Cisco Videoscape Distribution Suite
Origin Server Release 2.1.1
Software Installation and
Configuration Guide

November 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
Contents

About This Book ix
  Document Revision History ix
  Audience ix
  Objective x
  Document Organization x
  Document Conventions xi
  Related Publications xii
  Obtaining Documentation and Submitting a Service Request xii

Product Overview 1-1
  Overview 1-1
  Feature Support 1-1
    Acquisition, Recording, and Playout of HLS Live and TSTV 1-3
    Load Balance Live Stream Acquisitions from Playout Node to Acquisition Node 1-3
    In-Memory-Live Streaming 1-3
    Stream-Aware Native HLS Pass-Through Mode 1-4
    Multiple Manifest Files for HLS Pass-Through Mode 1-5
    Web Video Text Tracks (WebVTT) Support for HLS Pass-Through Live 1-5
    NDS-HLS Support 1-6
    Delivery of HDS, HLS, and HSS VOD Content from NAS 1-7
    Delivery of ABR ODE for CF VOD Content on the NAS 1-7
    DRM Support 1-7
    Encryption Enhancements 1-7
    ODE Playout for HDS, HLS, and HSS Formats 1-13
    Trick Mode Support for HDS, HLS, and HSS Playback 1-13
  Admission Control 1-18
    System-Wide Admission Control Criteria 1-19
    Admission Control Averages 1-19
  API Management 1-19
  Asset Resolution 1-19
    Asset Resolution for ODE 1-20
    Default Asset Resolver File 1-20
    Cache-Control Enhancements 1-21
    Cache-Control Headers Support 1-21
Support for If-Modified-Since for Native ABR for HLS Live and for HDS, HLS, and HSS VOD 1-23
Support for If-Modified-Since for ODE Playout from CF VOD on the NAS 1-25
External Storage Devices—NAS 1-25
High Availability—Resiliency and Redundancy 1-26
Service Engine Redundancy 1-26
Service Router Redundancy 1-26
Operational Enhancements 1-26
Cross-Domain Policy File for HDS Playback 1-26
Customized Asset URLs 1-27
Display Usage for TMPFS and NSS Usage 1-29
Alarm Enhancements 1-29
Origin Services 1-29
VOSM 1-32
Authentication, Authorization, and Accounting 1-32
Device Management 1-32
Origin Services Management 1-33
Service Engine (SE) 1-33
Media Delivery Applications 1-33
Linear Stream Acquisition 1-33
Capture Controller 1-33
Web Engine 1-34
Service Router (SR) 1-34
Request Routing Engine 1-34
Coverage Zone File 1-38
Device Modes 1-39
System Topology 1-39
Virtual Machine (VM) Support 1-41
Provisioning of New Features 1-41

CHAPTER 2
Installing the VDS-OS on UCS Platforms 2-1
Installing the Hardware 2-2
Connecting a UCS Cisco Integrated Management Controller (CIMC) Port 2-2
Configuring the CIMC 2-3
Configuring the BIOS 2-5
Configuring the BIOS to Boot from a CD-ROM 2-6
Configuring Remote Presence 2-7
Setting Up a UCS B200 for the VDS-OS Software using the GUI 2-8
Installing the VDS-OS Software 2-25
Mounting a Virtual ISO and Rebooting the UCS 2-25
Connecting to a CIMC Serial Console and Installing the Software 2-27
Checking the BIOS Boot Order 2-27
Un-Mapping the ISO File 2-27
Exiting the VDS-OS Installer and Rebooting the UCS 2-27
Setting Up the VDS-OS Software 2-28

CHAPTER 3
Deploying the VDS-OS As a Virtual Machine 3-1
Deploying a VM Using vSphere 3-1
Deploying a VM Using vCenter (Recommended) 3-1
Deploying a Stand-Alone VM Without vCenter 3-4
Deploying a VM Using a Power CLI Script 3-6
Configuring the UCS B200 for Load Balancing 3-7
Add a vNIC Adapter Policy 3-7
Add a vNIC to the Host 3-7
Configure the vNIC 3-7

CHAPTER 4
Getting Started with Configuration 4-1
Initial Device Configuration 4-1
Logging In To the VOSM 4-1
Activating and Synchronizing the Devices 4-3
Activating and Setting NTP for Each Device 4-3
Activating All Inactive Service Engines 4-5
Navigating the VOSM 4-7
Devices, Services, and Other Tables 4-7
Devices Home Page 4-8
Task Bar 4-9
Configuring Primary and Standby VOSMs 4-11
Changing a Standby to a Primary VOSM 4-12
Recovering from Two Primary VOSMs 4-13
Typical Configuration Workflow 4-13

