NOTICE</td>
<td>5</td>
</tr>
<tr>
<td>DEBUG_OTHER(msg)</td>
<td>LOG_INFO</td>
<td>6</td>
</tr>
</tbody>
</table>

**Note**

Starting from Release 4.6, the Ingest code paths is introduced.

- The MACRO DEBUG (msg) is mapped to log level LOG_NOTICE (5).
- The important debug logs is available in DEBUG macro.
- Lesser predominant debug logs is moved to DEBUG_OTHER macro.
- The default log level for AIM is set as LOG_NOTICE.

### CDSM Log Files

The CDSM has the following logs:

- httpd.log.<yyyymmdd>—Apache error log
- httpd_access.log.<yyyymmdd>—Apache access log
- CDSM.log.<yyyymmdd>—CDSM GUI log
- CDSM-ws.log.<yyyymmdd>—Web Services log

All log files use UTC for the log entry time stamps and filenames. All four files are located in /arroyo/log directory.
The default log level for httpd.log is LOG_WARNING and the setting is preserved. The log level for httpd.log (facility is httpd) can be configured by using the `/home/isa/logging/logconfig` tool. The `logconfig` tool overwrites the LogLevel value in the httpd.conf file with the new value and the `service vds-httpd restart` command is issued.

The httpd_access.log (facility is httpd_access) is always on and the log level cannot be changed with the `logconfig` tool.

Following is an example of a log entry in the httpd_access.log file:

```
02-09-2011 15:44:09.937115 UTC vqe-dev-29 161.44.183.124 - - [02/Sep/2011:08:44:09 -0700] "POST /includes/configGrpSubmitAjax.php HTTP/1.1" 200 12
```

Following is an example of a log entry in the httpd.log file:

```
2-09-2011 15:45:07 UTC vqe-dev-29 [notice] Apache/2.2.9 (Unix) PHP/5.2.6 configured -- resuming normal operations
```

## Server Configuration Files

The server configuration settings are stored in the `.arroyorc` file and the setupfile file. This section describes the different parameters for each file.

### Note

This section is informational only. All changes to the configuration files should be accomplished through the initial configuration and CDSM GUI.

### Table A-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>

## 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 205/220/250/420 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
• 4 = Cache

groupid
All servers that are part of the same VDS system (managed by one CDSM) have the same group ID. This group ID should be unique across an enterprise. The purpose of the group ID is to allow servers in a group to recognize each other as belonging to the same group. If two server groups were on the same VLAN and they had the same group number, they would conflict and cause issues. This is much more likely to be an issue in a lab environment with shared resources than an actual production deployment, but this should still be managed.

serverid
Every server in the group has to have a unique ID ranging from 1 to 255. It is a good idea to use a standardized numbering solution; for example, all 1xx serverids are Streamers and all 2xx server IDs are Vaults.

vault
This parameter has the IP address of a Vault in the system. Each “vault” line represents an individual Vault. There may be multiple vault lines. Starting from Release 3.9.1, if a replication group is created for vault server type, the replication group ID is also specified in the third column to indicate the replication group to which the vault belongs. If the server is not assigned to any of the replication group, the replication group ID is assigned 0.

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. Starting from Release 3.9.1, if a replication group is created for streamer server type, the replication group ID is also specified in the third column to indicate the replication group to which the server belongs. If the server is not assigned to any of the replication group, the replication group ID is assigned 0.

cache
This is the IP address of a Cache in the system. Each “cache” line represents an individual Cache. There may be multiple cache lines. Starting from Release 3.9.1, if a replication group is created for cache server type, the replication group ID is also specified in the third column to indicate the replication group to which the server belongs. If the server is not assigned to any of the replication group, the replication group ID is assigned 0.

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. The default replication group ID for controller is 0.

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 name of the management interface. If NIC bonding is enabled, bond0 is displayed.

**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 are intended for the database.

**dbnetport**

This is the port number where the applications address messages are 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.

**vproxy**

The virtual IP address of replication group master of vault server type. The replication group ID is indicated in the third column.

**sproxy**

The virtual IP address of replication group master of streamer server type. The replication group ID is indicated in the third column.

**cproxy**

The virtual IP address of replication group master of cache server type. The replication group ID is indicated in the third column.

Sample .arroyorc file of vault after a replication group is created

```
[root@cc_rtsp_v1_190 ~]# cat /home/isa/.arroyorc
self 1
repgpid 1
groupid 250
serverid 190
partno CDE220-2A-C
mgmtif eth0
dbdomsoc /tmp/isadb
ingestif 1
controller 10.197.102.179 0 -> Default id for controllers
vault 10.197.102.191 3 -> Replication group id 3
vproxy 10.197.102.196 4 -> Replication group id 4
cproxy 10.197.102.180 5 -> Replication group id 5
```
Description of the replication_config Settings

This section describes the different parameters of the replication config file. The .replication_config file is located in the /home/isa directory and is created once a replication group is configured. This file contains the same fields as .arroyorc file and three additional fields for all replication group masters.

vproxy
The virtual IP address of replication group master of vault server type. The replication group ID is indicated in the third column.

sproxy
The virtual IP address of replication group master of streamer server type. The replication group ID is indicated the third column.

cproxy
The virtual IP address of replication group master of cache server type. The replication group ID is indicated in the third column.

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-9 for more information.

groupid #
An identifier that identifies the group of servers within the VDS. See the “groupid” section on page A-9 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-22.

### 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.
**igb adapters**
The maximum transmit bandwidth of the igb 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 protocol timing log file.

**test #**
Specifies the test mode of the server. The default is 4, which means to run the server in production mode.

**cache_dscp #**
Used to set the DSCP bits on cache-fill packets. The default value is 0.

**cache_ecn #**
Used to set the ECN bits on cache-fill packets. The default value is 0. This parameter should not be used.

**transport_dscp #**
Used to set the DSCP bits on transport/streaming packets. The default value is 0.

**transport_ecn #**
Used to set the ECN bits on transport/streaming packets. The default value is 0. This parameter should not be used.

**trickspeedsv2 # # # # # # # #**
Used to specify up to 8 speeds for generating trick objects during ingest. This parameter is applicable only to Vaults. The defaults are 5, –5, 10, –10, 32, and –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** 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.

```plaintext
default source ip <ip in dot notation> tport <minportno> - <maxportno> cport <portno>
```

Used to affect source packets if no specific information is provided in the individual mandatory e1000 interface entries.

- **ip**—The default source IP address for an interface. This value is overridden by the mandatory e1000 interface entry. This IP address is not meaningful in a Layer 3 network. However, today it must have a non-zero value for the other values to be looked at.

- **tport**—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.

```plaintext
bms address <ip> <port>
```

The IP address and port of the back office.

```plaintext
enable MD5Checksum <0 or 1>
```

Specifies the setting to generate MD5Checksum for the content. This parameter is applicable only to vaults.

```plaintext
enable role fail over DbDown <0 or 1>
```

To perform the role fail over on DB connectivity loss on Streamers/SSVs, set it to 1, otherwise set it to 0. This parameter is applicable only to Streamers/SSVs.
db connectivity retry count #

Used to set the maximum number of times to re-try before confirming DB connectivity loss. Check this value check prior to doing fail over on streamers when the enable role fail over DBDown is set to 1. The default value is 30. The valid range is 10 to 10000. This parameter is applicable only to Streamers/SSVs.

stream mpeg pause behavior <0 or 1 or 2>

Specifies the behavior of streamer on issuing a pause in the STB.

- Set to 0 if you want streamer to stream only null packets and maintain a constant bit rate on issuing a pause in the STB. The default behavior is Only Null Packets
- Set to 1 if you want streamer to stream dummy P-frames and maintain a constant bit rate on issuing a pause in the STB.
- Set to 2 if you want streamer to stream PCR packet at less than 100msec interval along with null packets and maintain a constant bit rate on issuing a pause in the STB.

This parameter is applicable only to Streamers.

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"
```

```diff
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
```

```diff
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
```

```diff
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
```

VDS-Related Releases

The RTSP VDS 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 VDS RTSP overlay image, enter the following command:

```
# cat /arroyo/image/tags
```

```diff
linux/linux              kernel-2_6_18-2009-01-15-01
snmp/statsd              statasd-2009-01-14-03
snmp/agent.531           snmpd-2009-01-16-01
```
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 CSserver on the Streamer, Vault, or ISV, enter the following command:

```
# strings avs_cserver.ko | grep CServer
Average setup time spent in CSserver =
AVS CSserver Release #1-Ncserver-e013-2008-11-17-05 Mon Nov 17 18:54:01 PST 2008
ENV_ISA_SR DEBUG
AVS CSserver 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 CSserver settings, status, and version, enter the following command:

```
# cat /proc/calypso/status/server_settings
AVS CSserver 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
eth13       4       465        3439540716        4454799830
```

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:

1. Reboot the server.
2. When a blue screen displays a list of Linux versions, press the `E` key to edit the kernel entry.
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.
4. Remove the 115200 from the console parameter (for example, `console=ttySO,115200n8`).
5. Add the word “Single” or the letter “S” to the end of the line.
6. Press **Enter**.
7. Press the `B` key to boot the Linux kernel into single-user mode.
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**

The disk drive order is irrelevant when reinserting disk drives after transporting a chassis, or transferring disk drives from one chassis to another.

To view the statistics of the internal boot drive, the disk drive that contains the software, enter the `df -k` command.

```
# df -k
```

```
Filesystem  1k-blocks   Used   Available Use% Mounted on
/dev/hda1   10317828 3764936   6028776  39% /       
/dev/hda2   20641788 1711372  17881776   9% /arroyo 
/dev/hda3 32542772  1828  17881776  1% /arroyo/db
/dev/hda6 35641888 1185880  32645480   4% /arroyo/log
none       1681200        0  1681200   0% /dev/shm
```

To view the statistics of a removable SATA or SCSI disk drive, use the following commands:

```
# cat /proc/calypso/status/streamer/diskinfo
```

```
Disk Info:  
Disks(12) Op(12)  
Storage: T(804G) A(21%) U(0)  
BW: (99%) w(1.35M/s) r(0/s)  
I/O Util: w(1.0%) e(0) a(0%)  
Disk[ 2][67.0G] A[20%] B[0x]  
Disk[ 3][67.0G] A[21%] B[0x]  
Disk[ 4][66.5G] A[22%] B[0x]  
Disk[ 5][67.0G] A[20%] B[0x]  
Disk[ 6][67.0G] A[21%] B[0x]  
Disk[ 7][67.0G] A[20%] B[0x]  
Disk[ 8][67.0G] A[20%] B[0x]  
Disk[ 9][67.0G] A[21%] B[0x]  
Disk[10][67.0G] A[20%] B[0x]  
Disk[12][67.0G] A[20%] B[0x]  
```
CDSM GUI Disk Monitor Page Reports a Disk Warning

If the CDSM GUI Disk Monitor page reports a disk warning, check the disk drive status in the /arroyo/log/protocoltiming.log.<date> log file and the /var/log/debugmessages log file.

```
# 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 19:03:46 vault219 kernel: Waiting for 8 disks to finish initializing
Nov 20 19:03:47 vault219 kernel: Waiting for 7 disks to finish initializing
Nov 20 19:03:47 vault219 kernel: Waiting for 6 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 5 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 4 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 3 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 2 disks to finish initializing
Nov 20 19:03:48 vault219 kernel: Waiting for 1 disks to finish initializing
Nov 20 19:03:50 vault219 kernel: Total disk space = 24.0TB on 24 disk drives (Lost disks = 0)
```

**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 run Setup
```

*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**.

Step 6  Press **F10** to save and exit the BIOS Setup Utility.

---

Disabling USB Ports and Password-Protecting the BIOS

Disabling USB Ports and Password-Protecting the BIOS

The following procedure provides instructions on disabling the USB ports and password-protecting the BIOS. Disabling the USB ports and password-protecting the BIOS provides a way to secure the server from anyone outside the allowed administrative group from accessing the server through the USB port.
If the USB port is required to perform an operation (for example, a software upgrade), the operator can log in to the BIOS using the BIOS password and enable the USB port for the operation. After the operation is complete, the operator logs back in to the BIOS and disables the USB port.

To set the BIOS password and disable the USB ports, do the following:

---

**Step 1** Reboot the server.

**Step 2** To enter the BIOS Setup Utility on a VDS server (Vault, Caching Node, Streamer, or ISV), press the **Delete** key when you see the following text:

*Press DEL to runSetup*

To enter the BIOS Setup Utility on a CDSM or VVIM, press **F2**.

The BIOS menu is displayed with the Main tab selected.

Use the Right Arrow and Left Arrow keys to select a menu tab, and the Up Arrow and Down Arrow keys to select a menu item.

**Step 3** To set the Administrator password, do the following:

- **a.** Use the **Right Arrow** key to navigate to the **Security** menu. The Security options are displayed. The Administrator has read/write permission. The User has read-only permission.

- **b.** Use the **Down Arrow** key to navigate to the **Administrator Password** option and press **Enter**. The Create New Password dialog box is displayed.

- **c.** Enter the password.

To set a user password, use the **Down Arrow** key to highlight the **User Password**, press **Enter**, and enter the password in the Create New Password dialog box.

**Step 4** To disable the USB ports, do the following:

- **a.** Use the **Left Arrow** key to navigate to the **Advanced** menu. The Advanced options are displayed.

- **b.** Use the **Down Arrow** key to navigate to the **USB Configuration** option and press **Enter**. The USB Configuration options are displayed.

- **c.** Use the **Down Arrow** key to navigate to the **USB Controller** and press **Enter**. The USB Controller dialog box is displayed.

- **d.** Use the **Up Arrow** and **Down Arrow** keys to highlight **Disabled** and press **Enter**. The USB Configuration options show Disabled for all USB options.

**Step 5** To save your settings, press **F10**. The Save & Reset confirmation dialog box is displayed.

Use the **Right Arrow** and **Left Arrow** keys to highlight **Yes** and press **Enter**.

---

After rebooting the server, to enter the BIOS Setup Utility, you are prompted to enter the BIOS password. To have read/write permission, enter the Administrator password. To have read-only permission, enter the User password.

To enable the USB ports, reboot the server, do the following:

---

**Step 1** Reboot the server.

**Step 2** Enter the BIOS Setup Utility on a VDS server (Vault, Caching Node, Streamer, or ISV) by pressing the **Delete** key when you see the following text:

*Press DEL to runSetup*
To enter the BIOS Setup Utility on a CDSM or VVIM, press F2.

The BIOS menu is displayed with the Main tab selected.

**Step 3** Use the Left Arrow key to navigate to the Advanced menu. The Advanced options are displayed.

**Step 4** Use the Down Arrow key to navigate to the USB Configuration option and press Enter. The USB Configuration options are displayed.

**Step 5** Use the Down Arrow key to navigate to the USB Controller and press Enter. The USB Controller dialog box is displayed.

**Step 6** Use the Up Arrow and Down Arrow keys to highlight Enabled and press Enter. The USB Configuration options show Enabled for all USB options.

**Step 7** To save your settings, press F10. The Save & Reset confirmation dialog box is displayed.

Use the Right Arrow and Left Arrow keys to highlight Yes and press Enter.

---

### Network

The following commands are useful for checking your network configuration and activity.

To view the ARP table, enter the following command:

```
# arp -a
```

```
jetsam.v.com (111.0.110.151) at 00:00:0C:07:AC:00 [ether] on eth0
VDS17-m1.v.com (111.0.210.170) at 00:30:48:58:58:1A [ether] on eth0
? (111.0.210.175) at 00:30:48:32:0A:5A [ether] on eth0
VDS17-s1.v.com (111.0.210.172) at 00:04:23:DB:89:44 [ether] on eth0
VDS17-s1.v.com (111.0.210.172) at 00:04:23:DB: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 eth0
111.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
0.0.0.0         111.0.210.1     0.0.0.0         UG        0 0          0 eth0
```

To view the VDS 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 VDS routing table, enter the following command:

```
# cat /arroyo/test/RoutingTable
```

```
default gateway 111.1.13.1
network 111.1.13.1 netmask 255.255.255.240 gateway 0.0.0.0
```

To view the VDS remote server table, enter the following command:
# cat /arroyo/test/RemoteServers
remote server
id 141
ip 111.1.9.20
ip 111.1.9.21
ip 111.1.9.22
ip 111.1.9.23
ip 111.1.9.24
end remote server
remote server
id 143
ip 111.1.9.25
ip 111.1.9.26
end remote server
remote server
id 144
ip 111.1.9.27
ip 111.1.9.28
ip 111.1.9.29
ip 111.1.9.30
end remote server

Interface Information

To view basic interface information, use the `ifconfig` command.

```
# ifconfig eth0
eth0    Link encap:Ethernet  HWaddr 00:04:23:D8:9A:80
        inet addr:111.0.110.41  Bcast:111.0.110.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:13946269 errors:0 dropped:0 overruns:0 frame:0
        TX packets:11594110 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 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.

```
# 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-VDS
PCI_Vendor                       0x8086
PCI_Device_ID                    0x10a7
PCI_Subsystem_Vendor             0x15d9
PCI_Subsystem_ID                 0x10a7
PCI_Revision_ID                  0x02
PCI_Bus                         14
PCI_Slot                         0
PCI_Bus_Type                     UNKNOWN
PCI_Bus_Speed                    UNKNOWN
PCI_Bus_Width                    UNKNOWN
IRQ                              194
System_Device_Name               eth0
Current_HWaddr                   00:30:48:C3:26:9E
Permanent_HWaddr                 00:30:48:C3:26:9E

Link                             up
Speed                            1000
```
**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

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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_Carrier_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_Frame_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_CRC_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_FIPO_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Tx_Aborted_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_Over_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Tx_Carrier_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Rx_Long_Length_Errors</td>
<td>0</td>
</tr>
<tr>
<td>Tx_Abort_Late_Coll</td>
<td>0</td>
</tr>
<tr>
<td>Rx_CSum_Offload_Good</td>
<td>406625</td>
</tr>
<tr>
<td>Rx_CSum_Offload_Errors</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHY_Media_Type</td>
<td>Copper</td>
</tr>
<tr>
<td>PHY_Cable_Length</td>
<td>Unknown Meters (+/- 20 Meters)</td>
</tr>
<tr>
<td>PHY_Extended_10Base_T_Distance</td>
<td>Unknown</td>
</tr>
<tr>
<td>PHY_Cable_Polarity</td>
<td>Normal</td>
</tr>
<tr>
<td>PHY_Disable_Polarity_Correction</td>
<td>Enabled</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_MDI_X_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>
Appendix A  Troubleshooting

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.

**Step 1** During the server bootup, press the **Delete** key to enter the BIOS Setup Utility.

**Step 2** Navigate to the Advanced menu and choose **Advanced Chipset Control**.

**Step 3** Choose **ECC Error Type** and change the setting to **NMI** (Figure A-2).

**Figure A-2**  BIOS Setup Utility—Advanced Chipset Control

```
Advanced Chipset Control

<table>
<thead>
<tr>
<th>Function</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAM Data Integrity</td>
<td>Enabled</td>
</tr>
<tr>
<td>ECC Error Type</td>
<td>NMI</td>
</tr>
</tbody>
</table>

When an ECC error occurs, it generates an interrupt. Select the type of interrupt to report: NMI Non-Maskable, SMI System Management, SCI System Control
```

**Step 4** Press **F10** to save and exit.

Serial Console Port Settings

The CDE servers ship with the following serial console settings: 115200 baud rate, no parity, 8 data bits, and 1 stop bit (115200-N-8-1). To verify the serial console settings, check the following:

- **BIOS Settings**—Determines the speed during the very beginning of the boot process up to and including the GRUB menu. In the BIOS Setup Utility, check that the Console Redirection in the Advanced menu is set to VT100.
• /etc/boot/menu.lst—Determines the speed 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
```

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 5-42. 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
```

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 `root` and start the database.

```
$ service avsdb start
```

Log into the server as `root` and start the statsd.

```
$ service statsd start
```

Check that the RTSP listener is running on the correct port.

```
$ vdsServices status
$ netstat -an | grep 554
```

Check if rtsp, avsdb, statsd are running.

### Process Monitoring with monit

The **monit** monitoring application is integrated into the **arroyo** and the **init** script that is used for starting and stopping all FSI/RTSP related applications. When an application is started using the **arroyo start <appname>** or **service <appname> start** command, the **arroyo** script not only starts the application but also instructs **monit** to start monitoring the application while it is running. In the event the application crashes, monit restarts the application. When an application is stopped using the **arroyo stop**
<appname> command or service <appname> stop, not only does the arroyo script stop the application, but it also instructs monit to stop monitoring the application so that there is no race condition where the user is trying to stop the application using the arroyo stop <appname> or service <appname> stop command while monit keeps restarting it. To see if the monit daemon is running on the system, enter the ps -elf | grep monit command.

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 ?        00:00:53 /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.

```
# service vds-httpd 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 VDS, do the following:
**Step 1** Log in to the Vault or Streamer as *root*.

**Step 2** Verify two-way database connectivity with the CDSM.

```bash
# netstat -an | grep 9999
```

**Step 3** Verify statsd is running.

```bash
# ps -aef | grep statsd
```

**Step 4** Verify the correct version and permissions for `/home/stats/svrinit` or `svrinit_15` are being used.

```bash
# ls -l /home/stats/
```

**Step 5** On the Vault and the Streamer, initialize the VDS host in the database by using `svrinit_15`. Use the following options:

- Option `-i` for the server physical IP address (eth0)
- Option `-s` for the subnet mask of the network
- Option `-h` for the host name
- Option `-d` to deregister

For example, first deregister the VDS host using the `-d` option, then initialize the VDS host.

```bash
# svrinit_15 -i <ip_address> -s <subnet_mask> -h <host_name> -d
# svrinit_15 -i <ip_address> -s <subnet_mask> -h <host_name>
```

**Step 6** If you still have trouble getting the tables initialized, then log in to the CDSM GUI with an engineering access user account and add the Streamer or Vault by clicking the **Maintain > Software > System Configs** page and using the **Add New Server** option.

---

**Database Monitoring**

To monitor a stuck database thread problem, use the following command:

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

Two connections for each Vault and Streamer should be listed with a status of “ESTABLISHED.” If two-way connection does not exist, then stop the database using the following command:

```bash
# service avsdb stop
Stopping avsdb: [OK]
```

If the database is stuck and `service avsdb stop` does not take effect, use `ps –ef | grep avsdb` to query the process ID (PID), then use the **kill -9 {pid}** command to kill the avsdb process, and lastly restart the database.

Check the avsdb status using the following command:

```bash
$ service avsdb status
avsdb dead but subsys locked
```
Ingest Issues

This section includes the following ingest issues:

- Ingest Interface, page A-29
- Bad Content, page A-33
- Network, page A-33

Ingest Interface

This section includes the following topics on troubleshooting the ingest interface:

- FSI Starts but Cannot Ingest Content, page A-29
- FSI Does Not Start, page A-29
- Troubleshooting collectd, page A-30
- Content Not Ingesting, page A-30
- Asset Ingest Manager Restart Causes Endless Loop, page A-31
- Asset Ingest Manager crashing, page A-33

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 /arroyo/log/fsi.log when FSI is started.

```
11/05/2008 19:04:50.035191|fsid.cc|444|366702208| Initializing fsi daemon...
11/05/2008 19:04:50.035470|fsid.cc|445|366702208| main(): Thread ID: 366702208
11/05/2008 19:04:50.035520|fsid.cc|447|366702208| Initializing FSI configuration...
11/05/2008 19:04:50.035552|DatabaseConnection.cc|62|366702208| Successfully connected database socket.
11/05/2008 19:04:50.035654|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 4-109 for more information.

**Action 2:** Log in to the server as *root* and start the FSI service.

```
$ service fsi start
```

**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.

**Troubleshooting collectd**

To verify if collectd process is running or not, enter the following command:

```
pgrep collectd
```

To verify the collectd TCP connections to and from the Controllers, enter the following command:

```
netstat -an | grep 8999
```

To start the collectd process, enter the following command:

```
service collectd start
```

To stop the collectd process, enter the following command:

```
service collectd stop
```

If health, Ddisk, vitals, NIC and process status are not displayed correctly for a server then check if collectd is running in the corresponding server and the controller.

**Content Not Ingesting**

**Cause 1:** Cannot connect to the FTP server (for example, Lysis Content Ingest Server).

**Action 1:** Check the network connectivity and user access.

Check the network connectivity, access control lists (ACLs), user access privileges, and so on for the FTP server.

**Action 2:** Verify the manual FTP request.

Verify that a manual FTP request to the FTP server from the user *isa* is working and list the content to be ingested.

**Cause 2:** Content is not correctly named in the ADI XML file.

**Action 1:** View the aim.log file.

```
cat aim.log | grep FTPP
```
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 `service aim stop` command followed by the `service aim start` command.
6. If necessary, restart the FTP server.

**Cause 4:** Asset Name larger than 128 bytes.

**Action 1:** Do the following:

1. Add a line `ASSETNAME_128BYTE_TRUNCATION=1` in `/home/isa/bss/etc/aim.conf` file.
2. Restart AIM.

**Cause 5:** Asset Name larger than 64 bytes.

**Action 1:** Do the following:

1. Add a line `ASSETNAME_64BYTE_TRUNCATION=1` in `/home/isa/bss/etc/aim.conf` file.
2. Restart AIM.

**Cause 6:** Cannot find the file in the FTP server.

**Action 1:** Verify the following:

While ingestion of a VOD asset, VDS-TV is provided with an FTP URL and the FTP URL path must be considered as a relative path instead of an absolute path.

For example, Content URL: ftp://user:pass@ftphost/directorypath/filename.ts
After FTP login and transfer mode settings, the ingest system is expected to GET this file from directorypath/filename.ts and **NOT** /directorypath/filename.ts

### Asset Ingest Manager Restart Causes Endless Loop

**Cause 1:** AIM has orphaned threads.

**Action 1:** Check the aim.log for endless looping message.
Ingest Issues

Appendix A      Troubleshooting

12/12/2007|11:47:16.684597|AIMCache          |0164|01024|Trying to load dynamic libs........
12/12/2007|11:47:16.745753|AIMCache          |0182|01024|Shared lib error[libAVSNGOD_AIM.so: cannot open shared object file: No such file or directory]
12/12/2007|11:47:16.745911|AIMCache          |0182|01024|Shared lib error[libAVSISA_AIM.so: cannot open shared object file: No such file or directory]
12/12/2007|11:47:16.746031|AIMCache          |0182|01024|Shared lib error[libAVSWideVine_AIM.so: cannot open shared object file: No such file or directory]
---

12/12/2007|15:55:20.321800|AIMDbManager      |0021|02051|AIM config change detected.....
12/12/2007|15:55:20.322220|AIMCache          |0316|02051|DB Tag[.0.0.0:20004/][[]
12/12/2007|15:55:20.322670|AIMDbManager      |0054|02051|Config change from [http://0.0.0.0:20004/][]
12/12/2007|15:55:20.323040|AIMDbManager      |0055|02051|Config change to   [.0.0.0:20004/][[]
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|15:56:20.445230|AIMCache          |0316|02051|DB Tag[0004/][[]
12/12/2007|15:56:20.445690|AIMDbManager      |0054|02051|Config change from [.0.0.0:20004/][[]
12/12/2007|15:56:20.446060|AIMDbManager      |0055|02051|Config change to   [0004/][[]
12/12/2007|15:56:20.446900|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 root and stop the AIM service, verify there are no orphaned AIM threads, and restart the AIM service.

```
$ service aim stop
$ ps -aef | grep AVSIngestMgr
 isa    7291  7243   0 20:59 pts/0     00:00:00 grep AVSIngestMgr
$ service aim start
```

Cause 2: The master Vault AIM is in a degraded state.

Check the aim.log on the slave Vault to verify it is in a waiting state.

```
12/12/2007|14:57:08.954182|AVSIngestMgrISA | 0178|01024|******* AIMd starting****
12/12/2007|14:57:08.955726|pTCP              |0065|01024|Host info 10.212.17.12:5555
12/12/2007|14:57:08.961349|pTCP              |0065|01024|Host info *:5555
12/12/2007|14:57:08.961442|pRunMaster        |0029|01024|process is not the master, waiting on notification
```

Action 1: Cause a failover between the master and slave Vaults.
On the master Vault, stop the 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 root and restart the AIM service. This Vault becomes the new standby and the AIM process is in waiting mode.

Asset Ingest Manager crashing

**Cause 1:** AIM content path length greater than 128 bytes

**Action 1:** Verify that the maximum length of the absolute path location of an asset is 128 bytes.

Asset Ingest Manager Response Codes

The response codes sent by the software to back-office at different instances are listed below:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Response Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>No XML on FTP server</td>
<td>500 Internal Server Error</td>
</tr>
<tr>
<td>No video file on FTP server</td>
<td>500 Internal Server Error</td>
</tr>
<tr>
<td>Incorrect username or password on FTP server</td>
<td>500 Internal Server Error</td>
</tr>
<tr>
<td>Incorrect path on FTP server</td>
<td>500 Internal Server Error</td>
</tr>
<tr>
<td>Package ingested into vault</td>
<td>500 Internal Server Error</td>
</tr>
<tr>
<td>Video file ingested into vault</td>
<td>500 Internal Server Error</td>
</tr>
<tr>
<td>No such package</td>
<td>500 Internal Server Error</td>
</tr>
<tr>
<td>No such video file</td>
<td>HTTP/1.1 404 Content Not Found</td>
</tr>
</tbody>
</table>

Bad Content

Variable bit rate (VBR) encoded content is not currently supported. See the “VDS Content Quality Guidelines” section on page A-55 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 VDS, then the network must support jumbo frames. We recommend that the network support jumbo frames even when the jumbo frame option is disabled.
Appendix A  Troubleshooting

Content Processing Issues

This section includes the following content processing issues:

- Listing Content
- Orphan GOID mirroring during reboot of vaults
- Content Mirroring
- Verifying GOIDs
- Trick-Mode Issues

Listing Content

To view the actual stored content versus what the database reports, enter the following commands:

```
$ cd /arroyo/db/avsdb_util/
$ ./avsdb_util.py -s avsdb_tabletemplate.s -i 403 -o db_content_list
$ cat db_content_list/avsdb_util_output.csv
```

Orphan GOID mirroring during reboot of vaults

In steady state with no new contents being added or removed, if constant mirroring activity is seen during reboot of any group of vaults system then:

Enter the following command in all the vaults:

```
echo 1 > /proc/calypso/tunables/performisacheck
```

Content Mirroring

To enable content mirroring locally on one Vault, do the following:

Step 1  Modify the /home/isa/.arroyorc file by adding the following line:

```
cserver_opts "vault local copy count 2"
```

Step 2  Verify that the change has propagated to the /arroyo/test/vault/setupfile file.
The line “vault local copy count 2” should be added to the setupfile file.

Alternatively, enable local mirroring using the tunables. You can also use the tunables to verify the settings.

```bash
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 4-85.

**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:

```
$ 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:

- Tracking Cache-Fill Source
- Rules for ISV Interoperability with Vaults and Streamers
- Network

**Tracking Cache-Fill Source**

You can track whether or not a GOID for a stream is filling remotely or locally by enabling and tracking it in the fill.log. Streams can share the same GOID; in which case it is not possible to tell which stream is currently filling the data.

To track the cache-fill source of a stream, do the following:

**Step 1**
Find the stream that is playing in the c2k.log on the Streamer, along with the content that was requested (GOID number).

**Step 2**
Enable the fill.log on the Caching Nodes the Streamer is mapped to.

```
echo 1 */proc/calypso/tunables/enableFillLog
```

**Step 3**
On the Caching Nodes, use the `tail` command to follow the log and `grep` for the GOID.

Following is an example fill.log:

```
18:30:23  44 DISK 000814a4132455c4 0000c1f7 to 00014e3e 0ea6 FINISHED 0x0000f558
18:30:23  4 NET  000864b26ab0a076 3fde3a14 to 3fe86299 3a98 TRUNCATE 0x3fdeb83c
18:30:24  4 NET  000864b26ab0a076 3fde3a14 to 40000000 3a98 FINISHED 0x3fdeb834
18:30:24  4 NET  000864b26ab0a076 3fde3a14 to 3fdeb83c 3a98 CANCEL 0x3fdeb93e
18:30:25  44 DISK 000884b7c94042f4 3ff3730d to 3ffca5d0 3a98 CANCEL 0x3f3fcb5
18:30:25  43 DISK 000884b7c94042f4 3ff3730d to 3ffca5d0 3a98 FINISHED 0x3f3fcb5
18:30:27  43 DISK 000814a4132455c4 001fadb to 0002d79d 0ea6 START  delay 14376
18:30:28  43 DISK 000854b26ab11667 3ffdbb92 to 3fffd4198 0ea6 FINISHED 0x3fffd4198
```

START - fill started from DISK or NET
FINISHED - fill finished
CANCEL - fill cancelled
TRUNCATE - fill truncated to new ending sector offset
Burst and delay times are in microseconds. Bursts are sent immediately at a high rate. The delay time specifies when to start sending the data at rate, up to 30 seconds into the future.

If no Caching Nodes are reporting fill for the GOID, then the content is being filled from memory.

**Step 4**

Disable the fill logs on the Caching Nodes when finished.

```
    echo 0 > /proc/calypso/tunables/enableFillLog
```

---

### 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

For more network troubleshooting methods, see the “Network” section on page A-33.

---

### 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:c2k_p_setdestination: stream 3 localStreamHandle 0 ip 0xe0016401 port 10000
15-Jan-2008 20:42:41 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

==> rtsp.log <=
01/15/2008|21:43:03|3.585614|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|21:43:03.585846|StreamImpl.cc|1981|Stream Position       = 1152089708
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|*****************************************************************************
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 5-26.

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
- back office is out of synchronization with the VDS 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.<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 5-35.

**Action 2:** Set up a stream to play to a multicast address.

If this is successful, then there is a network problem, which is either a default gateway or unreachable remote client. You can verify whether it is successful by looking at the /home/stats/ifstats information.

**Action 3:** If streaming to a multicast address is not successful, check that the Vaults can be reached.

Check the /arroyo/log/protocoltiming.log.<date> log file for the number of reachable remote servers. Additionally, if there is a cache-fill issue, you will see a large megabit value for the re-xmit buffer.

You can also check the /arroyo/log/c2k.log.<date> log file for any unreachable Vaults.

**Cause 3:** The c2k.log file reports “no streamer available, out of capacity.”

The protocoltiming.log file reports “remote vaults 0 caches 0.” This means the Streamer and Vault have lost connection with each other.

**Action 1:** Check the route configured on the servers.

Use the `cat /arroyo/test/RoutingTable` command to verify correct route table entries.

Check the routing table using the CDSM GUI by clicking **Configure > Server Level > Route Tables**. For more information, see the “Configuring the Route Table” section on page 4-93.
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 set-top
- VDS Is Streaming but No Video Is Playing on the set-top

**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:
    ```bash
    /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 VDS 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:
    ```bash
    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.
Appendix A      Troubleshooting

Streaming and Playout Issues

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
# service rtsp start
```

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 /arroyo/log/rtsp.log file for the set-top responses within the
inactivity timeout interval.

This scenario could be caused by the set-top possibly not responding, or the set-top response may be
going lost in the network.

No Video Playing on the set-top

Check the /arroyo/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 set-top
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=CAN36099.mpg RTSP/1.0 CSeq: 10 User-Agent: OpenTV VOD 1
Transport: MP2T/DVBC/QAM;unicast;client=168892769.6501124101;destination=172.23.68.2;client_port=1
06/13/2007|20:23:33.548631|RTSPPTCListener.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|20:23:33.548886|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|20:23:33.549416|StreamImpl.cc|1745|Stream setup - URL = CAN36099.mpg, downstream address = -10.0.0.0!172.23.68.2!1
06/13/2007|20:23:33.550150|QuativeSession.cc|782|SETUP Response: RTSP/1.0 200 OK CSeq: 10 Session:1179649; timeout=300
Transport: MP2T/DVBC/QAM;unicast;client=168892769.6501124101;destination=172.23.68.2;client_port=1
Location:rtsp://10.212.16.18:554
06/13/2007|20:23:33.550377|PersistenceConnection.cc|137|Repository operation successfully completed
06/13/2007|20:23:37.313753|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:23:37.325864|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:25:37.39193|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:26:37.350250|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:27:37.362401|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:28:37.374832|RTSPMsgHandler.cc|1161|In production mode, accepting incoming SETUP requests
06/13/2007|20:29:13.075941|LivenessManager.cc|213|Session has timed-out, initiating teardown process.Session: 1179649
06/13/2007|20:29:13.076127|RTSPMsgHandler.cc|671|Current session count = 1
```
VDS Is Streaming but No Video Is Playing on the set-top

Check the /arroyo/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 VDS.
- Describe request is sent from the set-top, followed by describe ok response and details returned from VDS.
- Play request is sent from set-top, followed by play ok response sent from VDS.
- Teardown request is sent from set-top, followed by teardown performed by VDS.

The possible causes for the above message flows are the following:

- set-top 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 VDS. 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 set-top.

Following is an example of the rtsp.log file showing the request and response messages.

```
11/29/2007|16:10:57.195106|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
11/29/2007|16:10:57.195911|QuativeSession.cc|684|Message: RTSP/1.0 200 OK M CSeq: 90 M Session: 30801921 M Content-Type: application/sdp M Content-Length: 170 M v=0 M o=- 3405337857 3405337857 IN IP4 10.236.141.67 s=RTSP Session t=0 0 M m=video 0 udp M2T M c=IN IP4 0.0.0.0 i=CAN0000095932.mpg a=type:vod a=range:npt=0.0-3814.142
11/29/2007|16:10:57.195975|QuativeSession.cc|694|Successfully sent message to STB
11/29/2007|16:10:57.377850|RTSPTCPListener.cc|298|Valid RTSP request received. port = 554
11/29/2007|16:10:57.377986|RTSPMsgHandler.cc|644|Current session count = 1
11/29/2007|16:10:57.378120|StreamImpl.cc|1121|play(*, from: 0 to: 2147483647)
11/29/2007|16:10:57.378179|StreamImpl.cc|588|handleContent(), url: *, play content now: 1, no flush: 0
11/29/2007|16:10:57.378235|StreamImpl.cc|697|handlePlay(), loop content: 0, play content now: 1, no flush: 0
```

```
SETUP rtsp://87.231.193.114:554/?AssetId=CAN0000095932.mpg RTSP/1.0 CSeq: 2 M User-Agent: OpenTV VOD 1 M Transport: MP2T/DVBC/QAM;unicast;client=170027388.4312020202;destination=172.23.77.2;client_port=16 M
11/29/2007|16:10:56.952766|RTSPQuativeSession.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|16:10:56.956430|QuativeSession.cc|786|SETUP Response: RTSP/1.0 200 OK CSeq: 2 M Session: 30801921 M Transport: MP2T/DVBC/QAM;unicast;client=170027388.4312020202;destination=172.23.77.2;client_port=16 M Location: rtsp://87.231.193.114:554 M
11/29/2007|16:10:57.195106|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
11/29/2007|16:10:57.195911|QuativeSession.cc|684|Message: RTSP/1.0 200 OK M CSeq: 90 M Session: 30801921 M Content-Type: application/sdp M Content-Length: 170 M v=0 M o=- 3405337857 3405337857 IN IP4 10.236.141.67 s=RTSP Session t=0 0 M m=video 0 udp M2T M c=IN IP4 0.0.0.0 i=CAN0000095932.mpg a=type:vod a=range:npt=0.0-3814.142
11/29/2007|16:10:57.195975|QuativeSession.cc|694|Successfully sent message to STB
11/29/2007|16:10:57.377850|RTSPTCPListener.cc|298|Valid RTSP request received. port = 554
11/29/2007|16:10:57.377986|RTSPMsgHandler.cc|644|Current session count = 1
11/29/2007|16:10:57.378120|StreamImpl.cc|1121|play(*, from: 0 to: 2147483647)
11/29/2007|16:10:57.378179|StreamImpl.cc|588|handleContent(), url: *, play content now: 1, no flush: 0
11/29/2007|16:10:57.378235|StreamImpl.cc|697|handlePlay(), loop content: 0, play content now: 1, no flush: 0
```
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:

```bash
grep "RTSP/1.0 4" rtsp.log
grep "RTSP/1.0 5" rtsp.log
```

To search for content read errors, use the following command:

```bash
grep "Error Reading Content Data" rtsp.log
```

To search for stopped sessions, use the following command:

```bash
grep "stream_session: stopped" rtsp.log
```

To search for SETUP requests, use the following command:

```bash
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.
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)
- 2105 Pause Timeout Reached
- 2108 Duplicate QAM Detection
- 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.
- 8801/2107 When Session reaches live point the RTSP server sends either 8801 or 2107 as announce codes to the set top depending on the configuration. The default value is 8801 and when DROP1x is enabled, the announce code sent is 2107.

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-5 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>
This section covers the following database issues and troubleshooting methods:

- Database Replication
- Corruption Recovery

### Database Issues

<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)

<table>
<thead>
<tr>
<th>State</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSF_DUPLICATE_QAM_DETECTION</td>
<td>677</td>
<td>return &quot;Server Setup Failed - Duplicate QAM Detection&quot;</td>
</tr>
<tr>
<td>SSF_ASSET_NOT_FOUND</td>
<td>771</td>
<td>return &quot;Server Setup Failed - Asset Not Found&quot;</td>
</tr>
<tr>
<td>SSF_SOP_NOT_AVAILABLE</td>
<td>772</td>
<td>return &quot;Server Setup Failed - SOP Not Available&quot;</td>
</tr>
<tr>
<td>SSFUNKNOWN_SOP_GROUP</td>
<td>773</td>
<td>return &quot;Server Setup Failed - Unknown SOP Group&quot;</td>
</tr>
<tr>
<td>SSFUNKNOWN_SOP_NAMES</td>
<td>774</td>
<td>return &quot;Server Setup Failed - Unknown SOP Names&quot;</td>
</tr>
<tr>
<td>SSFINSUFF_VOLUME_BW</td>
<td>775</td>
<td>return &quot;Server Setup Failed - Insufficient Volume Bandwidth&quot;</td>
</tr>
<tr>
<td>SSFINSUFF_NETWORK_BW</td>
<td>776</td>
<td>return &quot;Server Setup Failed - Insufficient Network Bandwidth&quot;</td>
</tr>
<tr>
<td>SSFINVALID_REQUEST</td>
<td>777</td>
<td>return &quot;Server Setup Failed - Invalid Request&quot;</td>
</tr>
<tr>
<td>SSFINTERNAL_ERROR</td>
<td>778</td>
<td>return &quot;Server Setup Failed - Internal Error&quot;</td>
</tr>
</tbody>
</table>
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
```

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-47.

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:

- Database could not be started. See the “Services Monitor” section on page 5-42 for more information.
Bidirectional connections are lost between servers. See the “Required Services Not Starting or Running Correctly” section on page A-26.

The following error message is listed in the /arroyo/log/avsdb-err.log.yyyyMMdd file:

tavsdb: unable to allocate memory for mutex; resize mutex region

```bash
# tail -f avsdb-err.log.20081111
```
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region
tavsdb: unable to allocate memory for mutex; resize mutex region

The /home/isa/Berkeley/DATADIR/REPLAY.db file increases to several GB.

```bash
$ ls -ltr
```
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002824
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002825
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002826
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002837
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002838
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002839
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002840
-rw-r----- 1 isa isa 10485760 Nov 11 17:46 log.0000002841
-rw-r----- 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-47.

### Corruption Recovery

**Caution**

Escalate to tier-three support before making any intrusive database changes.

If the CDSM database is corrupted and the Vault database is not corrupted, do the following:

---

**Step 1**

As user `root`, stop the CDSM database.

```
# service avsdb stop
```

**Step 2**

Confirm that the database is shut down.

```
# ps -ef | grep avsdb
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
```
Check avsdb status using the following command:

```bash
# service avsdb status
avsdb dead but subsys locked
```

if "avsdb dead but subsys locked" message appears then remove the file /var/lock/subsys/avsdb and start avsdb

```bash
# service avsdb status
avsdb is stopped
```

**Step 3**  
Delete all files in the /arroyo/db/DATADIR directory.

**Step 4**  
As user `root`, stop the Vault database.

```bash
$ service avsdb stop
Stopping avsdb: [OK]
$
```

**Step 5**  
Confirm that the database is shut down.

```bash
# 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.

```bash
$ service avsdb start
Starting avsdb: [OK]
$
```

**Step 8**  
As user `root`, restart the CDSM database.

```bash
$ service avsdb start
Starting avsdb: [OK]
$
```

**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 VDS 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 4-27 for more information.

3. Upload channel schedules by importing the electronic program guide (EPG). See the “Uploading an EPG File” section on page 7-22 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 VDS 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 /arroyo/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.

**Ingest Troubleshooting with SSM enabled**

For a live recording with real time capture type and source specific multicast support enabled, while recording if there is a primary source (feed) problem recording vault will failover to secondary source(if available). Default timeout for this source failover is 30 seconds. This value can be adjusted with a tunable `/proc/calypso/tunables/recording_nodatatimeout` up to 10 seconds.

**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 F-3.
**Frequently Asked Questions**

**Q.** How do I check and make sure the database is running properly?

**A.** After starting the database, you should see two sockets (listening and non-listening) connecting to the database on each of the remote servers on port 9999. You can check them by using the `netstat -an | grep 9999` command.

For example, the following output of the `netstat` command shows that the server (172.22.97.194) has both the listening and non-listening sockets binding on port 9999 to echo the four remote servers (172.22.97.192, 172.22.97.193, 172.22.97.195 and 172.22.97.191).

```
# netstat -an | grep 9999
tcp 0 0 172.22.97.194:9999 172.22.97.195:48652 ESTABLISHED
tcp 0 0 172.22.97.194:9999 172.22.97.191:42732 ESTABLISHED
tcp 0 0 172.22.97.194:54563 172.22.97.195:9999 ESTABLISHED
tcp 0 0 172.22.97.194:39342 172.22.97.191:9999 ESTABLISHED
tcp 0 0 172.22.97.194:9999 172.22.97.192:40207 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/.arroyorc` file.

**Serviceability and Manageability**

**Q.** How do I check the calypso server status?

**A.** Log in to the server as `root` and enter the `cat /proc/calypso/status/server_settings` command.

**Q.** How do I check central processing unit (CPU)?

**A.** Log in to the server as `root` and enter the `cat /proc/cpuinfo` command.

**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:

```
# service vds-httpd stop
# service vds-httpd start
# service vds-httpd 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?
A. `# 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=tty0 console=ttyS0,115200
kdb=off panic=1
```

Q. What do I do if the KDB prompt is displayed when the server restarts after a failure?
A. Boot into single user-mode (see the “Kernel Crash” section on page A-17).

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]# $ service avsdb stop
Stopping avsdb: [OK]
$ [root@ssv3 root]# $ ps -ef |grep avs
Wait for all avs processes to stop, then reboot the server.
[root@ssv3 root]# $ reboot
```

Q. How do I check the routing table and gateway?

A. Log in to the server as `root` and check the file `/arroyo/test/RoutingTable`.

```
# cat /arroyo/test/RoutingTable
default gateway 192.169.131.250
network 192.169.131.0 netmask 255.255.255.0 gateway 0.0.0.0
default cache gateway 192.169.131.250
local cache network 192.169.131.0 netmask 255.255.255.0
```

Q. How do I get information on a content stream that seems corrupted; for example, there is macroblocking, the stream stops and restarts, and so on?

A. Log in to the server as `root` and enter the following commands:

```
# echo 2 > /proc/calypso/tunables/cm_logserverinfo
# cat /arroyo/log/serverinfo.log.01132009
```

Check the last set of output lines to see the current content states.

Object Count=37708 LengthUnknown=0
CouldNotRepair=0 IsDamaged=0 BeingRepaired=0 BeingCopied=0
needCrcValidate=37708 isFragFlag=0 isFragd=0 Defrag=0 Smooth=0
BeingFilled=0 OutOfService=0 NeedsISACheck=0
BeingDeleted=0 HasHoles=0 CopyHoles=0 SectorHoles=0
Object Status Check Complete.

Q. How do I know if a content object has “holes”?

A. Log in to the server as `root` and view the `/var/log/debugmessages`. There is a message in the debug messages file about the GOID and the content holes.

Q. How do I delete ingests that are “stuck” in the active ingest state?
A. Log in to the server as root and do the following:

- Create a file that details a list of actions to perform. The following command

  ```
  $ cat delete
  3, 403, one.mpg
  ```

  displays the contents of the file ‘delete’ which indicates “one.mpg” asset should be deleted from table 403.

- Execute the following utility:

  ```
  $./avsdb_util.py -s avsdb_tabletemplate.s -i <input_action file> -o <output_directory>
  ```

  EXAMPLE

  ```
  $./avsdb_util.py -s avsdb_tabletemplate.s -i delete -o DEL
  ```

  where:

  - avsdb_util.py is a python utility
  - avsdb_tabletemplate.s is a file containing details of all tables fixed for a release
  - input_action_file is an input file containing a list of actions to perform
  - output_directory dumps output to this directory in a file named "avsdb_util_output.csv"

  WARNING: DEL directory is not available
  WARNING: Will create DEL output directory to proceed further

  ```
  $ cat DEL/avsdb_util_output.csv
  ```

Q. How do I manually ingest content from the command line?

A. Log in to the server as root and enter the following commands:

  ```
  # su - isa
  # cd ~/SDClient
  ```

  Update the SDClient.cfg file with the local IP address.

  ```
  # ./sdClient
  ```

  Follow the SDClient menus.
Other

Q. How do I view the CServer code configuration file?

A. Log in to the server as root and enter the `cat /arroyo/test/<server type>/setupfile` command. The server type is one of the following: vault, streamer, or ssv.

```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 3 1 maxrate 900000 localip 0c0a80040
localip 0c0a80040
e1000 adapters: maxrate 965
e1000 0: streaming 1 fill 0
e1000 1: streaming 1 fill 0
e1000 3: streaming 0 fill 1

streamer 1 vault 1
serverid 64
groupid 64
maxpacketsize 1316
management eth0
ingest eth0
trickspeedsv2 10 0 0 0 0 0 0 0
ftpout if eth0 max utilization mbps 0 max sessions 0
fake cylindermap 1
test 4
```

Q. How do I know if a subsystem on a server is overloaded?

A. View the `.arroyo.log.protocoltiming.log.<date>` file. When you see the “COST REQUEST NO CAPACITY;” message, it means that the server is running out of capacity and it cannot accept new streaming requests.

Also, when you see a line in the `/arroyo/log/c2k.log.<date>` file that says the following:

```
01-May-2007 17:40:44 UTC :err:ServeStream::reserveStream: refused streamhandle 4 for
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:

```bash
# su - isa
# cd ~/StreamsDriver
# touch DEBUGGING_ON
# ~/IntegrationTest/debugging_on_off
# ./stop_driver
# ./run_driver
```

Q. How do I update the remote server from /arroyo/test/RemoteServers?

A. Log in to the server as root and enter the following commands:

```bash
# echo 1 > /proc/calypso/test/readremoteservers
```
VDS 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 30 Mbps. There is no minimum bit rate. The ES video bit rate, as specified in the MPEG-2 sequence header, is ignored. The bit rate of an individual ES is not significant. The aggregate transport stream must have a constant bit rate. An individual ES (particularly, the video ES), however, does not have this bit rate requirement.

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. If ingested as a single item, the content must be under 12 hours in duration or under 30 GB in size, whichever occurs first. If the content is chunked, the overall size of the content must be under 120 GB, while there is no restriction on the duration of the content.
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-tops.

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 VDS 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-12
- Creating Stream Destination Bulk Configuration Files, page B-14
- Creating Route Table XML Configuration Files, page B-15
- Creating SNMP Agent XML Configuration Files, page B-16
- Creating DNS Server XML Configuration Files, page B-17
- Creating NTP Server XML Configuration Files, page B-18
- Creating FSI Setup XML Configuration Files, page B-19
- Creating RTSP Setup XML Configuration Files, page B-20
- Creating Logging XML Configuration Files, page B-23
- Creating Syslog XML Configuration Files, page B-24
- Creating Server Setup XML Configuration Files, page B-25
- System-Level Configuration XML Schema, page B-29
- Array-Level Configuration XML Schema, page B-52
- Server-Level Configuration XML Schema, page B-70
- Maintain Section Configuration XML Schema, page B-88

**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 System-Level CDSM configuration pages that offer Bulk Configuration by importing the Bulk Configuration XML file:

- QAM Gateway
- Headend Setup (For gigabit Ethernet streaming mode. ASI streaming headend configuration is imported as part of the QAM Gateway page configuration importing.)
- Stream Destination
Introduction

To enable the optional Bulk Configuration feature with the Backup and Restore capabilities, see the “Bulk Import/Export Configuration” section on page F-5.

The Bulk Import/Export Configuration option provides the following features:

- System Level Configuration Backup and Restore
- Array Level Configuration Backup and Restore
- Server-Level Configuration Backup and Restore
- Maintain Section Configuration Backup and Restore

System Level Configuration Backup and Restore

All system-level configuration pages are supported, except Error Repair, Billing Service, and Shared Recorder Setting.

Through the System-Level Configuration Backup and Restore feature, it is possible to backup (export) the system-level configuration for all VDS servers in a system, modify the parameters as appropriate, and restore (import) the configuration to all VDS servers in the existing system or all VDS servers in a new system.

In addition to complete backup and restore functionality for all system-level configurations for the specified VDS servers, this feature also offers export and import on each system-level configuration page for all VDS servers managed by the CDSM (or VVIM).

Note

The restore and import function does not overwrite the following pre-existing system-level configuration settings:

- System DNS
- System NTP
- Host Service
- QAM Gateway
- Stream Destination
- Parent/Child Service Groups
- Input Channels
- Output Channels
- Source Output Port

All other supported pre-existing system-level configuration settings are overwritten.

Using the System-Level Configuration Backup and Restore Feature

Using the Backup and Restore feature involves the following tasks:

- Backup or Restore the System-Level Configuration
- Export or Import Specific System-Level Configurations
Appendix B      Creating Bulk Configuration Files

Introduction

Backup or Restore the System-Level Configuration

The Backup & Restore page offers the ability to backup all the system-level configuration parameters of the VDS, modify the configuration parameters as appropriate, and restore all the system-level configuration parameters to a new VDS or the existing VDS.

To backup the system-level configuration, do the following:

Step 1  Choose Maintain > Software > Backup & Restore. The Backup and Restore page is displayed.
Step 2  From the Configuration Level drop-down list, select System Level.
Step 3  Click Backup.

The File Download dialog box is displayed offering you the options to Save, Open, or Cancel the action. Save presents a Save As dialog box, which allows you to select the location and filename used to save the XML file. Open opens the XML file.

To restore a backup, do the following:

Step 1  Choose Maintain > Software > Backup & Restore. The Backup and Restore page is displayed.
Step 2  Click Browse to navigate to the XML configuration file to restore. The Choose File to Upload dialog box is displayed.

The last location that was accessed to either save a backup or restore a configuration file is remembered.
Step 3  Navigate to the location where the XML configuration file was saved, select it, and click Open.

The file location and filename are displayed in the Configuration File Location text box.
Step 4  Click Restore.

The backup configuration XML file is restored to all servers specified in the backup.

Export or Import Specific System-Level Configurations

The Import/Export System Configuration option offers the ability to export or import the specific system-level configuration for all the VDS servers. All system-level configuration pages are supported, except Error Repair, Billing Service, and Shared Recorder Setting.

After the export XML configuration file has been created, you can edit the values of the configuration parameters as appropriate for the existing VDS or a new VDS.

To export or import the configuration of a specific System Level configuration page for all VDS servers, do the following:

Step 1  Display the System Level configuration page by choosing Configure > System Level and one of the supported system-level configuration pages.
Step 2  To export the configuration to an XML file, click Export.

The File Download dialog box is displayed offering you the options to Save, Open, or Cancel the action. Save presents a Save As dialog box, which allows you to select the location and filename used to save the XML file. Open opens the XML file.
Step 3  
To import a configuration XML file, do the following:

a. Click Browse to navigate to the XML configuration file to restore. The Choose File to Upload dialog box is displayed.

   The last location that was accessed to either save a backup or restore a configuration file is remembered.

b. Navigate to the location where the XML configuration file was saved, select it, and click Open.

   The file location and filename are displayed in the Configuration File Location text box.

c. Click Import.

   The backup configuration XML file is restored to all servers specified in the XML configuration file.

---

Array Level Configuration Backup and Restore

All array-level configuration pages are supported, except Error Repair, Session Gateway, Manual Ingest, Media Scheduler, Barker Stream/Playlist, Playout Scheduler, Playout Exporter, and EPG Exporter.

Through the Array-Level Configuration Backup and Restore feature, it is possible to backup (export) the array-level configuration for all VDS servers in a system, modify the parameters as appropriate, and restore (import) the configuration to all VDS servers in the existing system or all VDS servers in a new system.

In addition to complete backup and restore functionality for all array-level configurations for the specified VDS servers, this feature also offers export and import on each array-level configuration page for all VDS servers managed by the CDSM (or VVIM).

Using the Array-Level Configuration Backup and Restore Feature

Using the Backup and Restore feature involves the following tasks:

- Backup or Restore the Array-Level Configuration
- Export or Import Specific Array-Level Configurations

Backup or Restore the Array-Level Configuration

The Backup & Restore page offers the ability to backup all the array-level configuration parameters of the VDS, modify the configuration parameters as appropriate, and restore all the array-level configuration parameters to a new VDS or the existing VDS.

To backup the array-level configuration, do the following:

---

Step 1  Choose Maintain > Software > Backup & Restore. The Backup and Restore page is displayed.

Step 2  From the Section Level drop-down list, select Configure Level.

Step 3  From the Configuration Level drop-down list, select System Level.

Step 4  Click Backup.
The File Download dialog box is displayed offering you the options to Save, Open, or Cancel the action. Save presents a Save As dialog box, which allows you to select the location and filename used to save the XML file. Open opens the XML file.

To restore a backup, do the following:

**Step 1** Choose Maintain > Software > Backup & Restore. The Backup and Restore page is displayed.

**Step 2** Click Browse to navigate to the XML configuration file to restore. The Choose File to Upload dialog box is displayed.

The last location that was accessed to either save a backup or restore a configuration file is remembered.

**Step 3** Navigate to the location where the XML configuration file was saved, select it, and click Open.

The file location and filename are displayed in the Configuration File Location text box.

**Step 4** Click Restore.

The backup configuration XML file is restored to all servers specified in the backup.

---

**Export or Import Specific Array-Level Configurations**

The Import/Export System Configuration option offers the ability to export or import the specific array-level configuration for all the VDS servers. All array-level configuration pages are supported, except Error Repair, Session Gateway, Manual Ingest, Media Scheduler, Barker Stream/Playlist, Playout Scheduler, Playout Exporter, and EPG Exporter.

After the export XML configuration file has been created, you can edit the values of the configuration parameters as appropriate for the existing VDS or a new VDS.

To export or import the configuration of a specific Array Level configuration page for all VDS servers, do the following:

**Step 1** Display the Array Level configuration page by choosing Configure > Array Level and one of the supported array-level configuration pages.

**Step 2** To export the configuration to an XML file, click Export.

The File Download dialog box is displayed offering you the options to Save, Open, or Cancel the action. Save presents a Save As dialog box, which allows you to select the location and filename used to save the XML file. Open opens the XML file.

**Step 3** To import a configuration XML file, do the following:

a. Click Browse to navigate to the XML configuration file to restore. The Choose File to Upload dialog box is displayed.

The last location that was accessed to either save a backup or restore a configuration file is remembered.

b. Navigate to the location where the XML configuration file was saved, select it, and click Open.

The file location and filename are displayed in the Configuration File Location text box.

c. Click Import.
The backup configuration XML file is restored to all servers specified in the XML configuration file.

Server-Level Configuration Backup and Restore

The Server-Level Configuration Backup and Restore feature provides exportation of the server-level VDS server configuration parameters, as well as comprehensive import of all server-level configuration settings.

Through the Server-Level Configuration Backup and Restore feature, it is possible to backup (export) the server-level configuration for a VDS server or all VDS servers in a system, modify the parameters as appropriate, and restore (import) the configuration to a new VDS server or all the VDS servers in a new system.

The Server-Level Configuration Backup and Restore feature provides backup and restore functions of all server-level configuration parameters for the following groups:

- All VDS servers
- VDS servers of a certain type (Streamers, Vaults, Caching Nodes, or ISVs)
- Individual VDS servers
- Subset of all VDS servers or VDS servers of a certain type

In addition to complete backup and restore functionality for all server-level configurations for the specified VDS servers, this feature also offers export and import on each server-level configuration page for all VDS servers managed by the CDSM (or VVIM).

Note

The restore and import function do not overwrite any pre-existing server-level configuration settings (only new settings are imported or restored) on the following pages:

- Route Table
- Server DNS
- NTP Server

The restore and import function overwrite all pre-existing settings on the following server-level configuration pages:

- Server Setup (and Interface Setup)
- SNMP Agent
- FSI Setup
- RTSP Setup (In the Client section, only new clients are imported or restored, pre-existing client settings are retained.)
- Logging
- Syslog
- Recorder Setup
Adding a New VDS Server into an Existing System

Previously, when adding a new VDS server into an existing system, after running the `vdsinit` script to install the software, and the `vdsconfig` script to initially configure some basic settings, the user needed to log in to the CDSM GUI and manually enter the configuration on each server-level page.

With the addition of the Server-Level Configuration Backup and Restore feature, after running the `vdsinit` and `vdsconfig` scripts, the user can back up the server-level configuration on a VDS server that has similar configuration, modify the values for the new VDS server, and restore the configuration on the new VDS server. After which, only the System-Level and Array-Level configuration needs to be completed for the new VDS server.

Replacing a VDS Server and Complete Backup and Restore

The Server-Level Configuration Backup and Restore feature can be used in combination with the existing procedures for a complete backup and restore of a VDS server. For a complete backup and restore of the configuration files and database files for a VDS server, continue to use the procedure documented in the *Cisco VDS-TV Installation, Upgrade, and Maintenance Guide, Release 4.4* which uses the `preupgrade` script to back up the entire VDS server and the `upgrade` script to restore the entire VDS server. These procedures are used to perform a complete backup and restore of the same VDS server, and to replace a VDS server. As a preparation to the backup procedures, you need to write down the following settings:

- Management IP address
- Gateway IP address network mask
- Network mask
- Stream and cache interface IP address
- Streamer ID
- Stream Group ID
- QAM Gateways (System Level configuration)
- Route tables
- Name Service IP address (ISA only) (System and Array Level configuration)
- Ingest IP address
- Service Groups (System Level configuration)

Now, with the Server-Level Configuration Backup and Restore feature and the System-Level Configuration Backup and Restore feature, you can back up all the server-level and system-level configuration settings for the VDS server, and just write down the Array Level settings.

Using the Server-Level Configuration Backup and Restore Feature

Using the Backup and Restore feature involves the following tasks:

- **Backup or Restore Specific VDS Servers**
- **Export or Import Specific Server-Level Configurations**
Introduction

Backup or Restore Specific VDS Servers

The Backup & Restore page offers the ability to backup all the server-level configuration parameters of specific VDS servers, modify the configuration parameters as appropriate, and restore all the server-level configuration parameters to new VDS servers. Starting from VDS-TV release 3.4, Backup and restore page is also used to generate the backup XML for an ISR.

After the backup XML configuration file has been created, you can edit and upload the values of the configuration parameters or the XML file can be saved unchanged and used later to restore as appropriate for the new VDS server or all VDS servers in the new system.

To backup specific VDS servers, do the following:

---

**Step 1**  Choose `Maintain > Software > Backup & Restore`. The Backup and Restore page is displayed.

**Step 2**  From the **Select Server type to backup** drop-down list, select one of the following:

- All
- SSV (known as ISV)
- Vault
- Streamer
- Cache (known as Caching Node)
- Recorder
- Streamer-Recorder

All servers of the type selected are listed in the Servers to backup field.

**Step 3**  To remove individual servers from the Servers to backup field to the Server List field, do the following:

a. Select the servers by clicking each one while holding down the Ctrl key, or use the Shift key to select a contiguous group of servers, or if only one server needs to be selected, simply click the server.

b. Click the left arrow (<) and all the selected servers are moved to the Server list field.

To move servers from the Server List field to the Servers to backup field, use the same methods to select the servers and click the right arrow (>).

To move all the servers to the Server List field, use the double-left arrow (<<). To move all the servers to the Servers to backup field, use the double-right arrow (>>).

**Step 4**  After all the servers to be backed up are in the Servers to backup field, click **Backup**.

The File Download dialog box is displayed offering you the options to **Save**, **Open**, or **Cancel** the action.

**Save** presents a Save As dialog box, which allows you to select the location and filename used to save the XML file. **Open** opens the XML file.

---

To restore a backup, do the following:

---

**Step 1**  Choose `Maintain > Software > Backup & Restore`. The Backup and Restore page is displayed.

**Step 2**  In the Restore Server Configurations section at the bottom of the page, click **Browse** to navigate to the XML configuration file to restore. The Choose File to Upload dialog box is displayed.

The last location that was accessed to either save a backup or restore a configuration file is remembered.

**Step 3**  Navigate to the location where the XML configuration file was saved, select it, and click **Open**.
Appendix B      Creating Bulk Configuration Files

Introduction

The file location and filename are displayed in the Configuration File Location text box.

Step 4
Click Restore.
The backup configuration XML file is restored to all servers specified in the backup.

Export or Import Specific Server-Level Configurations

The Import/Export Server Configuration option offers the ability to export or import the specific server-level configuration for all the VDS servers. The following Server Level configuration pages have the export and import feature:

- Server Setup (includes the Interface Setup configurations)
- Route Table
- SNMP Agent
- Server DNS
- NTP Server
- Logging
- Syslog
- FSI Setup (RTSP environments)
- RTSP Setup (RTSP environments)
- Recorder Setup

After the export XML configuration file has been created, you can edit the values of the configuration parameters as appropriate for the new VDS server or all VDS servers in the new system.

To export or import the configuration of a specific Server Level page for all VDS servers, do the following:

Step 1
Display the Server Level configuration page by choosing Configure > Server Level and one of the following:

- Server Setup
- Route Table
- SNMP Agent
- Server DNS
- NTP Server
- Logging
- Syslog
- FSI Setup (RTSP environments only)
- RTSP Setup (RTSP environments only)
- Recorder Setup

Step 2
To export the configuration to an XML file, click Export.
The File Download dialog box is displayed offering you the options to Save, Open, or Cancel the action. Save presents a Save As dialog box, which allows you to select the location and filename used to save the XML file. Open opens the XML file.
Step 3

To import a configuration XML file, do the following:

a. Click **Browse** to navigate to the XML configuration file to restore. The Choose File to Upload dialog box is displayed.

   The last location that was accessed to either save a backup or restore a configuration file is remembered.

b. Navigate to the location where the XML configuration file was saved, select it, and click **Open**.

   The file location and filename are displayed in the Configuration File Location text box.

c. Click **Import**.

   The backup configuration XML file is restored to all servers specified in the XML configuration file.

---

**Maintain Section Configuration Backup and Restore**

In maintain section configuration pages only System Thresholds are supported for Servers.

The following maintain section configuration pages are supported for Software,

- Application Configuration
- CDSM/VVIM Setup
- System Configs
- Database Configs
- Configuration Generator
- ID Management
- Stream Monitor Listener

Through the Maintain section Configuration Backup and Restore feature, it is possible to backup (export) the maintain section configuration for all VDS servers in a system, modify the parameters as appropriate, and restore (import) the configuration to all VDS servers in the existing system or all VDS servers in a new system.

In addition to complete backup and restore functionality for all maintain section configurations for the specified VDS servers, this feature also offers export and import on each maintain section configuration page for all VDS servers managed by the CDSM (or VVIM).

**Using the Maintain Section Configuration Backup and Restore Feature**

Using the Backup and Restore feature involves the following tasks:

- **Backup or Restore the Maintain Section Configuration**
- **Export or Import Specific Maintain Section Configurations**

**Backup or Restore the Maintain Section Configuration**

The Backup & Restore page offers the ability to backup all the maintain section configuration parameters of the VDS, modify the configuration parameters as appropriate, and restore all the maintain section configuration parameters to a new VDS or the existing VDS.
To backup the maintain section configuration, do the following:

**Step 1** Choose Maintain > Software > Backup & Restore. The Backup and Restore page is displayed.

**Step 2** From the Section Level drop-down list, select Maintain Section.

**Step 3** Click Backup.

The File Download dialog box is displayed offering you the options to Save, Open, or Cancel the action. Save presents a Save As dialog box, which allows you to select the location and filename used to save the XML file. Open opens the XML file.

To restore a backup, do the following:

**Step 1** Choose Maintain > Software > Backup & Restore. The Backup and Restore page is displayed.

**Step 2** Click Browse to navigate to the XML configuration file to restore. The Choose File to Upload dialog box is displayed.

The last location that was accessed to either save a backup or restore a configuration file is remembered.

**Step 3** Navigate to the location where the XML configuration file was saved, select it, and click Open.

The file location and filename are displayed in the Configuration File Location text box.

**Step 4** Click Restore.

The backup configuration XML file is restored to all servers specified in the backup.

### Export or Import Specific Maintain Section Configurations

The Import/Export System Configuration option offers the ability to export or import the specific maintain section configuration for all the VDS servers.

In maintain section configuration pages only System Thresholds are supported for Servers.

The following maintain section configuration pages are supported for Software,

- Application Configuration
- CDSM/VVIM Setup
- System Configs
- Database Configs
- Configuration Generator
- ID Management
- Stream Monitor Listener

After the export XML configuration file has been created, you can edit the values of the configuration parameters as appropriate for the existing VDS or a new VDS.

To export or import the configuration of a specific Maintain section configuration page for all VDS servers, do the following:

**Step 1** Display the Maintain section configuration page by selecting Maintain tab which supports maintain section configuration pages.
To export the configuration to an XML file, click Export. The File Download dialog box is displayed offering you the options to Save, Open, or Cancel the action. Save presents a Save As dialog box, which allows you to select the location and filename used to save the XML file. Open opens the XML file.

To import a configuration XML file, do the following:

- Click Browse to navigate to the XML configuration file to restore. The Choose File to Upload dialog box is displayed. The last location that was accessed to either save a backup or restore a configuration file is remembered.
- Navigate to the location where the XML configuration file was saved, select it, and click Open. The file location and filename are displayed in the Configuration File Location text box.
- Click Import. The backup configuration XML file is restored to all servers specified in the XML configuration file.

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 4-39.

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>QAMList</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</td>
<td>QAMMAC Preference</td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID</td>
<td>QAMMAC</td>
</tr>
</tbody>
</table>
Appendix B  Creating Bulk Configuration Files

Creating Headend Setup Bulk Configuration Files

For information about the values of the attributes, see the “Configuring QAM Gateways” section on page 4-5. 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 4-85.

Note

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the VDS. 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
<QAMList xmlns="http://www.cisco.com/schemas/VCPBU/VDS-TV/R0/ciscowebsvcs" >
  <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>
  <QAM IP="1.1.1.2">
    <QAMStreamGroupPreference StreamGroupName="SG1" QAMMAC="00:00:00:00:00:01" Preference="None"/>
    <QAMStreamGroupPreference StreamGroupName="SG2" QAMMAC="00:00:00:00:00:02" Preference="High"/>
  </QAM>
</QAMList>
```

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>
<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/VDS-TV/R0/ciscowebsvcs" >
  <ServiceGroupToStreamGroup ServiceGroup="4666669" StreamGroup="NEWTEST" />
  <ServiceGroupToStreamGroup ServiceGroup="4666668" StreamGroup="s234" />
  <ServiceGroupToStreamGroup ServiceGroup="4666664" StreamGroup="NEWTEST" />
</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 F-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 4-9.

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/VDS-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 XML 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 4-93.

Table B-4 defines the XML Configuration file elements for the Route Table page.

<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 Route</td>
<td>ServerID, GroupID</td>
<td>Defines a route table.</td>
</tr>
<tr>
<td>Route</td>
<td>—</td>
<td>Network, SubnetMask, Gateway, RouteType</td>
<td>Defines a route.</td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring the Route Table” section on page 4-93. 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 4-85.

Note: The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the VDS. 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 XML Configuration file used to populate the Route Table page (VIP is not configured in this example):

```xml
<?xml version="1.0" encoding="UTF-8"?>

<routeTableList xmlns="http://www.cisco.com/schemas/VCPBU/VDS-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="7.2.21.0" SubnetMask="255.255.255.0" Gateway="1.1.1.10" RouteType="cServer Source"/>
  </routeTable>
</routeTableList>
```
Creating SNMP Agent XML Configuration Files

The SNMP Agent page is used to configure SNMP communication. Table B-5 defines the XML Configuration file elements for the SNMP Agent page.

<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></td>
<td></td>
<td>ServerID GroupID</td>
<td></td>
</tr>
<tr>
<td>SNMPAgent</td>
<td></td>
<td>SNMPCommunity SNMPTrapStation</td>
<td>Defines an SNMP agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMPVACM SNMPUSM</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></td>
<td>—</td>
<td>Identifies the VDS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ServerID GroupID</td>
<td></td>
</tr>
<tr>
<td>SNMPCommunity</td>
<td></td>
<td>Name Permissions</td>
<td>Defines the community for the SNMP agent.</td>
</tr>
<tr>
<td>SNMPTrapStation</td>
<td></td>
<td>TrapStation Version TrapCommunity</td>
<td>Defines the trap station for the SNMP agent.</td>
</tr>
<tr>
<td>SNMPVACM</td>
<td></td>
<td>User Access Authentication OID</td>
<td>Defines a View-Based Access Control Model (VACM) user.</td>
</tr>
<tr>
<td>SNMPUSM</td>
<td></td>
<td>—</td>
<td>Defines a User-Based Security Model (USM) user.</td>
</tr>
</tbody>
</table>
For information about the values of the attributes, see the “Configuring the SNMP Agent” section on page 4-95. 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 4-85.

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the VDS. The ALL value is case sensitive.

Following is an example of the XML Configuration file used to populate the SNMP Agent page (only SNMPv2c is configured in this example):

```xml
<?xml version="1.0" encoding="UTF-8"?>
<SNMPAgentList
    xmlns="http://www.cisco.com/schemas/VCPBU/VDS-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" />
        <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 DNS Server XML Configuration Files

The Server DNS page is used to configure the DNS servers. Table B-6 defines the XML 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 DomainSuffix DNSServer</td>
<td>—</td>
<td>Defines the DNS server settings.</td>
</tr>
<tr>
<td>Server</td>
<td>— ServerID GroupID</td>
<td>—</td>
<td>Identifies the VDS server.</td>
</tr>
</tbody>
</table>
Creating NTP Server XML Configuration Files

The NTP Server page is used to configure the NTP servers. Table B-7 defines the XML 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>NTPServer</td>
<td>NTPServer</td>
<td>—</td>
<td>Marks the beginning and ending of the NTP settings.</td>
</tr>
<tr>
<td>NTPServer</td>
<td>NTPServerIP</td>
<td>—</td>
<td>Defines the NTP settings.</td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>NTPServerID GroupID</td>
<td>Identifies the VDS server.</td>
</tr>
<tr>
<td>NTPServerIP</td>
<td>—</td>
<td>—</td>
<td>Defines the NTP server.</td>
</tr>
</tbody>
</table>
Creating FSI Setup XML Configuration Files

The FSI Setup page is used to configure the FSI. Table B-8 defines the XML Configuration file elements for the FSI Setup page.

For information about the values of the attributes, see the “Configuring FSI Setup” section on page 4-109. 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 4-85.