CHAPTER 5
Configuring Devices 5-1
Configuring Locations 5-1
Configuring Device Groups 5-3
Working with Device Groups 5-5
Aggregate Settings 5-7
Device Group Overlap 5-8
Configuring the Service Engine 5-9
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activating a Service Engine</td>
<td>5-9</td>
</tr>
<tr>
<td>Assigning Devices to Device Groups</td>
<td>5-13</td>
</tr>
<tr>
<td>Assigning Devices to Origin Services</td>
<td>5-14</td>
</tr>
<tr>
<td>Service Control</td>
<td>5-15</td>
</tr>
<tr>
<td>Configuring Transaction Logs</td>
<td>5-15</td>
</tr>
<tr>
<td>Application Control</td>
<td>5-17</td>
</tr>
<tr>
<td>Configuring Web Engine HTTP Cache Freshness</td>
<td>5-18</td>
</tr>
<tr>
<td>General Settings</td>
<td>5-19</td>
</tr>
<tr>
<td>Login Access Control</td>
<td>5-19</td>
</tr>
<tr>
<td>Authentication</td>
<td>5-27</td>
</tr>
<tr>
<td>Scheduling Database Maintenance</td>
<td>5-31</td>
</tr>
<tr>
<td>Setting Storage Handling</td>
<td>5-32</td>
</tr>
<tr>
<td>Network Settings</td>
<td>5-34</td>
</tr>
<tr>
<td>Configuring Notification and Tracking</td>
<td>5-50</td>
</tr>
<tr>
<td>Configuring Troubleshooting</td>
<td>5-65</td>
</tr>
<tr>
<td>Configuring Service Router Settings</td>
<td>5-65</td>
</tr>
<tr>
<td>Configuring the Service Router</td>
<td>5-66</td>
</tr>
<tr>
<td>Activating a Service Router</td>
<td>5-66</td>
</tr>
<tr>
<td>Configuring Routing Settings</td>
<td>5-68</td>
</tr>
<tr>
<td>Configuring Redirect Burst Control</td>
<td>5-68</td>
</tr>
<tr>
<td>Configuring Load Monitoring</td>
<td>5-69</td>
</tr>
<tr>
<td>Configuring Transaction Logs for the Service Router</td>
<td>5-71</td>
</tr>
<tr>
<td>Configuring the VOSM</td>
<td>5-72</td>
</tr>
</tbody>
</table>

### CHAPTER 6

**Creating Origin Services and Live Channels**  

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Origin Services</td>
<td>6-1</td>
</tr>
<tr>
<td>Creating an Origin Service</td>
<td>6-1</td>
</tr>
<tr>
<td>Service Definition</td>
<td>6-2</td>
</tr>
<tr>
<td>General Settings</td>
<td>6-3</td>
</tr>
<tr>
<td>SE Assignment</td>
<td>6-4</td>
</tr>
<tr>
<td>Assign Network Storage Shares</td>
<td>6-5</td>
</tr>
<tr>
<td>Asset Resolver Settings</td>
<td>6-6</td>
</tr>
<tr>
<td>Cross-Domain Settings</td>
<td>6-6</td>
</tr>
<tr>
<td>Content Protection Settings</td>
<td>6-6</td>
</tr>
<tr>
<td>View Assigned Live Channels</td>
<td>6-7</td>
</tr>
<tr>
<td>Creating Live Channels</td>
<td>6-7</td>
</tr>
<tr>
<td>Channel Definition</td>
<td>6-8</td>
</tr>
<tr>
<td>Assign Origin Service</td>
<td>6-9</td>
</tr>
<tr>
<td>Assign Acquisition Node</td>
<td>6-9</td>
</tr>
</tbody>
</table>
### Assign Network Storage Shares 6-10
### Capture Resources 6-10
### Publish Resources 6-11
### Capture Schedule 6-13

#### CHAPTER 7
**Configuring the System** 7-1

- Configuring AAA 7-1
  - Creating, Editing, and Deleting Users 7-2
  - Creating, Editing, and Deleting Roles 7-5
  - Creating, Editing, and Deleting Domains 7-6
- Changing a Password 7-7
- Configuring System Settings 7-8
  - System Properties 7-8
  - Configuring Device Offline Detection 7-9
  - Configuring Service Routing 7-10
    - Coverage Zone File Registration 7-10
    - Configuring Global Routing 7-12
  - Asset Resolver File Registration 7-12
  - Defining Network Storage Shares 7-13
  - Creating Mount Option Profiles for Network Storage Shares 7-14
- Viewing or Downloading XML Schema Files 7-15

#### CHAPTER 8
**Monitoring the VDS-OS** 8-1

- System Monitoring 8-1
  - System Status 8-1
    - Device Alarms 8-4
    - Service Alarms 8-5
  - System Home Page 8-6
  - System Audit Logs 8-6
  - System Port Numbers 8-7
- Device Monitoring 8-8
  - Devices Table 8-9
  - Devices Home Page 8-11
  - Using show, clear, and alarm Commands 8-12
    - Using the VOSM show, clear, or alarm Command Tool 8-13
  - Core Dump Files 8-16
  - CPU Utilization 8-17
- Origin Service Monitoring 8-18
  - Virtual Origin Services Table 8-18
Monitoring Live Channels  8-18
  Live Channel Table  8-19
  Channel States  8-19
  Channel Control  8-19
  Capture Resource Table  8-19
  Publish Resource Table  8-20
Viewing Statistics  8-20
  Viewing Service Engines and Device Group Statistics  8-21
  Viewing Routing Statistics  8-22
Log Files  8-22
Transaction Logs  8-23
  Transaction Log Formats for Web Engine  8-23
  Usage Guidelines for Log Files  8-28
    Working Logs  8-28
    Archive Working Log  8-29
    Exporting Log Files  8-29
  Service Router Transaction Log Fields  8-31
  Service Monitor Transaction Logs  8-31
  Content Manager Transaction Log Fields  8-35
  Capture Controller Transaction Log Fields  8-36