Table B-8  XML 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>FSISetup</td>
<td>FSISetup</td>
<td>—</td>
<td>Marks the beginning and ending of the FSI settings.</td>
</tr>
<tr>
<td>Server</td>
<td>Server</td>
<td>ServerID</td>
<td>Defines the FSI settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GroupID</td>
<td></td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring FSI Setup” section on page 4-109. 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 4-85.

Note

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the VDS. The ALL value is case sensitive.

Following is an example of the XML 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/VDS-TV/R0/ciscowebsvcs" >
    <NTPServer>
        <Server ServerID="ALL" GroupID="ALL"/>
        <NTPServerIP>198.168.1.10</NTPServerIP>
        <NTPServerIP>172.31.2.11</NTPServerIP>
    </NTPServer>
</NTPServerList>
```
Following is an example of the XML 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/VDS-TV/R0/ciscowebsvcs" >

    <FSISetup IPAddress="171.1.1.1"
        ServerPort="333"
        FTPClientPort="555"
        FTPOutServerPort="5001"
        FTPOutLoginTTL="64"
        ContentRootPath="/videcontent/"
        AsyncCallbackURL="http://1.1.1.1/test.php" >

        <Server ServerID="61" GroupID="1111"/>

    </FSISetup>

</FSISetupList>
```

### Creating RTSP Setup XML Configuration Files

The RTSP Setup page is used to configure the RTSP. Table B-9 defines the XML Configuration file elements for the RTSP Setup page.

<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>Defines the RTSP settings.</td>
</tr>
<tr>
<td></td>
<td>RTSPClientList</td>
<td>See the RTSP Setup Fields table for a description of the values and the applicable fields for your RTSP deployment.</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></td>
<td>—</td>
<td>ServerID</td>
<td>Identifies the VDS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GroupID</td>
<td></td>
</tr>
<tr>
<td></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 4-103. 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 4-85.

**Note** The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the VDS. The ALL value is case sensitive.
Following are examples of the XML 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/VDS-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"
        MaintenanceMode="on">
        <Server ServerID="5" GroupID="111"/>
    <RTSPClient ReceivePort="111" SendPort="222" ReceiveBuffer="65535" Model="nCube" Transport="TCP" />
    <RTSPClient ReceivePort="999" SendPort="888" ReceiveBuffer="65535" Model="Diego" Transport="TCP" />
    </RTSPSetup>
</RTSPSetupList>
```

**RTSP RTSP Deployment**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
    xmlns="http://www.cisco.com/schemas/VCPBU/VDS-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"
        MaintenanceMode="off">
        <Server ServerID="2" GroupID="1111"/>
    <RTSPClient ReceivePort="3111" SendPort="9222" ReceiveBuffer="65535" Model="nCube" Transport="TCP" />
    <RTSPClient ReceivePort="3999" SendPort="9888" ReceiveBuffer="65535" Model="Diego" Transport="TCP" />
    </RTSPSetup>
</RTSPSetupList>
```

**NGOD RTSP Deployment**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
    xmlns="http://www.cisco.com/schemas/VCPBU/VDS-TV/R0/ciscowebsvcs" >
    <RTSPSetup MasterStreamingIP="1.1.1.1"
        BackofficeTimeout="3000"
        RTSPServerIP="121.1.1.2"
        RTSPServerPort="5000"
        LSCPAddress="1.1.1.1"
        LSCPPort="1111"
        LSCPResponsePadding="on"
        ComponentName="xyz"
        MaintenanceMode="on">
        <Server ServerID="2" GroupID="1111"/>
    </RTSPSetup>
</RTSPSetupList>
```
IPTV RTSP Deployment

<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
  xmlns="http://www.cisco.com/schemas/VCPBU/VDS-TV/R0/ciscowebsvcs" >
  <RTSPSetup MasterStreamingIP="1.1.1.1"
               SessionInactivityTimeout="22000"
               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>

EventIS on-vpath RTSP Deployment

<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
  xmlns="http://www.cisco.com/schemas/VCPBU/VDS-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"
               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/VDS-TV/R0/ciscowebsvcs" >
  <RTSPSetup MasterStreamingIP="172.1.1.1"
               SessionInactivityTimeout="22000"
               AuthenticationManagerIP="121.1.1.2"
               AuthenticationManagerPort="5000"
               ServerIP="10.1.1.1"
               ServerPort="5555"
               StreamControlIP="191.1.1.2"
               StreamControlPort="9000"
               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>
Creating Logging XML Configuration Files

Table B-10 XML Configuration File Elements for Server-Level Logging

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogConfigList</td>
<td>LogConfig</td>
<td>—</td>
<td>Marks the beginning and ending of the logging settings.</td>
</tr>
<tr>
<td>LogConfig</td>
<td>Server</td>
<td>Facility</td>
<td>Defines the logging.</td>
</tr>
<tr>
<td></td>
<td>GroupID</td>
<td>—</td>
<td>Identifies the VDS server.</td>
</tr>
<tr>
<td>Facility</td>
<td>debug-flags</td>
<td>name</td>
<td>Defines the logging facility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>local-log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>remote-log</td>
<td></td>
</tr>
<tr>
<td>debug-flags</td>
<td>—</td>
<td>flag</td>
<td>Defines the debug flags for the specified facility.</td>
</tr>
</tbody>
</table>

For information about the values of the attributes, see the “Configuring the Server Level Logging” section on page 4-110. 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 4-85.

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the VDS. The ALL value is case sensitive.

Following is an example of the XML Configuration file used to populate the Server-Level Logging page:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RTSPSetupList
   xmlns="http://www.cisco.com/schemas/VCPBU/VDS-TV/R0/ciscowebsvcs" >
   <RTSPSetup MasterStreamingIP="172.1.1.1"
     SessionInactivityTimeout="2000"
     CallbackServerIP="129.1.1.2"
     CallbackServerPort="4000"
     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>
```
Creating Syslog XML Configuration Files

The Server-Level Syslog page is used to configure the syslog settings. Table B-11 defines the XML Configuration file elements for the Server-Level Syslog page.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyslogConfigList</td>
<td>SyslogConfig</td>
<td>—</td>
<td>Marks the beginning and ending of the syslog settings.</td>
</tr>
<tr>
<td>Server</td>
<td>Server</td>
<td>RemoteLogging IPAddress Port</td>
<td>Defines the logging.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>—</td>
<td>Identifies the VDS server.</td>
</tr>
</tbody>
</table>
Creating Server Setup XML Configuration Files

The Server Setup page is used to configure the VDS server settings. The elements and attributes vary depending on the type of VDS server (Vault, Caching Node, Streamer, or ISV). The XML Configuration File for the Server Setup also includes the settings on the Interface Setup page. Table B-12 defines the XML Configuration file elements for the Server Setup and Interface Setup page.

Table B-12 XML Configuration File Elements for Server Setup and Interface Setup

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerConfigList</td>
<td>VaultServerConfig StreamerServerConfig CacheServerConfig SSVServerConfig</td>
<td>—</td>
<td>Marks the beginning and ending of the server settings.</td>
</tr>
<tr>
<td>VaultServerConfig</td>
<td>Server SimpleDSCPMarking CustomDSCPMarking InterfaceConfig</td>
<td>PartNumber HostName ArrayID JumboCFrames VaultMirrorCopies VaultLocalCopies DSCPMarkingMethod DualCAS DefaultGateway FTPOutInterface FTPOutBandwidth FTPOutSession TTL SourceIP CachePort MaxNoOfInterfaces</td>
<td>Defines the Vault settings.</td>
</tr>
<tr>
<td>CacheServerConfig</td>
<td>Server SimpleDSCPMarking CustomDSCPMarking InterfaceConfig</td>
<td>PartNumber HostName ArrayID JumboCFrames DSCPMarkingMethod</td>
<td>DefaultGateway TTL SourceIP CachePort MaxNoOfInterfaces</td>
</tr>
</tbody>
</table>
### Table B-12  XML Configuration File Elements for Server Setup and Interface Setup

<table>
<thead>
<tr>
<th>Tag</th>
<th>Elements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StreamerServerConfig</td>
<td>Server, SimpleDSCPMarking, CustomDSCPMarking, InterfaceConfig</td>
<td>PartNumber, TTL, TransportDSCP, CacheDSCP, NullStream, StunPlayErrorDelay, StunPlayTimeout, HostName, ArrayID, SourceIP</td>
<td>Defines the Streamer settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TransportPortStart, TransportPortEnd, CachePort, StreamerIsCache, JumboSFrames, JumboCFrames, DSCPMarkingMethod, DualCAS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DefaultGateway, MaxNumberOfInterfaces</td>
<td></td>
</tr>
<tr>
<td>SSVServerConfig</td>
<td>Server, SimpleDSCPMarking, CustomDSCPMarking, InterfaceConfig</td>
<td>PartNumber, HostName, ArrayID, NullStream, StunPlayErrorDelay, StunPlayTimeout, SourceIP, TransportPortStart, TransportPortEnd, CachePort, StreamerIsCache, JumboSFrames</td>
<td>Defines the ISV settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JumboCFrames, VaultMirrorCopies, VaultLocalCopies, DSCPMarkingMethod, DualCAS, DefaultGateway, FTPOutInterface, FTPOutBandwidth, FTPOutSession, TTL, MaxNumberOfInterfaces</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>—</td>
<td>ServerID, GroupID</td>
<td>Identifies the VDS server.</td>
</tr>
<tr>
<td>SimpleDSCPMarking</td>
<td>—</td>
<td>ControlDSCP, DataDSCP, StreamDSCP, HTTPDSCP</td>
<td>Defines simple DSCP marking.</td>
</tr>
<tr>
<td>InterfaceConfig</td>
<td>—</td>
<td>Name, Type, IPAddress, SubnetMask, TransportPort, CachePort, Number, FTP</td>
<td>Defines interface settings on VDS server.</td>
</tr>
</tbody>
</table>
For information about the values of the attributes, see the “Configuring the Servers” section on page 4-85 and the “Configuring the Interfaces” section on page 4-80. 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 4-85.

The ServerID and GroupID attributes can have the value ALL if the configuration applies to all servers in the VDS. The ALL value is case sensitive.

Following is an example of the XML Configuration file used to populate the Server Setup page and Interface Setup page (only Vaults and Streamers are configured in this example):

```xml
<?xml version="1.0" encoding="utf-8"?>
<ServerConfigList xmlns="http://www.cisco.com/schemas/VCPBU/VDS-TV/R0/ciscowebsvcs">
  <VaultServerConfig ArrayID="0" SourceIP="" CachePort="" VaultLocalCopies="0" VaultMirrorCopies="2" TTL="32">
    <FTPOutSession="" FTPOutBandwidth="" FTPOutInterface="" HostName="V1-91" PartNumber="CDE220-2A-C" JumboFrames="Disable" DSCPMarkingMethod="Simple" DualCAS="Disable" DefaultGateway="10.78.178.1" MaxNoOfInterfaces="10">
      <Server ServerID="91" GroupID="9499" />
      <SimpleDSCPMarking ControlDSCP="0" DataDSCP="0" />
    </FTPOutSession>
    <InterfaceConfig Name="eth0" Type="Management" IPAddress="192.168.100.91" SubnetMask="255.255.255.0" TransportPort="" Number="0" FTP="Disable" />
    <InterfaceConfig Name="eth1" Type="Ingest" IPAddress="192.168.100.91" SubnetMask="255.255.255.0" TransportPort="" Number="1" FTP="Disable" />
    <InterfaceConfig Name="eth2" Type="Cache" IPAddress="192.169.101.12" TransportPort="" Number="2" FTP="Disable" />
    <InterfaceConfig Name="eth3" Type="Cache" IPAddress="192.169.101.13" TransportPort="" Number="3" FTP="Disable" />
    <InterfaceConfig Name="eth4" Type="Cache" IPAddress="192.169.101.14" TransportPort="" Number="4" FTP="Disable" />
    <InterfaceConfig Name="eth5" Type="Cache" IPAddress="192.169.101.15" TransportPort="" Number="5" FTP="Disable" />
    <InterfaceConfig Name="eth6" Type="Cache" IPAddress="192.169.101.16" TransportPort="" Number="6" FTP="Disable" />
    <InterfaceConfig Name="eth7" Type="Cache" IPAddress="192.169.101.17" TransportPort="" Number="7" FTP="Disable" />
    <InterfaceConfig Name="eth8" Type="Cache" IPAddress="192.169.101.18" TransportPort="" Number="8" FTP="Disable" />
    <InterfaceConfig Name="eth9" Type="Cache" IPAddress="192.169.101.19" TransportPort="" Number="9" FTP="Disable" />
  </VaultServerConfig>
</ServerConfigList>
```

< VaultServerConfig ArrayID="0" SourceIP="192.168.207.65" CachePort="48879" VaultLocalCopies="1" VaultMirrorCopies="2">
  <FTPOutSession="" FTPOutBandwidth="" FTPOutInterface="" HostName="V2-92" PartNumber="CDE220-2A-C" JumboFrames="Disable" DSCPMarkingMethod="Simple" DualCAS="Disable" DefaultGateway="10.78.178.1" MaxNoOfInterfaces="10">
    <Server ServerID="92" GroupID="9499" />
    <SimpleDSCPMarking ControlDSCP="0" DataDSCP="0" />
  </FTPOutSession>
  <InterfaceConfig Name="eth0" Type="Management" IPAddress="192.168.100.92" SubnetMask="255.255.255.0" TransportPort="" Number="0" FTP="Disable" />
  <InterfaceConfig Name="eth1" Type="Ingest" IPAddress="192.168.100.92" SubnetMask="255.255.255.0" TransportPort="" Number="1" FTP="Enable" />
  <InterfaceConfig Name="eth2" Type="Cache" IPAddress="192.169.101.10" TransportPort="" Number="2" FTP="Disable" />
  <InterfaceConfig Name="eth3" Type="Cache" IPAddress="192.169.101.11" TransportPort="" Number="3" FTP="Disable" />
  <InterfaceConfig Name="eth4" Type="Cache" IPAddress="192.169.101.12" TransportPort="" Number="4" FTP="Disable" />
  <InterfaceConfig Name="eth5" Type="Cache" IPAddress="192.169.101.13" TransportPort="" Number="5" FTP="Disable" />
</VaultServerConfig>
Appendix B  Creating Bulk Configuration Files

Creating Server Setup XML Configuration Files

```xml
<InterfaceConfig Name="eth6" Type="Cache" IPAddress="192.169.101.14" TransportPort="" Number="6"
FTP="Disable" />
<InterfaceConfig Name="eth7" Type="Cache" IPAddress="192.169.101.15" TransportPort="" Number="7"
FTP="Disable" />
<InterfaceConfig Name="eth8" Type="Cache" IPAddress="192.169.101.16" TransportPort="" Number="8"
FTP="Disable" />
<InterfaceConfig Name="eth9" Type="Cache" IPAddress="192.169.101.17" TransportPort="" Number="9"
FTP="Disable" />
</VaultServerConfig>
<StreamServerConfig TTL="32" ArrayID="1" HostName="S1-96" PartNumber="CDE220-2C2-C" NullStream="Enable"
SourceIP="192.168.207.65" TransportPortStart="48879" TransportPortEnd="48879" CachePort="48879"
StreamerIsCache="Disable" JumboSFrames="Disable" JumboCFrames="Disable" DSCPMarkingMethod="Simple"
DualCAS="Disable" DefaultGateway="10.78.178.1" MaxNoOfInterfaces="14">
<NIC Interface="eth0" Type="Management" IPAddress="10.78.178.96" SubnetMask="255.255.255.0"
Number="0" FTP="Enable" />
<InterfaceConfig Name="eth2" Type="Stream/Cache" IPAddress="192.169.101.30" TransportPort="" CachePort="”
Number="2" FTP="Disable" />
<InterfaceConfig Name="eth3" Type="Stream/Cache" IPAddress="192.169.101.31" TransportPort="" CachePort="”
Number="3" FTP="Disable" />
<InterfaceConfig Name="eth4" Type="Stream/Cache" IPAddress="192.169.101.32" TransportPort="" CachePort="”
Number="4" FTP="Disable" />
<InterfaceConfig Name="eth5" Type="Stream/Cache" IPAddress="192.169.101.33" TransportPort="“ CachePort="”
Number="5" FTP="Disable" />
<InterfaceConfig Name="eth6" Type="Stream/Cache" IPAddress="192.169.101.34" TransportPort="” CachePort="”
Number="6" FTP="Disable" />
<InterfaceConfig Name="eth7" Type="Stream/Cache" IPAddress="192.169.101.35" TransportPort="” CachePort="”
Number="7" FTP="Disable" />
<InterfaceConfig Name="eth8" Type="Stream/Cache" IPAddress="192.169.101.36" TransportPort="” CachePort="”
Number="8" FTP="Disable" />
<InterfaceConfig Name="eth9" Type="Stream/Cache" IPAddress="192.169.101.37" TransportPort="” CachePort="”
Number="9" FTP="Disable" />
<InterfaceConfig Name="eth10" Type="Stream/Cache" IPAddress="192.169.101.38" TransportPort="”
CachePort="” Number="10" FTP="Disable" />
<InterfaceConfig Name="eth11" Type="Stream/Cache" IPAddress="192.169.101.39" TransportPort="”
CachePort="” Number="11" FTP="Disable" />
<InterfaceConfig Name="eth12" Type="Stream/Cache" IPAddress="192.169.101.40" TransportPort="”
CachePort="” Number="12" FTP="Disable" />
<InterfaceConfig Name="eth13" Type="Stream/Cache" IPAddress="192.169.101.41" TransportPort="”
CachePort="” Number="13" FTP="Disable" />
</StreamServerConfig>
<StreamServerConfig TTL="32" ArrayID="1" HostName="S2-97" PartNumber="CDE220-2S3-C" NullStream="Enable"
SourceIP="192.168.207.65" TransportPortStart="48879" TransportPortEnd="48879" CachePort="48879"
StreamerIsCache="Disable" JumboSFrames="Disable" JumboCFrames="Disable" DSCPMarkingMethod="Simple"
DualCAS="Disable" DefaultGateway="10.78.178.1" MaxNoOfInterfaces="14">
<NIC Interface="eth0" Type="Management" IPAddress="10.78.178.97" SubnetMask="255.255.255.0"
Number="0" FTP="Enable" />
<InterfaceConfig Name="eth2" Type="Stream/Cache" IPAddress="192.169.101.42" TransportPort="” CachePort="”
Number="2" FTP="Disable" />
<InterfaceConfig Name="eth3" Type="Stream/Cache" IPAddress="192.169.101.43" TransportPort="” CachePort="”
Number="3" FTP="Disable" />
<InterfaceConfig Name="eth4" Type="Stream/Cache" IPAddress="192.169.101.44" TransportPort="” CachePort="”
Number="4" FTP="Disable" />
<InterfaceConfig Name="eth5" Type="Stream/Cache" IPAddress="192.169.101.45" TransportPort="” CachePort="”
Number="5" FTP="Disable" />
<InterfaceConfig Name="eth6" Type="Stream/Cache" IPAddress="192.169.101.46" TransportPort="” CachePort="”
Number="6" FTP="Disable" />
<InterfaceConfig Name="eth7" Type="Stream/Cache" IPAddress="192.169.101.47" TransportPort="” CachePort="”
Number="7" FTP="Disable" />
<InterfaceConfig Name="eth8" Type="Stream/Cache" IPAddress="192.169.101.48" TransportPort="” CachePort="”
Number="8" FTP="Disable" />
</StreamServerConfig>
```
System-Level Configuration XML Schema

The System-Level Configuration XML schema file describes and dictates the content of the System-Level Configuration XML file. The ciscoweb_svc_bulk_sysconfig.xsd file contains the XML schema.

```xml
<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/System/DNS elements -->
</xs:schema>
```
<xs:element name="DomainSuffix" type="xs:string" />
<xs:element name="DNSServer" type="ws:IsValidIP" />
<xs:element name="DNS">
  <xs:complexType>
    <xs:sequence>
      <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/System/NTP elements -->
<xs:element name="NTPServer" type="ws:IsValidIP" />
<xs:element name="NTP">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:NTPServer" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Host Service elements -->
<xs:element name="HostService">
  <xs:complexType>
    <xs:attribute name="Name" type="xs:string" />
    <xs:attribute name="IPAddress" type="ws:IsValidIP" />
  </xs:complexType>
</xs:element>
<xs:element name="HostServiceList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:HostService" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/ArrayName elements -->
<xs:element name="ArrayName">
  <xs:complexType>
    <xs:attribute name="ArrayID" type="xs:string" />
    <xs:attribute name="Name" type="xs:string" />
    <xs:attribute name="Vendor" type="xs:string" />
  </xs:complexType>
</xs:element>
<xs:element name="ArrayNameConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ArrayName" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/QAMGateway/ elements -->
<xs:element name="Server">
  <xs:complexType>
<xs:element name="QAMStreamGroupPreference">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="StreamGroupName" type="xs:string" />
    <xs:attribute name="QAMMAC" type="xs:string" />
    <xs:attribute name="Preference" type="xs:string" />
  </xs:complexType>
</xs:element>

<xs:element name="TSIDOutLink">
  <xs:complexType>
    <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:complexType>
</xs:element>

<xs:element name="QAMASILink">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:TSIDOutLink" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="Number" type="xs:string" />
    <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: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 name="StreamDestination">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamGroupPreference" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="SubnetAddress" type="xs:string" />
    <xs:attribute name="SubnetMask" type="xs:string" />
  </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>

<xs:element name="StreamDestinationConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamDestinationList" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="ReloadServiceGroup" type="xs:boolean" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamDestinationConfig1">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamDestinationList" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="ReloadServiceGroup" type="xs:boolean" />
  </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="ServiceGroup">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamGroupPreference" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="Group" type="xs:string" />
  </xs:complexType>
</xs:element>

<xs:element name="Headend">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ServiceGroup" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:ServiceGroupToStreamGroup" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Shared or Distributed ISA Setup -->

<xs:element name="ISA-GeneralSettings">
  <xs:complexType>
    <xs:attribute name="VaultMasterIP" type="ws:IsValidIP" />
    <xs:attribute name="VaultMasterPort" type="ws:NotNullPort" />
    <xs:attribute name="WebServicePort" type="ws:NotNullPort" />
    <xs:attribute name="StreamingMode" type="ws:StreamingMode" />
    <xs:attribute name="MSASupport" type="ws:EnableDisableEnum" />
    <xs:attribute name="Pre-EncryptionSupport" type="ws:EnableDisableEnum" />
    <xs:attribute name="TME-SCE" type="ws:TME-SCE" />
    <xs:attribute name="FTPOutPort" type="ws:NotNullPort" />
  </xs:complexType>
</xs:element>

<xs:element name="ISA-ContentStoreSettings">
  <xs:complexType>
    <xs:attribute name="Name" type="ws:NotNullstring" />
    <xs:attribute name="Kind" type="ws:NotNullstring" />
    <xs:attribute name="FactoryID" type="ws:NotNullstring" />
    <xs:attribute name="FactoryKind" type="ws:NotNullstring" />
    <xs:attribute name="NoOfThreads" type="xs:positiveInteger" />
    <xs:attribute name="FTPServerPort" type="ws:NotNullPort" />
  </xs:complexType>
</xs:element>

<xs:element name="CORBAEventChannels">
  <xs:complexType>
    <xs:attribute name="EventChannelID" type="ws:NotNullstring" />
    <xs:attribute name="EventChannelKind" type="ws:NotNullstring" />
    <xs:attribute name="ContentChannelID" type="ws:NotNullstring" />
    <xs:attribute name="ContentChannelKind" type="ws:NotNullstring" />
    <xs:attribute name="FactoriesID" type="ws:NotNullstring" />
  </xs:complexType>
</xs:element>
<xs:attribute name="FactoriesKind" type="ws:NotNullstring"/>
<xs:attribute name="EventChannelFactory" type="ws:NotNullstring"/>
<xs:attribute name="LoadQueryInterval" type="xs:positiveInteger"/>
</xs:complexType>
</xs:element>

<xs:element name="ISASetup">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ISA-GeneralSettings" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:ISA-ContentStoreSettings" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:CORBAEventChannels" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Parent/Child Service Group elements -->
<xs:element name="ChildServiceGroup" type="xs:positiveInteger" />
<xs:element name="ParentService">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ChildServiceGroup" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ParentChildServiceGroups">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ParentService" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Ingest Tuning elements -->
<xs:element name="TrickModeSettings">
  <xs:complexType>
    <xs:attribute name="Speed0" type="xs:string"/>
    <xs:attribute name="Speed1" type="xs:string"/>
    <xs:attribute name="Speed2" type="xs:string"/>
    <xs:attribute name="Speed3" type="xs:string"/>
    <xs:attribute name="Speed4" type="xs:string"/>
    <xs:attribute name="Speed5" type="xs:string"/>
    <xs:attribute name="Speed6" type="xs:string"/>
    <xs:attribute name="Speed7" type="xs:string"/>
    <xs:attribute name="Speed8" type="xs:string"/>
    <xs:attribute name="Speed9" type="xs:string"/>
  </xs:complexType>
</xs:element>
<xs:element name="FailIngestSettings">
  <xs:complexType>
    <xs:attribute name="PSIErrors" type="ws:EnableDisableEnum"/>
    <xs:attribute name="BitRateErrors" type="ws:EnableDisableEnum"/>
    <xs:attribute name="ErrorCountMethod" type="ws:ErrorCountMethod"/>
  </xs:complexType>
</xs:element>
<xs:element name="IngestTuningSettings">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:TrickModeSettings" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:FailIngestSettings" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/MPEG Tuning elements -->

<xs:element name="MPEGTuningSettings">
  <xs:complexType>
    <xs:attribute name="PrgIDStdize" type="ws:EnableDisableEnum"/>
    <xs:attribute name="PSI" type="ws:EnableDisableEnum"/>
    <xs:attribute name="SeqEndRemove" type="ws:EnableDisableEnum"/>
    <xs:attribute name="RateStdize" type="ws:EnableDisableEnum"/>
    <xs:attribute name="Md5Checksum" type="ws:EnableDisableEnum"/>
    <xs:attribute name="AddNULLsAtFTPOUT" type="ws:EnableDisableEnum"/>
    <xs:attribute name="DynamicTricks" type="ws:EnableDisableEnum"/>
    <xs:attribute name="PTSNPTMode" type="ws:PTSNPTMode"/>
    <xs:attribute name="C2ATimeout" type="ws:C2ATimeOut"/>
    <xs:attribute name="FFResume" type="ws:EnableDisableEnum"/>
    <xs:attribute name="RWSkip" type="ws:EnableDisableEnum"/>
    <xs:attribute name="FwdJump" type="ws:EnableDisableEnum"/>
    <xs:attribute name="SkippingStoneMode" type="ws:EnableDisableEnum"/>
    <xs:attribute name="Relaxation" type="ws:EnableDisableEnum"/>
    <xs:attribute name="FreePassJump" type="ws:EnableDisableEnum"/>
    <xs:attribute name="FreePassFastForward" type="ws:EnableDisableEnum"/>
    <xs:attribute name="DelayedJumpAhead" type="ws:EnableDisableEnum"/>
    <xs:attribute name="FreePassTime" type="xs:nonNegativeInteger"/>
    <xs:attribute name="PreVODAdOnce" type="ws:EnableDisableEnum"/>
    <xs:attribute name="Forwardskip" type="ws:EnableDisableEnum"/>
    <xs:attribute name="DualCAS" type="ws:EnableDisableEnum"/>
    <xs:attribute name="PauseBehavior" type="ws:PauseBehaviorEnum"/>
    <xs:attribute name="MPEGIndexFormat" type="ws:MPEGIndexMode"/>
    <xs:attribute name="EOSForPause" type="ws:EnableDisableEnum"/>
  </xs:complexType>
</xs:element>

<!-- Configure/System/VOD Market AMS Setup/Exporter elements -->

<xs:element name="MBO">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:MPEGTuningSettings" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="MBOList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:MBO" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/AMS Setup/Exporter elements -->
<xs:element name="AMS">
  <xs:complexType>
    <xs:attribute name="DomainName" type="xs:string" />
    <xs:attribute name="IPAddress" type="ws:IsValidIP" />
    <xs:attribute name="Port" type="ws:NotNullPort" />
  </xs:complexType>
</xs:element>

<xs:element name="AMSList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:AMS" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Content Distribution Rules Setup elements -->
<xs:element name="ContentRule">
  <xs:complexType>
    <xs:attribute name="Provider" type="ws:NotNullRangedNameString32" use="required" />
    <xs:attribute name="Product" type="ws:NotNullRangedNameString32" use="required" />
    <xs:attribute name="Market" type="ws:NotNullRangedNameString" use="required" />
    <xs:attribute name="Protocol" type="ws:ProtocolEnum" use="required" />
    <xs:attribute name="Exclude" type="ws:NullRangedNameString" use="optional" />
    <xs:attribute name="Status" type="xs:string" use="optional" />
  </xs:complexType>
</xs:element>

<xs:element name="ContentRuleList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ContentRule" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Package Priority Rules Setup elements -->
<xs:element name="PackageRule">
  <xs:complexType>
    <xs:attribute name="AssetId" type="ws:NullRangedNameString64" use="optional" />
    <xs:attribute name="Key" type="ws:NotNullRangedNameString32" use="optional" />
    <xs:attribute name="Title" type="ws:NullRangedNameString64" use="optional" />
  </xs:complexType>
</xs:element>

<xs:element name="PackageRuleList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:PackageRule" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:attribute name="ProviderId" type="ws:NullRangedNameString64" use="optional"/>
<xs:attribute name="Product" type="ws:NullRangedNameString64" use="optional"/>
<xs:attribute name="WindowsDays" type="ws:YesNoEnum" use="optional"/>
<xs:attribute name="AdditionalMatch" type="ws:NullRangedNameString64" use="optional"/>
<xs:attribute name="RuleExpiration" type="ws:NullRangedNameString64" use="required"/>
</xs:complexType>
</xs:element>

<xs:element name="PackageRuleList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:PackageRule" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Metadata Normalization Rules Setup elements -->
<xs:element name="MetadataRule">
  <xs:complexType>
    <xs:attribute name="Provider" type="xs:string" use="required"/>
    <xs:attribute name="Product" type="xs:string" use="required"/>
    <xs:attribute name="Market" type="ws:NotNullRangedNameString" use="required"/>
    <xs:attribute name="Price" type="ws:NotNullstring" use="required"/>
    <xs:attribute name="NewPrice" type="ws:NotNullstring" use="optional"/>
    <xs:attribute name="Exclude" type="xs:string" use="optional"/>
  </xs:complexType>
</xs:element>

<xs:element name="MetadataRuleList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:MetadataRule" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Monitor/System/Publishing Queue Elements Setup elements -->
<xs:element name="PackageQueue">
  <xs:complexType>
    <xs:attribute name="Priority" type="ws:NullRangedNameString250" use="optional"/>
    <xs:attribute name="PackageName" type="xs:string" use="optional"/>
    <xs:attribute name="AssetName" type="xs:string" use="optional"/>
    <xs:attribute name="Market" type="xs:string" use="optional"/>
    <xs:attribute name="CurrentStatus" type="ws:CurrentStatusEnum" use="optional"/>
    <xs:attribute name="TimeInserted" type="xs:string" use="optional"/>
    <xs:attribute name="UserAction" type="ws:UserActionEnum" use="optional"/>
  </xs:complexType>
</xs:element>

<xs:element name="PublishingQueueManagement">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:PackageQueue" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<!-- Configure/System/Ingest Manager elements -->

<xs:element name="GeneralSettings">
  <xs:complexType>
    <xs:attribute name="Host" type="xs:string"/>
    <xs:attribute name="CallbackPort" type="ws:NotNullPort"/>
    <xs:attribute name="AddlPackWindow" type="xs:positiveInteger"/>
    <xs:attribute name="FTPPTimeOut" type="xs:nonNegativeInteger"/>
    <xs:attribute name="PublishMode" type="ws:OnOffEnum"/>
    <xs:attribute name="MaxRetryCount" type="xs:nonNegativeInteger"/>
    <xs:attribute name="SendDeleteRequest" type="ws:YesNoEnum"/>
    <xs:attribute name="UseAssetID" type="ws:YesNoEnum"/>
    <xs:attribute name="ManageCORBA" type="ws:YesNoEnum"/>
    <xs:attribute name="RequireNotice" type="ws:YesNoEnum"/>
    <xs:attribute name="PubTimeDelay" type="xs:nonNegativeInteger"/>
    <xs:attribute name="FTPPush" type="ws:EnableDisableEnum"/>
    <xs:attribute name="FTPsWithType" type="ws:FTPServerMountEnum"/>
    <xs:attribute name="MetaDataPublish" type="ws:EnableDisableEnum"/>
    <xs:attribute name="MetaDataPublishURL0" type="xs:string"/>
    <xs:attribute name="MetaDataPublishURL1" type="xs:string"/>
    <xs:attribute name="FullyQualifiedName" type="ws:YesNoEnum"/>
    <xs:attribute name="EnableLoadBalancing" type="ws:YesNoEnum"/>
    <xs:attribute name="NumberOfThreadsPerMarket" type="ws:Range1To16"/>
    <xs:attribute name="PublishTimeOut" type="ws:Range1To600"/>
    <xs:attribute name="QualifyDelimiter" type="ws:MaxRange4"/>
    <xs:attribute name="ResetMarketQueue" type="ws:YesNoEnum"/>
    <xs:attribute name="TCPKeepAliveSupport" type="ws:EnableDisableEnum"/>
    <xs:attribute name="MarketConnectTimeout" type="ws:Range1To25"/>
  </xs:complexType>
</xs:element>

<xs:element name="IngestSettings">
  <xs:complexType>
    <xs:attribute name="IngestMask" type="xs:nonNegativeInteger"/>
    <xs:attribute name="NameServiceHost" type="ws:IsValidIP"/>
    <xs:attribute name="NameServicePort" type="ws:NotNullPort"/>
    <xs:attribute name="NotifyServiceHost" type="ws:IsValidIP"/>
    <xs:attribute name="NotifyServicePort" type="ws:NotNullPort"/>
    <xs:attribute name="NotifyEventChannelFactory" type="ws:NotNullstring"/>
    <xs:attribute name="EventChannelsID" type="ws:NotNullstring"/>
    <xs:attribute name="EventChannelsKind" type="ws:NotNullstring"/>
    <xs:attribute name="FactoriesID" type="ws:NotNullstring"/>
    <xs:attribute name="FactoriesKind" type="ws:NotNullstring"/>
    <xs:attribute name="PackageChannelID" type="ws:NotNullstring"/>
    <xs:attribute name="PackageChannelKind" type="ws:NotNullstring"/>
    <xs:attribute name="PackageFactoryId" type="ws:NotNullstring"/>
    <xs:attribute name="PackageFactoryKind" type="ws:NotNullstring"/>
    <xs:attribute name="PackageFactoryName" type="ws:NotNullstring"/>
    <xs:attribute name="PackageFactoryServerId" type="xs:positiveInteger"/>
    <xs:attribute name="CiscoSOAPURL" type="ws:NotNullstring"/>
    <xs:attribute name="ProdisSOAPURL" type="ws:NotNullstring"/>
  </xs:complexType>
</xs:element>

<xs:element name="BackOffice">
  <xs:complexType>
    <xs:attribute name="Name" type="xs:string"/>
    <xs:attribute name="URL" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="BackOfficeSettings">
  <xs:complexType>
    <xs:sequence>
      <!-- BackOffice settings -->
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element ref="ws:BackOffice" minOccurs="0" maxOccurs="unbounded" />
</xs:complexType>
<xs:sequence>
<xs:attribute name="MaxRetryCount" type="xs:string" />
<xs:attribute name="RetryInterval" type="xs:string" />
<xs:attribute name="BackOfficeTimeout" type="xs:string" />
</xs:complexType>
</xs:element>

<xs:element name="ContentStoreSettings">
<xs:complexType>
<xs:attribute name="Type" type="ws:ContentStoreType"/>
<xs:attribute name="URL" type="xs:string"/>
<xs:attribute name="OpenStreamTimeOut" type="xs:string" />
</xs:complexType>
</xs:element>

<xs:element name="EncryptionSettings">
<xs:complexType>
<xs:attribute name="Type" type="ws:EncryptionType"/>
<xs:attribute name="URL" type="xs:string" />
<xs:attribute name="FTPURL" type="xs:string" />
</xs:complexType>
</xs:element>

<xs:element name="IngestManagerSettings">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:GeneralSettings" minOccurs="0" maxOccurs="unbounded" />
<xs:element ref="ws:IngestSettings" minOccurs="0" maxOccurs="unbounded" />
<xs:element ref="ws:BackOfficeSettings" minOccurs="0" maxOccurs="unbounded" />
<xs:element ref="ws:ContentStoreSettings" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="AuthenticationManagerSettings">
<xs:complexType>
<xs:attribute name="Protocol" type="ws:AuthProtocol"/>
<xs:attribute name="IPAddress" type="ws:IsValidIP" use="required"/>
<xs:attribute name="Port" type="ws:NotNullPort" use="required"/>
<xs:attribute name="TimeOut" type="xs:positiveInteger"/>
<xs:attribute name="EventISHostName" type="xs:string"/>
<xs:attribute name="EventISPort" type="ws:NotNullPort"/>
<xs:attribute name="TraxisURL" type="xs:string"/>
<xs:attribute name="TraxisRetryInterval" type="xs:string"/>
<xs:attribute name="ServerThreadPool" type="xs:positiveInteger" use="required"/>
</xs:complexType>
</xs:element>

<xs:element name="AuthenticationManager">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:AuthenticationManagerSettings" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>
<!-- Configure/System/Ingest Server Manager elements -->

<xs:element name="IngestDriverServer">
  <xs:complexType>
    <xs:attribute name="Port" type="ws:NotNullPort"/>
    <xs:attribute name="NoOfThreads" type="xs:string"/>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Ingest Driver Server Settings elements -->

<xs:element name="IngestDriverServerSettings">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:IngestDriverServer" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Shared Recorder Settings elements -->

<xs:element name="RecorderSharedConfig">
  <xs:complexType>
    <xs:attribute name="RecorderManagerIP" type="ws:IsValidIP" use="required"/>
    <xs:attribute name="NTPServerIP" type="ws:IsValidIP" use="required"/>
    <xs:attribute name="HeartbeatInterval" type="ws:Range2To30" use="required"/>
    <xs:attribute name="RecorderLocation" type="xs:string" use="required"/>
    <xs:attribute name="RecordingModify" type="ws:ValueIs15" use="required"/>
    <xs:attribute name="SCTE35AdMarkers" type="ws:SCTE35AdMarkers" use="required"/>
    <xs:attribute name="RecorderManagerPort" type="ws:RecorderPort" use="required"/>
    <xs:attribute name="ProtocolVersion" type="ws:ProtocolVersion" use="required"/>
    <xs:attribute name="ThreadpoolSize" type="ws:ThreadPoolSize" use="required"/>
    <xs:attribute name="StatusReportInterval" type="ws:StatusReportInterval" use="required"/>
    <xs:attribute name="HTTPRequestTimeout" type="ws:HTTPRequestTimeout" use="required"/>
    <xs:attribute name="HTTPResponseTimeout" type="ws:HTTPResponseTimeout" use="required"/>
    <xs:attribute name="RecordingBandwidth" type="ws:Range1To100" use="required"/>
    <xs:attribute name="DeliveryBandwidth" type="ws:Range1To100" use="required"/>
    <xs:attribute name="StorageCapacity" type="ws:Range1To100" use="required"/>
    <xs:attribute name="LocationVirtualIP" type="ws:IsValidIP" use="required"/>
    <xs:attribute name="LocationSubnetMask" type="ws:IsValidSubNetMask" use="required"/>
    <xs:attribute name="HTTPDSCP" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="MceIP" type="ws:MceIP" use="required"/>
    <xs:attribute name="McePort" type="ws:NotNullPort" use="required"/>
    <xs:attribute name="MceUdsDir" type="ws:NotNullString" use="required"/>
    <xs:attribute name="RetryStatusAttempts" type="ws:Range0To100" use="required"/>
    <xs:attribute name="RetryStatusInterval" type="ws:Range60To3600" use="required"/>
    <xs:attribute name="RecordingValidationAge" type="ws:Range0To10" use="required"/>
  </xs:complexType>
</xs:element>

<!-- Configure/System/VBO Setup/Exporter elements -->

<xs:element name="VBO">
  <xs:complexType>
    <xs:attribute name="VHO" type="xs:positiveInteger"/>
    <xs:attribute name="DomainName" type="xs:string"/>
    <xs:attribute name="IPAddress" type="ws:IsValidIP"/>
<xs:attribute name="Port" type="ws:NotNullPort"/>
<xs:attribute name="ReceiveTimeOut" type="xs:positiveInteger"/>
<xs:attribute name="ODRMMotifyUrl" type="xs:string"/>
<xs:attribute name="ODRMNameSpace" type="xs:string"/>
<xs:attribute name="SetupNamespace" type="xs:string"/>
<xs:attribute name="SetupInterfaceUrl" type="xs:string"/>
<xs:attribute name="VBOIMNameSpace" type="xs:string"/>
<xs:attribute name="VBOIMInterfaceURI" type="xs:string"/>
</xs:complexType>
</xs:element>

<xs:element name="VBOList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VBO" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:simpleType name="MceIP">
  <xs:restriction base="xs:string">
    <xs:enumeration value="127.0.0.1"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValueIs5">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="5" />
    <xs:maxInclusive value="5" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValueIs15">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="15" />
    <xs:maxInclusive value="15" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range0To10">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="10" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range0To100">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range1To100">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range60To3600">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="60" />
    <xs:maxInclusive value="3600" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Range2To30">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="2"/>
    <xs:maxInclusive value="30"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range1To16">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="16"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range1To25">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="25"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range1To600">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="600"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ProtocolVersion">
  <xs:restriction base="xs:string">
    <xs:enumeration value="I02"/>
    <xs:enumeration value="I04"/>
    <xs:enumeration value="i02"/>
    <xs:enumeration value="i04"/>
    <xs:enumeration value="2"/>
    <xs:enumeration value="4"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ThreadpoolSize">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="16"/>
    <xs:maxInclusive value="16"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StatusReportInterval">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="60"/>
    <xs:maxInclusive value="60"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="HTTPRequestTimeout">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="5"/>
    <xs:maxInclusive value="5"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="HTTPResponseTimeout"
<xs:simpleType name="Range1To60">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="60" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="RecorderPort">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="50005" />
    <xs:maxInclusive value="65535" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="SCTE35AdMarkers">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Retain"/>
    <xs:enumeration value="Discard"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IsValidSubNetMask">
  <xs:restriction base="xs:string">
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="DSCPLimit">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="63" />
  </xs:restriction>
</xs:simpleType>

<!-- Configure/System/IP Nicknames elements -->

<xs:element name="IPNickName">
  <xs:complexType>
    <xs:attribute name="IPAddress" type="ws:IsValidIP"/>
    <xs:attribute name="NickName" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="QAMIPNickName">
  <xs:complexType>
    <xs:attribute name="IPAddress" type="ws:IsValidIP"/>
    <xs:attribute name="NickName" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="IPNickNames">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:IPNickName" minOccurs="0" maxOccurs="unbounded" />  
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element ref="ws:QAMIPNickName" minOccurs="0" maxOccurs="unbounded" />
</xs:complexType>
</xs:element>

<!-- Configure/System/Media Importer/Exporter elements -->
<xs:element name="MediaImporterSettings">
  <xs:complexType>
    <xs:attribute name="ImporterType" type="ws:ImporterType"/>
    <xs:attribute name="TransformerType" type="ws:TransformerType"/>
    <xs:attribute name="AutoImport" type="ws:EnableDisableEnum"/>
    <xs:attribute name="FTPServerIP" type="ws:IsValidIP"/>
    <xs:attribute name="FTPPath" type="ws:NotNullstring"/>
    <xs:attribute name="UserName" type="ws:NotNullstring"/>
    <xs:attribute name="Password" type="xs:string"/>
    <xs:attribute name="RetryCount" type="xs:positiveInteger"/>
    <xs:attribute name="RetryInterval" type="xs:positiveInteger"/>
    <xs:attribute name="Schedule" type="ws:Schedule"/>
    <xs:attribute name="ImportDays" type="xs:string"/>
    <xs:attribute name="Protocol" type="ws:ProtocolTypes"/>
    <xs:attribute name="AuthenticationMode" type="ws:AuthModeTypes"/>
    <xs:attribute name="PublicKeyPath" type="ws:NotNullstring"/>
    <xs:attribute name="Passphrase" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="MediaExporterSettings">
  <xs:complexType>
    <xs:attribute name="PreNotification" type="xs:positiveInteger"/>
    <xs:attribute name="NotifyURLPrefix" type="ws:NotNullstring"/>
    <xs:attribute name="NotifyHostIP" type="ws:IsValidIP"/>
    <xs:attribute name="NotifyHostPort" type="ws:NotNullPort"/>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Media Service elements -->
<xs:element name="MediaServiceSettings">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:MediaImporterSettings" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:MediaExporterSettings" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/Input Channels elements -->
<xs:element name="Channel">
  <xs:complexType>
    <xs:attribute name="Name" type="xs:string"/>
    <xs:attribute name="MulticastIP" type="ws:IsValidIP"/>
    <xs:attribute name="Port" type="ws:NotNullPort"/>
    <xs:attribute name="ChannelCode" type="ws:NotNullstring"/>
    <xs:attribute name="ChannelID" type="xs:nonNegativeInteger"/>
    <xs:attribute name="CategoryID" type="xs:nonNegativeInteger"/>
    <xs:attribute name="GenreCategory" type="ws:NotNullstring"/>
    <xs:attribute name="NetworkCategory" type="ws:NotNullstring"/>
    <xs:attribute name="CatalogID" type="xs:nonNegativeInteger"/>
    <xs:attribute name="Product" type="ws:NotNullstring"/>
    <xs:attribute name="ProviderName" type="ws:NotNullstring"/>
    <xs:attribute name="ProviderID" type="ws:NotNullstring"/>
  </xs:complexType>
</xs:element>
<xs:element name="ProgramSchedules">
  <xs:complexType>
    <xs:attribute name="Import" type="ws:YesNoEnum"/>
    <xs:attribute name="FileExtension" type="ws:TribuneFeedExtensionEnum"/>
  </xs:complexType>
</xs:element>

<xs:element name="InputChannels">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Channel" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="ws:ProgramSchedules" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="OutputChannel">
  <xs:complexType>
    <xs:attribute name="Name" type="xs:string"/>
    <xs:attribute name="DestIP" type="ws:IsValidIP"/>
    <xs:attribute name="DestPort" type="ws:NotNullPort"/>
  </xs:complexType>
</xs:element>

<xs:element name="OutputChannelConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:OutputChannel" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="SOP">
  <xs:complexType>
    <xs:attribute name="Name" type="xs:string"/>
    <xs:attribute name="VirtualIP" type="ws:IsValidIP"/>
  </xs:complexType>
</xs:element>
System-Level Configuration XML Schema

<!-- Configure/System/CallSign elements -->
<xs:element name="CallSign">
  <xs:complexType>
    <xs:attribute name="Name" type="xs:string"/>
    <xs:attribute name="IPAddress" type="ws:IsValidIP"/>
    <xs:attribute name="Port" type="ws:NotNullPort"/>
    <xs:attribute name="BitRate" type="xs:string"/>
    <xs:attribute name="PrimarySourceIP" type="xs:string"/>
    <xs:attribute name="BackupSourceIP" type="xs:string"/>
  </xs:complexType>
</xs:element>

<!-- Configure/System/CallSignSetup elements -->
<xs:element name="CallSignSetup">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:CallSign" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/System/LogConfig elements -->
<xs:element name="flag">
  <xs:complexType>
    <xs:attribute name="name" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="debug-flags">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:flag" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="Facility">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:debug-flags" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="name" type="xs:string"/>
    <xs:attribute name="local-log" type="xs:string"/>
    <xs:attribute name="remote-log" type="xs:string"/>
  </xs:complexType>
</xs:element>

<xs:element name="LogConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Facility" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<!-- SyslogConfig elements -->
<xs:element name="SyslogConfigDetails">
  <xs:complexType>
    <xs:attribute name="RemoteLogging" type="ws:EnableDisableEnum"/>
    <xs:attribute name="IPAddress" type="ws:IsValidIP"/>
    <xs:attribute name="Port" type="ws:NotNullPort"/>
  </xs:complexType>
</xs:element>

<xs:element name="SyslogConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SyslogConfigDetails" minOccurs="0"
        maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="SystemConfiguration">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:DNS" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:NTP" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:HostNameList" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:HostServiceList" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:ContentRuleList" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:PackageRuleList" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:MetadataRuleList" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:AMSList" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:QAMList" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:IngestManagerSettings" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:AuthenticationManager" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:IngestTuningSettings" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:MPEGTuning" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:RecorderSharedConfig" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:IPNickNames" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:MediaServiceSettings" minOccurs="0"
        maxOccurs="1" />
      <xs:element ref="ws:InputChannels" minOccurs="0"
        maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element ref="ws:SourceOutputPort" minOccurs="0" maxOccurs="1" />
<xs:element ref="ws:OutputChannelConfig" minOccurs="0" maxOccurs="1" />
<xs:element ref="ws:CallSignSetup" minOccurs="0" maxOccurs="1" />
<xs:element ref="ws:IngestDriverServerSettings" minOccurs="0" maxOccurs="1" />
<xs:element ref="ws:LogConfig" minOccurs="0" maxOccurs="1" />
<xs:element ref="ws:SyslogConfig" minOccurs="0" maxOccurs="1" />
</xs:sequence>
</xs:complexType>
</xs:element>

<xs:simpleType name="AdMarker">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Retain" />
    <xs:enumeration value="Discard" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="EnableDisableEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Enable" />
    <xs:enumeration value="Disable" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ImporterType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Host" />
    <xs:enumeration value="Other" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TransformerType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="OCN" />
    <xs:enumeration value="Tribune" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Schedule">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Daily" />
    <xs:enumeration value="Weekly" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StreamingMode">
  <xs:restriction base="xs:string">
    <xs:enumeration value="ASI" />
    <xs:enumeration value="GigE" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TME-SCE">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Disable" />
    <xs:enumeration value="Enable for OpenStream" />
    <xs:enumeration value="Enable for MystroMDN" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="PauseBehaviorEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Only NULL packets" />
    <xs:enumeration value="P-frames" />
    <xs:enumeration value="PCR with NULL packets" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="YesNoEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Yes" />   
    <xs:enumeration value="No" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="CurrentStatusEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Waiting" />  
    <xs:enumeration value="Publishing" />
    <xs:enumeration value="On Hold" />
    <xs:enumeration value="Complete" />
    <xs:enumeration value="Failed" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="UserActionEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="" />  
    <xs:enumeration value="Hold" />
    <xs:enumeration value="Resume" />
    <xs:enumeration value="Delete" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TribuneFeedExtensionEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="gz" />  
    <xs:enumeration value="xml" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IsValidIP">
  <xs:restriction base="xs:string">
    <xs:pattern
value="((\[[1-9]{1,2}|1(0-9\d|0\d\d|1\d\d|2(0|1)\d|22\d|23[0-3])\]|25[0-5])\.){3}(\[[1-9]{1,2}|1(0-9\d|0\d\d|1\d\d|2(0|1)\d|22\d|23[0-3])\]|25[0-5])" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IsTime">
  <xs:restriction base="xs:string">
    <xs:pattern
value="(((\[0-1]\d|2[0-3])\-(\[0-5]\d))|((\[0-1]\d|2[0-3])\-(\[0-5]\d)){3})" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NotNullPort">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="65535" />
  </xs:restriction>
</xs:simpleType>
Appendix B      Creating Bulk Configuration Files

System-Level Configuration XML Schema

<xs:simpleType name="ErrorCountMethod">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Per Minute(s)" />
    <xs:enumeration value="Per Sample" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="AuthProtocol">
  <xs:restriction base="xs:string">
    <xs:enumeration value="EventIS" />
    <xs:enumeration value="Cisco" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="FTPServerMountEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="FTP" />
    <xs:enumeration value="CIFS" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContentStoreType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Disable" />
    <xs:enumeration value="ISA" />
    <xs:enumeration value="FSI" />
    <xs:enumeration value="NGOD" />
    <xs:enumeration value="OpenStream" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="EncryptionType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Disable" />
    <xs:enumeration value="Verimatrix" />
    <xs:enumeration value="WideVine" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="AudioType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Mono" />
    <xs:enumeration value="Stereo" />
    <xs:enumeration value="Dolby Pro" />
    <xs:enumeration value="Dolby ProLogic" />
    <xs:enumeration value="DD 5.1" />
    <xs:enumeration value="Dolby Digital 5.1" />
    <xs:enumeration value="Dolby 5.1" />
    <xs:enumeration value="DD" />
    <xs:enumeration value="Dolby D" />
    <xs:enumeration value="Dolby Digital" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContentType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="HD" />
    <xs:enumeration value="SD" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="PTSNPTMode">
<xs:simpleType name="MPEGIndexMode">
  <xs:restriction base="xs:string">
    <xs:enumeration value="iGate"/>
    <xs:enumeration value="NGOD"/>
    <xs:enumeration value="ATIS"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="C2ATimeOut">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1000"/>
    <xs:maxInclusive value="5000"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NotNullstring">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OnOffEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="On"/>
    <xs:enumeration value="Off"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NotNullRangedNameString32">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
    <xs:maxLength value="32"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NotNullRangedNameString64">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
    <xs:maxLength value="64"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NotNullRangedNameString">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
    <xs:maxLength value="63"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NullRangedNameString">
  <xs:restriction base="xs:string">
    <xs:minLength value="0"/>
    <xs:maxLength value="63"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NullRangedNameString64">
  <xs:restriction base="xs:string">
    <xs:minLength value="0"/>
  </xs:restriction>
</xs:simpleType>
Array-Level Configuration XML Schema

The Array-Level Configuration XML schema file describes and dictates the content of the Array-Level Configuration XML file. The ciscowebsvc_bulk_arrayconfig.xsd file contains the XML schema.

<?xml version="1.0" encoding="UTF-8"?>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  
  <xsd:simpleType name="NullRangedNameString250">
    <xsd:restriction base="xsd:string">
      <xsd:minLength value="1" />
      <xsd:maxLength value="250" />
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="MaxRange4">
    <xsd:restriction base="xsd:string">
      <xsd:minLength value="1" />
      <xsd:maxLength value="4" />
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="ProtocolEnum">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="ATIS"/>
      <xsd:enumeration value="FTP"/>
      <xsd:enumeration value="atis"/>
      <xsd:enumeration value="ftp"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="TrueFalse">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="true"/>  
      <xsd:enumeration value="True"/>  
      <xsd:enumeration value="TRUE"/> 
      <xsd:enumeration value="false"/> 
      <xsd:enumeration value="False"/> 
      <xsd:enumeration value="FALSE"/> 
      <xsd:enumeration value="%"/> 
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="ProtocolTypes">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="FTP"/>
      <xsd:enumeration value="SFTP"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="AuthModeTypes">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="Password"/>
      <xsd:enumeration value="Public Key"/>
    </xsd:restriction>
  </xsd:simpleType>

</xsd:schema>
<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/Array Level/Array DNS elements -->
<xs:element name="DomainSuffix" type="ws:NotNullString" />  
<xs:element name="DNSServer" type="ws:IsValidIP" />

<xs:element name="ArrayDNS">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:DomainSuffix" minOccurs="0" maxOccurs="16" />
      <xs:element ref="ws:DNSServer" minOccurs="0" maxOccurs="16" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="ArrayDNSConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ArrayDNS" minOccurs="1" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Array NTP Server elements -->
<xs:element name="NTPServerIP" type="ws:IsValidIP" />

<xs:element name="ArrayNTP">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:NTPServerIP" minOccurs="0" maxOccurs="16" />
    </xs:sequence>
    <xs:attribute name="GroupID" type="xs:positiveInteger" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="ArrayNTPConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ArrayNTP" minOccurs="1" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Streamer BMS elements -->
<xs:element name="LSCP_Open">
  <xs:complexType>
    <xs:attribute name="Timeout" type="xs:positiveInteger" use="required" />  
    <xs:attribute name="ReasonCode" type="xs:positiveInteger" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="LSCP_BOS">
  <xs:complexType>
    <xs:attribute name="Timeout" type="xs:positiveInteger" use="required" />
    <xs:attribute name="ReasonCode" type="xs:positiveInteger" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="LSCP_Pause">
  <xs:complexType>
    <xs:attribute name="Timeout" type="xs:positiveInteger" use="required" />
    <xs:attribute name="ReasonCode" type="xs:positiveInteger" use="required" />
  </xs:complexType>
</xs:element>
<xs:complexType>
  <xs:attribute name="Timeout" type="xs:positiveInteger" use="required" />
  <xs:attribute name="ReasonCode" type="xs:positiveInteger" use="required" />
</xs:complexType>
</xs:element>

<xs:element name="LSCP_BOS">
  <xs:complexType>
    <xs:attribute name="Timeout" type="xs:positiveInteger" use="required" />
    <xs:attribute name="ReasonCode" type="xs:positiveInteger" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="LSCP_1xReadFailure">
  <xs:complexType>
    <xs:attribute name="ReasonCode" type="xs:positiveInteger" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="AdvancedISASettingsList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:LSCP_Open" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LSCP_BOS" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LSCP_Pause" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LSCP_EOS" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LSCP_1xReadFailure" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="LSCPService">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:AdvancedISASettingsList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LSCPOpen" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LSCP_BOS" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="StreamServiceID" type="ws:NotNullString" use="required" />
    <xs:attribute name="StreamServiceKind" type="ws:NotNullString" use="required" />
    <xs:attribute name="MasterNoOfThreads" type="xs:positiveInteger" use="required" />
    <xs:attribute name="PlayNoOfThreads" type="xs:positiveInteger" use="required" />
    <xs:attribute name="LSCPResponsePad" type="ws:EnableDisableEnum" use="required" />
    <xs:attribute name="LSCPClientProtocol" type="ws:LSCPClientProtocol" use="required" />
    <xs:attribute name="AdvancedISASettings" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="OpenStreamResourceServices">
  <xs:complexType>
    <xs:attribute name="ServiceName" type="ws:NotNullString" use="required" />
    <xs:attribute name="ServicePollTime" type="xs:positiveInteger" use="required" />
    <xs:attribute name="StreamTimeout" type="xs:positiveInteger" use="required" />
    <xs:attribute name="StreamSourcePort" type="ws:NotNullPort" use="required" />
  </xs:complexType>
</xs:element>
<xs:element name="SessionGateway" type="ws:NotNullString" />
<xs:element name="SessionGateways">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SessionGateway" minOccurs="0" maxOccurs="5" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="StreamerBMSConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:OpenStreamSettings" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CORBAEventChannels" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LSCPService" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:OpenStreamResourceServices" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:SessionGateways" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Vault BMS elements -->
<xs:element name="OpenStreamSettings">
  <xs:complexType>
    <xs:attribute name="StreamMasterIP" type="ws:IsValidIP"/>
    <xs:attribute name="ContentServiceMasterIP" type="ws:IsValidIP"/>
    <xs:attribute name="Port" type="ws:NotNullPort" use="required"/>
    <xs:attribute name="HeadendID" type="ws:NotNullString" use="required"/>
    <xs:attribute name="StreamSourceConfig" type="ws:StreamSourceConfig"/>
    <xs:attribute name="StreamingMode" type="ws:StreamingMode"/>
    <xs:attribute name="MSASupport" type="ws:EnableDisableEnum"/>
    <xs:attribute name="TME-SCE" type="ws:TME-SCE"/>
    <xs:attribute name="FTPOutPort" type="ws:NotNullPort"/>
  </xs:complexType>
</xs:element>
<xs:element name="ContentService">
  <xs:complexType>
    <xs:attribute name="ContentStoreName" type="ws:NotNullString" use="required"/>
    <xs:attribute name="ContentStoreKind" type="ws:NotNullString" use="required"/>
    <xs:attribute name="ContentFactoryID" type="ws:NotNullString" use="required"/>
    <xs:attribute name="ContentFactoryKind" type="ws:NotNullString" use="required"/>
    <xs:attribute name="ContentNoOfThreads" type="xs:positiveInteger" use="required"/>
    <xs:attribute name="PreEncryptionSupport" type="ws:EnableDisableEnum"/>
    <xs:attribute name="FTPClientPort" type="ws:NotNullPort"/>
    <xs:attribute name="FTPServerPort" type="ws:NotNullPort" use="required"/>
    <xs:attribute name="FTPMoOfAttempts" type="xs:positiveInteger"/>
    <xs:attribute name="FTPTimeout" type="xs:positiveInteger"/>
  </xs:complexType>
</xs:element>
<xs:element name="CORBA Services"
<xs:attribute name="NameServiceIP" type="ws:IsValidIP" use="required" />
<xs:attribute name="NameServicePort" type="ws:NotNullPort" use="required" />
<xs:attribute name="NotifyServiceIP" type="ws:IsValidIP" />  
<xs:attribute name="NotifyServicePort" type="ws:NotNullPort" use="required"/>
<xs:attribute name="NotifyServiceFactory" type="ws:NotNullString" use="required" />
</xs:complexType>
</xs:element>

<xs:element name="CORBAEventChannels">
    <xs:complexType>
        <xs:attribute name="EventChannelID" type="ws:NotNullString" use="required" />
        <xs:attribute name="EventChannelKind" type="ws:NotNullString" use="required" />
        <xs:attribute name="ContentChannelID" type="ws:string" />
        <xs:attribute name="ContentChannelKind" type="ws:string" />
        <xs:attribute name="StreamChannelID" type="ws:string" />
        <xs:attribute name="StreamChannelKind" type="ws:string" />
        <xs:attribute name="FactoriesID" type="ws:NotNullString" use="required" />
        <xs:attribute name="FactoriesKind" type="ws:NotNullString" use="required" />
        <xs:attribute name="EventChannelFactory" type="ws:NotNullString" use="required" />
        <xs:attribute name="AdManagerEventChannel" type="ws:string" />
        <xs:attribute name="LoadQueryInterval" type="ws:positiveInteger" />
    </xs:complexType>
</xs:element>

<xs:element name="VaultBMSConfig">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:OpenStreamSettings" minOccurs="0" maxOccurs="1" />
            <xs:element ref="ws:ContentService" minOccurs="0" maxOccurs="1" />
            <xs:element ref="ws:CORBAServices" minOccurs="0" maxOccurs="1" />
            <xs:element ref="ws:CORBAEventChannels" minOccurs="0" maxOccurs="1" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Session Gateway elements -->
<xs:element name="SessionGatewaySettings">
    <xs:complexType>
        <xs:attribute name="ResourceManagerIP" type="ws:IsValidIP" use="required" />
        <xs:attribute name="ResourceManagerPort" type="ws:NotNullPort" use="required" />
        <xs:attribute name="FailoverIP" type="ws:IsValidIP" use="required" />
        <xs:attribute name="FailoverPort" type="ws:NotNullPort" use="required" />
        <xs:attribute name="FailoverAttempts" type="ws:positiveInteger" use="required" />
        <xs:attribute name="FailoverTime" type="ws:positiveInteger" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="SessionGatewayConfig">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:SessionGatewaySettings" minOccurs="0" maxOccurs="1" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Stream Groups Setup elements -->
<xs:element name="StreamGroupMembers">
    <xs:complexType>
<xs:element name="StreamGroupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamGroupMembers" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/SSV Groups Setup elements -->
<xs:element name="SSVGroupMembers">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="SSVGroupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SSVGroupMembers" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="FadeFrameSupport" type="ws:EnableDisableEnum" use="required" />
    <xs:attribute name="SSVGroupRole" type="ws:StreamGroupRole" /> 
  </xs:complexType>
</xs:element>

<xs:element name="SSVGroupsConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SSVGroupConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/VHO Setup elements -->
<xs:element name="StreamGroup">
  <xs:complexType>
    <xs:attribute name="Name" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamGroupsConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamGroupConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="VHOGroupMembers">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:StreamGroup" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="VHOGroupConfig">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:VHOGroupMembers" minOccurs="0" maxOccurs="unbounded" />
            <xs:element ref="ws:ControlSetupIPConfig" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="VHOGroupsConfigList">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:VHOGroupConfig" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Configure/Array/Replicate Group Setup/Exporter elements -->

<xs:element name="Server">
    <xs:complexType>
        <xs:attribute name="IPAddress" type="ws:IsValidIP" use="required" />
        <xs:attribute name="ServerID" type="ws:NotNullString" use="required" />
        <xs:attribute name="GroupID" type="ws:NotNullString" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="ReplicationGroupMembers">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="ReplicationGroupConfig">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:ReplicationGroupMembers" minOccurs="0" maxOccurs="unbounded" />
            <xs:attribute name="GroupName" type="ws:NotNullString" />
            <xs:attribute name="IPAddress" type="ws:IsValidIP" />
            <xs:attribute name="SubnetMask" type="ws:IsValidSubNetMask" />
            <xs:attribute name="Type" type="ws:ReplicateTypeEnum" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="ReplicationGroupConfigList">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:ReplicationGroupConfig" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
Array-Level Configuration XML Schema

<!-- Configure/Array Level/Vault Groups Setup elements -->
<xs:element name="VaultGroupMembers">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="VaultGroupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VaultGroupMembers" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required"/>
    <xs:attribute name="LocationVirtualIP" type="ws:IsValidIP"/>
    <xs:attribute name="LocationSubnetMask" type="ws:IsValidSubNetMask"/>
    <xs:attribute name="GroupID" type="xs:positiveInteger"/>
    <xs:attribute name="LocationSite" type="ws:LocationSite"/>
  </xs:complexType>
</xs:element>

<xs:element name="VaultGroupsConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VaultGroupConfig" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Ingest Steering elements -->
<xs:element name="Product">
  <xs:complexType>
    <xs:attribute name="Name" type="ws:NotNullString" use="required"/>
  </xs:complexType>
</xs:element>

<xs:element name="AssignedProducts">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Product" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="VaultGroup">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:AssignedProducts" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="Name" type="ws:NotNullString" use="required"/>
    <xs:attribute name="Mirror" type="ws:YesNoEnum"/>
  </xs:complexType>
</xs:element>

<xs:element name="VaultGroupList"/>
<xs:complexType>
  <xs:sequence>
    <xs:element ref="ws:VaultGroup" minOccurs="0" max_occurs="unbounded" />
  </xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="IngestSteeringConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VaultGroupList" minOccurs="0" max_occurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Cache Groups Setup elements -->
<xs:element name="CacheGroupMembers">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" max_occurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="Volume">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Volume" minOccurs="0" max_occurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="AssignedVolumes">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Volume" minOccurs="0" max_occurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="CacheGroupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:CacheGroupMembers" minOccurs="0" max_occurs="unbounded" />
      <xs:element ref="ws:AssignedVolumes" minOccurs="0" max_occurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="LocationVirtualIP" type="ws:IsValidIP" />
    <xs:attribute name="LocationSubnetMask" type="ws:IsValidSubNetMask" />
    <xs:attribute name="GroupID" type="xs:positiveInteger" />
    <xs:attribute name="Port" type="ws:NotNullPort" />
  </xs:complexType>
</xs:element>

<xs:element name="CDNGroupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:AssignedVolumes" minOccurs="0" max_occurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="LocationVirtualIP" type="ws:IsValidIP" />
    <xs:attribute name="LocationSubnetMask" type="ws:IsValidSubNetMask" />
    <xs:attribute name="Port" type="ws:NotNullPort" />
  </xs:complexType>
</xs:element>
<xs:element name="CacheGroupsConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:CacheGroupConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="CDNGroupsConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:CDNGroupConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Cache to Cache Map elements -->

<xs:element name="CacheToCacheMapConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:CacheGroupPreferences" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="StreamGroupPreference">
  <xs:complexType>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="Preference" type="ws:PreferenceEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CacheGroupPreference">
  <xs:complexType>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="Preference" type="ws:PreferenceEnum" use="required" />
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Cache to Vault Map elements -->

<xs:element name="VaultGroupPreference">
  <xs:complexType>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="Preference" type="ws:PreferenceEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CacheGroupPreferences">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VaultGroupPreference" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:CacheGroupPreference" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
</xs:complexType>
</xs:element>

<xs:element name="StreamGroupPreferences">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:StreamGroupPreference" minOccurs="0" maxOccurs="unbounded" />
<xs:element ref="ws:CacheGroupPreference" minOccurs="0" maxOccurs="unbounded" />
<xs:element ref="ws:VaultGroupPreference" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
<xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
</xs:complexType>
</xs:element>

<xsl:element name="StreamToCacheMapConfig">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:StreamGroupPreferences" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>

<xsl:element name="CacheToVaultMapConfig">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:CacheGroupPreferences" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>

<!-- Configure/Array Level/D5 Setup elements -->
<xsl:element name="Policy" type="ws:PolicyEnum" />

<xsl:element name="SOPConfig">
<xs:complexType>
<xs:attribute name="Name" type="ws:NotNullString" use="required" />
<xs:attribute name="LoopbackAddress" type="ws:IsValidIP" use="required" />
</xs:complexType>
</xs:element>

<xsl:element name="Policies">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:Policy" minOccurs="0" maxOccurs="2" />
</xs:sequence>
</xs:complexType>
</xs:element>

<xsl:element name="SOPConfigList">
<xs:complexType>
<xs:sequence>
<xs:element ref="ws:SOPConfig" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="D5SetupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Policies" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:SOPConfigList" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="ModelName" type="ws:NotNullString" use="required" />
    <xs:attribute name="SignificantResourceUsage" type="xs:positiveInteger" use="required" />
    <xs:attribute name="ODRMUrl" type="ws:NotNullString" use="required" />
    <xs:attribute name="NotifyInterval" type="xs:positiveInteger" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="D5SetupConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:D5SetupConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Vault Redundancy Map elements -->
<xs:element name="VaultRedundancyMap">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VaultGroup" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="VaultRedundancyMapConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VaultRedundancyMap" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Master Vault Group elements -->
<xs:element name="GroupConfig">
  <xs:complexType>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="ActAsMaster" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="VHOGroup">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:GroupConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:IngestDriverClientConfig" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>
<!-- Array-Level Configuration XML Schema

Appendix B: Creating Bulk Configuration Files

Array-Level Configuration XML Schema

<xs:element name="MasterVaultGroupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:GroupConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:VHOGroup" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Control Setup IP elements -->
<xs:element name="ControlSetupIPConfig">
  <xs:complexType>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="IPAddress" type="ws:IsValidIP" />
    <xs:attribute name="SubnetMask" type="ws:IsValidSubNetMask" />
    <xs:attribute name="IPType" type="ws:IPType" />
    <xs:attribute name="SetupID" type="xs:positiveInteger" />
  </xs:complexType>
</xs:element>

<xs:element name="ControlSetupIPConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VHOGroupConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:ControlSetupIPConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/VHO ISA Setup elements -->
<xs:element name="StreamerBMSSettings">
  <xs:complexType>
    <xs:attribute name="StreamMasterIP" type="ws:IsValidIP" />
    <xs:attribute name="StreamMasterPort" type="ws:NotNullPort" use="required" />
    <xs:attribute name="HeadendID" type="ws:NotNullString" use="required" />
    <xs:attribute name="StreamSourceConfig" type="ws:StreamSourceConfig" />
    <xs:attribute name="StreamingMode" type="ws:StreamingMode" />
    <xs:attribute name="MSASupport" type="ws:EnableDisableEnum" />
    <xs:attribute name="TME-SCE" type="ws:TME-SCE" />
  </xs:complexType>
</xs:element>

<xs:element name="GeneralSettings">
  <xs:complexType>
    <xs:attribute name="VirtualOrLocalMasterIP" type="ws:IsValidIP" />
    <xs:attribute name="VaultMasterPort" type="ws:NotNullPort" />
    <xs:attribute name="VirtualMasterPort" type="ws:NotNullPort" />
    <xs:attribute name="WebServicePort" type="ws:NotNullPort" use="required" />
    <xs:attribute name="PreEncryptionSupport" type="ws:EnableDisableEnum" use="required" />
    <xs:attribute name="FTPOutPort" type="ws:NotNullPort" />
  </xs:complexType>
</xs:element>

<xs:element name="VHOISAConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:StreamerBMSSettings" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CORBA Services" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LSCPService" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:OpenStreamResourceServices" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="AssignedGroup">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VHOISAConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>

</xs:element name="AssignedGroups">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:AssignedGroup" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="SiteSetupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:AssignedGroups" minOccurs="0" maxOccurs="unbounded" />
      <xs:attribute name="SiteName" type="ws:NotNullString" use="required" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="SiteSetupConfigurationsList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SiteSetupConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Thin pipe Map elements -->
<xs:element name="SiteConfig">
  <xs:complexType>
    <xs:attribute name="SiteName" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="ConfiguredSites">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SiteConfig" minOccurs="0" maxOccurs="128" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="SubnetConfig">
  <xs:complexType>
    <xs:attribute name="Network" type="ws:IsValidIP" use="required" />
    <xs:attribute name="SubnetMask" type="ws:IsValidSubNetMask" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="SubnetConfigurations">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SubnetConfig" minOccurs="0" maxOccurs="64" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="ThinPipeMapConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ConfiguredSites" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:SubnetConfigurations" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="Pipe" type="ws:NotNullString" use="required" />
    <xs:attribute name="LocalSite" type="ws:NotNullString" use="required" />
    <xs:attribute name="MaxTransmitBW" type="ws:NotNullString" use="required" />
    <xs:attribute name="MaxRcvBW" type="ws:NotNullString" use="required" />
    <xs:attribute name="LimitTrafficToHTTPSubnets" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="ThinPipeMapConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ThinPipeMapConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Array Level/Stream To CDN Map elements -->
<xs:element name="CDNGroup">
  <xs:complexType>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
    <xs:attribute name="Preference" type="ws:PreferenceEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="VolumePreferences">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:CDNGroup" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="Name" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamToCDNGroupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:VolumePreferences" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="GroupName" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>
Array-Level Configuration XML Schema

<!-- Configure/Array Level/Ingest Driver Client elements -->
<xs:element name="IngestDriverClientConfig">
  <xs:complexType>
    <xs:attribute name="Timeout" type="xs:positiveInteger" use="required" />
    <xs:attribute name="AssetFactoryID" type="ws:NotNullString" use="required" />
    <xs:attribute name="AssetFactoryKind" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>

<!-- Start of Bulk Array Configuration Elements-->
<xs:element name="ArrayConfiguration">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ArrayDNSConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:ArrayNTPConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:StreamGroupsConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:SSVGroupsConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:VHOGroupsConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:VaultGroupsConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:IngestSteeringConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CacheGroupsConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CDNGroupsConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:ReplicationGroupConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CacheToCacheMapConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CacheToVaultMapConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:StreamToCacheMapConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:StreamToCDNMapConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:VaultRedundancyMapConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:MasterVaultGroupConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:ControlSetupIPConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:StreamerBMSConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:VaultBMSConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:VHOISAConfigurationSettings" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:simpleType name="ArrayLevelProps">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Medium"/>
    <xs:enumeration value="Low"/>
    <xs:enumeration value="None"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StreamSourceConfig">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Control IP"/>
    <xs:enumeration value="Default Stream Source IP"/>
    <xs:enumeration value="Stream Interface IP"/>
    <xs:enumeration value="None"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StreamGroupRole">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Stream Delivery"/>
    <xs:enumeration value="Setup/Control"/>
    <xs:enumeration value="None"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StreamingMode">
  <xs:restriction base="xs:string">
    <xs:enumeration value="ASI"/>
    <xs:enumeration value="GigE"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TME-SCE">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Disabled"/>
    <xs:enumeration value="Enable for OpenStream"/>
    <xs:enumeration value="Enable for MystroMDN"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="LSCPClientProtocol">
  <xs:restriction base="xs:string">
    <xs:enumeration value="TVGuide"/>
    <xs:enumeration value="RTI"/>
    <xs:enumeration value="VODLink"/>
    <xs:enumeration value="CV"/>
    <xs:enumeration value="Cisco(RTSP)"/>
    <xs:enumeration value="TTV(RTSP)"/>
    <xs:enumeration value="LSCP Pause At EOS"/>
    <xs:enumeration value="Cisco(RTSP)+TrickRestrict"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NotNullPort">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="65535"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="YesNoEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Yes"/>
    <xs:enumeration value="No"/>
  </xs:restriction>
</xs:simpleType>
Server-Level Configuration XML Schema

The Server-Level Configuration XML schema file describes and dictates the content of the Server-Level Configuration XML file. The ciscowebsvc_bulk_config.xsd file contains the XML schema.