CHAPTER 9
Maintaining the VDS-OS  9-1
Software Upgrade  9-1
  Getting a Software File from Cisco.com  9-1
  Finding the Software Version of the Devices  9-2
  Configuring the Software Image Settings  9-2
  Upgrading the Software  9-4
    Downgrading the Software  9-5
    Interoperability Considerations  9-5
    Upgrading Software by Device Groups  9-6
    Upgrading an SE, SR, or VOSM  9-8
    Upgrading a Virtual Machine (VM)  9-8
Rebooting Devices  9-8
Deleting a Device  9-9
  Deleting a Warm Standby VOSM  9-11
Replacing a Device  9-12
  Replacing a VOSM  9-12
  Replacing an SE, SR, or VDS-OS  9-13
  Replacing a VM across OVA Releases  9-14
## Contents

**Cisco Media Origination System Release 2.0.0 Installation and Configuration Guide**

### Backup and Recovery Procedures 9-14
- Performing Backup and Restore on the VOSM Database 9-15
- Using the VDS-OS Software Recovery CD-ROM 9-16
  - System Software Components 9-16
  - Getting the VDS-OS Software Recovery File from Cisco.com 9-16
  - Installing the Software Using the Recovery CD-ROM 9-17
- Recovering the System Software 9-17
- Recovering a Lost Administrator Password 9-20
- Recovering from Missing Disk-Based Software 9-21
- Recovering VDS-OS Network Device Registration Information 9-24

### Troubleshooting 9-25
- Check the Ingest Log 9-25
- Check the DASH and ODE Statistics on the Service Engine 9-25
- Enable Debug Trace for the Web-Engine 9-26
- Check the Web-Engine Statistics 9-26
- Troubleshoot 404, 500, and 504 Errors 9-27
  - Check the Translog 9-27
  - Check the Web-Engine Error Logs 9-27

## Appendix A

### Creating Asset Resolver Files A-1
- Asset Resolver File Structure and Syntax A-2
  - Pattern Matching A-5
  - Rule Action Processing A-5
- Asset Resolver File Examples A-6
  - Default Asset Resolver File A-6
  - Asset Resolver Rule for HLS Live Service A-8
  - Asset Resolver Rules for CF VOD—Unique ContentID in the URL A-8
  - Asset Resolver Rules for CF VOD—ContentID as the Manifest File Name A-9
  - Asset Resolver Rule for Content Protection A-11
  - Setting the HTTP Response Cache-Control Header A-11
    - Global Cache-Control Configuration for an Origin Service A-11
    - Cache-Control Configuration for a Specific HLS .m3u8 or .ts File URL A-12
    - Generic HTTP Response Header A-12
- Troubleshooting the Asset Resolver A-12

## Appendix B

### Creating Coverage Zone Files B-1
- Introduction B-1
  - Zero-IP Based Configuration B-2
  - Invalid IPv4 Addresses in Coverage Zone File B-3
About This Book

This preface describes the audience, use, and organization of the *Cisco Media Origination System Release 2.0.0 Installation and Configuration Guide*. The preface also outlines the document conventions and support information.

This preface contains the following sections:
- Document Revision History, page ix
- Audience, page ix
- Objective, page x
- Document Organization, page x
- Document Conventions, page xi
- Related Publications, page xii
- Obtaining Documentation and Submitting a Service Request, page xii

Document Revision History

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

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OL-28084-04</td>
<td>October 2013</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>

Audience

This guide is for the networking professional managing the Cisco Videoscape Distribution Suite Origin Server system, hereafter referred to as the VDS-OS. Before using this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of Ethernet, local area networking, and Internet streaming.
Objective

This guide provides the information you need to configure and monitor the VDS-OS.

This guide provides procedures for using the commands that have been created or changed for use with the VDS-OS. It does not provide detailed information about these commands.

This guide does not describe system messages you might encounter or how to install your VDS-OS. See the “Related Publications” section on page xii for links to documentation online.

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

Document Organization

This document contains the following chapters and appendices:

<table>
<thead>
<tr>
<th>Chapter or Appendix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Product Overview”</td>
<td>Provides a brief introduction to the VDS-OS.</td>
</tr>
<tr>
<td>Chapter 2, “Installing the VDS-OS on UCS Platforms”</td>
<td>Provides detailed instructions for installing the VDS-OS software on Cisco Unified Computing System (UCS) platforms.</td>
</tr>
<tr>
<td>Chapter 3, “Deploying the VDS-OS As a Virtual Machine”</td>
<td>Provides detailed instructions for deploying VDS-OS as a virtual machine (VM).</td>
</tr>
<tr>
<td>Chapter 4, “Getting Started with Configuration”</td>
<td>Provides information about initially configuring the devices to communicate with the VOSM, configuring a standby VOSM, navigating the VOSM, and a typical configuration workflow.</td>
</tr>
<tr>
<td>Chapter 5, “Configuring Devices”</td>
<td>Provides information on configuring the devices in the VDS-OS.</td>
</tr>
<tr>
<td>Chapter 6, “Creating Origin Services and Live Channels”</td>
<td>Provides information about configuring origin services.</td>
</tr>
<tr>
<td>Chapter 7, “Configuring the System”</td>
<td>Provides information on system configuration for the VDS-OS.</td>
</tr>
<tr>
<td>Chapter 8, “Monitoring the VDS-OS”</td>
<td>Provides information on monitoring the VDS-OS.</td>
</tr>
<tr>
<td>Chapter 9, “Maintaining the VDS-OS”</td>
<td>Provides information on upgrading the VDS-OS software, deleting devices from the system, performing disk maintenance, and removing content from the system.</td>
</tr>
<tr>
<td>Appendix A, “Creating Asset Resolver Files”</td>
<td>Provides information on creating an Asset Resolver file.</td>
</tr>
<tr>
<td>Appendix B, “Creating Coverage Zone Files”</td>
<td>Provides information on creating and validating a Coverage Zone file.</td>
</tr>
<tr>
<td>Appendix C, “Creating Capture Schedule Files”</td>
<td>Provides information on creating Capture Schedule files.</td>
</tr>
</tbody>
</table>
Document Conventions