Note

The following System-Level configuration pages that are included in the Server-Level XML schema are obsolete and replaced in the System-Level XML schema:

- QAM Gateway
- Headend Setup (For gigabit Ethernet streaming mode. ASI streaming headend configuration is imported as part of the QAM Gateway page configuration importing.)
- Stream Destination

```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:attribute name="PartNumber" type="xs:string" />
            <xs:attribute name="Type" type="xs:string" />
        </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:schema>
```
<xs:complexType name="Server">
  <xs:sequence>
    <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
    <xs:element ref="ws:Route" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>

<xs:element name="RouteTable">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<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:attribute name="TrapCommunity" type="xs:string" />
  </xs:complexType>
</xs:element>

<xs:element name="SNMPVACM">
  <xs:complexType>
    <xs:attribute name="User" type="xs:string" />
    <xs:attribute name="Access" type="xs:string" />
    <xs:attribute name="Authentication" type="xs:string" />
    <xs:attribute name="OID" type="xs:string" />
  </xs:complexType>
</xs:element>

<xs:element name="SNMPUSM">
  <xs:complexType>
    <xs:attribute name="User" type="xs:string" />
    <xs:attribute name="Authentication" type="xs:string" />
    <xs:attribute name="AuthenticationPassword" type="xs:string" />
    <xs:attribute name="Encryption" type="xs:string" />
    <xs:attribute name="EncryptionPassword" 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:sequence>
  </xs:complexType>
</xs:element>
Server-Level Configuration XML Schema

maxOccurs="unbounded" />
  <xs:element ref="ws:SNMPTrapStation" minOccurs="0" maxOccurs="unbounded" />

<xs:element ref="ws:SNMPVACM" minOccurs="0" maxOccurs="unbounded" />
<xs:element ref="ws:SNMPUSM" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>

<x:s: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:attribute name="ReceivePort" type="ws:NotNullPort" />
    <xs:attribute name="SendPort" type="ws:NotNullPort" />
    <xs:attribute name="ReceiveBuffer" type="ws:EnumReceiveBuffer" />
    <xs:attribute name="Model" type="ws:EnumRTSPDeploymentType" />
    <xs:attribute name="Transport" type="ws:EnumTransport" />
  </xs:complexType>
</xs:element>

<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="ws:IsValidIP" />
    <xs:attribute name="LoopingSessionTimeout" type="xs:nonNegativeInteger" />
    <xs:attribute name="SessionInactivityTimeout" type="xs:nonNegativeInteger" />
    <xs:attribute name="SessionPauseTimeout" type="xs:nonNegativeInteger" />
    <xs:attribute name="RTSPServerIP" type="ws:IsValidIP" />
    <xs:attribute name="RTSPServerPort" type="ws:NotNullPort" />
    <xs:attribute name="ReconnectIP" type="xs:string" />
    <xs:attribute name="ReconnectPort" type="ws:NotNullPort" />
    <xs:attribute name="MaxHistory" type="xs:nonNegativeInteger" />
    <xs:attribute name="MaintenanceMode" type="ws:EnumOnOff" />
    <xs:attribute name="LSCPAddress" type="ws:IsValidIP" />
    <xs:attribute name="LSCPPort" type="ws:NotNullPort" />
    <xs:attribute name="LSCPResponsePadding" type="ws:EnumOnOff" />
    <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="BackupAuthenticationManagerIP" type="xs:string" />
    <xs:attribute name="BackupAuthenticationManagerPort" type="xs:positiveInteger" />
    <xs:attribute name="CallbackServerIP" type="xs:string" />
    <xs:attribute name="CallbackServerPort" type="ws:NotNullPort" />
    <xs:attribute name="ServerIP" type="xs:string" />
    <xs:attribute name="ServerPort" type="ws:NotNullPort" />
    <xs:attribute name="StreamControlIP" type="xs:string" />
  </xs:attribute>
</xs:complexType>
</xs:element>
<xs:complexType>
  <xs:attribute name="StreamControlPort" type="ws:NotNullPort" />
  <xs:attribute name="DBConnectSize" type="xs:positiveInteger" />
  <xs:attribute name="UDPPacketSize" type="xs:positiveInteger" />
  <xs:attribute name="ThreadpoolSize" type="xs:positiveInteger" />
  <xs:attribute name="SessionMax" 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" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="IPAddress" type="ws:IsValidIPOrNull" />
    <xs:attribute name="ServerPort" type="ws:Port" />
    <xs:attribute name="FTPClientPort" type="ws:Port" />
    <xs:attribute name="FTPOutServerPort" type="ws:Port" />
    <xs:attribute name="FTPOutLoginTTL" type="xs:nonNegativeInteger" />
    <xs:attribute name="ContentRootPath" type="xs:string" />
    <xs:attribute name="AsyncCallbackURL" type="xs:string" />
  </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>

<!-- 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="1" 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="DNSList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:DNS" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
Server-Level Configuration XML Schema

<!-- Configure/Server/NTPServer elements -->
<xs:element name="NTPServerIP" type="xs:string" />

<!-- Configure/Server/NTPServer elements -->
<xs:element name="NTPServer">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="1" maxOccurs="unbounded" />
      <xs:element ref="ws:NTPServerIP" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Server/NTPServerList elements -->
<xs:element name="NTPServerList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:NTPServer" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- SyslogConfig elements -->
<xs:element name="SyslogConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="1" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="RemoteLogging" type="ws:EnableDisableEnum" use="required" />
    <xs:attribute name="IPAddress" type="ws:IsValidIP" />
    <xs:attribute name="Port" type="ws:NotNullPort" />
  </xs:complexType>
</xs:element>

<!-- Configure/Server/SyslogConfigList elements -->
<xs:element name="SyslogConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SyslogConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Configure/Server/LogConfig elements -->
<xs:element name="flag">
  <xs:complexType>
    <xs:attribute name="name" type="xs:string" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="debug-flags">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:flag" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="Facility">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Facility" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:complexType name="LogConfig">
  <xs:sequence>
    <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
    <xs:element ref="ws:Facility" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>

<xs:element name="LogConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:LogConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="RecorderSharedConfig">
  <xs:complexType>
    <xs:attribute name="RecorderManagerIP" type="ws:IsValidIP" use="required" />
    <xs:attribute name="NTPServerIP" type="ws:IsValidIP" use="required" />
    <xs:attribute name="HeartbeatInterval" type="ws:Range2To30" use="required" />
    <xs:attribute name="RecorderLocation" type="ws:ValueIs15" />
    <xs:attribute name="RecordingModify" type="ws:SCTE35AdMarkers" use="required" />
    <xs:attribute name="RecorderManagerPort" type="ws:RecorderPort" use="required" />
    <xs:attribute name="ProtocolVersion" type="ws:ProtocolVersion" use="required" />
    <xs:attribute name="ThreadPoolSize" type="ws:ThreadPoolSize" />
    <xs:attribute name="StatusReportInterval" type="ws:StatusReportInterval" />
    <xs:attribute name="HTTPRequestTimeout" type="ws:HTTPRequestTimeout" />
    <xs:attribute name="HTTPResponseTimeout" type="ws:HTTPResponseTimeout" />
    <xs:attribute name="RecordingBandwidth" type="ws:Range1To100" use="required" />
    <xs:attribute name="DeliveryBandwidth" type="ws:Range1To100" use="required" />
    <xs:attribute name="StorageCapacity" type="ws:Range1To100" use="required" />
    <xs:attribute name="LocationVirtualIP" type="ws:IsValidIP" use="required" />
    <xs:attribute name="LocationSubnetMask" type="ws:IsValidSubNetMask" use="required" />
    <xs:attribute name="HTTPDSCP" type="ws:DSCPLimit" use="required" />
    <xs:attribute name="MceIP" type="ws:MceIP" />
    <xs:attribute name="McePort" type="ws:NotNullPort" use="required" />
    <xs:attribute name="MceUdsDir" type="ws:NotNullString" use="required" />
    <xs:attribute name="RetryStatusAttempts" type="ws:Range0To100" use="required" />
    <xs:attribute name="RetryStatusInterval" type="ws:Range60To3600" use="required" />
    <xs:attribute name="RecordingValidationAge" type="ws:Range0To10" use="required" />
  </xs:complexType>
</xs:element>

<!-- Configure/Server/DB Backup elements -->
<xs:element name="DbBackupConfigList"/>
<xs:complexType>
  <xs:sequence>
    <xs:element ref="ws:DbBackupConfig" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="DbBackupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="1" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="LiveBackupService" type="ws:EnableDisableEnum" use="required"/>
    <xs:attribute name="BackupServerIp" type="ws:IsValidIP" use="required"/>
    <xs:attribute name="SecondaryBackupServerIp" type="ws:IsValidIPOrNull" />
    <xs:attribute name="LoggingInterval" type="ws:Range1To3600" use="required"/>
    <xs:attribute name="OverallBandwidth" type="ws:Range0To1000" use="required"/>
    <xs:attribute name="PerSessionBandwidth" type="ws:Range0To1000" use="required"/>
  </xs:complexType>
</xs:element>

<xs:element name="RecorderServerConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:RecorderServerConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:StreamerRecorderConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="RecorderServerConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="1" maxOccurs="unbounded" />
      <xs:choice>
        <xs:element ref="ws:InterfaceConfig" minOccurs="0" maxOccurs="unbounded" />
        <xs:element ref="ws:ComplexInterfaceConfig" minOccurs="0" maxOccurs="unbounded" />
      </xs:choice>
    </xs:sequence>
    <xs:attribute name="PartNumber" type="xs:string" />
    <xs:attribute name="HostName" type="xs:string" use="required"/>
    <xs:attribute name="ArrayID" type="xs:integer" />
    <xs:attribute name="DefaultGateway" type="ws:IsValidIP" use="required"/>
    <xs:attribute name="DefaultGatewayDevice" type="ws:IsValidDefaultGatewayDevice" use="required"/>
    <xs:attribute name="HTTPDSCP" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="Status" type="xs:string" />
    <xs:attribute name="ComponentName" type="xs:string" />
    <xs:attribute name="ModelName" type="xs:string" />
    <xs:attribute name="RecorderManagerIP" type="ws:IsValidIP" use="required"/>
    <xs:attribute name="RetryStatusAttempts" type="ws:Range0To100" use="required"/>
    <xs:attribute name="RetryStatusInterval" type="ws:Range0To3600" use="required"/>
    <xs:attribute name="RecordingValidationAge" type="ws:Range0To10" use="required"/>
  </xs:complexType>
</xs:element>
<xs:complexType>
  <xs:sequence>
    <xs:element ref="ws:Server" minOccurs="1" maxOccurs="unbounded" />
    <xs:element ref="ws:SimpleDSCPMarking" minOccurs="0" maxOccurs="1" />
    <xs:element ref="ws:CustomDSCPMarking" minOccurs="0" maxOccurs="1" />
    <xs:element ref="ws:InterfaceConfig" minOccurs="0" maxOccurs="unbounded" />
    <xs:element ref="ws:BondInterfaceConfig" minOccurs="0" maxOccurs="1" />
  </xs:sequence>
  <xs:attribute name="PartNumber" type="xs:string" use="required" />
  <xs:attribute name="HostName" type="xs:string" />
  <xs:attribute name="ArrayID" type="xs:integer" />
  <xs:attribute name="NullStream" type="xs:string" />
  <xs:attribute name="StunPlayErrorDelay" type="ws:StunPlayErrorDelayLimit" />
  <xs:attribute name="StunPlayTimeout" type="ws:StunPlayTimeoutLimit" />
  <xs:attribute name="SourceIP" type="ws:IsValidIPOrNull" />
  <xs:attribute name="TransportPortStart" type="ws:Port" />
  <xs:attribute name="TransportPortEnd" type="ws:Port" />
  <xs:attribute name="CachePort" type="ws:Port" />
  <xs:attribute name="TCPTraffic" type="ws:EnableDisableEnum" />
  <xs:attribute name="StreamerIsCache" type="ws:EnableDisableEnum" />
  <xs:attribute name="JumboSFrames" type="ws:EnableDisableEnum" />
  <xs:attribute name="JumboCFrames" type="ws:EnableDisableEnum" />
  <xs:attribute name="VaultMirrorCopies" type="ws:VaultMirrorCopiesLimit" />
  <xs:attribute name="VaultLocalCopies" type="ws:VaultLocalCopiesLimit" />
  <xs:attribute name="DSCPMarkingMethod" type="ws:DSCPMarkingMethod" />
  <xs:attribute name="DualCAS" type="ws:EnableDisableEnum" />
  <xs:attribute name="DefaultGateway" type="ws:IsValidIPOrNull" />
  <xs:attribute name="DefaultGatewayDevice" type="ws:IsValidDefaultGatewayDevice" use="required" />
  <xs:attribute name="FTPOutInterface" type="xs:string" />
  <xs:attribute name="FTPOutBandwidth" type="ws:FTPOutBandwidthRange" />
  <xs:attribute name="FTPOutSession" type="ws:FTPOutSessionRange" />
  <xs:attribute name="TTL" type="xs:positiveInteger" />
  <xs:attribute name="MaxNoOfInterfaces" type="xs:integer" />
</xs:complexType>
<xs:element name="StreamServerConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="1" maxOccurs="unbounded" />
      <xs:element ref="ws:SimpleDSCPMarking" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CustomDSCPMarking" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:InterfaceConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:BondInterfaceConfig" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="PartNumber" type="xs:string" use="required" />
    <xs:attribute name="TTL" type="xs:positiveInteger" />
    <xs:attribute name="TransportDSCP" type="xs:integer" />
    <xs:attribute name="CacheDSCP" type="xs:integer" />
    <xs:attribute name="NullStream" type="ws:EnableDisableEnum" />
    <xs:attribute name="LivePlayback" type="ws:EnableDisableEnum" />
    <xs:attribute name="HostName" type="xs:string" />
    <xs:attribute name="ArrayID" type="xs:integer" />
    <xs:attribute name="SourceIP" type="ws:IsValidIPOrNull" />
    <xs:attribute name="TransportPortStart" type="ws:Port" />
    <xs:attribute name="TransportPortEnd" type="ws:Port" />
    <xs:attribute name="CachePort" type="ws:Port" />
    <xs:attribute name="TCPTraffic" type="ws:EnableDisableEnum" />
    <xs:attribute name="StreamerIsCache" type="ws:EnableDisableEnum" />
    <xs:attribute name="JumboSFrames" type="ws:EnableDisableEnum" />
    <xs:attribute name="JumboCFrames" type="ws:EnableDisableEnum" />
    <xs:attribute name="DSCPMarkingMethod" type="ws:DSCPMarkingMethod" />
    <xs:attribute name="DualCAS" type="ws:EnableDisableEnum" />
    <xs:attribute name="DefaultGateway" type="ws:IsValidIPOrNull" />
    <xs:attribute name="DefaultGatewayDevice" type="ws:IsValidDefaultGatewayDevice" use="required" />
    <xs:attribute name="MaxNoOfInterfaces" type="xs:integer" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamerRecorderConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="1" maxOccurs="unbounded" />
      <xs:element ref="ws:SimpleDSCPMarking" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CustomDSCPMarking" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="PartNumber" type="xs:string" use="required" />
    <xs:attribute name="TTL" type="xs:positiveInteger" />
    <xs:attribute name="TransportDSCP" type="xs:integer" />
    <xs:attribute name="CacheDSCP" type="xs:integer" />
    <xs:attribute name="NullStream" type="ws:EnableDisableEnum" />
    <xs:attribute name="LivePlayback" type="ws:EnableDisableEnum" />
    <xs:attribute name="HostName" type="xs:string" />
    <xs:attribute name="ArrayID" type="xs:integer" />
    <xs:attribute name="SourceIP" type="ws:IsValidIPOrNull" />
    <xs:attribute name="TransportPortStart" type="ws:Port" />
    <xs:attribute name="TransportPortEnd" type="ws:Port" />
  </xs:complexType>
</xs:element>
<xs:attribute name="CachePort" type="ws:Port" />
<xs:attribute name="StreamerIsCache" type="ws:EnableDisableEnum" />
<xs:attribute name="JumboSFrames" type="ws:EnableDisableEnum" />
<xs:attribute name="JumboCFrames" type="ws:EnableDisableEnum" />
<xs:attribute name="DSCPMarkingMethod" type="ws:DSCPMarkingMethod" />
<xs:attribute name="DualCAS" type="ws:EnableDisableEnum" />
</xs:complexType>
</xs:element>

<xs:element name="VaultServerConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:SimpleDSCPMarking" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CustomDSCPMarking" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:InterfaceConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:BondInterfaceConfig" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="PartNumber" type="xs:string" use="required" />
    <xs:attribute name="HostName" type="xs:string" />
    <xs:attribute name="ArrayID" type="xs:integer" />
    <xs:attribute name="JumboCFrames" type="xs:string" />
    <xs:attribute name="VaultMirrorCopies" type="xs:nonNegativeInteger" />
    <xs:attribute name="VaultLocalCopies" type="xs:nonNegativeInteger" />
    <xs:attribute name="DSCPMarkingMethod" type="ws:DSCPMarkingMethod" />
    <xs:attribute name="DualCAS" type="xs:string" />
    <xs:attribute name="DefaultGateway" type="ws:IsValidIPOrNull" />
    <xs:attribute name="DefaultGatewayDevice" type="ws:IsValidDefaultGatewayDevice" use="required" />
    <xs:attribute name="FTPOutInterface" type="xs:string" />
    <xs:attribute name="FTPOutBandwidth" type="ws:FTPOutBandwidthRange" />
    <xs:attribute name="FTPOutSession" type="ws:FTPOutSessionRange" />
    <xs:attribute name="CachePort" type="ws:Port" />
    <xs:attribute name="TTL" type="xs:positiveInteger" />
    <xs:attribute name="SourceIP" type="ws:IsValidIPOrNull" />
    <xs:attribute name="MaxNoOfInterfaces" type="xs:integer" />
  </xs:complexType>
</xs:element>

<xs:element name="CacheServerConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:SimpleDSCPMarking" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CustomDSCPMarking" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:InterfaceConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:BondInterfaceConfig" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="PartNumber" type="xs:string" use="required" />
    <xs:attribute name="HostName" type="xs:string" />
    <xs:attribute name="ArrayID" type="xs:integer" />
    <xs:attribute name="JumboCFrames" type="ws:EnableDisableEnum" />
    <xs:attribute name="DSCPMarkingMethod" type="ws:DSCPMarkingMethod" />
    <xs:attribute name="DefaultGateway" type="ws:IsValidIPOrNull" />
    <xs:attribute name="DefaultGatewayDevice" type="ws:IsValidDefaultGatewayDevice" use="required" />
    <xs:attribute name="TTL" type="xs:positiveInteger" />
  </xs:complexType>
</xs:element>
<xs:element name="ControllerServerConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="1" maxOccurs="unbounded" />
      <xs:element ref="ws:InterfaceConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:BondInterfaceConfig" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="HostName" type="xs:string" />
    <xs:attribute name="PartNumber" type="xs:string" use="required" />
    <xs:attribute name="DefaultGateway" type="ws:IsValidIPOrNull" />
    <xs:attribute name="MaxNoOfInterfaces" type="xs:integer" />
  </xs:complexType>
</xs:element>

<xs:complexType name="InterfaceTypeRange">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="7" />
  </xs:restriction>
</xs:complexType>

<xs:complexType name="FTPOutBandwidthRange">
  <xs:restriction base="xs:integer">
    <xs:pattern value="([0-9]|(1[0-9])|(2[0-9])|(3[0-2]))" />
  </xs:restriction>
</xs:complexType>

<xs:complexType name="FTPOutSessionRange">
  <xs:restriction base="xs:integer">
    <xs:pattern value="([0-9]|([1-9][0-9]|1[0-9][0-9]|2[0-9][0-9]|3[0-2]))" />
  </xs:restriction>
</xs:complexType>

<xs:complexType name="StunPlayErrorDelayLimit">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="2999" />
  </xs:restriction>
</xs:complexType>

<xs:complexType name="StunPlayTimeoutLimit">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="299" />
  </xs:restriction>
</xs:complexType>

<xs:simpleType name="IsValidIP">
  <xs:restriction base="xs:string">
    <xs:pattern value="((\[1-9]?(\[0-9]?)\|[1-9]?\[0-9]?)\|[1-9]?(\[0-9]?)\|[1-9]?\[0-9]?)\|(10000))" />
  </xs:restriction>
</xs:simpleType>
Appendix B      Creating Bulk Configuration Files

Server-Level Configuration XML Schema

<xsd:simpleType name="IsValidIPOrNull">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="()|((1-9)?[0-9] |[1-9] |[0-9] |[0-9] |[0-9] |[2|0|4][0-9]|25[0-5])\.\d{3}(1-9)?[0-9] |[0-9] |[0-9] |[0-9] |[2|0|4][0-9]|25[0-5])" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="IsValidSubNetMask">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="((255 |254 |252 |248 |240 |224 |192 |128\.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0)" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="IsValidSubNetMaskOrNull">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="()|((255 |254 |252 |248 |240 |224 |192 |128\.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0) |(255\.|255 |254 |252 |248 |240 |224 |192 |128 \.|0\.0\.0)" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="IsValidMAC">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="([0-9a-fA-F]{2}:){5}([0-9a-fA-F]{2})" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="NotNullstring">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="VaultMirrorCopiesLimit">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="0" />
    <xsd:maxInclusive value="10" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="VaultLocalCopiesLimit">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="1" />
    <xsd:maxInclusive value="4" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="ValueIs5">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="5" />
    <xsd:maxInclusive value="5" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="ValueIs15">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="15" />
    <xsd:maxInclusive value="15" />
  </xsd:restriction>
</xsd:simpleType>
<xs:simpleType name="Range0To10">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="10" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range0To100">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range60To3600">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="60" />
    <xs:maxInclusive value="3600" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range1To100">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range1To3600">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="3600" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range0To1000">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="1000" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range2To30">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="2" />
    <xs:maxInclusive value="30" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ProtocolVersion">
  <xs:restriction base="xs:string">
    <xs:enumeration value="I02"/>
    <xs:enumeration value="I04"/>
    <xs:enumeration value="i02"/>
    <xs:enumeration value="i04"/>
    <xs:enumeration value="2"/>
    <xs:enumeration value="4"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ThreadpoolSize">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="StatusReportInterval">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="60" />
    <xs:maxInclusive value="60" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="HTTPRequestTimeout">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="5" />
    <xs:maxInclusive value="5" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="HTTPResponseTimeout">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="5" />
    <xs:maxInclusive value="5" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Range1To60">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="60" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="RecorderPort">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="50005" />
    <xs:maxInclusive value="65535" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="SCTE35AdMarkers">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Retain"/>
    <xs:enumeration value="Discard"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IsValidDefaultGatewayDevice">
  <xs:restriction base="xs:string">
    <xs:enumeration value="bond0"/>
    <xs:enumeration value="eth0"/>
    <xs:enumeration value="eth1"/>
    <xs:enumeration value="eth2"/>
    <xs:enumeration value="eth3"/>
    <xs:enumeration value="eth4"/>
    <xs:enumeration value="eth5"/>
    <xs:enumeration value="eth6"/>
    <xs:enumeration value="eth7"/>
    <xs:enumeration value="eth8"/>
    <xs:enumeration value="eth9"/>
    <xs:enumeration value="eth10"/>
    <xs:enumeration value="eth11"/>
    <xs:enumeration value="eth12"/>
  </xs:restriction>
</xs:simpleType>
Server-Level Configuration XML Schema

<xs:element name="SimpleDSCPMarking">
  <xs:complexType>
    <xs:attribute name="ControlDSCP" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="StreamDSCP" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="HTTPDSCP" type="ws:DSCPLimit" use="optional"/>
  </xs:complexType>
</xs:element>

<xs:element name="CustomDSCPMarking">
  <xs:complexType>
    <xs:attribute name="ControlTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="StreamTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="HTTPTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="CommittedRateLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLiveIngestTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="DriveFailureRepairTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="LowestPriorityDataSmoothingTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="CommittedRateTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="MirroringTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="CommittedRateLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLiveIngestTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="DriveFailureRepairTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="LowestPriorityDataSmoothingTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="CommittedRateTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="MirroringTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="CommittedRateLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLiveIngestTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="DriveFailureRepairTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="LowestPriorityDataSmoothingTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="CommittedRateTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="MirroringTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="CommittedRateLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLiveIngestTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="DriveFailureRepairTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="LowestPriorityDataSmoothingTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="CommittedRateTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="MirroringTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="required"/>
    <xs:attribute name="HighestPriorityRxTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="CommittedRateLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLostPktRecovery" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="MirroringLiveIngestTraffic" type="ws:DSCPLimit" use="optional"/>
    <xs:attribute name="DriveFailureRepairTraffic" type="ws:DSCPLimit" use="optional"/>
<xs:complexType name="InterfaceType">
  <xs:simpleType name="InterfaceType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="Not Used"/>
      <xs:enumeration value="Management"/>
      <xs:enumeration value="Ingest"/>
      <xs:enumeration value="Stream"/>
      <xs:enumeration value="Cache"/>
      <xs:enumeration value="General"/>
      <xs:enumeration value="Stream Control"/>
      <xs:enumeration value="Locate"/>
      <xs:enumeration value="Ingest/Stream/Cache"/>
      <xs:enumeration value="Ingest/Cache"/>
    </xs:restriction>
  </xs:simpleType>
</xs:complexType>

<xs:simpleType name="Port">
  <xs:restriction base="xs:string">
    <xs:pattern
      value="()|([1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|[0-5][0-9][0-9][0-9][0-9]|" />
    <!--Port allow only in the range of 1 to 65535-->
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NotNullPort">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="65535"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Vlan">
  <xs:restriction base="xs:nonNegativeInteger">
    <xs:minInclusive value="0"/>
    <xs:maxInclusive value="4095"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="ServerConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SSVServerConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:VaultServerConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:StreamServerConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:CacheServerConfig" minOccurs="0" maxOccurs="unbounded" />
      <xs:element ref="ws:RecorderServerConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
Server-Level Configuration XML Schema

<xs:element name="ServerConfiguration">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:RouteTableList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:SNMPAgentList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:DNSList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:NTPServerList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:RTSPSetupList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:FSISetupList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:RecorderServerConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:DbBackupConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:ServerConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:LogConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:SyslogConfigList" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:simpleType name="EnumOnOff">
  <xs:restriction base="xs:string">
    <xs:enumeration value="On"/>
    <xs:enumeration value="Off"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="EnumReceiveBuffer">
  <xs:restriction base="xs:positiveInteger">
    <xs:enumeration value="65535"/>
    <xs:enumeration value="512000"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="EnumRTSPDeploymentType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="ncube"/>
    <xs:enumeration value="digeo"/>
    <xs:enumeration value="ngod"/>
    <xs:enumeration value="myrio"/>
    <xs:enumeration value="telenet"/>
    <xs:enumeration value="eventis"/>
    <xs:enumeration value="quative"/>
    <xs:enumeration value="voo"/>
    <xs:enumeration value="cisco"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="EnumTransport">
  <xs:restriction base="xs:string">
    <xs:enumeration value="TCP"/>
    <xs:enumeration value="UDP"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="SubInterfaceConfigIdRange">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="4095" />
  </xs:restriction>
</xs:simpleType>

<xs:element name="ComplexInterfaceConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:SubInterfaceConfig" minOccurs="0"
                  maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="Name" type="xs:string" />
    <xs:attribute name="Type" type="ws:InterfaceType" />
    <xs:attribute name="IPAddress" type="ws:Is ValidIPOrNull" />
    <xs:attribute name="SubnetMask" type="ws:IsValidSubNetMaskOrNull" />
    <xs:attribute name="TransportPort" type="ws:Port" />
    <xs:attribute name="CachePort" type="ws:Port" />
    <xs:attribute name="Number" type="xs:integer" />
  </xs:complexType>
</xs:element>

<xs:element name="SubInterfaceConfig">
  <xs:complexType>
    <xs:attribute name="Id" type="ws:SubInterfaceConfigIdRange" />
    <xs:attribute name="Type" type="ws:SubInterfaceType" />
    <xs:attribute name="IPAddress" type="ws:IsValidIP" />
    <xs:attribute name="SubnetMask" type="ws:IsValidSubNetMaskOrNull" />
  </xs:complexType>
</xs:element>

<xs:element name="BondInterfaceConfig">
  <xs:complexType>
    <xs:attribute name="Name" type="xs:string" />
    <xs:attribute name="SlaveInterfaces" type="xs:string" />
  </xs:complexType>
</xs:element>

<xs:simpleType name="SubInterfaceSubType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="VLAN" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="SubInterfaceType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Ingest" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="MceIP">
  <xs:restriction base="xs:string">
    <xs:enumeration value="127.0.0.1"/> 
  </xs:restriction>
</xs:simpleType>
Maintain Section Configuration XML Schema

The Maintain Section Configuration XML schema file describes and dictates the content of the Maintain Section Configuration XML file. The ciscowebsvc_bulk_maintainconfig.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">
    <!-- Maintain/Software/Database Configs elements -->
    <xs:element name="ProvisionMultiple3Report">
        <xs:complexType>
            <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
        </xs:complexType>
    </xs:element>

    <xs:element name="ProvisionMultiple2Report">
        <xs:complexType>
            <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
        </xs:complexType>
    </xs:element>

    <xs:element name="ContentObjectReport">
        <xs:complexType>
            <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
        </xs:complexType>
    </xs:element>

    <xs:element name="ContentObject3Report">
        <xs:complexType>
            <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
        </xs:complexType>
    </xs:element>

    <!-- InterfaceSetupConfigList element -->
    <xs:element name="InterfaceSetupConfigList">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ws:InterfaceSetupConfig" minOccurs="0" maxOccurs="unbounded" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <!-- InterfaceSetupConfig element -->
    <xs:element name="InterfaceSetupConfig">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
                <xs:element ref="ws:InterfaceConfig" minOccurs="0" maxOccurs="unbounded" />
                <xs:element ref="ws:BondInterfaceConfig" minOccurs="0" maxOccurs="1" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```
<xs:complexType>
  <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
</xs:complexType>
</xs:element>

<xs:element name="PackageRetryReport">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CacheStatsReport">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CV_RecordingReport">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="PurchaseRecordingReport">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamReport">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamReportByGroup">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamReportByServer">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamTrick15Report">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamTrickReport">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="BarkerReport">
  <xs:complexType>
    <xs:attribute name="Setting" type="ws:EnableDisableEnum" use="required" />
  </xs:complexType>
</xs:element>
<xs:element name="DatabaseConfig">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:ProvisionMultiple3Report" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:ProvisionMultiple2Report" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:ContentObjectReport" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:ContentObject3Report" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:ContentObject4Report" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:PackageRetryReport" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:CacheStatsReport" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:CV_RecordingReport" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:PurchaseRecordingReport" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:StreamReport" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:StreamReportByGroup" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:StreamReportByServer" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:StreamTrick15Report" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:StreamTrickReport" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:BarkerReport" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="DatabaseConfigs">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:DatabaseConfig" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Maintain / Software / System Configs Elements -->

<xs:element name="PopularityBasedCaching">
    <xs:complexType>
        <xs:attribute name="PopularityHalfLife" type="ws:PBC_Config" use="required"/>
    </xs:complexType>
</xs:element>

<xs:element name="ContentListingConfig">
    <xs:complexType>
        <xs:attribute name="Value" type="ws:ContentLimit" use="required"/>
    </xs:complexType>
</xs:element>

<xs:element name="SystemConfig">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:PopularityBasedCaching" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="ws:ContentListingConfig" minOccurs="0" maxOccurs="1"/>
            <xs:attribute name="GroupMap" type="ws:Vendor" use="required"/>
            <xs:attribute name="ServerGroupMap" type="ws:Vendor" use="required"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="SystemConfigs">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="ws:SystemConfig" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
Maintain Section Configuration XML Schema

<!-- Maintain / Server / System Thresholds -->
<xs:element name="CiscoContentStoreMaster">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoContentStoreSlave">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoResourceManager">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoCacheServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoDBServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoSNMPServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoSystemManager">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoPrimaryStreamSetupService">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoStreamControlService">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoFSIMaster">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>
<xs:element name="CiscoFSIServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoRTSPServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoAssetManager">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoIngestManager">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoBWMgrServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoCollectDServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoPlayoutProcessor">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoAVSLauncher">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoCDSMWebServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoCDSMImporterServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CiscoCDSMExporterServer">
  <xs:complexType>
    <xs:attribute name="Monitored" type="ws:YesNoEnum" use="required" />
  </xs:complexType>
</xs:element>
<xs:element name="Services">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:CiscoContentStoreMaster" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CiscoContentStoreSlave" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CiscoPrimaryStreamSetupService" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:CiscoStreamControlService" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="DNSSettings">
  <xs:complexType>
    <xs:attribute name="Attempts" type="ws:ValidAttempts" use="required" />
    <xs:attribute name="Timeout" type="ws:ValidTimeout" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="PerformanceParameters">
  <xs:complexType>
    <xs:attribute name="PortLoss" type="ws:ValidPortLoss" use="required" />
    <xs:attribute name="DiskLoss" type="ws:ValidDiskLoss" use="required" />
    <xs:attribute name="DiskCapacityNotify" type="ws:ValidDiskCapacityNotify" use="required" />
    <xs:attribute name="DiskCapacityWarning" type="ws:ValidDiskCapacityWarning" use="required" />
    <xs:attribute name="LinuxFileSystemUsage" type="ws:ValidFileSystemUsage" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="SystemThresholdConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:PerformanceParameters" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:DNSSettings" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:Services" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="SystemThresholds">
  <xs:complexType>
    <!-- More XML schema content here -->
  </xs:complexType>
</xs:element>
<xs:element name="Server">
  <xs:complexType>
    <xs:attribute name="ServerID" type="ws:ValidServerID" use="required" />
    <xs:attribute name="ServerIP" type="ws:IsValidIP" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="DeliveryServers">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:Server" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="ApplicationConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:DeliveryServers" minOccurs="0" maxOccurs="1" />
      <xs:attribute name="Application" type="ws:ApplicationEnum" use="required" />
      <xs:attribute name="StreamDeliveryMode" type="ws:DeliveryModeEnum" use="required" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="ApplicationConfigurations">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ApplicationConfig" minOccurs="0" maxOccurs="2" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="UDP">
  <xs:complexType>
    <xs:attribute name="IP" type="ws:IsValidIP" use="required" />
    <xs:attribute name="Port" type="ws:NotNullPort" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamMonitorListenerConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:UDP" minOccurs="0" maxOccurs="2" />
      <xs:attribute name="Support" type="ws:EnableDisableEnum" use="required" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="StreamMonitorListenerConfigs">
  <xs:complexType>
    <xs:sequence>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element ref="ws:StreamMonitorListenerConfig" minOccurs="0" maxOccurs="1" />
</xs:complexType>
</xs:element>

<!-- Maintain / Software / ID Management -->
<xs:element name="IDManagementConfig">
  <xs:complexType>
    <xs:attribute name="GroupIDStart" type="ws:ValidServerID" use="required" />
    <xs:attribute name="ServerIDStart" type="ws:ValidServerID" use="required" />
    <xs:attribute name="SetupIDStart" type="ws:ValidServerID" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="IDManagementConfigs">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:IDManagementConfig" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Maintain / Software / VVIM/CDSM Setup page -->
<xs:element name="DeployedCServerVersion">
  <xs:complexType>
    <xs:attribute name="CServerVersion" type="ws:NotNullString" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamFailoverSupport">
  <xs:complexType>
    <xs:attribute name="FailoverSupport" type="ws:OnOffEnum" use="required" />
    <xs:attribute name="RetryCount" type="ws:RetryCountRange" />
  </xs:complexType>
</xs:element>

<xs:element name="RoleFailoverOnDBConnectivityLoss">
  <xs:complexType>
    <xs:attribute name="FailoverSupport" type="ws:OnOffEnum" use="required" />
    <xs:attribute name="RetryCount" type="ws:RetryCountRange" />
  </xs:complexType>
</xs:element>

<xs:element name="FailoverOnBMSConnectivityLoss">
  <xs:complexType>
    <xs:attribute name="FailoverSupport" type="ws:OnOffEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="StreamSteering">
  <xs:complexType>
    <xs:attribute name="Mode" type="ws:SteeringModeEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="DeploymentNetworkConfig">
  <xs:complexType>
    <xs:attribute name="Networked" type="ws:NetworkConfigEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="NICBonding">
  <xs:complexType>
<xs:element name="bs:description" type="ws:EnabledDisabledEnum" use="required" />
</xs:complexType>
</xs:element>