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

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

**Caution**

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

**Note**

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

**Tip**

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

These documents provide complete information about the VDS-OS and are available from the Cisco.com site:

- *Cisco Videoscape Distribution Suite Origin Server Release 2.1.1 API Guide*
- *Cisco Videoscape Distribution Suite Origin Server Release 2.1.1 Command Reference*
- *Cisco Videoscape Distribution Suite Origin Server Release 2.1.1 Alarms and Error Messages Guide*
- *Release Notes for Cisco Videoscape Distribution Suite Origin Server Release 2.1.1*
- *Open Sources Used in Cisco Videoscape Distribution Suite Origin Server Release 2.1.1*
- *Cisco Videoscape Distribution Suite Release 2.1.1 Documentation Roadmap*

You can access the software documents at the following URL:


Documentation for the UCS hardware platforms can be found at the following URLs:

- *Cisco UCS C200 Installation and Service Guide*
- *Cisco UCS C210 Installation and Service Guide*
- *Cisco UCS B200 M3 Blade Server Installation and Service Note*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What’s New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What’s New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.
Product Overview

Overview

The Cisco Videoscape Distribution Suite Origin Server (VDS-OS) provides content origination and media processing capabilities on a unified platform that can be managed by the Virtual Origin System Manager (VOSM).

The VDS-OS provides a unified origin solution that can be used to reduce the complexity of heterogeneous Adaptive Bit Rate (ABR) origin servers and traditional content libraries. In addition to supporting some of the major ABR origin functions, it also provides standards-based interfaces for content origination. The VDS-OS system can be your authoritative source of content for different content service ecosystems. It provides a unified ABR content origination framework for on-demand encapsulation (ODE), linear (live) streaming, and time-shifted content. The VDS-OS also has integrated capabilities to convert ABR live video to video-on-demand (VOD) assets based on predefined schedules.

Feature Support

This section lists all of the features in VDS-OS R2.1.1.

- Acquisition, Recording, and Playout of HLS Live and TSTV, page 1-3
  - Load Balance Live Stream Acquisitions from Playout Node to Acquisition Node, page 1-3
  - In-Memory-Live Streaming, page 1-3
  - Stream-Aware Native HLS Pass-Through Mode, page 1-4
  - Multiple Manifest Files for HLS Pass-Through Mode, page 1-5
  - Web Video Text Tracks (WebVTT) Support for HLS Pass-Through Live, page 1-5
  - NDS-HLS Support, page 1-6
- Delivery of HDS, HLS, and HSS VOD Content from NAS, page 1-7
- Delivery of ABR ODE for CF VOD Content on the NAS, page 1-7
  - DRM Support, page 1-7
    - Cisco Key Store 1.1
- Cisco VMS-KMS
- Verimatrix VCAS 3.3
  - Encryption Enhancements, page 1-7
  - ODE Playout for HDS, HLS, and HSS Formats, page 1-13
  - HTTP-Sourced Common Media Format—cDVR, TSTV (HLS)
  - NAS-Sourced Common Media Format—VOD (HLS)
  - Trick Mode Support for HDS, HLS, and HSS Playback, page 1-13
- Admission Control, page 1-18
- API Management, page 1-19
- Asset Resolution, page 1-19
- Cache-Control Enhancements, page 1-21
  - Cache-Control Headers Support, page 1-21
  - Support for If-Modified-Since for Native ABR for HLS Live and for HDS, HLS, and HSS VOD, page 1-23
  - Support for If-Modified-Since for ODE Playout from CF VOD on the NAS, page 1-25
- External Storage Devices—NAS, page 1-25
- High Availability—Resiliency and Redundancy, page 1-26
- Operational Enhancements, page 1-26
  - Cross-Domain Policy File for HDS Playback, page 1-26
  - Customized Asset URLs, page 1-27
  - Default Asset Resolver File, page 1-20
  - Display Usage for TMPFS and NSS Usage, page 1-29
  - Alarm Enhancements, page 1-29
- Origin Services, page 1-29
- VOSM, page 1-32
  - Authentication, Authorization, and Accounting, page 1-32
  - Device Management, page 1-32
  - Origin Services Management, page 1-33
- Service Engine (SE), page 1-33
  - Media Delivery Applications, page 1-33
  - Linear Stream Acquisition, page 1-33
  - Capture Controller, page 1-33
  - Web Engine, page 1-34
- Service Router (SR), page 1-34
  - Request Routing Engine, page 1-34
  - Coverage Zone File, page 1-38
- Device Modes, page 1-39
- System Topology, page 1-39
Chapter 1      Product Overview

Feature Support

- Virtual Machine (VM) Support, page 1-41
- Provisioning of New Features, page 1-41

Acquisition, Recording, and Playout of HLS Live and TSTV

- Load Balance Live Stream Acquisitions from Playout Node to Acquisition Node, page 1-3
- In-Memory-Live Streaming, page 1-3
- Stream-Aware Native HLS Pass-Through Mode, page 1-4
- Multiple Manifest Files for HLS Pass-Through Mode, page 1-5
- Web Video Text Tracks (WebVTT) Support for HLS Pass-Through Live, page 1-5
- NDS-HLS Support, page 1-6

Load Balance Live Stream Acquisitions from Playout Node to Acquisition Node

The VDS-OS load-balances requests to the Playout node among all active Acquisition nodes, using round-robin routing at a per publish resource level.

The routing occurs between active Acquisition nodes. An Acquisition node is considered active for a publish resource as long as it is able to successfully serve out content for the publish resource. The set of active Acquisition nodes is rotated so that each new client request for which there is no available cached content in the Playout node is routed to a different node, distributing the load evenly across all nodes. Failed nodes are isolated to avoid response time delays, and client requests are retried periodically until successful.

In-Memory-Live Streaming

You can use In-Memory-Live Streaming to optimize or even eliminate the use of NAS. In-Memory-Live Streaming enables you to deploy live services with a small time-shift buffer (DVR window) in RAM. The relatively small size of the buffer means that In-Memory-Live Streaming supports only limited in-session time-shifting.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services such as start-over based on the time-shift buffer are not supported.</td>
</tr>
</tbody>
</table>

When configuring In-Memory-Live Streaming, keep the following considerations in mind:

- You must configure a live publish resource and a small time-shift buffer on the VOSM’s Publish Resources page.
  - Enter a **Time-Shift Window** size, in minutes, for In-Memory-Live Streaming. The valid range is 1 to 120 minutes. The default setting is 1 minute.
  - Select the **In-Memory Live** checkbox to enable In-Memory-Live Streaming. By default, In-Memory-Live Streaming is disabled.
- You can also use REST APIs on VOSM to configure In-Memory Live publishing with a time-shift buffer.
- For an in-memory publish resource, VDS-OS stores all manifest and segments files in RAM. VDS-OS reserves an appropriate amount of RAM (TMPFS) when the in-memory publish resource is started. If there is insufficient RAM, the in-memory publish resource is not created.
• For an in-memory pass-through publish resource, the VDS-OS stores the variant manifests in the
NAS, if a NAS is configured for the origin service. Otherwise, the VDS-OS stores the variant
manifests on the local disk.

For more information about configuring a publish resource for In-Memory-Live Streaming, see the
“Publish Resources” section on page 6-11.

Stream-Aware Native HLS Pass-Through Mode

The VDS-OS supports native HLS Live service in pass-through mode. In pass-through mode, the
VDS-OS does not interpret or republish any content received from the HLS encoder or packager or
encapsulator (that is, the CMP or CME).

When configuring a pass-through native HLS publish resource, keep the following considerations in
mind:

• The VDS-OS publishes the live service using the name that was received from the packager. That
is, the Capture Resource URL is same as the Publish Resource URL in pass-through mode.
• The VDS-OS publishes all streams as received from the packager. The VDS-OS does not select or
filter streams.
• The time-shift buffer (DVR window) is controlled by the packager. The VDS-OS deletes the
segments when it receives an HTTP DELETE from the packager.

You must configure the time-shift buffer on the VOSM’s Publish Resources page, and it must match
the time-shift buffer that is used on the encoder or packager. The time-shift buffer determines when
to delete segments, if an HTTP DELETE is not received from the packager, under error conditions.
• You must configure all profile and stream information for a pass-through publish resource on the
VOSM’s Publish Resources page.
• When the VDS-OS detects the loss of a stream, as in republish mode, it generates an alarm and
updates the status of the capture resource and the channel on the VOSM.
• As a part of HLS Live publishing, the stream manifests are updated as new segments are added to
the stream manifest. However, the variant (master) playlist, which describes the stream manifest, is
not updated while publishing is in-progress.
• The variant playlist is sent to the VDS-OS only when live publishing starts. Therefore, take special
care when the channel is started or restarted on the encoder or packager.
• You must start a live channel or publish resource on the VOSM before you start it on the encoder or
packager. This ensures that the VDS-OS resources are ready to ingest content pushed by the encoder
or packager.
• If the bit rate changes in HLS Live pass-through mode, you must stop the packager that is running
with the old configuration before starting VOSM with the new configuration. When you start the
HLS Live channel in VOSM, you must also start the packager within five (5) minutes, or the channel
will move to Failed state.
• If a channel or publish resource is stopped on the VOSM, the stopped asset is cleaned up. Therefore,
after the publish resource is restarted, the channel must also be restarted on the encoder or packager,
to ensure that the variant playlist is published correctly.

For more information about configuring a pass-through native HLS publish resource, see the “Publish
Resources” section on page 6-11.
Multiple Manifest Files for HLS Pass-Through Mode

The VDS-OS can support more than one variant playlist for an HLS Live asset. The variant playlists can be used to create different logical assets from the same physical asset, based on devices (such as iPhone or Apple-TV) or policies (such as gold and silver users, or high-definition and standard-definition users).