<xs:element name="bs:InstallationType">
  <xs:complexType>
    <xs:attribute name="bs:Installation" type="ws:InstallationTypeEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:StreamDestination">
  <xs:complexType>
    <xs:attribute name="bs:Type" type="ws:DestinationTypeEnum" use="required" />
    <xs:attribute name="bs:Options" type="ws:DestinationTypeOptionsEnum" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:SplunkSupport">
  <xs:complexType>
    <xs:attribute name="bs:Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:ParentChildServiceGroups">
  <xs:complexType>
    <xs:attribute name="bs:Mode" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:RedirectServer">
  <xs:complexType>
    <xs:attribute name="bs:Support" type="ws:OnOffEnum" use="required" />
    <xs:attribute name="bs:Port" type="ws:NotNullPort" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:VBOConfiguration">
  <xs:complexType>
    <xs:attribute name="bs:Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:AssetScaleCoexistenceSupport">
  <xs:complexType>
    <xs:attribute name="bs:Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:BulkImportExportConfig">
  <xs:complexType>
    <xs:attribute name="bs:Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:SSVGroups">
  <xs:complexType>
    <xs:attribute name="bs:Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="bs:TrickModeCapture">
  <xs:complexType>
/**
 * Define the XML schema for the Bulk Configuration File.
 */
<xs:schema xmlns:ws="http://example.com/ws">
  <xs:element name="Configuration">
    <xs:complexType>
      <xs:attribute name="TrickModeCapture" type="ws:EnabledDisabledEnum" use="required" />
      <xs:attribute name="StreamReportCapture" type="ws:EnabledDisabledEnum" use="required" />
    </xs:complexType>
    <xs:element name="FailIngestTuning">
      <xs:complexType>
        <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
      </xs:complexType>
    </xs:element>
    <xs:element name="VaultGroups">
      <xs:complexType>
        <xs:attribute name="Mode" type="ws:EnabledDisabledEnum" use="required" />
      </xs:complexType>
    </xs:element>
    <xs:element name="ARPParameters">
      <xs:complexType>
        <xs:attribute name="Parameters" type="ws:ARPParametersEnum" use="required" />
        <xs:attribute name="ARPFormat" type="ws:ARPFormatEnum" />
        <xs:attribute name="ARPDestinationIP" type="ws:ARPDestinationEnum" />
      </xs:complexType>
    </xs:element>
    <xs:element name="WatermarkingSupport">
      <xs:complexType>
        <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
      </xs:complexType>
    </xs:element>
    <xs:element name="ManageRecorders">
      <xs:complexType>
        <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
      </xs:complexType>
    </xs:element>
    <xs:element name="ATISC2Setup">
      <xs:complexType>
        <xs:attribute name="Mode" type="ws:ATISC2ModeEnum" use="required" />
        <xs:attribute name="DomainName" type="xs:string" />
        <xs:attribute name="ChunkDuration" type="ws:ChunkDurationRange" />
      </xs:complexType>
    </xs:element>
    <xs:element name="PackagePriorityRulesConfig">
      <xs:complexType>
        <xs:attribute name="TitleWeight" type="ws:TitleWeightRange" use="required" />
        <xs:attribute name="ProviderIDWeight" type="ws:WeightRange" use="required" />
        <xs:attribute name="WindowWeight" type="ws:WeightRange" use="required" />
      </xs:complexType>
    </xs:element>
    <xs:element name="TCPKeepAliveSettings">
      <xs:complexType>
        <xs:attribute name="Time" type="ws:TCPTimeRange" use="required" />
        <xs:attribute name="Interval" type="ws:TCPIntervalRange" use="required" />
        <xs:attribute name="Probes" type="ws:TCPProbesRange" use="required" />
      </xs:complexType>
    </xs:element>
    <xs:element name="DNSResolutionSupport">
    </xs:element>
  </xs:complexType>
</xs:schema>
Appendix B  Creating Bulk Configuration Files

Maintain Section Configuration XML Schema

```xml
<xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
</xs:complexType>
</xs:element>

<xs:element name="TCPWindowScaleSupport">
    <xs:complexType>
        <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="TVODSetup">
    <xs:complexType>
        <xs:attribute name="Mode" type="ws:EnabledDisabledEnum" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="ThinPipeManagement">
    <xs:complexType>
        <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="IngestResiliency">
    <xs:complexType>
        <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="VODErrorRepair">
    <xs:complexType>
        <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
        <xs:attribute name="ActivationKey" type="xs:string" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="MediaScheduler">
    <xs:complexType>
        <xs:attribute name="Support" type="ws:OnOffEnum" use="required" />
        <xs:attribute name="TransformerType" type="ws:TransformerTypeEnum" />
        <xs:attribute name="StartDayOfYear" type="ws:StartDayOfYearEnum" />
        <xs:attribute name="ActivationKey" type="xs:string" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="RealTimeCapture">
    <xs:complexType>
        <xs:attribute name="Type" type="ws:RealTimeCaptureEnum" use="required" />
    </xs:complexType>
</xs:element>

<xs:element name="VirtualVideoInfrastructure">
    <xs:complexType>
        <xs:attribute name="VVIOptions" type="ws:EnabledDisabledEnum" use="required" />
        <xs:attribute name="ManagementSystemRole" type="ws:CDSMRoleEnum" />
        <xs:attribute name="CacheFillProtocol" type="ws:CacheFillProtocolEnum" />
        <xs:attribute name="VaultCacheMgrIP" type="ws:IsValidIP" />
        <xs:attribute name="StreamDomainName" type="xs:string" />
        <xs:attribute name="StreamingMode" type="ws:StreamingMode" />
    </xs:complexType>
</xs:element>

<xs:element name="ContentStorage">
    http://www.w3.org/2001/XMLSchema
```
<xs:complexType>
  <xs:attribute name="ContentStorage" type="ws:ContentStorageEnum" use="required" />
  <xs:attribute name="ChangeNotifications" type="ws:EnabledDisabledEnum" />
</xs:complexType>
</xs:element>

<xs:element name="RemoteSetupControlService">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
    <xs:attribute name="GlobalSourceIP" type="ws:IsValidIP" />
    <xs:attribute name="GlobalSourcePort" type="ws:NotNullPort" />
    <xs:attribute name="MinimumStreamsPerPort" type="ws:MinimumStreamsPerPort" />
    <xs:attribute name="SingleSessionTimeout" type="ws:SingleSessionTimeout" />
    <xs:attribute name="SessionsPerControl" type="ws:SessionsPerControl" />
  </xs:complexType>
</xs:element>

<xs:element name="PlayoutProcessor">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="PlayoutScheduler">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
    <xs:attribute name="LocalizedEPGExtensions" type="ws:OnOffEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="IngestManager">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:OnOffEnum" use="required" />
    <xs:attribute name="UpStreamIngestSystem" type="ws:UpStreamIngestSystem" use="required" />
    <xs:attribute name="ActivationKey" type="xs:string" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="RTSPDeployment">
  <xs:complexType>
    <xs:attribute name="Type" type="ws:RTSPDeploymentTypeEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="ContentPropagation">
  <xs:complexType>
    <xs:attribute name="Mode" type="ws:ContentPropagationEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="FutureRecording">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="DuplicateQAMDetection">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>
Maintain Section Configuration XML Schema

<xs:element name="ThirdPartyCDN">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="VolumeNameBased">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="CVAccountSettings">
  <xs:complexType>
    <xs:attribute name="HomeID" type="xs:integer" use="required" />
    <xs:attribute name="SetTopBoxAddress" type="xs:integer" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="AuthenticationManager">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:OnOffEnum" use="required" />
    <xs:attribute name="Protocol" type="ws:AuthenticationManagerProtocol" />
  </xs:complexType>
</xs:element>

<xs:element name="D5Interface">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:EnabledDisabledEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="IngestSteering">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:OnOffEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="ServiceGroupSteering">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:OnOffEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="HealthMonitoring">
  <xs:complexType>
    <xs:attribute name="Support" type="ws:OnOffEnum" use="required" />
  </xs:complexType>
</xs:element>

<xs:element name="ASMSetupConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:DeployedCServerVersion" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:StreamFailoverSupport" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:RoleFailoverOnDBConnectivityLoss" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:FailoverOnBMSConnectivityLoss" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:StreamSteering" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:DeploymentNetworkConfig" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:NICBonding" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:InstallationType" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ASMSetupConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ASMSetupConfig" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Maintain / Software / Configuration Generator -->
<xs:element name="ConfigurationGeneratorConfig">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ConfigurationGeneratorConfig" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:complexType name="ws:ConfigurationGeneratorConfig">
  <xs:attribute name="StreamDomainName" type="ws:NotNullString" use="required" />
  <xs:attribute name="StreamManagerIP" type="ws:IsValidIP" use="required" />
  <xs:attribute name="StreamGroupIDStart" type="ws:ValidStreamGroupIDStart" use="required" />
  <xs:attribute name="StreamGroupIDEnd" type="ws:ValidStreamGroupIDEnd" use="required" />
  <xs:attribute name="ServerIDStart" type="ws:ValidServerIDStart" use="required" />
  <xs:attribute name="ServerIDEnd" type="ws:ValidServerIDEnd" use="required" />
  <xs:attribute name="SetupIDStart" type="ws:ValidSetupIDStart" use="required" />
  <xs:attribute name="SetupIDEnd" type="ws:ValidSetupIDEnd" use="required" />
</xs:complexType>

<xs:element name="ConfigurationGeneratorConfigList">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ConfigurationGeneratorConfig" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Start of Bulk Maintain Configuration Elements-->
<xs:element name="MaintainConfiguration">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="ws:ASMSetupConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:SystemConfigs" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:SystemThresholds" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:ConfigurationGeneratorConfigList" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:IDManagementConfigs" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:ApplicationConfigurations" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:DatabaseConfigs" minOccurs="0" maxOccurs="1" />
      <xs:element ref="ws:StreamMonitorListenerConfigs" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- End of Bulk Maintain Configuration Elements-->
<xs:simpleType name="NotNullString">
  <xs:restriction base="xs:string">
    <xs:minLength value="1" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidStreamGroupIDStart">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="10001" />  
    <xs:pattern value="([1-9]{1,2})?0-9{3}1" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidStreamGroupIDEnd">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="20000" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="ValidServerIDStart">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1001"/>
    <xs:pattern value="((\[1-9\]?[0-9]*)\(00|25|50|75\)1)"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidServerIDEnd">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1250"/>
    <xs:pattern value="((\[1-9\]?[0-9]*)\(00|25|50|75\)0)"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidSetupIDStart">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="255"/>
    <xs:pattern value="((1|3|5|7|9){1})|((1[0-9]?1|3|5|7|9){1})|((2[0-4]?1|3|5|7|9){1})|((51|3|5){1})"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidSetupIDEnd">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="2"/>
    <xs:maxInclusive value="254"/>
    <xs:pattern value="((2|4|6|8){1})|((1[0-9]?0|2|4|6|8){1})|((2[0-4]?0|2|4|6|8){1})|((50|2|4){1})"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ApplicationEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Barker"/>
    <xs:enumeration value="Playout"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="DeliveryModeEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Active-Standby"/>
    <xs:enumeration value="Active-Active"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="EnableDisableEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Enabled"/>
    <xs:enumeration value="Disabled"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="YesNoEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Yes"/>
    <xs:enumeration value="No"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Vendor">
  <xs:restriction base="xs:string">
    <xs:enumeration value="ISA-OpenStream" />
    <xs:enumeration value="RTSP/FSI" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContentLimit">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="100" />
    <xs:maxInclusive value="10000" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="PBC_Config">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="8760" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidPortLoss">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="10" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidDiskLoss">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="25" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidDiskCapacityNotify">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="75" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidDiskCapacityWarning">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="85" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidFileSystemUsage">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="90" />
    <xs:maxInclusive value="100" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidAttempts">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="5" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="ValidTimeout">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1"/>
    <xs:maxInclusive value="30"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ValidServerID">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IsValidIP">
  <xs:restriction base="xs:string">
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NotNullPort">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1"/> 
    <xs:maxInclusive value="65535"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OnOffEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="On"/>
    <xs:enumeration value="Off"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="SteeringModeEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Silo"/>
    <xs:enumeration value="Multi"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NetworkConfigEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="L2"/>
    <xs:enumeration value="L3"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="RetryCountRange">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="10"/> 
    <xs:maxInclusive value="10000"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="EnabledDisabledEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Enabled"/>
    <xs:enumeration value="Disabled"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="InstallationTypeEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="ISA 4.x" />
    <xs:enumeration value="RTSP 4.x" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="DestinationTypeEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Cable" />
    <xs:enumeration value="IPTV" />
    <xs:enumeration value="Mixed" />
    <xs:enumeration value="Auto" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="DestinationTypeOptionsEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="NAT" />
    <xs:enumeration value="None" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ARPParametersEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Use Defaults" />
    <xs:enumeration value="Customize" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ARPFormatEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Request Packets" />
    <xs:enumeration value="Reply Packets" />
    <xs:enumeration value="Both" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ARPDestinationEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Source IP" />
    <xs:enumeration value="All Hosts" />
    <xs:enumeration value="Default Gateway" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ATISC2ModeEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="None" />
    <xs:enumeration value="Client" />
    <xs:enumeration value="Server" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ChunkDurationRange">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="50" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TitleWeightRange">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="50" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="WeightRange">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="25" />
    <xs:maxInclusive value="75" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TCPTimeRange">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="5" />
    <xs:maxInclusive value="14400" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TCPIntervalRange">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="5" />
    <xs:maxInclusive value="150" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TCPProbesRange">
  <xs:restriction base="xs:positiveInteger">
    <xs:minInclusive value="1" />
    <xs:maxInclusive value="20" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TransformerTypeEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="OCN" />
    <xs:enumeration value="SA Tribune" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StartDayOfYearEnum">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="1" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="RealTimeCaptureEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Real Time Capture (non-Media Scheduler)" />
    <xs:enumeration value="Real Time Capture OFF" />
    <xs:enumeration value="Real Time Capture (Media Scheduler)" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StreamingMode">
  <xs:restriction base="xs:string">
    <xs:enumeration value="ASI" />
    <xs:enumeration value="GigE" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContentStorageEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="None" />
  </xs:restriction>
</xs:simpleType>
<xs:enumeration value="Shared" />
<xs:enumeration value="Distributed" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="MinimumStreamsPerPort">
<xs:restriction base="xs:integer">
<xs:minInclusive value="0" />
<xs:maxInclusive value="10" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="SingleSessionTimeout">
<xs:restriction base="xs:positiveInteger">
<xs:minInclusive value="2" />
<xs:maxInclusive value="20" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="SessionsPerControl">
<xs:restriction base="xs:positiveInteger">
<xs:minInclusive value="10" />
<xs:maxInclusive value="2000" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="UpStreamIngestSystem">
<xs:restriction base="xs:string">
<xs:enumeration value="PMG" />
<xs:enumeration value="AMS" />
<xs:enumeration value="Generic" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="RTSPDeploymentTypeEnum">
<xs:restriction base="xs:string">
<xs:enumeration value="DSM-CC" />
<xs:enumeration value="RTSP" />
<xs:enumeration value="NGOD" />
<xs:enumeration value="IPTV" />
<xs:enumeration value="Quative" />
<xs:enumeration value="EventIS(on vpath)" />
<xs:enumeration value="EventIS(off vpath)" />
<xs:enumeration value="Cisco" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContentPropagationEnum">
<xs:restriction base="xs:string">
<xs:enumeration value="Propagated" />
<xs:enumeration value="NOT Propagated" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="AuthenticationManagerProtocol">
<xs:restriction base="xs:string">
<xs:enumeration value="Event IS" />
<xs:enumeration value="Cisco" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="CDSMRoleEnum">
<xs:restriction base="xs:string">
<xs:enumeration value="VVI and Stream Manager" />
</xs:restriction>
</xs:simpleType>
<xs:enumeration value="VVI (Vault/Cache) Manager" />
<xs:enumeration value="Stream Manager" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="CacheFillProtocolEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="CCP" />
    <xs:enumeration value="HTTP" />
  </xs:restriction>
</xs:simpleType>
</xs:schema>
Appendix B  Creating Bulk Configuration Files
BMS Communication

This appendix describes the required Business Management System (BMS) configuration settings necessary for communicating with the Cisco Videoscape Distribution Suite-TV (VDS-TV).

OpenStream/ISA

This section is not meant to replace the OpenStream installation manual. Instead, it is more of a “cheat sheet” offering a list of values that must be the same on both the OpenStream BMS and the VDS to ensure communication between them. For more information, see the Open Stream Installation Manual.

The VDS communicates with the OpenStream BMS through the OpenStream CORBA Naming and Notification Services. Table C-1 describes the IP addresses of the OpenStream CORBA Naming and Notification Services that must be configured on the VDS.

Table C-1 OpenStream IP Addresses

<table>
<thead>
<tr>
<th>Content Delivery System Parameter</th>
<th>OpenStream Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name Service IP</td>
<td>The IP address of the CORBA Naming Service used by the OpenStream BMS. Typically, this service resides on the same server as the OpenStream BMS.</td>
</tr>
<tr>
<td>Notify Service IP</td>
<td>The IP address of the CORBA Notification Service used by the OpenStream BMS. Typically, this service resides on the same server as the OpenStream BMS.</td>
</tr>
</tbody>
</table>

In addition to the IP addresses of the Naming and Notification Services, the parameters described in Table C-2 must have the same values on both the OpenStream BMS and the VDS.

Table C-2 OpenStream and Content Delivery System Parameters

<table>
<thead>
<tr>
<th>OpenStream Parameter</th>
<th>Content Delivery System Field</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name Service Port</td>
<td>Name Service Port</td>
<td>5000</td>
</tr>
<tr>
<td>Notify Service Port</td>
<td>Notify Service Port</td>
<td>5005</td>
</tr>
<tr>
<td>Notify Event Channel Factory</td>
<td>Event Channel Factory</td>
<td>DefaultEventChannelFactory</td>
</tr>
<tr>
<td>Event Channels (Root)</td>
<td>Event Channel ID</td>
<td>EventChannels</td>
</tr>
<tr>
<td>Event Channels Kind</td>
<td>Event Channel Kind</td>
<td>Context</td>
</tr>
</tbody>
</table>
Lastly, there are four other parameters that need to be considered when configuring the OpenStream BMS and the VDS. They are:

- Headend ID
- LSC Response Padding
- Sessions Poll Time
- Stream Timeout Time

These four parameters in the VDS with their default values work properly with the OpenStream BMS.

### Table C-2  OpenStream and Content Delivery System Parameters (continued)

<table>
<thead>
<tr>
<th>OpenStream Parameter</th>
<th>Content Delivery System Field</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Channel</td>
<td>Event Channel Content ID</td>
<td>ContentChannel</td>
</tr>
<tr>
<td>Event Channel Content Kind</td>
<td>Event Channel Content Kind</td>
<td>Factory</td>
</tr>
<tr>
<td>Stream Channel</td>
<td>Event Channel Stream ID</td>
<td>StreamChannel</td>
</tr>
<tr>
<td>Stream Channel Kind</td>
<td>Event Channel Stream Kind</td>
<td>Factory</td>
</tr>
<tr>
<td>Factories (Root)</td>
<td>Factories ID</td>
<td>Factories</td>
</tr>
<tr>
<td>Factories Kind</td>
<td>Factories Kind</td>
<td>Context</td>
</tr>
<tr>
<td>ContentStoreFactory:</td>
<td>Content Store Factory ID</td>
<td>ArroyoContentStoreFactory_XXXX Where XXXX is a unique number within the Content Delivery System. The Kind type of Factory is appended to the ID before registering with the CORBA Naming Service.</td>
</tr>
<tr>
<td></td>
<td>Content Store Name</td>
<td>ArroyoContentStore_XXXX Where XXXX is a unique number within the Content Delivery System. The Kind type of Factory is appended to the ID before registering with the CORBA Naming Service.</td>
</tr>
<tr>
<td>StreamService:</td>
<td>StreamSvc Master ID</td>
<td>ArroyoStreamService_XXXX Where XXXX is a unique number within the Content Delivery System. The Kind type of Factory is appended to the ID before registering with the CORBA Naming Service.</td>
</tr>
<tr>
<td>StreamingMode</td>
<td>Streaming Mode</td>
<td>The default is 1, representing that the streaming mode of the next device is Gigabit Ethernet.</td>
</tr>
</tbody>
</table>
SNMP MIB and Trap Information

This appendix describes the Simple Network Management Protocol (SNMP) traps sent by the Cisco Videoscape Distribution Suite-TV (VDS-TV).

- Overview, page D-1
- SNMP Management Objects and Traps, page D-2
- RFC Compliance, page D-6

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 4-95.

Note

We recommend configuring a VLAN for management traffic.

SNMP management features on the servers include:
- SNMPv1, SNMPv2c, and SNMPv3
- Standard MIBs

SNMP Agent

The SNMP agent of the server uses certain variables that are included in a Cisco Management Information Base (MIB) file.

The SNMP agent is controlled by the following commands:

```
# service snmpd start
# service snmpd stop
# service snmpd restart
```

The snmpd service rc script automatically configures the snmpd service to be started in Linux run-levels 5 and 6. To make any changes to this behavior, the `chkconfig` or `ntsysv` commands can be used. The following command configures snmpd to be managed by using the `chkconfig` command:
### SNMP Log

The SNMP log file, snmpd.log, is located in the `/arroyo/log` directory. All log entries use UTC for the time stamp. All VDS-TV-specific SNMP traps are logged in the snmpd.log file.

### SNMP Agent on a CDSM or VVIM

The SNMP agent on the CDSM must be manually configured, you cannot configure the SNMP settings on the CDSM by using the `Configure > Server Level > SNMP` page. Check that the snmpd.conf file on the CDSM is properly configured by logging in to the CDSM as user `root`, going to the `/usr/local/share/snmp` directory and viewing the snmpd.conf file. If the SNMP settings are not correct, manually configure them by editing the snmpd.conf file.

### SNMP Management Objects and Traps

The VDS SNMP agent and Management Information Base (MIB) file are compliant with the Internet Engineering Task Force (IETF) standards for SNMP v1, SNMP v2c, and SNMPv3. For a list of SNMP-associated Request For Comment (RFC) specifications, see the “RFC Compliance” section on page D-6.

The Cisco CDS-TV MIBs consist of the following:

- CISCO-CDS-TV-MIB.my
- CISCO-CDSTV-SERVICES-MIB.my
- CISCO-CDSTV-FSI-MIB.my
- CISCO-CDSTV-INGESTMGR-MIB.my
- CISCO-CDSTV-BWMGR-MIB.my
- CISCO-CDSTV-INGEST-TUNING-MIB.my
- CISCO-CDSTV-CS-STATS-MIB.my
- CISCO-CDSTV-AUTHMGR-MIB.my
- CISCO-CDSTV-SERVER-MIB.my
- CISCO-CDSTV-ISA-MIB.my (Only applicable to ISA environments)

The Cisco CDS-TV MIBs are available through the CDSM, and are 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 D-1 describes the traps in the CISCO-CDS-TV-MIB.

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cdstvDiskHealthUp</code></td>
<td>Previously inactive disk is now active and ready, that is, the disk has returned to the OK (0) state.</td>
</tr>
<tr>
<td><code>cdstvDiskHealthDown</code></td>
<td>Active disk is now inactive, that is, it has left the OK (0) state.</td>
</tr>
<tr>
<td><code>cdstvServiceUp</code></td>
<td>Previously stopped service is now running, that is, it has left the not running state. The <code>cdstvServiceName</code> object, which contains the name of the service, is sent with the trap.</td>
</tr>
<tr>
<td><code>cdstvServiceDown</code></td>
<td>Previously running service is now stopped, that is, it has left the running state. The <code>cdstvServiceName</code> object, which contains the name of the service, is sent with the trap.</td>
</tr>
<tr>
<td><code>cdstvDiskUsageHigh</code></td>
<td>Disk usage on the system has crossed the maximum usage threshold. The <code>cdstvDiskUsagePercent</code> object, which contains the percentage of the disk that is used, is sent with the trap.</td>
</tr>
<tr>
<td></td>
<td>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 7-15.</td>
</tr>
<tr>
<td></td>
<td>When the disk usage exceeds the threshold set for the Disk Capacity Notify field, the <code>cdstvDiskUsageHigh</code> trap is sent.</td>
</tr>
<tr>
<td><code>cdstvDiskUsageNormal</code></td>
<td>Disk usage on the system has returned to a value within the usage threshold. The <code>cdstvDiskUsagePercent</code> object, which contains the percentage of the disk that is used, is sent with the trap.</td>
</tr>
<tr>
<td><code>cdstvLinuxFSUsageHigh</code></td>
<td>Linux file system (FS) usage on the server has crossed the maximum usage threshold. The <code>cdstvLinuxFSMountPoint</code> and <code>cdstvLinuxFSUsagePercent</code> objects, which contain the mount point and the percentage used, are sent with the trap.</td>
</tr>
</tbody>
</table>
### SNMP Management Objects and Traps

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdstvLinuxFSUsageNormal</td>
<td>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>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>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>Previously abnormal system health parameter is now normal; that is, it has left the not OK state. See Table D-2 on page D-6 for the descriptions of the objects sent with this trap.</td>
</tr>
<tr>
<td>cdstvSysHealthDown</td>
<td>Previously normal system health parameter is now abnormal; that is, it has left the OK state. See Table D-2 on page D-6 for the descriptions of the objects sent with this trap.</td>
</tr>
<tr>
<td>cdstvBrokenAsset</td>
<td>Signifies that one or more assets on a Vault or ISV are broken. A trap is sent whenever the number of broken assets found changes, whether from 0 to n, n to m, or m to 0. The trap contains one object, cdstvBrokenAssets, which specifies the current number of broken assets. The broken asset information stays in memory and is not persisted in the database. <strong>Note</strong>: The cdstvBrokenAssets value is only valid if the Vault is the master Vault, which can be verified by the cdstvVaultMasterSlaveStatus object.</td>
</tr>
<tr>
<td>cdstvServerStatusSlave</td>
<td>This server is now a slave. The cdstvServerMasterSlaveStatus object is set when the server status changes to master or slave; it has two possible values: master (1) and slave (2). A value of 0 means that the status is not yet available from statsd.</td>
</tr>
<tr>
<td>cdstvServerStatusMaster</td>
<td>This server is now a master. The cdstvServerMasterSlaveStatus object is set when the server status changes to master or slave; it has two possible values: master (1) and slave (2). A value of 0 means that the status is not yet available from statsd.</td>
</tr>
<tr>
<td>cdstvSetupIpChanged</td>
<td>Setup IP address has changed (Streamer and ISV only). If Setup IP and Control IP are the same (Setup/Control IP) and both change simultaneously, both cdstvSetupIpChanged and cdstvControlIpChanged traps are sent.</td>
</tr>
<tr>
<td>cdstvControlIpChanged</td>
<td>Control IP address has changed (Streamer and ISV only). If Setup IP and Control IP are the same (Setup/Control IP) and both change simultaneously, both cdstvSetupIpChanged and cdstvControlIpChanged traps are sent.</td>
</tr>
</tbody>
</table>
Monitored Broken Assets SNMP Traps

After the statsd process is started, it waits 5 minutes (300 seconds) before collecting statistics. If a broken asset occurs within these 5 minutes, it is detected and the cdstvBrokenAsset trap is sent.

After the first cycle of collecting statistics is complete, statsd waits 60 minutes from the beginning of the previous cycle before collecting statistics again. This repeats every 60 minutes.

**Note**

If at any point mirroring is active, the statistics collection is skipped.

The time delay in receiving the cdstvBrokenAsset trap after a broken asset occurs depends on how much time is left until the next time statsd collects content statistics.

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 5-42.

For the cdstvServiceUp and cdstvServiceDown traps in the CISCO-CDSTV-SERVICES-MIB, 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 VDS 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 VDS servers and the states and thresholds are displayed on the Server Vitals page. See the “Server Vitals” section on page 5-37. 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 F-20.
Table D-2 describes the objects that are sent with the cdstvSysHealthUp and cdstvSysHealthDown traps.

### Table D-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 D-3 is a list of SNMP RFC standards.

### Table D-3 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>
</tbody>
</table>
### Table D-3  SNMP RFC Standards (continued)

<table>
<thead>
<tr>
<th>RFC Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<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>
<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>
</tbody>
</table>
Table D-3  SNMP RFC Standards (continued)

<table>
<thead>
<tr>
<th>RFC Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<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>
Using the VDS-TV Streamer Application Monitoring Tool

This appendix describes the Cisco Videoscape Distribution Suite-TV (VDS-TV) Streamer Application Monitoring Tool (AMT) that can be used to monitor the VOD Error Repair feature. For more information about VOD Error Repair, see the “VOD Error Repair” section on page 1-11.

- Overview, page E-1
- AMT Statistics, page E-3

Overview

The AMT is a browser-based tool installed on the Streamer and used to display the settings and statistics of the VOD Error Repair feature.

The Error Repair page provides a retransmission overview of the following:

- Incoming RTCP NACK requests
- Retransmission packets sent
- Verification that requested and sent repair packets match

The RTP Session page provides details on each RTP stream. You can use this information to verify that the RTP session configuration is correct.

Initializing AMT on the Streamer

AMT is installed on every Streamer as part of the Cisco VDS-TV software. There are some additional steps that are required to complete the installation of AMT.

To initialize the AMT, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Start a Telnet or SSH session to the Streamer, logging in as user root.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Run the <code>gen_cert.sh</code> script to create the SSL certificate.</td>
</tr>
</tbody>
</table>
| Step 3 | Edit the rc.local file. Uncomment the following lines:  
  
  `service httpd start`
  `service tomcat5 start` |
Overview

Logging In to AMT

AMT uses HTTP over SSL to access the browser-based GUI. Any valid Linux username and password can be used to log in to AMT. The username does not have to belong to any special group.

To log in to AMT, do the following:

**Step 1**

Using your web browser, enter the IP address or hostname of your Streamer.

For example, if the IP address of your Streamer is 192.168.0.235, you can access it by entering https://192.168.0.235 in the address or location text box of your browser program.

The username and password dialog box is displayed.

**Step 2**

Enter a Linux username and password for this Streamer and click **OK**. The AMT System Application Status page is displayed (Figure E-1).

**Figure E-1** AMT System Application Status Page

![AMT System Application Status Page](image-url)
AMT Statistics

This section provides general information about the information displayed in AMT.

Click Refresh to update the displayed data. The AMT statistical data is not updated automatically. The last refresh date and time are displayed to the right of the Refresh button.

Table E-1 describes the information displayed for each page of AMT.

<table>
<thead>
<tr>
<th>Navigation Tree and Tab</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Tabs</td>
<td></td>
</tr>
<tr>
<td>Application Status</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>- System Up Time—Length of time the Streamer has been up and running</td>
</tr>
<tr>
<td></td>
<td>- Platform—CDE model hosting the TV Streamer Content Delivery Application (CDA)</td>
</tr>
<tr>
<td></td>
<td>- VDS Version—VDS-TV software release number</td>
</tr>
<tr>
<td></td>
<td>- VOD Session Status Summary—Percentage of active and inactive RTP sessions</td>
</tr>
<tr>
<td>Hardware</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>- Processor—CPU model and speed</td>
</tr>
<tr>
<td></td>
<td>- Memory—Total Random Access Memory (RAM) installed in kilobytes (KB).</td>
</tr>
<tr>
<td>System Info</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>- Hostname—Hostname of the Streamer</td>
</tr>
<tr>
<td></td>
<td>- OS Version—Linux operating system software version</td>
</tr>
<tr>
<td></td>
<td>- NTP Server—NTP server configured for this Streamer</td>
</tr>
<tr>
<td></td>
<td>- DNS Server—DNS servers configured for this Streamer</td>
</tr>
<tr>
<td>Network</td>
<td>Lists the output of the ifconfig command.</td>
</tr>
<tr>
<td>System Status</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>- Host Uptime—Length of time the Streamer has been up and running</td>
</tr>
<tr>
<td></td>
<td>- Services—Services running on the Streamer</td>
</tr>
<tr>
<td></td>
<td>- File System Disk Space—Used and available disk space</td>
</tr>
<tr>
<td>CServer</td>
<td>CServer status.</td>
</tr>
</tbody>
</table>

Cisco VDS-TV RTSP Software Configuration Guide
### RTP Sessions

Displays the following information on VOD Sessions that can be filtered by session ID, or session destination and subnet mask:

- Status
- Session ID
- Content name
- Source IP address and port
- Destination IP address and port
- Bit rate (Kbps)
- Repair Enabled

If a filter is entered, click **Submit** to see the filtered results. If the number of VOD sessions spans several pages, click the **Prev Page** and **Next Page** to view the other pages.

### Error Repair

**Configuration**

Displays the configuration settings for this Streamer that were set on the CDSM GUI. For more information, see Chapter 4, “Configuring the VDS.”

**Statistics**

Displays the following information:

- Generic NACK Messages Received
  - Total Messages
  - Invalid Messages
- Repair RTP Packets
  - Requested
  - Sent
  - Not Sent
- Inbound and Outbound Error Repair Request Average Rate (packets per second)
  - 5 Second (interval)
  - 1 Minute (interval)
  - 5 Minute (interval)
  - 15 Minute (interval)
- Advanced—Displays Advanced Debug Statistics for Error Repair. Click **Advanced** to see these statistics.

For more information about the Error Repair statistics, see the “Viewing Error Repair Statistics” section on page E-5.

**Excess BW**

Displays histogram for Error Repair e-Factor. For more information, see the “Viewing Excess Bandwidth” section on page E-7.
Viewing Error Repair Statistics

When you click Error Repair in the navigation tree and click the Statistics tab, AMT displays the Error Repair statistics tab (see Figure E-2).

Table E-1  AMT GUI Pages (continued)

<table>
<thead>
<tr>
<th>Navigation Tree and Tab</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTCP Exporter Configuration</td>
<td>Displays configuration settings for the VQM CDA.</td>
</tr>
</tbody>
</table>
| RTCP Exporter Statistics | Displays the following information:  
  - VQM CDA configuration settings  
  - VQM CDA configuration status  
  - VQM CDA operational status  
  - RTCP Exporter Packets Exported  
  - RTCP Exporter Packets Dropped  
  - Advanced—Displays Advanced Debug Statistics for VQM. Click Advanced to see these statistics. |

Figure E-2  Error Repair Statistics Page
Table E-2 lists the information in the Error Repair Statistics page.

### Table E-2 Error Repair Statistics

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Generic NACK Messages Received</strong></td>
<td></td>
</tr>
<tr>
<td>Total Messages</td>
<td>Number of NACK messages received by this Streamer.</td>
</tr>
<tr>
<td>Invalid Messages</td>
<td>Number of invalid messages received by this Streamer. Invalid messages are received messages that, for example, cannot be parsed.</td>
</tr>
<tr>
<td><strong>Repaired RTP Packets</strong></td>
<td></td>
</tr>
<tr>
<td>Requested</td>
<td>Number of RTP packets set-tops have requested for ER from this Streamer.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of RTP packets sent by this Streamer that have succeeded in repairing an error.</td>
</tr>
<tr>
<td>Not Sent</td>
<td>Number of failed RTP packets that were not repaired by the Streamer. The Streamer may not be able to send an ER packet for several reasons, including the following:</td>
</tr>
<tr>
<td></td>
<td>• Most likely cause is that the ER requests were bursty and exceeded the ER rate-policer limit at one point.</td>
</tr>
<tr>
<td></td>
<td>• Requested RTP packets were not found in the Streamer memory cache.</td>
</tr>
<tr>
<td></td>
<td>• Streamer failed to send the RTP packets because of a socket sendto() failure.</td>
</tr>
<tr>
<td><strong>Inbound and Outbound Error Repair Average Rate (packets per second)</strong></td>
<td>5 second, 5 minute, 1 minute, 15 minute For each time period, the average number of packets per second that the Streamer has received (inbound) or sent (outbound) to set-tops to repair errors (Unicast Retransmission).</td>
</tr>
</tbody>
</table>
Viewing Excess Bandwidth

When you click **Error Repair** in the navigation tree and click the **Excess BW** tab, AMT displays the Excess BW page (see Figure E-3).

**Figure E-3 Excess BW Page**

If Error Repair is enabled and active, you can choose to display a client e-factor histogram or table by clicking the icons in the upper-right corner of the page. Use the **Select a histogram** drop-down menu to select Error Repair histograms.

An e-factor is an excess bandwidth fraction that determines the rate at which packets are sent during Error Repair. The data displayed in the histograms and tables include the following:

- E-factor count with the number of times a client e-factor has been calculated. This appears on the vertical axis in the histograms.
- E-factor distribution of the client e-factor percentages that have been used. This appears on the horizontal axis in the histograms. If the distribution is widely dispersed, there can be more than one grouping of percentages.

Move the slider below the histograms to change the way in which the histograms are displayed. The e-factor percentages cannot be negative values.
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 F-2
- CDSM or VVIM Setup, page F-3
- System Configuration, page F-20
- Database Configs, page F-22

The Engineering access level is primarily used for initializing the Cisco Videoscape Distribution Suite-TV (VDS-TV) 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 VDS. 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.

*Note*

The **Configuration File Location** field is displayed, along with the **Browse**, **Import**, and **Export** buttons. To import a 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. To export the configuration to an XML file, click **Export**.

For information on enabling the Bulk Import/Export Configuration feature, see the “**Bulk Import/Export Configuration**” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

Deployed CServer Version

This field is always set to 4.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 back office independence.

Role Failover on DB Connectivity Loss

The role failover support on DB connectivity loss is available for both the ISA and RTSP environments. On enabling the role failover support, if there is a DB connectivity loss in the primary streamer, the back-up streamer is set as the primary streamer and takes over any active stream sessions without loss of state and back-office independence. The role failover support is enabled by default.

You can also specify the number of times to re-try before confirming the DB connectivity loss. The default value is 30 and range is 10-10000.

*Note*

- On DB connectivity loss in the primary streamer, the back-up streamer is set as the primary streamer only if the back-up server is available and configured to accept the primary role.
- If the back-up server DB is down or if the AVSlauncher is down in the back-up server, the primary role is retained by the current server.
- The user can disable this support by choosing OFF.
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 for ASI streaming and Gigabit Ethernet streaming.

Deployment Network Config

Specify whether your VDS network topology is a Layer 2 or Layer 3 network.

NIC Bonding

Starting from VDS-TV Release 3.7, NIC Bonding is supported on the management interfaces. Check the Enabled checkbox to configure NIC bonding in Configure > Server Level > Interface Setup page. By default, NIC Bonding is enabled.