The VDS-OS allows the logical assets to contain streams that overlap. For example, given profiles A, B, C, and D, one playlist can contain all four profiles; another can contain profiles A, B, and C; and another can contain profiles C and D.

If you have 4 profiles A, B, C and D, then you can have variant manifests where variant1 contains A, B, C and Variant2 contains B, C, D and so on.

To support multiple manifest files, the VDS-OS allows the following VOSM capture resource URLs:

http://vos.domain.net/channel/cap/res/hls/variant.m3u8

http://vos.domain.net/channel/cap/res/hls/

The VDS-OS returns code 2xx for all .m3u8 file ingest requests that fall under a configured capture resource, regardless of whether a pass-through or republish publish resource is configured.

For example, given the above capture resource with two profiles, stream1 and stream2. If the VDS-OS receives ingest requests stream1.m3u8, stream2.m3u8, and variant.m3u8, it returns a 2xx code.

However, the VDS-OS also returns a 2xx code for other .m3u8 ingest requests from a packager. If a corresponding pass-through publish resource is configured for the capture resource, the VDS-OS stores the files in the configured storage, as appropriate. If a pass-through publish resource is not configured, the files are not stored anywhere.

You must configure the multiple variant manifests as multiple presentations.

```
<output_stream>
  <stream_id>00000000-0000-0000-0000-00000000a800</stream_id>
  <input_id type="video" >1a4d4523-b19a-4cdf-a161-5bdea5990e4d</input_id>
  <input_id type="audio" >dda41af9-63a4-4713-833d-834df194af78</input_id>
  <streamname>mid800</streamname>
  <streambitrate>80000</streambitrate>
</output_stream>
```

```
<presentations>
  <presentation name="variant1">
    <outputstream stream_id="00000000-0000-0000-0000-00000000a800" />
  </presentation>
  <presentation name="variant2">
    <outputstream stream_id="00000000-0000-0000-0000-00000000a800" />
  </presentation>
</presentations>
```

The expiry or max-age for multiple variants is the same as that for a single variant manifest: the arrival rate.

Web Video Text Tracks (WebVTT) Support for HLS Pass-Through Live

The VDS-OS supports WebVTT for pass-through HLS Live.

WebVTT support requires a .vtt file that is used for subtitles and captioning video content.

- There is one .vtt file per segment per language that is common to all of the profiles.
- Usually, all of the .vtt files for a given language are contained in a folder at the publish resource root, with one folder per language. However, any directory structure works with pass-through.
There is a separate manifest file that contains all of the .vtt segments per language. The manifest file is usually stored along with the stream manifest files and variant manifest at the publish resource root. The variant manifest contains information about the subtitles that each stream can use.

- The MIME type for .vtt files is text/vtt.
- The .vtt file’s max-age is set to the end of the DVR window, the same as for the .ts file.
- The .vtt manifest file’s max-age is set to the segment arrival rate, the same as for the stream manifest file.

### NDS-HLS Support

The VDS-OS supports NDS-HLS.

NDS-HLS has a .ptr file, which is a custom manifest file, used by NDS-HLS desktop clients, that contains information similar to that found in stream and variant manifests.

- You can use an ABR-enabled NDS StreamShaper or an ABR-E to POST NDS-HLS with a .ptr file.
- Each live publish resource is associated with its own latest.ptr file that is updated periodically.
- Each VOD asset is associated with an assetname.ptr file.
- We recommend that all of the latest.ptr files be contained in a folder at the publish resource root, the same location where the index.m3u8 file is kept. However, any directory structure works with pass-through.
- The .ptr file’s expiry time is set to the segment arrival rate, the same as for the stream manifest file.

The following sample shows a typical latest.ptr file for a live channel:

```
1.1
Streamshaper/5.8.0.8/196
Live
326E28-326E31 10000 10
0
Mon, 20 May 2013 16:28:36 GMT 53159555200 13295548751

400  400  368  208
600  600  640  368
1200 1200  640  368
2200 2200  720  416
```

The following sample shows a typical .ptr file for a VOD asset:

```
1.1
XTVEncryptor/5.7.0.268/1428
VOD
0-170 10000
0
Mon, 08 Oct 2012 20:39:56 GMT 99497160000 3685080

64  64  320  192
300 300  384  224
600  600  480  272
900  900  640  368
1300 1300  640  480
1600 1600  720  576
```
Delivery of HDS, HLS, and HSS VOD Content from NAS

The VDS-OS accesses VOD content stored on the network-attached storage (NAS) devices managed by the operator. The VOD content is used for recording and DVR buffering.