Installation Type

The only options are ISA 4.X and RTSP 4.X.

Stream Destination

The possible settings for Stream Destination are Cable, IPTV, Mixed, and Auto.

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.

The Mixed option for Stream Destination allows both cable and IPTV configuration. Previously, only one Stream Destination type was allowed. The Mixed option makes the QAM Gateway page and associated Headend Setup page available, along with the Stream Destination page.

In ISA environments, the Mixed option is only available for Gigabit Ethernet streaming. The Streaming Mode is set on the following configuration pages:

- VVI with Content Storage set to Shared—Shared ISA Setup page
- VDS (legacy)—Streamer BMS page
Appendix F      Engineering Access Level Pages

Cisco VDS-TV RTSP Software Configuration Guide

CDSM or VVIM Setup

- VVI with centralized management (combined VVIM and Stream Manager)—Streamer BMS page
- VVI with Content Storage set to Distributed—CDSM Setup page under VVI section

The Auto option was added for RTSP environments, where it typically is not necessary to explicitly configure QAM gateways or IPTV subnets. The Auto option removes these configuration pages from the CDSM GUI. The Auto option is not supported for ISA environments.

---

Note

The Stream Destination feature is available only for single-site steering and in ISA environments that use Gigabit Ethernet streaming as the streaming mode.

---

NAT Support

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. All session setup messages go through the back office before reaching the RTSP server, while all stream control messages go directly to the RTSP server from the set-top for IPTV networks using NAT.

The supported LSCP client protocols for the NAT Traversal feature are the Cisco (RTSP) and TTV (RTSP). The LSCP Client Protocol must be set to one of these two options on the Streamer BMS page.

---

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.

---

Asset Scale Co-Existence Support

Starting from Release 3.9, VDS-TV supports one million assets in the overall system. Choose Enabled, to maintain the asset in old and upgraded database. Choose Disabled, If all servers associated with the controller are upgraded to latest VDS-TV image that supports one million assets. By default, Asset Scale Co-Existence Support is enabled.

---

Note

Disabling asset co-existence support is an irreversible process and the assets are maintained only in the upgraded database. Disable co-existence support only after upgrading all the servers to version 3.9 or higher.

---

Bulk Import/Export Configuration

Bulk Import/Export Configuration provides a method of configuring common configuration parameters for all the servers at one time by means of an XML file, and provides export (backup) and import (restore) capabilities to the Server-Level and System-Level configuration pages. For more information, see Appendix B, “Creating Bulk Configuration Files.”
SSV Groups

When SSV Groups is enabled, Stream Groups, Vault Groups, and Cache Groups are disabled.

Note

The SSV Group optional feature is only applicable to RTSP environments and for a CDS that uses only ISVs.

If redundancy is required, you must enable Vault Groups for the Vault Redundancy Map page to be displayed. The Vault Redundancy Map page allows mapping of ISVs for mirrored content.

If low-bandwidth mapping is required, you must enable Thin Pipe Management. 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

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 drill down, 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 drill down are the following:

- Stream Play History
- Streams by Array
- Streams per STM-MAC
- Bandwidth per Service Group
- System Failures

When Trick Mode Capture is disabled, the session ID in the Stream Activity reports no longer links to the Stream Play History drill down and the **Graph Stream** button is removed from the Stream Monitor page.

Fail Ingest Tuning

The Fail Ingest Tuning setting is enabled by default and is available for the CDSM, VVI with central management, and VVIM; it is not available for the Stream Manager. When enabled, the Fail Ingest Tuning fields are displayed on the **Configure > System Level > Ingest Tuning** page and provides the ability to configure the ingest error detection settings for all Vaults in the VDS.
Vault Groups

When Vault Groups 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. Content is mirrored among as many as four Vault Groups (one Vault Group ingests the content and up to three Vault Groups mirror the content), which may be in different geographic regions. The Vault Groups feature adds the Vault Groups, Master Vault Group, and Vault Redundancy Map configuration pages to the Array Level.

Note

The maximum number of Vault Groups is 30. Prior to 3.5.2 release, the maximum number of vault groups supported is 20.

Watermarking Support

Enabling Watermarking Support is required for the Digital Watermarking feature and means that the licensing terms of the watermarking vendor has been acknowledged and accepted. For more information about this feature, see the “Digital Video Watermarking” section on page 1-9.

ARP Parameters

Choose the following parameters to configure ARP messages used in Master Failover for either Request Packets (arping -U) and/or Reply Packets (arping -A) and a Destination IP.

Choose **Use Defaults** to automatically select default values for both ARP Format as well as Destination IP. Choose **Customize** for selecting preferred values.

Manage Recorders

This feature is not activated in this release. This feature is for the nDVR feature for RTSP environments. The CDSM supports the configuration and monitoring of Cisco Recorders. To enable the **Manage Recorder** option in the CDSM, a file named “recEnable.txt” must be placed in the /arroyo/www/htdocs/initial directory. The content of the file is not read by the CDSM, its presence is merely required to enable this feature. When found, the CDSM Setup page displays the **Manage Recorders** option.

When Manage Recorders is enabled, the following new CDSM GUI pages are available:

- Configure > System Level > Shared Recorder Settings
- Configure > Server Level > Recorder Setup

The **Configure > Server Level** pages applicable to the Recorders are the following:

- Interface Setup
- Recorder Setup
- Route Table
- SNMP Agent
Future Recording Support

Starting from Release 3.9, VDS-TV supports future recording playlist elements in the SETUP request sent by the STB. Check the Enabled check box to provide support for future recording.

Duplicate QAM Detection

Starting from Release 4.4, if a new session requests the QAM used by the existing session SETUP response with error code “677 Server Setup Failed – Duplicate QAM Detection” is sent by the RTSP service to backoffice. Also an ANNOUNCE message with “Notice code 2108: Duplicate QAM Detection” is sent to the existing session. By default, duplicate QAM detection is enabled for NGOD deployment.

Note

This feature is applicable only for NGOD deployment.

DNS Resolution Support

Starting from VDS-TV Release 3.4, DNS Resolution support is provided on the streamers. DNS Resolution support is applicable only for ATIS C2 client Setup configuration. Check the Enabled check box to specify streamers in the sites require DNS Resolution support. By default, DNS Resolution is disabled.

Starting from VDS-TV Release 4.4, DNS resolution support is provided on the streamers in RTSP-NGOD deployments as well.

TCP Window Scaling Support

Starting from VDS-TV Release 3.9, TCP Window Scaling supported on the vaults, streamer and cache for RTSP NGOD deployment. Choose Enabled to support TCP Window Scaling on vaults/streamers and cache in RTSP NGOD deployment.

TVOD Setup

The TV On Demand (TVOD) feature enables broadcast recording of live content for a Virtual Video Infrastructure (VVI) system in an ISA environment VDS and interacting with the Ericsson OpenStream back office. When TVOD Setup is Enabled, the CallSign Setup page is displayed (Configure > System Level > CallSign Setup).

To ensure the TVOD server is running, log in to the Vault as user isa, go to the /home/isa/IntegrationTest directory, and run the ./show_calypso_services script. The TVOD Manager should be listed as running.
Thin Pipe Management

Thin Pipe Management allows you to configure low-bandwidth connections between local and remote sites. A local site consists of groups of servers in the same site, for example, all the Streamers in a Stream Group are considered part of the same site, or local site. A remote site consists of groups of servers in other Stream Groups, Cache Groups, and Vault Groups. Use the Thin Pipe Map page to configure this feature.

Ingest Resiliency

The Ingest Resiliency feature allows parallel redundant copy of the active recording. If enabled then a parallel redundant copy should be recorded. When a recording starts, there should be doing two recordings (one with #B#) for this feature. It should delete the backup copy on recording completion if the first recording is completed successfully. The backup copy will be swapped with the original if the first recording is failed. Choose either Disabled or Enabled below and click Submit at the bottom.

VOD Error Repair

The VOD Error Repair is a licensed feature and requires a software activation key to enable it. For more information about activating the VOD Error Repair, see the “Initializing the VDS and Activating the Optional Features” section on page 3-3.

The VOD Error Repair feature retransmits lost packets to improve the quality of the end-user video experience. The VOD Error Repair feature uses negative acknowledgement (NACK) retransmission methods to implement retransmission-based error repair.

The VOD Error Repair settings can be configured on the System Level, Array Level, and the Server Level. Error Repair and RTP Encapsulation can only be enabled at the System Level and Array Level.

Setting the Client Protocol to Cisco RTSP

The client must be set to Cisco RTSP.

For RTSP environments, log in as a user with Engineering access. The CDSM Setup page is displayed. In the RTSP Deployment Type section, set the Deployment Type to Cisco.

For ISA environments, on the Streamer BMS page (Configure > Array Level > Streamer BMS), in the LSCP Services section, set the LSCP Client Protocol to Cisco (RTSP), and click Submit.

For ISA environments with VVIs and Shared Content Store or Virtual Content Store, the LSCP Services section is on the Configure > Array Level > VHO ISA Settings.

Error Repair Client on set-top

VOD Error Repair feature requires that the set-top have the Cisco Visual Quality Experience Client (VQE-C) software running on it. The VQE-C is the error-repair client software, which has the following capabilities:

- Receives RTP video packets
- Detects missing packets
- Requests retransmission of missing packets
- Merges retransmitted packets with original stream
Cisco VDS-TV RTSP Software Configuration Guide

Appendix F: Engineering Access Level Pages

CDSM or VVIM Setup

- Collects statistics and counters for monitoring
- Complies with the Cisco RTSP syntax for VOD Error Repair

The VQE-C is a software development kit (SDK) that is available for download through the open-source program.

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 in an ISA environment with Shared Content Store. For more information about CCP Streamers and HTTP Streamers, see the “Caching Node Workflow” section on page 2-12.

Note

ISA environments only support CCP, while RTSP environments support both CCP and 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.

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
To configure a Stream Manager that uses split-domain management, set the VVI fields as follows:

- **Cache Fill Protocol**—CCP
- **VVI Options**—Enabled
- **Management System Role**—Stream Manager
- **Cache Fill Protocol**—CCP
- **VVI (Vault/Cache) Manager VVIM IP**—IP address of the VVIM
- **Stream Domain Name**—Domain name for the Stream Domain
- **Streaming Mode**—ASI or gigE (Must be set to gigE for the Content Storage feature)

### Configuring ISA Regionalization

To configure ISA Regionalization on a Stream Manager, set the CDSM Setup fields as follows:

- **Vault Group**—**Enabled**
- **Content Storage**—**Distributed**
- **VVI**—Configure with the following settings:
  - **VVI**: Enabled
  - **Management System Role**: **Stream Manager**
  - **Cache Fill Protocols**: CCP
  - **VVIM IP**: IP address of the VVIM
  - **Stream Domain Name**: name of the Stream Manager
  - **Streaming Mode**: Gige

To configure ISA Regionalization on a VVIM, set the VVIM Setup fields as follows:

- **Vault Group**—**Enabled**
- **Content Storage**—**Distributed**
- **VVI**—Configure with the following settings:
  - **VVI**: Enabled
  - **Management System Role**: **VVI (Vault/Cache) Manager**
  - **Cache Fill Protocols**: CCP

For more information on configuring ISA Regionalization, see the “ISA Regionalization Configuration Workflow” section on page 3-9.

### Configuring Virtual Content Store

To configure Virtual Content Store on a Stream Manager, set the CDSM Setup fields as follows:

- **Vault Group**—**Disabled**
- **Content Storage**—**Distributed**
- **VVI**—Configure with the following settings:
To configure Virtual Content Store on a VVIM, set the VVIM Setup fields as follows:

- **VVI: Enabled**
- **Management System Role:** Stream Manager
- **Cache Fill Protocols:** CCP
- **VVIM IP:** IP address of the VVIM
- **Stream Domain Name:** name of the Stream Manager
- **Streaming Mode:** GigE

For more information on configuring Virtual Content Store, see the “Virtual Content Store Configuration Workflow” section on page 3-10.

### Content Storage

The Content Storage feature applies to ISA environments and has the following options:

- **Shared**
- **Distributed**

---

**Note**

Content Storage is required for VVI with split-domain management in an ISA environment.

### Shared

The Shared Content Storage, also known as Shared Content Store (SCS) 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 back office (VBO). When SCS is enabled, the Shared ISA Setup page is added to the Configure > System Level pages in the VVIM, and the VHO ISA Setup page is added to the Configure > Array Level in the CDSM. The Shared ISA Setup page has all the Content Store information configured on the Vaults that is shared with all the VBOs. The VHO ISA Setup page has the Stream Services information for similar groups of Stream Groups in the same VHO.

### Distributed

The Distributed Content Storage option allows for two configurations:

- **ISA Regionalization**—Allows the use of a centralized storage facility containing both Vaults and Caching Nodes in a Virtual Video Infrastructure (VVI), while maintaining a localized or remote VDS at each Headend. For more information, see the “ISA Regionalization” section on page 2-16.
  ISA Regionalization requires that Vault Groups be enabled on the Stream Manager CDSM.
• Vault Virtualization—Replaces the SCS with the Virtual Content Store (VCS). No content is ingested at the local VHO. All ingests and deletions of content occur at the central location, and both ingests and deletions are initiated by the local BMS at each local VHO, just as they were in the SCS. However, the VHOs do not need to communicate with the super headend (SHE) as they did with the SCS feature. With VCS, communication of ingestions and deletions is handled by the Ingest Driver client residing on the master Streamer in each VHO and the Ingest Driver server residing on the master Vault in the SHE. Vault Virtualization requires that Vault Groups be disabled on the Stream Manager CDSM. For more information, see the “Virtual Content Store” section on page 2-20.

**VVI**

When **Distributed** is selected as the Content Storage type, Streaming Mode (ASI or Gige) option is added under VVI. Streaming Mode must be set to **Gige** for the Content Storage feature, whether Shared or Distributed is selected. For Shared, the streaming mode is configured on the VHO ISA Setup page. For Distributed, the streaming mode is selected on the CDSM Setup page.

**Change Notifications**

When VVIM or Stream Manager is the role for a Distributed Content Storage, then the **Change Notification** option is available. When Change Notifications is enabled, notifications are sent and received between the Stream Manager and the VVIM when changes are made to the Vault Groups and Cache Groups.

**Remote Setup and Control Service Support**

The Remote Setup and Control Server Support feature allows the Setup and Control servers of the Streamers to be placed in a different location than the Play servers of the Streamers. All control traffic (setup and control) goes to one Streamer (Setup and Control server), and all video data traffic is served from the Streamers designated as the Play servers.

As part of this feature, there is never just one stream transmitted on a single Ethernet interface. There is always at least two active streams transmitted on an interface. For more information, see the “Remote Setup and Control Server” section on page 2-10.

**Note**

The Remote Setup and Control Server Support feature is supported on a Virtual Video Infrastructure (VVI) with split-domain management in an ISA environment and Content Storage configured as either Shared or Distributed.

The VOD Error Repair feature is not supported with the Remote Setup and Control Server Support feature.

Table F-1 describes the Remote Setup and Control Service Support fields. Configure the settings as appropriate.
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 VDS 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.

The Media Scheduler has the option to set the Importer/Transformer Type to either OCN or SA Tribune. This setting is determined by your deployment.

The Start Day of Year for Asset ID Generation is either 0 or 1. The setting is determined by what Cisco VDS-TV software release you initially started using Media Scheduler in. In Release 2.1 and earlier releases, the Asset ID starts with 0 per design. In Release 2.2 and later releases, the Asset ID starts with 1 per design.

### Table F-1 Remote Setup and Control Service Support Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Source IP</td>
<td>IP address used by the Streamers acting as the Play servers for transmitting streams. The Global Source Address is defined on all Streamers (Setup, Control, and Play), is hosted on the primary Setup server, and is managed in a fault-tolerant manner.</td>
</tr>
<tr>
<td>Global Source Port</td>
<td>Port number used in conjunction with the Global Source IP address for transmitting stream data. The default is 4000.</td>
</tr>
<tr>
<td>Minimum Streams Per Port</td>
<td>Minimum number of streams allowed on each stream interface on the Streamer Play servers. The default is 0. The range is from 0 to 10.</td>
</tr>
<tr>
<td>Single Session Timeout</td>
<td>Amount of time, in seconds, the first play request can be held on a Play server waiting for a second play request. If the timeout is reached, the first play session fails and the stream request is sent back to the Control server for relocation. The default is 10. The range is from 2 to 20.</td>
</tr>
<tr>
<td>Sessions Per Control</td>
<td>Number of sessions allowed per Control server. The default is 1000. The range is from 10 to 2000.</td>
</tr>
</tbody>
</table>

**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.

*Note* To seed the database with the HomeID field for Real-Time Capture (non-Media Scheduler), you must run the `cv-account-add-homeid0` script as user `isa` in the `/home/isa` directory on the Vault (or ISV). See your Cisco customer representative to get the `cv-account-add-homeid0` script.
Playout Processor

Note

The Playout Processor feature is supported on a Virtual Video Infrastructure (VVI) with split-domain management in an ISA environment and Content Storage configured as shared.

The Playout Processor feature supports the service running on the controller to receive the Playout history (Trick Mode Event) details from Streamer database and to place it into the controller database. If you disable this feature, the transmission of Playout history (Trick Mode Event) details from Streamer reaches Controller database with the help of AVSDB replication flow.

Playout Scheduler

Playout Scheduler is only available in an ISA environment on a VVI with central management or a legacy CDSM.

The TV Playout features incorporates the TV Playout functionality from a previous release and adds enhancements to these features. The TV Playout feature includes Public, Education, and Government (PEG) channels and Barker Streams. PEG channels differ from traditional broadcast channels in that the service provider itself must ingest and stream the content rather than receiving and forwarding a satellite feed.

The Playout Scheduler has the following options

- Playout Scheduler—On/Off
- Localized EPG Extension—On/Off

For information on the configuration workflow of the Playout Scheduler and the associated CDSM GUI pages, see the “TV Playout Configuration Workflow” section on page 3-11.

Localized EPG Extensions

To enable Localized EPG Extensions, the Playout Scheduler must be enabled.

Localized EPG Extensions adds the **Configure > Array Level > EPG Exporter** page. The EPG Exporter allows you to create an XML file that contains information from the Playout Scheduler for viewing, saving, and importing into a system to create program listings.

When content is selected for ingest on the **Configure > Array Level > Manual Ingest** page, there are two additional fields for Localized EPG Extensions:

- Localized Name
- Localized Description

The **Monitor > System Level > Completed Ingest** page displays the Localized Name and Localized Description fields and allows them to be edited.

The **Configure > Array Level > Barker/Stream Playlist** displays the Localized Name in the content selection field.

The **Configure > Array Level > Playout Scheduler** displays the original ingest name of the content object, not the Localized Name.
**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 VDS 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)
- Cisco

The deployment configuration differs depending on the type of headend.

**Bitrate Parameters Support**

As per NGOD IO3 specification, the back office requests the VDS vault to issue/response A3 message TransferStatus and GetTransferStatus that supports bitrate parameters avgBitRate and maxBitRate. To enable this feature in Cisco VDS-TV 3.5 release, do the following:

- For all vaults, open the /home/issa/bss/etc/fsi.conf file.
- Set PureIO3 = 1 to enable NGOD IO3 flag
- Restart FSI service.

**Disabling Mandatory A3 Interface Header Check**

Starting from Release 3.9, If A3 interface request headers sent from back-office to VDS-TV FSI servers does not contain the mandatory header "content-type: text/xml", the request is rejected by the FSI service and “Bad Request” response is sent to the back-office

To support the back-office systems that has not implemented this mandatory header check, do the following:

- For all vaults, open the /home/issa/bss/etc/fsi.conf file.
- Set FSI_A3_HEADER_CHECK_RELAX=1
- Restart FSI service.
Support for teardown after session inactivity

In Cisco VDS-TV 3.5 Release, RTSP server will teardown a session when the period of inactivity is MAX_ATTEMPTS_FOR_TEARDOWN_ANNOUNCE_TO_BO multiplied by session inactivity timeout (GUI configured data) seconds. For example, if session inactivity timeout is 5 seconds and MAX_ATTEMPTS_FOR_TEARDOWN_ANNOUNCE_TO_BO is 5 the RTSP server will teardown a session after a 25 sec period of inactivity. To enable this feature, do the following:

- For all streamers, open the /home/isa/bss/etc/rtsp.conf file.
- Set MAX_ATTEMPTS_FOR_TEARDOWN_ANNOUNCE_TO_BO = <x>
- Restart rtsp service in the Primary streamer.

Configuring Hung Stream Timeout

Streams which are not responded for more than configured timeout values are declared as hung streams. When Hung streams are identified, either Announce 4400 or error code 503 Service unavailable errors is sent.

Timeout interval for hung streams can be configured in rtsp.conf file. The default value is 5 seconds. To set timeout interval do the following:

- Add a line RTSP_CALLBACK_TIMEOUT_DELAY_MILLSECS=5000 in /home/isa/bss/etc/rtsp.conf file.
- Restart RTSP service.

Configuring Transaction Delay Debug Statements

**FSI-DB and FSI-CSERVER Transaction Threshold**

The time taken for FSI-DB and FSI-CServer transaction is measured in the code. If the transaction time is more than the threshold then the logs with took message appears. The default value is 2 seconds. This threshold value is configurable in the fsi.conf.

To set timeout interval do the following:

- Add a line FSITransacTimeMs=2000 in /home/isa/bss/etc/fsi.conf file for FSI-DB threshold.
- Add a line CSERVER_TRANSACTION_THRESHOLD_MILLSECS=2000 in /home/isa/bss/etc/fsi.conf file for FSI-CSERVER threshold.
- Restart FSI service.

**RTSP-DB and RTSP-CSERVER Transaction Threshold**

The time taken for RTSP-DB and RTSP-CServer transaction is measured in the code. If the transaction time is more than the threshold then the logs with took message appears. The default value is 2 seconds. This threshold value is configurable in the rtsp.conf.

To set timeout interval do the following:

- Add a line RTSP_DB_TRANSACTION_THRESHOLD_MILLSECS=2000 in /home/isa/bss/etc/rtsp.conf file for RTSP-DB threshold.
- Add a line CSERVER_TRANSACTION_THRESHOLD_MILLSECS=2000 in /home/isa/bss/etc/rtsp.conf file for RTSP-CSERVER threshold.
• Restart RTSP service.

Configuring the enabling/disabling of ANNEX TABLE, STREAM TRICK REPORT TABLE, SESSION TABLE, MSA TABLE, PRINT CONTAINER SIZE

New flags are introduced in rtsp.conf which has the capability of enabling and disabling the ANNEX TABLE, STREAM TRICK REPORT TABLE, SESSION TABLE, MSA TABLE at run time. Another flag is introduced which has the capability of enabling/disabling the printing of important statistics in RTSP service.

This settings can be done at run time and takes around 60 secs to get reflected.

To enable the prints and the tables edit the /home/isa/bss/etc/rtsp.conf and add or modify the following lines:

```
PRINT_CONTAINER_SIZE=1
DISABLE_RTSP_ANNEX_TABLE=0
DISABLE_TRICK_REPORT_TABLE=0
DISABLE_RTSP_SESSION_TABLE=0
DISABLE_MSA_EVENT_TABLE=0
```

To disable the prints and the tables edit the /home/isa/bss/etc/rtsp.conf and add or modify the following lines:

```
PRINT_CONTAINER_SIZE=0
DISABLE_RTSP_ANNEX_TABLE=1
DISABLE_TRICK_REPORT_TABLE=1
DISABLE_RTSP_SESSION_TABLE=1
DISABLE_MSA_EVENT_TABLE=1
```

Content Propagation

The Content Propagation setting determines whether content information is propagated to the Streamers or not. This setting is applicable only to RTSP environments.

When the RTSP Deployment Type is set to NGOD, set the Content Propagation to Not Propagated. This setting allows content information to be stored on the Caching Nodes in VVI RTSP NGOD deployments. The Streamers check their local database for a record of the content. If the content is not found, the Caching Nodes are queried for the content record.

For all other RTSP Deployment Types, set the Content Propagation to Propagated. This allows content information to be stored on the Streamers.

Third Party CDN Support

Third Party CDN Support feature enables filling from both third party CDN (Split Domain) and within our CDN (Single Domain). Choose either Disable or Enable and click Submit.

This feature is applicable only to RTSP environments.

VDS-TV streamers are enabled to stream content sourced from third party vendors or from Cisco CDN located in a different region/province.
When Third Party CDN Support is enabled, CDN Group Locator page and Stream to CDN Group Map page under Configure > Array Level are available for configuration of third party CDNs.

### Volume Name Based Support

Volume Name Based Support feature enables cache filling from CDNs based on the Volume name. Choose either Disable or Enable and click Submit. This feature is applicable only to RTSP environments.

VDS streamers are enabled to locate/fetch content based on the volume name specified in the RTSP/HTTP request. The volume name specified in the RTSP request enables to identify C2 Locate Port IP for Cisco CDN Caching node as well as third party CDN.

### Content Swap Support

Starting from Cisco VDS-TV Release 3.5, VDS streamers are enabled to swap playing of different contents in a session. The PAID (Content ID) that the subscriber wants to swap will be contained in the NGOD C1 request from set-top to the streamer. The extension defined by Cisco for passing the PAID (Content ID) is as follows:

```
PLAY rtsp://10.78.156.168:5553/CNTSWP/Provider::contentOne.mpg RTSP/1.0
```

**Note** Provider::contentOne.mpg is an example of a Content ID. CNTSWP is a unique identifier that distinguishes the content swap URL.

### Authentication Manager

The Authentication Manager is an optional feature and is only for specific RTSP environments (EventIS). The Authentication Manager communicates with the back office to validate a request received from a set-top before setting up a session.

The Protocol options are for selecting the RTSP deployment type for the Authentication Manager. Cisco is used for the Cisco RTSP deployment and EventIS is used for the EventIS RTSP deployment.

### D5 Support

This feature is applicable only to RTSP environments. When D5 Support is enabled in Maintain > Software > CDSM Setup page, D5 Interface page under Configure > Array Level is available for configuring the stream group settings. D5 interface is supported between VDS streaming server and ODRM. This HTTP over XML based interface is used by streaming server to notify the ODRM of streaming server configuration and streaming statistics/current resource usage. It is also used by ODRM to query the streaming server status and current resource usage.
Ingest Steering

The Ingest Steering feature works with the Vault Groups feature. When Ingest Steering is enabled (along with Vault Groups), the Ingest Steering configuration page displays at the Array Level. The Vault Group Setup page offers the ability to assign Vaults to a Vault Group. The Ingest Steering page offers the ability to map the product ID of the content to a Vault Group that ingests the content.

Note
Changes to the Ingest Steering configuration do not take effect immediately.
- If there is ingest activity, wait two hours for FSI to reload the new configuration.
- If there is no ingest activity, restarting the FSI process on the master Vault could make the changes take effect immediately.

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 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 of the server, as well as thresholds, for monitored system components. 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 Configuration

To access the CDSM or VVIM System Configuration page, choose Maintain > Software > System Configs. The System Configs page contains critical VDS parameters that are set at the time of the initial installation of the VDS. Generally, the default settings are appropriate for all environments.

Caution
If these parameters are changed after the VDS is in service, your VDS may not function properly.

Note
If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”
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

Specifies that the License Map is set to 0 and no further configuration of this parameter is required.

Control IP Map

Specifies that the Control IP Map is set to 1 and no further configuration of this parameter is required.

Popularity Based Caching

In most cases, the default setting (12 hours) of the Popularity Half Life field is sufficient, but in cases where a significant fraction of viewed content has a “flash” popularity pattern shorter than the popularity half-life value, changing the setting may result in a better cache-hit rate overall.

Content Listing Configuration

Starting from Release 4.4, VDS-TV allows you to specify the number of content items to be listed in the Content drop-down list. The default value is 100 and the range is from 100-10000.

AIM Configuration

After enabling the Ingest manager option under the VVIM Setup page, the user can set the default settings for the Ingest Manager by clicking on set defaults button. The user can then proceed to Configure > System Level > Ingest Manager page to do the remaining configuration.

Add New Server

Should you experience problems adding a new server into the VDS, and you have tried the solutions covered in the “CDSM GUI Does Not Register the Vaults and Streamers” section on page A-27, you can use the Add New Server section.
Database Configs

To access the CDSM or VVIM Database Configuration page, choose Maintain > Software > Database Configs. The Database Configs page enables the administrator to enable/disable a set of report monitoring tables. By default, all the reports are enabled.

If Bulk Import/Export Configuration is enabled, the Configuration File Location field is displayed, along with the Browse, Import, and Export buttons. To import a 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. To export the configuration to an XML file, click Export.

For information on enabling the Bulk Import/Export Configuration feature, see the “Bulk Import/Export Configuration” section on page F-5. For information about creating a Bulk Import/Export Configuration file see Appendix B, “Creating Bulk Configuration Files.”

Exercise caution while disabling reports because these reports can be used for billing purposes.

Table F-2 lists the report monitoring tables that can be enabled/disabled by the administrator.

<table>
<thead>
<tr>
<th>Database Table Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision Multiple 3</td>
<td>This table is populated with streaming data and is applicable for ISA with regionalization and RTSP deployments. By choosing Disabled, the user cannot do the following:</td>
</tr>
<tr>
<td></td>
<td>• Differentiate between a single stream session and a playlist via GUI in Stream Playlist History Report available in Report &gt; System Level &gt; Stream Activity page</td>
</tr>
<tr>
<td></td>
<td>• View detailed playlist information in StreamListHistory Everstream API.</td>
</tr>
<tr>
<td>Provision Multiple 2</td>
<td>This table is populated with streaming data and is applicable for ISA with regionalization and RTSP deployments. By choosing Disabled, the user cannot do the following:</td>
</tr>
<tr>
<td></td>
<td>• Differentiate between a single stream session and a playlist via GUI in Stream Playlist History Report available in Report &gt; System Level &gt; Stream Activity page</td>
</tr>
<tr>
<td></td>
<td>• View detailed playlist information in StreamListHistory Everstream API.</td>
</tr>
<tr>
<td>Content Object</td>
<td>This table is populated with ingestion data and is applicable for ISA and RTSP deployments. This table is not used for any GUI reporting.</td>
</tr>
</tbody>
</table>
### Table F-2 Report Monitoring Tables

<table>
<thead>
<tr>
<th>Database Table Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Content Object 3    | This table is populated with ingestion data and is applicable for RTSP deployment. By choosing **Disabled**, the user cannot do the following:  
  - Generate the Content Popularity Report available in **Report > System Level > Stream Activity** page for the duration the report table was disabled.  
  - Generate the Playout History Report available in **Report > System Level > Stream Activity**.  
  - View the deleted content information in SteamListHistory API. |
| Content Object 4    | This table is populated with ingestion data and is applicable for ISA deployment. By choosing **Disabled**, the user cannot do the following:  
  - Generate the Content Popularity Report available in **Report > System Level > Stream Activity** page for the duration the report table was disabled.  
  - Generate the Playout History Report available in **Report > System Level > Stream Activity**.  
  - View the deleted content information in SteamListHistory API. |
| Package Retry       | Obsolete    |
| Cache Stats         | This table is populated with streaming data and is applicable for ISA and RTSP deployments. By choosing **Disabled**, the user cannot do the following:  
  - View the data in Cache Fill/Bandwidth Report available in **Report > System Level > Stream Activity** page. |
| CV Recording        | This table is populated with live recording data and is applicable for RTSP deployment. This table is not used for any GUI reporting. |
| Purchase Recording  | Obsolete    |
| Stream Report       | This table is populated with streaming data and is applicable for ISA and RTSP deployments. This table is not used for any GUI reporting. |
| Stream Report by Group | This table is populated with streaming data and is applicable for ISA and RTSP deployments. This table is not used for any GUI reporting. |
### Database Table Name | Description |
--- | --- |
Stream Report by Server | This table is populated with streaming data and is applicable for ISA and RTSP deployments. This table is not used for any GUI reporting. |
Stream Trick 15 | Obsolete |
Stream Trick | Obsolete |
Barker | This table is populated with streaming data and is applicable for deployments where barker is supported. By choosing disabled the user cannot view the barker data in the following GUI pages:  
- Barker Monitor  
- Barker Setup  
- Playout Scheduler  
- Playout Exporter  
- Output Channels  
- Barker Stream/Playlists |
CDDM Management Utility

This appendix describes the management utility for Cisco Videoscape Distribution Suite-TV (VDS-TV) Content Delivery Devices.

- Utility Name, page G-1
- Synopsis, page G-1
- Description, page G-1
- Options, page G-2
- Return Codes, page G-4
- Examples, page G-5

Utility Name

cddm - Content Delivery Device Management

Synopsis

cddm [options]
cddm [devnum]
cddm [options] [devnum]

Description

cddm is a management utility for CDS-TV’s Content Delivery Devices (CDD). It’s used to report a variety of device information and manage device configuration and events such as device failure and device replacement.

For options that require a device number, devnum can be set to any one value 1..n where n is equal to the number of storage devices. devnum may define a set of device numbers, for example,’1,3,5,7’. It may indicate a range of device numbers, for example,’13-24’ (the second device number in the range must be greater than the first device number) and it may define sets of ranges, for example,’1-8,16-24’ devnum may also be the word ‘all’ to indicate that options is to be applied to all devices. Note that only some options support multiple devices. Options that support multiple devices are indicated by an asterisk following the devnum in the option prototype.
Option **--show=** **state** is the default option when **options** is not defined.

**Options**

**-a <attribute>, --attrib=<attribute><devnum>**

Report the value of the specified attribute. If **devnum** is provided then **attribute** must be an attribute of the device. If **devnum** is not provided then **attribute** is considered a global attribute. For example **cddm --attributive 1**’ will return the name of the device vendor of device 1 and **cddm --attrib=max_error_rate** will report the global value for the maximum error rate health threshold applicable to all devices. See the **--show** option for sets of available attributes.

**-C <onoff>,--slot_check=<onoff>**

This option is used to check the proper connection of device cables and the working order of device lights. It will cause the identify light (red LED) of the devices to illuminate in a Johnson Counter fashion; starting with the first slot and progressing to the last slot in \(^{1/2}\) second steps. After all lights are on then all lights will be turned off in the same order. This behavior will repeat until this option is turned off.

**-F, --no-format**

This option is used to remove the default output formatting performed by other options. Only options subsequent to this option on the command line are effected.

**-I, --interrogate devnum**

Creates a report of events for the specified device. The source of the report may come from a variety of sources that will be identified in the report.

**-i [on|off], --identification [devnum]**

Turns on or off the specified device’s identifying indicator. For **identify**, if **on** or **off** is not specified then this option will toggle the state. The identifying indicator is typically a slow blinking red light (\(^{1}\) seconds period) found at the front of the slot associated with the device. The identifying indicator will remain on until it is turned off or the device fails at which time the indicator will be lit solidly.

**-r devnum, --remove devnum**

*Logically* removes the specified device prior to the device being **physically** removed from the chassis. A logically removed device will be dismounted from the file system and either spun-down or placed on standby (HDD or SSD, respectively).

When the device has completed the logical remove process, a notification will be posted on the console indicating that the device can be pulled. A logically-removed device’s red identifying indicator will be displaying a fast blink (\(^{1/2}\) second period or faster).

It is always best to logically remove a device before pulling it from the chassis. A failed device does not need to be logically removed.

**Note**  A logically removed device cannot be place back online until it has been removed from the chassis. **All contents of a logically removed device will be deleted** when it is reinserted into the chassis.

**-s value, --show=<set,set,...> <devnum>**

This is used to show selected sets of global or device information.

**Note**  Sets that require a devnum cannot be mixed with sets that do not require a devnum.
The collection of some device information has a negative impact on device performance, therefore, this impactive information is cached and automatically updated periodically usually when the device is idle. 

set selects one of the different categories of information defined as follows:

**all devnum**

Show all available device information.

**dev_spec**

Show device type specific information. This will report various points of information specific to the device technology and is a function of vendor implementation.

**errors devnum**

Shows all error counters.

**health devnum**

Shows information relative to a device’s health

**phys devnum**

Show physical information about the device; make, model, vendor, capacity, serial number, etc.

**raw**

This sub option will cause some information sets to be reported in raw data format. For example, this option will cause the SATA S.M.A.R.T. attributes reported in the **dev_spec** set to be reported as it’s collected from the device as opposed to interpreting it.

**smart devnum**

Shows available Self-Monitoring, Analysis and Reporting Technology values. These values are technology specific (SCSI, ATA) and implementation is varied from vendor to vendor.

**state devnum**

Show device state information only.

**stats devnum**

Show device statistical information

**update**

This sub option is not an information set, but instead, will force a refresh of the device information cache possibly momentarily impacting device performance.

**globals**

Show global settings used to monitor devices

**location devnum**

Show the location of a given device within a chassis

**-V --versions**

Reports the version of cddm and CDD drivers information.

**-v, --version**

Reports the version of cddm.

**--VIOLATE_POLICY**

This option is used to disable policy enforced by cddm. It is not recommended that this option be utilized except in extraneous cases. This option must precede other options on the command line for which policy is to violated.
**-X, --unsuspend devnum**

This option will unsuspend a not-yet-pulled suspended device. (See the `suspend` option.)

**-x [minutes], --suspend[=minutes] devnum**

The `suspend` option prepares a healthy device to be safely removed from the chassis and allowing it to be reinserted later without incurring data loss.

The CDE470 platform has two devices in each tray. When one device in a tray has failed the other device in the tray will need to be suspended before the tray is pulled from the chassis.

The volume on the suspended device is not dismounted from the file system but placed in a quiescent state. The file system will not attempt to access the volume during the suspend period. While a device is suspended, necessary data residing on the device will be reconstructed from data on other devices.

A device cannot remain suspended indefinitely due to a potential performance impact to the system. The default amount of time that a device may remain suspended is 20 minutes. A suspended and removed device that is reinserted before the suspend period expires will automatically and immediately be placed online and its volume returned to full operation.