Delivery of ABR ODE for CF VOD Content on the NAS

- DRM Support, page 1-7
- ODE Playout for HDS, HLS, and HSS Formats, page 1-13
- Trick Mode Support for HDS, HLS, and HSS Playback, page 1-13

DRM Support

The VDS-OS supports the following digital rights management (DRM) types:
- Cisco Key Store 1.1 for Standard HLS, Encryption Type aes_128_cbc (HTTP only; HTTPS is not supported)
- Cisco VMS-KMS for Standard HLS, Encryption Type aes_128_cbc (HTTPS is not supported)
- Cisco VMS-KMS PlayReady for HLS, Encryption Type aes_128_ctr (HTTPS is not supported)
- Cisco VMS-KMS PlayReady for HSS, Encryption Type aes_128_ctr (HTTPS is not supported)
- Verimatrix VCAS 3.3 for Standard HLS, Encryption Type aes_128_cbc
- Verimatrix VCAS 3.3 PlayReady for HSS, Encryption Type aes_128_ctr

Encryption Enhancements

- Cisco Key Store Server Integration, page 1-7
- Cisco VMS-KMS Integration, page 1-8
- Verimatrix Key Server Integration, page 1-10

Cisco Key Store Server Integration

The VDS-OS integrates with the Cisco Key Store server to acquire content encryption keys for HLS ODE and playout.

The VDS-OS supports only offline VOD and VOD generated by the Cisco Transcode Manager (CTM). The Common Format (CF) VOD asset is on the NAS. ODE is used to play out content in HLS format.

Key Store Server Information

The Key Store is a safe-box component that is responsible for the allocation of content keys, secure storage, scalable provisioning, and key access control.

To run Key Store, enter the following command:
nds_service nds_keystore start

To stop Key Store, enter the following command:
nds_service nds_keystore stop
Cisco VMS-KMS Integration

The VMS-KMS Media Suite Key Management Server (VMS-KMS) supports key retrieval for both HLS and PlayReady.

The VDS-OS supports only offline VOD and VOD generated by the Cisco Transcode Manager (CTM). The DASH VOD asset is on the NAS. ODE is used to play out content in HLS/HSS format.

Note
The VMS-KMS key server maintains a database of all incoming URLs. Even if a request is refused with HTTP error response code 404, the key server saves the URL in the database. So if the key server receives the same request again, even if the new request has the correct configuration, it still responds with error code 404.

VMS-KMS Key Server Info
- Keyset Template: Each DRM type has its own keyset template, identified by a unique ID.
- Keyset: Each asset is linked to a keyset, identified by a unique ID. Multiple requests for the same asset by different clients receive the same keyset.
- Key: Each keyset contains a 16-byte key.
- Domain of the VMS server
- Username
- Password

Creating the Keyset Templates
You must create a keyset template for each encryption methodology, such as HLS or PlayReady. To do so, use the following procedure:

Step 1  On the VMS, select Key Management > KeysetTemplates. The Manage Keyset Templates page is displayed.
Step 2  Click Add New. The Create New Keyset Template popup is displayed.

Step 3  Enter a Name of your choosing.
Step 4  Select a Key Provider.
Step 5
Select a DRM Type.

Step 6
Click Create to create the keyset template. The VMS automatically assigns a UUID (keyset template ID).

After you have configured the keyset templates on the VMS, you must add the content protection key profiles on the VOSM. Each origin service has its own Content Protection Settings. You can have multiple content protection key profiles, one for each key server and encryption type.

**VOSM Configuration for a VMS-KMS Key Profile**

The RSA private key file is needed to decrypt the key that is sent to the VDS-OS in the key server response. It is a part of the key profile for VMS-KMS. Therefore, you cannot add the RSA private key file until you have added the content protection key profile for VMS-KMS.

The RSA private key file is generated externally and received out-of-band.

Figure 1-1 shows the Creating New Content Protection Key Profile page for a VMS-KMS key profile.

For VMS-KMS, the content protection key profile requires the following information:

- **Profile Name** of your choosing
- **Profile Type**: **VMS-KMS**
- **Protocol**: **HTTP**
  
  **Note**: HTTPS is not supported for VMS-KMS.

- Domain Name of the VMS server
- Port of the VMS server
- Auth Key
There is a VDS-OS client identity, created on the VMS, that calls the REST API with the username (UID) and password (PWD). The Auth Key is generated using base64 encoding of the username:password, and the word Basic is appended to the beginning of the generated Auth Key. For example:

Authorization: Basic Vk9TX0NMSUVOVDpwYXNzd29yZA==

- Key Set Template ID
- Key Provider Type:
  - HLS-AES-128
  VMS-KMS with HLS-AES-128 supports only HLS requests, which can be played using the QuickTime player on a MAC.
  - PR-AES-128
  VMS-KMS with PR-AES-128 supports only HLS and HSS requests. There is currently no player support for HLS with PlayReady encryption. HSS requests can be played using the PlayReady test application.

- RSA Private Key File
- RSA Private Key File Destination Name

Creating Video Assets In the VMS-KMS Key Server
You can create, edit, and delete video assets as bundle content in the VMS-KMS key server. After you have created a bundle, you can mark it as active, and it then is available for productization. For detailed information about managing video asset bundles, see the information at the following URL:


where hostname is the domain name of the VMS server.

Verimatrix Key Server Integration
The VDS-OS integrates with the Verimatrix Video Content Authority System (VCAS) Key Server Version 3.3. The VCAS server provides key retrieval for HLS and PlayReady.

Verimatrix HLS Playout
The key request to the Verimatrix server is created based on the default request key template:

http://domain.com:1234/CAB/keyfile?r=1231234&t=VOD&p=0

Configure the domain and port using VOSM.

The response contains the key and the location header contains the key URI, which is sent to the end client for key retrieval. Additional information is appended to the location header, similar to the information that was sent in the request to the key server:

https://player.interface.dom/keyfile?r=1231234&t=VOD&p=0

Playout is supported only on the Verimatrix ViewRight player, which is available for download in the iOS App store.