If the suspend period expires before the device is reinserted then the device will be considered lost and its volume will be abandoned by the file system. A suspended device reinserted after the suspend period expires will be considered a new device and its current contents will be discarded. If, by happenstance, a suspended and removed device is replaced with another device then the suspended volume will be discarded by the file system and the replacement device will be considered new and its current contents discarded.

If a suspended device is not pulled from the chassis then it will return to online and normal operation when the suspend period expires. A suspended but not yet removed device can be unsuspended with the `unsuspend` option.

The `minutes` parameter may be provided to override the default suspend period. The `suspend` option with the `minute` parameter may be used on a device already suspended to modify the current suspend period.

---

**Note**

To preserve data resilience, cddm will enforce a policy of only one device suspended at a time. This option is valid for the CDE470 platform only.

---

### Return Codes

cddm will return 0 if the command is successful and non-zero if unsuccessful. A negative return value indicates a system failure. A positive is an error generated within `cddm` and defines as follows:

- 101 Invalid device
- 102 Invalid option
- 103 Invalid value
- 104 CDD drivers are not loaded
- 105 Incompatible drivers
- 106 Device not found
- 107 Policy violation
- 108 Unsupported option
Examples

```bash
cddm --show=all,dev_spec,smart 3
```

Produces the following output and indicates all available attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>alleged_media_errors</td>
<td>0</td>
</tr>
<tr>
<td>bytes_read</td>
<td>110080</td>
</tr>
<tr>
<td>bytes_written</td>
<td>4775341056</td>
</tr>
<tr>
<td>connection</td>
<td>21.2</td>
</tr>
<tr>
<td>device_type</td>
<td>SAS HDD</td>
</tr>
<tr>
<td>dev_link_rate</td>
<td>6000</td>
</tr>
<tr>
<td>dev_max_operating_temp</td>
<td>69</td>
</tr>
<tr>
<td>dev_max_operational_starts</td>
<td>0</td>
</tr>
<tr>
<td>dev_mfg_wk</td>
<td></td>
</tr>
<tr>
<td>dev_mfg_yr</td>
<td></td>
</tr>
<tr>
<td>dev_temp</td>
<td>23</td>
</tr>
<tr>
<td>direct_submits</td>
<td>20766</td>
</tr>
<tr>
<td>dubious_LBAs</td>
<td>0</td>
</tr>
<tr>
<td>errors</td>
<td>0</td>
</tr>
<tr>
<td>errors_reported</td>
<td>0</td>
</tr>
<tr>
<td>errors_reported_rate</td>
<td>0</td>
</tr>
<tr>
<td>errors_to_reset</td>
<td>0</td>
</tr>
<tr>
<td>eval_wait_time</td>
<td>0 ms</td>
</tr>
<tr>
<td>hard_resets</td>
<td>0</td>
</tr>
<tr>
<td>location</td>
<td>1.3.1.0</td>
</tr>
<tr>
<td>max_transfersize</td>
<td>262144</td>
</tr>
<tr>
<td>media_error_rate</td>
<td>0</td>
</tr>
<tr>
<td>media_errors</td>
<td>0</td>
</tr>
<tr>
<td>model</td>
<td>WD4001FYYG-01SL3</td>
</tr>
<tr>
<td>name</td>
<td>csd3</td>
</tr>
<tr>
<td>print_flags</td>
<td>0x0</td>
</tr>
<tr>
<td>proc_flags</td>
<td>0x20</td>
</tr>
<tr>
<td>reqs_free</td>
<td>20</td>
</tr>
<tr>
<td>reqs_in_cb_queue</td>
<td>0</td>
</tr>
<tr>
<td>reqs_in_progress</td>
<td>0</td>
</tr>
<tr>
<td>reqs_lost</td>
<td>0</td>
</tr>
<tr>
<td>reqs_queued</td>
<td>0</td>
</tr>
<tr>
<td>requests</td>
<td>468662</td>
</tr>
<tr>
<td>reset_rate</td>
<td>0</td>
</tr>
<tr>
<td>resets</td>
<td>0</td>
</tr>
<tr>
<td>retries</td>
<td>0</td>
</tr>
<tr>
<td>rev</td>
<td>VR07</td>
</tr>
<tr>
<td>sector_size</td>
<td>512</td>
</tr>
<tr>
<td>serial</td>
<td>WMC1P1989829</td>
</tr>
<tr>
<td>sick_cnt</td>
<td>0</td>
</tr>
<tr>
<td>slot</td>
<td>3</td>
</tr>
<tr>
<td>smart_age</td>
<td>00.09.45</td>
</tr>
<tr>
<td>smart_glist_count</td>
<td>0</td>
</tr>
<tr>
<td>smart_nonmedium_errors</td>
<td>3466</td>
</tr>
<tr>
<td>smart_rd_corrected_errors_long</td>
<td>1</td>
</tr>
<tr>
<td>smart_rd_corrected_errors_short</td>
<td>114490</td>
</tr>
<tr>
<td>smart_rd_correction_algorithm_use</td>
<td>1</td>
</tr>
<tr>
<td>smart_rd_retries</td>
<td>1</td>
</tr>
<tr>
<td>smart_rd_total_bytes_processed</td>
<td>47071765710848</td>
</tr>
<tr>
<td>smart_rd_total_corrected_errors</td>
<td>114491</td>
</tr>
<tr>
<td>smart_rd_uncorrected_errors</td>
<td>0</td>
</tr>
<tr>
<td>smart_startups</td>
<td>0</td>
</tr>
</tbody>
</table>
smart_status: OK
smart_wr_corrected_errors_long: 124
smart_wr_corrected_errors_short: 59641
smart_wr_correction_algorithm_use: 124
smart_wr_retries: 124
smart_wr_total_bytes_processed: 10133345524736
smart_wr_total_corrected_errors: 59765
smart_wr_uncorrected_errors: 0
state: 0x800007; DEV_ALLOCATED DEV_ATTACHED DEV_READY
timeout_comp_err: 0
timeout_comp_max: 0 ms
timeout_comp_min: 0 ms
timeout_comp_ok: 0
timeout_rate: 0
timeouts: 0
total_sectors: 7814037167
vendor: WD
smart_age: 00.09.45
smart_glist_count: 0
smart_nonmedium_errors: 3466
smart_rd_corrected_errors_long: 1
smart_rd_corrected_errors_short: 114490
smart_rd_correction_algorithm_use: 1
smart_rd_retries: 1
smart_rd_total_bytes_processed: 47071765710848
smart_rd_total_corrected_errors: 114491
smart_rd_uncorrected_errors: 0
smart_startups: 0
smart_status: OK
smart_wr_corrected_errors_long: 124
smart_wr_corrected_errors_short: 59641
smart_wr_correction_algorithm_use: 124
smart_wr_retries: 124
smart_wr_total_bytes_processed: 10133345524736
smart_wr_total_corrected_errors: 59765
smart_wr_uncorrected_errors: 0
dev_link_rate: 6000
dev_max_operating_temp: 69
dev_max_operational_starts: 0
dev_mfg_wk
dev_mfg_yr
dev_temp: 23

cddm --attrib=bytes_written 1
Will report the value of the number of byte written to the device since last system start, for example:
85269151744
cddm --supend=30 8
cddm --remove 17
cddm --identify=on 42
cddm --slot_check=on
VDS-TV Tunables

Tunables are configuration parameters for cserver which is a core component in Cisco Videoscape Distribution Suite-TV (VDS-TV).

- Debug Tunables, page H-1
- Info Tunables, page H-6
- Configuration Tunables, page H-9

**Debug Tunables**

Debug tunables are used in production environment to debug issues. Changes to these tunables affect the behaviour of the system. These tunables are Read and Write (RW) type tunables.

Table H-1 lists the Debug tunables.

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Description</th>
<th>Units/Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/internal/shutdown_adapter_index</td>
<td>Tunable to bring down adapter. Echo X is the input command line used. Eg. Echo 2 to bring down the second adapter. This affects driver code as well. This is equivalent to if down</td>
<td>index</td>
<td>1</td>
</tr>
<tr>
<td>/proc/calypso/internal/skip_resiliency_check</td>
<td>Popular contents are made available in another play streamer in the play group for resiliency. This reduces the cache working set size and thus reducing the cache efficiency. By setting this tunable, popular contents do not get duplicated to the other streamers but the cache working set size increases thus improving the cache efficiency</td>
<td>boolean</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/internal/dbg_verboosedump</td>
<td>To enable verbose level logging about the system onto the /var/log/messages</td>
<td>functionality (enable/disable)</td>
<td>0</td>
</tr>
</tbody>
</table>
### Debug Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Description</th>
<th>Units/Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/internal/disableControlNetworkAdapter</td>
<td>To simulate the loss of link state on the control adapter. Related tunable: /proc/calypso/internal/disableNetworkAdapter9</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableManagementNetworkAdapter</td>
<td>To simulate the loss of link state on the management adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter0</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter0 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter1</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter1 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter10</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter10 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter11</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter11 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter12</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter12 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter2</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter2 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter3</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter3 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter4</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter4 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter5</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter5 configured in /arroyo/test/setupfile adapter</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
</tbody>
</table>
### Table H-1 Debug Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Description</th>
<th>Units/Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter6</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter 6 configured in /arroyo/test/setupfile adapter</td>
<td>functionality(enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter7</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter 7 configured in /arroyo/test/setupfile adapter</td>
<td>functionality(enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter8</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter 8 configured in /arroyo/test/setupfile adapter</td>
<td>functionality(enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/disableNetworkAdapter9</td>
<td>To simulate the loss of link state on the configured cache fill interface adapter 9 configured in /arroyo/test/setupfile adapter</td>
<td>functionality(enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/internal/enable_dynamic_trick_read_history</td>
<td>To enable dynamic trick related locate and transfer request and response logging onto the readhistory.log.</td>
<td>functionality(enable/disable)</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/internal/enable_igate_receive_log</td>
<td>Enables/Initializes inband heartbeat mpeg ts packet at the time of play setup</td>
<td>functionality(enable/disable)</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/internal/enable_inband_heartbeat</td>
<td>Enables inband heartbeat mpeg ts packet at the time of play setup</td>
<td>functionality(enable/disable)</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/internal/enable_receive_capture</td>
<td>If the receive capture is turned on, then bad packets received will be logged into the receive.log Related tunable: /proc/calypso/internal/enable_receive_capture</td>
<td>functionality(enable/disable)</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/internal/enable_transmit_capture</td>
<td>To enable logging of the transmitted packets from the server Related tunable: /proc/calypso/internal/enable_transmit_capture</td>
<td>functionality(enable/disable)</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/internal/reset_adapter_index</td>
<td>To force execute the Adapter Reset Logic on a specified adapter index</td>
<td>functionality(enable/disable)</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table H-1  Debug Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Description</th>
<th>Units/Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/tunables/bwm_logLevel</td>
<td>To enable verbose logging on the bwm.log</td>
<td>LogLevel</td>
<td>DEBUG (DEBUG Builds), INFO (CRITICAL - 0x0001, ERROR - 0x0002, WARNING - 0x0003, INFO - 0x0004, DEBUG - 0x0005, DEBUG_V - 0x0006)</td>
</tr>
<tr>
<td>/proc/calypso/tunables/c2k_log_arp_info</td>
<td>To Log ARP packets/information onto the c2k.log</td>
<td>functionality (enable/disable)</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/c2k_loginusecs</td>
<td>To enable c2k logging in microseconds functionality</td>
<td>functionality (enable/disable)</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/c2k_verbose_dump</td>
<td>To enable verbose logging on the c2k.log</td>
<td>LogLevel</td>
<td>C2K_NOTICE_LEVEL - 5</td>
</tr>
<tr>
<td>/proc/calypso/tunables/cm_logserverinfo</td>
<td>To query the server status and enable the cm_logserverinfocommand tunable for avs_rtd to process the debug related request. Information is dumped in /arroyo/log/serverinfo.log</td>
<td>integer</td>
<td>1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/cm_logserverinfocommand</td>
<td>The avs_rtd script uses this tunable to pass run time debugger command to cserver Related tunable: /proc/calypso/tunables/cm_logserverinfocommand, /proc/calypso/tunables/cm_logserverinfogoid, /proc/calypso/tunables/cm_logserverinfogoidinfo.</td>
<td>String</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/cm_logserverinfogoid</td>
<td>Goes along with the /proc/calypso/tunables/cm_logserverinfocommand, Few values specified onto the cm_logserverinfo can take a optional param of GOID which can be specified onto this tunable</td>
<td>GOID</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/cm_logserverinfogoidinfo</td>
<td>To query the detailed status of Goid on all the Vault on the same group</td>
<td>GOID</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table H-1  Debug Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Description</th>
<th>Units/Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/tunables/debugevaluatemask</td>
<td>To enable verbose level logging for the evaluator framework related logs</td>
<td>LogLevel</td>
<td>All(DEBUG), EVAL_DBG_VERBOSE(OTHERS)</td>
</tr>
<tr>
<td>/proc/calypso/tunables/enableFillBandwidthLog</td>
<td>to enable the logging of fillbandwidth.log</td>
<td>functionality (enable/disable)</td>
<td>TRUE(DEBUG), FALSE(OTHERS)</td>
</tr>
<tr>
<td>/proc/calypso/tunables/enableFillLog</td>
<td>to enable the logging of fill.log</td>
<td>functionality (enable/disable)</td>
<td>TRUE(DEBUG), FALSE(OTHERS)</td>
</tr>
<tr>
<td>/proc/calypso/tunables/enableLostPacketLog</td>
<td>to enable the logging of lostpacket.log</td>
<td>functionality (enable/disable)</td>
<td>FALSE</td>
</tr>
<tr>
<td>/proc/calypso/tunables/enableLowPriorityStatsLog</td>
<td>to enable the lowprioritystats logging</td>
<td>functionality (enable/disable)</td>
<td>TRUE</td>
</tr>
<tr>
<td>/proc/calypso/tunables/enableReadHistoryLog</td>
<td>to enable readhistory.log</td>
<td>functionality (enable/disable)</td>
<td>TRUE(DEBUG), FALSE(OTHERS)</td>
</tr>
<tr>
<td>/proc/calypso/tunables/http_log_level</td>
<td>to enable verbose level logging on the http.log</td>
<td>LogLevel</td>
<td>LOG_INFO - 6 (range 0-7)</td>
</tr>
<tr>
<td>/proc/calypso/tunables/logsamplinginmsecs</td>
<td>Used by StatsFile Logging, Protocoltiming.log sampling</td>
<td>Seconds</td>
<td>10</td>
</tr>
<tr>
<td>/proc/calypso/tunables/msa_dumplevel</td>
<td>to enable the MSA event dump level</td>
<td>LogLevel</td>
<td>C2K_NOTICE_LEVEL</td>
</tr>
<tr>
<td>/proc/calypso/tunables/ping_with_icmp</td>
<td>to check the reachability of the destination IP by ICMP packets</td>
<td>IP</td>
<td>1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/ping_with_stun</td>
<td>to check the reachability over STUN. Performs stun handshake internally</td>
<td>IP</td>
<td>1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/stop_being_primary</td>
<td>to stop all the primary services running on the server and gracefully make backup to be the new primary</td>
<td>functionality (enable/disable)</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/streamevent_verbosedump</td>
<td>to enable the verbose logging on the streamevent.log</td>
<td>LogLevel</td>
<td>C2K_NOTICE_LEVEL</td>
</tr>
<tr>
<td>/proc/calypso/tunables/streamtrace_verbosedump</td>
<td>to enable the verbose logging on the streamtrace.log</td>
<td>LogLevel</td>
<td>LOG_WARNING</td>
</tr>
<tr>
<td>/proc/calypso/tunables/traceroute</td>
<td>To write the traceroute information into serverinfo log</td>
<td>IP</td>
<td>1</td>
</tr>
</tbody>
</table>
The Info tunables are used to get a snapshot of various parameters in the system. These tunables are Read only.

The following tunables are old and are not used:

- /proc/calypso/cm/cache2app_operational
- /proc/calypso/cm/cachehits
- /proc/calypso/cm/cachemisses
- /proc/calypso/cm/diskreadsectors
- /proc/calypso/cm/diskreadsegments
- /proc/calypso/cm/freedsegments
- /proc/calypso/cm/memoryhits
- /proc/calypso/cm/romreadsectors
- /proc/calypso/cmm/mapped/availableblocks
- /proc/calypso/cmm/mapped/totalblocks

Table H-2 lists the Info tunables.

<table>
<thead>
<tr>
<th>Tunable Name/Location</th>
<th>Description</th>
<th>Units/Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/cm/cach2app_operational</td>
<td>To check whether the cache2app services are operational or not</td>
<td>Status Value</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/cm/cachehits</td>
<td>To validate the number of objects fully present on the server</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/cm/cachemisses</td>
<td>To check the number of objects not being fully present on the server</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/cm/diskreadsectors</td>
<td>The count on the number of sectors read from the disk after starting a stream</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>Tunable name/Location</td>
<td>Description</td>
<td>Units/Type</td>
<td>Default Values</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>/proc/calypso/cm/disk/readsegments</td>
<td>To count on the number of object segments read from the disk for streaming</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/cm/free/segments</td>
<td>The total number of free object segments</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/cm/memoryhits</td>
<td>To trace the memory hits of the Object</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/cm/romreadsectors</td>
<td>Length of the object received from ROM in sectors</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/cm/mapped/availableblocks</td>
<td>The total number of memory blocks on the system</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/status/bwm_settings</td>
<td>To query the status of Bandwidth Manager and the thin pipes configured</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/diskbandwidthinfo</td>
<td>Verbose details on the disk bandwidth information</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/diskinfo</td>
<td>Verbose details of the Configured Disks on the server</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/hw_validation</td>
<td>To validate whether the Hardware configured is according to the Model of the device</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/networkbandwidth</td>
<td>Network Bandwidth related information</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/pipe_settings</td>
<td>The connected number of thin pipes</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/resiliencyinfo</td>
<td>To query the configured Service Address Information (Setup or control service, HTTP Redirector Service and Bandwidth Manager Service)</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/resiliencystatus</td>
<td>verbose level details about the configured Service Address</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/server_settings</td>
<td>To query the server configurations and other details related to the server</td>
<td>string</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/streamer/activestreamslots</td>
<td>To hold the count of streams which are currently streamed from this server</td>
<td>Count</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table H-2  Info Tunables (continued)

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Description</th>
<th>Units/Type</th>
<th>Default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/status/streamer/allocatedslots</td>
<td>“Allocated streams” is the streams that have been created. The sum of Allocated Stream from this streamer group should be close to the “alloc” field in the “LRR” line present in proto log</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/status/streamer/cutthruinfo</td>
<td>It displays the limitation on the Disk Write allowed for Object based on the PopularityBased Caching design. It gathers the information about CutThruMark which is used in cserver to determine the disk write required</td>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/status/streamer/fillinfo</td>
<td>To log the CCP Fill status</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/streamer/resiliencyinfo</td>
<td>To query the configured Service Address information (Setup or control service, HTTP Redirector Service and Bandwidth Manager Service)</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/streamer/streaminfo</td>
<td>To query the stream related information</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/syslog/last_open_error</td>
<td>Used to store the return value if a file can not be opened through syslog layer</td>
<td>int</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/status/syslog/last_write_error</td>
<td>Used to store the return value if a write to syslog fails</td>
<td>int</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/status/syslog/multiple_writes</td>
<td>Number of times a log message required multiple writes to the syslog socket. Generally we should be able to send one full message in one single write to the syslog socket</td>
<td>int</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/status/syslog/open_errors</td>
<td>Number of times system encountered errors at the time of opening a log file using syslog api</td>
<td>int</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/status/syslog/write_errors</td>
<td>Number of times log messages have failed to write to syslog layer</td>
<td>int</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/status/vault/fillinfo</td>
<td>To query the CCP Fill status on the vault</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/vault/httpinfo</td>
<td>Display the configured HTTP Adapter information</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/vault/laninfo</td>
<td>display the details of Capacity,Connections,Inbound request and outbound request</td>
<td>String</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Configuration Tunables

The Configuration tunables are used to configure the various parameters in the system. These tunables have a GUI counterpart. Table H-3 lists the Configuration tunables.

Table H-3  Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write</th>
<th>Description</th>
<th>Units/Type</th>
<th>default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/status/vault/settings</td>
<td></td>
<td>Display the vault settings like smoothing, mirroring, local copy and remote mirror copy</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/vault/streaminfo</td>
<td></td>
<td>Display the stream related information on the vault</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/cache/fillinfo</td>
<td></td>
<td>To query the CCP Fill status on the cache</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/cache/httpinfo</td>
<td></td>
<td>Display the configured HTTP Adapter information</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/status/cache/streaminfo</td>
<td></td>
<td>Display the stream related information on the cache</td>
<td>String</td>
<td>N/A</td>
</tr>
<tr>
<td>/proc/calypso/tunables/templatedebugversi</td>
<td></td>
<td>To provide the information related to the version of runtime debugger used in the system</td>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>on</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/proc/calypso/ingest_vault_max_display_count</td>
<td></td>
<td>Configured number of ingesting vault that needs to display the statistics</td>
<td>Count</td>
<td>10</td>
</tr>
</tbody>
</table>

Table H-2  Info Tunables (continued)
## Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write</th>
<th>Description</th>
<th>Units/Type</th>
<th>default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/proc/calypso/cm/active_trickspeed_5</code></td>
<td>Read</td>
<td>Tunable used to read the configured trick speed, which is configured from CDSM</td>
<td>Speed/Hex</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/cm/active_trickspeed_6</code></td>
<td>Read</td>
<td>Tunable used to read the configured trick speed, which is configured from CDSM</td>
<td>Speed/Hex</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/cm/active_trickspeed_7</code></td>
<td>Read</td>
<td>Tunable used to read the configured trick speed, which is configured from CDSM</td>
<td>Speed/Hex</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/cm/active_trickspeed_8</code></td>
<td>Read</td>
<td>Tunable used to read the configured trick speed, which is configured from CDSM</td>
<td>Speed/Hex</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/cm/active_trickspeed_9</code></td>
<td>Read</td>
<td>Tunable used to read the configured trick speed, which is configured from CDSM</td>
<td>Speed/Hex</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/cm/active_trickspeed_10</code></td>
<td>Read</td>
<td>Tunable used to read the configured trick speed, which is configured from CDSM</td>
<td>Speed/Hex</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/cm/active_trickspeed_11</code></td>
<td>Read</td>
<td>Tunable used to read the configured trick speed, which is configured from CDSM</td>
<td>Speed/Hex</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/test/arp_readroutingtable</code></td>
<td>Write</td>
<td>Tunable used to read entries from RoutingTable and update. Any change in routing table, we need to do &quot;echo 1 &gt; /proc/calypso/test/arp_readroutingtable&quot; for the new entry to take effect</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/test/readarptable</code></td>
<td>Write</td>
<td>Tunable used to read the configuration file /arrooyo/test/ArpTable entries and update. Any change in Arp table, we need to do &quot;echo 1 &gt; /proc/calypso/test/readarptable&quot; for the new entry to take effect</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td><code>/proc/calypso/test/readfillsourceconfig</code></td>
<td>Write</td>
<td>Tunable used to read the configuration file /arrooyo/test/FillSourceConfig entries and update. Any change in FillSourceConfig, we need to do &quot;echo 1 &gt; /proc/calypso/test/readfillsourceconfig&quot; for the new entry to take effect</td>
<td>bool</td>
<td>default 0</td>
</tr>
</tbody>
</table>
### Table H-3  Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write/RW type</th>
<th>Description</th>
<th>Units/Type</th>
<th>default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/test/read</td>
<td>Write</td>
<td>Tunable used to read the configuration file /arroyo/test/RecordingChannelMap entries and update. Any change in RecordingChannelMap, we need to do &quot;echo 1 &gt;/proc/calypso/test/readrecordingchann elsemap&quot; for the new entry to take effect.</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>recordingchannelmap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/proc/calypso/test/read</td>
<td>Write</td>
<td>Tunable used to read the configuration file /arroyo/test/RemoteServers entries and update. Any change in RemoteServers file, we need to do &quot;echo 1 &gt;/proc/calypso/test/readremoteservers&quot; for the new entry to take effect.</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>remoteservers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/proc/calypso/test/read</td>
<td>Write</td>
<td>Tunable used to read the configuration file /arroyo/test/StreamDestinationMap entries and update. Any change in StreamDestinationMap, we need to do &quot;echo 1 &gt;/proc/calypso/test/readstreamdestinationmap&quot; for the new entry to take effect.</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>streamdestinationmap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/proc/calypso/test/read</td>
<td>Write</td>
<td>Tunable used to read the configuration file /arroyo/test/SubnetTable entries and update. Any change in SubnetTable, we need to do &quot;echo 1 &gt;/proc/calypso/test/readsubnettable&quot; for the new entry to take effect.</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>subnettable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/proc/calypso/test/read</td>
<td>Write</td>
<td>Tunable used to read the configuration file /arroyo/test/TransportGroupIdTable entries and update. Any change in TransportGroupIdTable, we need to do &quot;echo 1 &gt;/proc/calypso/test/readsubnettable&quot; for the new entry to take effect.</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>tgidtable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/proc/calypso/test/shutdown</td>
<td>Write</td>
<td>Tunable used to shut down Cserver module processes</td>
<td>Bool</td>
<td>default 0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeed_0</td>
<td>Write</td>
<td>Tunable used to set both +ve and -ve trick speed as pair. Since this tunable does not have directional information, we can't have different +ve and -ve speed. This is older verison tunable.</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
</tbody>
</table>
### Table H-3 Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write/RW type</th>
<th>Description</th>
<th>Units/Type</th>
<th>default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/tunables/trickspeed_1</td>
<td>Write</td>
<td>Tunable used to set both +ve and -ve trick speed as pair. Since this tunable does not have directional information, we can't have different +ve and -ve speed. This is older version tunable</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeed_2</td>
<td>Write</td>
<td>Tunable used to set both +ve and -ve trick speed as pair. Since this tunable does not have directional information, we can't have different +ve and -ve speed. This is older version tunable</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_0</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_1</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_2</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_3</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_4</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_5</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_6</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_7</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_8</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_9</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_10</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/trickspeedv2_11</td>
<td>Write</td>
<td>Tunable used to set trick speed (+ve or -ve)</td>
<td>Speed/Hex</td>
<td>default -1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/stream_null_packets</td>
<td>Write</td>
<td>Tunable used to enable/disable the stream null packet logic at the remaining length. It fills the remaining length with null packets while adding the stream data in stream slot</td>
<td>bool</td>
<td>default 1</td>
</tr>
</tbody>
</table>
## Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write</th>
<th>Description</th>
<th>Units/Type</th>
<th>default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/tunables/stream_using_qam</td>
<td>Write</td>
<td>Write Tunable used to configure the setup, whether QAM or IP setup. If flag is not set then its IP setup and Motorola PreEncryption use original program number for Encryption data (Inband). If flag is set then its QAM based setup and Motorola pre Encryption refer program number and data from port (outband).</td>
<td>bool</td>
<td>default 1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/bwm_readConfFile</td>
<td>Write</td>
<td>Write Tunable used to read the configuration file /arroyo/test/BandwidthManager entries and update. Any change in Bandwidth manager configuration, we need to do &quot;echo 1 &gt;/proc/calypso/tunables/bwm_readConfFile&quot; for the new entry to take effect</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/cm_playnowatlivepoint</td>
<td>Write</td>
<td>Write Tunable used to enable/disable the play at live point. When the tunable is enabled, it allows to play at live point.</td>
<td>bool</td>
<td>default 1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/convert_npt_using_pts</td>
<td>Write</td>
<td>Write Usually play npt computation is based offset information, but using this tunable we could improve the accuracy. With tunable enable, the npt computation uses actual frame pts information, which improves the accuracy.</td>
<td>bool</td>
<td>default 1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/disable_fade_frame</td>
<td>Write</td>
<td>Write Tunable used to enable/disable the frame fading option at the file transition. When it enabled, there is no extra fade frame getting inserted at file transition. But when its disabled, there are 4 fade frames are getting inserted at the splice point.</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/ftpoutmaxrate</td>
<td>Write</td>
<td>Write Tunable used to configure the ftpmax rate for total active ftp sessions</td>
<td>Hex/bps</td>
<td>default 1900000</td>
</tr>
<tr>
<td>/proc/calypso/tunables/ftpoutmaxsessions</td>
<td>Write</td>
<td>Write Tunable used to configure the number of ftp sessions</td>
<td>no of session/Hex</td>
<td>default 0</td>
</tr>
</tbody>
</table>
Table H-3  Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write</th>
<th>Description</th>
<th>Units/Type</th>
<th>default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/tunables/popularity_half_life</td>
<td>Read</td>
<td>Tunable used to denote how often server play the content. The value set in popularity_half_life will determine the rate of increase of the bump-on-play value. The bump-on-play value is managed by the class BumpOnUse, which resides in cm/PopularityValue. Set via CDSM</td>
<td>Sec/Hex</td>
<td>default A880</td>
</tr>
<tr>
<td>/proc/calypso/tunables/read_etc_hosts</td>
<td>Write</td>
<td>Tunable used to read the etc hosts from /etc/hosts</td>
<td>bool</td>
<td>default 1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/pipe_add</td>
<td>Write</td>
<td>Tunable used to add the new pipe with any reboot</td>
<td>Pipe format</td>
<td>default empty</td>
</tr>
<tr>
<td>/proc/calypso/tunables/pipe_del</td>
<td>Write</td>
<td>Tunable used to delete the existing pipe</td>
<td>Pipe id</td>
<td>default empty</td>
</tr>
<tr>
<td>/proc/calypso/tunables/pipe_modify</td>
<td>Write</td>
<td>Tunable used to modify the existing pipe configuration</td>
<td>Pipe format</td>
<td>default empty</td>
</tr>
<tr>
<td>/proc/calypso/tunables/stream_from_local_array</td>
<td>write</td>
<td>Tunable used to enable to stream the content from local server. This tunable specifically to control server</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/vaultdecommission</td>
<td>Read</td>
<td>It will be read from setup file, Used to Make the Number of Mirror Copies needs to be present on the site</td>
<td>Number of copies</td>
<td>default 2</td>
</tr>
<tr>
<td>/proc/calypso/tunables/vaultmirrorcopies</td>
<td>Write</td>
<td>It decides the time interval at which the Bandwidth management updates are exchanged by server where servers report their bandwidth usage to primary and primary assigns bandwidth to other servers. When committed bandwidth out of bandwidth also it reports the BWM (happen two levels, first at 90% and then second time at 95%)</td>
<td>in sec</td>
<td>default 10</td>
</tr>
<tr>
<td>/proc/calypso/internal/offline</td>
<td>Write</td>
<td>Tunable used to offline the server, when its set server become offline.</td>
<td>bool</td>
<td>default 0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/bPSIFailsIngest</td>
<td>RW</td>
<td>It will make sure that trick code aborts the ingest when bitstream don't have PAT, PMT</td>
<td>Boolean</td>
<td>default TRUE</td>
</tr>
<tr>
<td>/proc/calypso/tunables/bRateFailsIngest</td>
<td>RW</td>
<td>If it is enabled, Ingest fails if Bitrate cannot be computed.</td>
<td>Boolean</td>
<td>default TRUE</td>
</tr>
</tbody>
</table>
## Table H-3  Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write (RW) type</th>
<th>Description</th>
<th>Units/Type</th>
<th>Default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/tunables/nCCErrorsFailIngest</td>
<td>RW</td>
<td>Controls number of CC errors allowed after which Ingest is marked failed</td>
<td>Number</td>
<td>None</td>
</tr>
<tr>
<td>/proc/calypso/tunables/nDiscErrorsFailIngest</td>
<td>RW</td>
<td>Number of discontinuity errors allowed after which ingest is marked failed</td>
<td>Number</td>
<td>None</td>
</tr>
<tr>
<td>/proc/calypso/tunables/nPicGapsFailIngest</td>
<td>RW</td>
<td>Number of PicGaps after which we fail ingest</td>
<td>Number</td>
<td>3</td>
</tr>
<tr>
<td>/proc/calypso/tunables/nSyncLossesFailIngest</td>
<td>RW</td>
<td>Amount of time in Hundredth of second in pic Gap which is considered as ingest failure</td>
<td>Time in hundredth of seconds</td>
<td>5 (seconds)</td>
</tr>
<tr>
<td>/proc/calypso/tunables/nSyncLossesinHSFailIngest</td>
<td>RW</td>
<td>Number of synclosses after which we fail ingest</td>
<td>Number</td>
<td>3</td>
</tr>
<tr>
<td>/proc/calypso/tunables/maintenancemirrorcopies</td>
<td>RW</td>
<td>No of copies for mirroring during server maintenance</td>
<td>Number</td>
<td>2</td>
</tr>
<tr>
<td>/proc/calypso/tunables/enable_rtp_rtx</td>
<td>RW</td>
<td>Enables VOD error repair feature with RTP RTX</td>
<td>Boolean</td>
<td>default 0 Range 0,1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/nEveryNMinutes</td>
<td>RW</td>
<td>to allow ingestion depending on the ingestknob settings such as a check on the error counts of sample based on time specified</td>
<td>Minutes</td>
<td>30</td>
</tr>
<tr>
<td>/proc/calypso/tunables/tm_restrict_enable_fw_resume</td>
<td>Write</td>
<td>This tunable used to enable/disable the streamer to resume the Fast forward after playing a Fast forward trick restricted content in 1x.</td>
<td>bool</td>
<td>default false</td>
</tr>
<tr>
<td>/proc/calypso/tunables/tm_restrict_enable_forward_jump</td>
<td>Write</td>
<td>tunable used to enable/disable the streamer to resume the forward jump after playing a forward jump restricted content in 1x</td>
<td>bool</td>
<td>default false</td>
</tr>
<tr>
<td>/proc/calypso/tunables/tm_restrict_enable_forward_jump_resume</td>
<td>Write</td>
<td>tunable used to enable/disable the streamer to resume the forward jump after playing a forward jump restricted content in 1x</td>
<td>bool</td>
<td>default false</td>
</tr>
<tr>
<td>/proc/calypso/tunables/tm_restrict_enable_rewind_skip</td>
<td>Write</td>
<td>Tunable used to enable/disable the rewind skip. If it enable then rewind jump to the beginning of the restricted content and continue rewinding from there</td>
<td>bool</td>
<td>default false</td>
</tr>
</tbody>
</table>
### Table H-3 Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write</th>
<th>Description</th>
<th>Units/Type</th>
<th>default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/tunables/vaultarraymirror</td>
<td>Write</td>
<td>This tunable used to Configure mirror partner, array id to which the server is mirroring. To stop the array mirroring we need to echo negative value of the partner array id</td>
<td>array id</td>
<td>default 1</td>
</tr>
<tr>
<td>/proc/calypso/cm/active_maxpacketsize</td>
<td>Read</td>
<td>Active Max packet size to be sent out on their streaming network</td>
<td>Packet Size</td>
<td>7 MPEG Cells for Standard Size packets, 21 MPEG Cells for Jumbo size packets</td>
</tr>
<tr>
<td>/proc/calypso/tunables/vaultlocalcopycount</td>
<td>RW</td>
<td>to configure the number of local mirror copy count on Mirroring Policy</td>
<td>count</td>
<td>1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/maintenancearraymirroringallowed</td>
<td>RW</td>
<td>to enable the array mirroring during the maintenance</td>
<td>functionalit y (enable/dis able)</td>
<td>TRUE</td>
</tr>
<tr>
<td>/proc/calypso/internal/cm_defaultGoidType</td>
<td>RW</td>
<td>To enable chunk GOID support</td>
<td>Number</td>
<td>0 – Default Value 2 – To enable goid chunking</td>
</tr>
<tr>
<td>/proc/calypso/tunables/http_new_c2_support</td>
<td>RW</td>
<td>If enabled, then OpenForWrite and AvailableRange tags are available as part of HTTP C2 Locate Response.</td>
<td>Boolean</td>
<td>1 - Default value</td>
</tr>
<tr>
<td>/proc/calypso/tunables/http_conformant_c2_available_range_syntax</td>
<td>RW</td>
<td>Controls the syntax of AvailableRange tag in HTTP C2 Locate Response.</td>
<td>Boolean</td>
<td>0- Default value</td>
</tr>
<tr>
<td>/proc/calypso/tunables/enable_Role_Failover_DbDown</td>
<td>RW</td>
<td>To enable/disable the role fail over support on DB connectivity loss in the streamers.</td>
<td>Number</td>
<td>1</td>
</tr>
<tr>
<td>/proc/calypso/tunables/db_connectivity_retries_check_count</td>
<td>RW</td>
<td>To set the number of retries before confirming the DB connectivity loss in the streamers.</td>
<td>Number</td>
<td>30</td>
</tr>
</tbody>
</table>
### Table H-3 Configuration Tunables

<table>
<thead>
<tr>
<th>Tunable name/Location</th>
<th>Read/Write (RW) type</th>
<th>Description</th>
<th>Units/Type</th>
<th>default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>/proc/calypso/tunables/streamPFramesDuringPause</td>
<td>RW</td>
<td>Tunable set on streamer to stream dummy P-frames and maintain a constant bit rate on issuing a pause in the STB</td>
<td>Number</td>
<td>0</td>
</tr>
<tr>
<td>/proc/calypso/tunables/streamPCRDuringPause</td>
<td>RW</td>
<td>Tunable set on streamer to stream PCR packet at less than 100msec interval along with null packets and maintain a constant bit rate on issuing a pause in the STB.</td>
<td>Number</td>
<td>0</td>
</tr>
</tbody>
</table>
Cisco VDS-TV RTSP Software Configuration Guide

Appendix H  VDS-TV Tunables

Configuration Tunables
Software Licensing Information

This appendix provides software license information related to the Cisco Videoscape Distribution Suite-TV (VDS-TV).

Notices

The document *Open Source Used in Cisco TV Content Delivery System, Release 4.8* contains licenses and related license information for open-source software included in Cisco VDS-TV, Release 4.8. The document is located at the following URL:


If you have any questions or problems accessing the link, please contact:

external-opensource-requests@cisco.com

Product Warranties

For product warranty information, refer to the warranty information in the Accessory Kit accompanying the product.