Verimatrix Smooth Playout
The VDS-OS creates the key request to the Verimatrix server based on the default request key template:
Configure the domain port using VOSM.
The response contains Playready DRM information. The body of the response might be empty.
All of the parameters are received as custom headers in the HTTP response. Playout is supported on any browser that supports the Microsoft Silverlight plugin.

**VOSM Configuration for a Verimatrix Profile**

The RSA private key file is needed to decrypt the key that is sent to the VDS-OS in the key server response. It is a part of the key profile for Verimatrix. Therefore, you cannot add the RSA private key file until you have added the content protection key profile for Verimatrix.

The RSA private key file is generated externally and received out-of-band.

*Figure 1-2* shows the Creating New Content Protection Key Profile page for a Verimatrix key profile.

*Figure 1-2  Creating New Content Protection Key Profile Panel for a Verimatrix Key Profile*

For Verimatrix, the content protection key profile requires the following information:

- Profile Name of your choosing
- Profile Type: **Verimatrix**
- Protocol: **HTTP** or **HTTPS**
- Domain Name of the Verimatrix server
- Port of the Verimatrix server
- Key Provider Type:
  - **HLS-AES-128**
    Verimatrix with HLS-AES-128 supports only HLS requests, which can be played using the QuickTime player on a MAC.
  - **PR-AES-128**
    Verimatrix with PR-AES-128 supports only HLS and HSS requests. There is currently no player support for HLS with PlayReady encryption. HSS requests with the Verimatrix PlayReady DRM can be played on any browser that supports the Microsoft Silverlight plugin.
Feature Support

Chapter 1      Product Overview

Adobe Access Encryption for Verimatrix

The VDS-OS supports Adobe Access encryption for Verimatrix. Adobe Access encryption requires access to an external Adobe Access license server, which you must configure in VOSM.

Step 1 Upload the following binary files for the license server and store them on the SE:
- Transport Certificate File
- License Certificate File
- Policy File
- Packager Certificate File

Step 2 Use the OS utility base64 command to encode each file in base64, then save the base64-encoded files on the SE.

Step 3 In the VOSM, select an origin service, then select **Content Protection Setting** in the left pane. The Content Protection Key Profiles panel is displayed.

Step 4 Click the **Create New Content Protection Key Profile** icon. The Creating New Content Protection Key Profile panel is displayed.

Step 5 Enter a Profile Name of your choosing, such as **adobe-server**.

Step 6 Select Profile Type **Adobe License Server**. The Adobe Access Files section is displayed.

Step 7 Enter the Adobe License Server URL - the URL of the license server.

Step 8 Choose the Transport Certificate File that you encoded for base64.

Step 9 Enter a Transport Certificate File Destination Name of your choosing.

Step 10 Choose the License Certificate File that you encoded for base64.

Step 11 Enter a License Certificate File Destination Name of your choosing.

Step 12 Choose the Policy File that you encoded for base64.
Step 13  Enter a Policy File Destination Name of your choosing.

Step 14  Choose the Packager Certificate File that you encoded for base64.

Step 15  Enter a Packager Certificate File Destination Name of your choosing.

Step 16  Enter the Packager Passcode that is associated with the Packager Certificate File. The passcode enables the VDS-OS to read the contents of the certificate.

Step 17  Click Submit to add the Adobe license server profile to the VOSM.

Step 18  Create a Verimatrix key profile (see the “VOSM Configuration for a Verimatrix Profile” section on page 1-11) with the following attributes:

- Profile Name of your choosing, such as verimatrix-adobe3
- Profile Type: Verimatrix
- Protocol: HTTP
- Key Provider Type: ADOBE-ACCESS
- Adobe Access License Server: Profile Name of the Adobe license server (adobe-server in this example)

Step 19  Click Submit.

Step 20  Add the new key profile (verimatrix-adobe3 in this example) to the Asset Resolver file publish information to enable Adobe Access encryption for Verimatrix. For more information, see the “Asset Resolution” section on page 1-19.

ODE Playout for HDS, HLS, and HSS Formats

The VDS-OS supports the playout of ODE CF VOD content on the NAS for the following formats:

- HDS—HTTP Dynamic Streaming
  The VDS-OS support for HDS supports only 2-second fragment delivery.

- HLS—Apple HTTP Live Streaming
  The VDS-OS support for HLS supports both 10-second and 2-second fragment delivery, depending on the Asset Resolver rule configuration. The default setting is 10-second fragment delivery.

- HSS—Microsoft HTTP Smooth Streaming
  The VDS-OS uses the Asset Resolver file that is assigned to the origin service to map the requested ABR URL to the stored CF asset.

Trick Mode Support for HDS, HLS, and HSS Playback

The VDS-OS supports trick mode for HDS, HLS, and HSS playback. Trick mode, also known as trick play, provides functions such as fast-forward and rewind for digital video systems such as VOD.

To support trick mode, the VDS-OS stores Increased Digital Resolution (IDR) information, such as the byte offset and the size, in the SSIX.

The VDS-OS supports the following trick mode controls:

- HDS
  - Fast-Forward 2x
  - Fast-Forward 8x
Chapter 1  Product Overview

Feature Support

- Rewind 2x
- Rewind 8x

- HLS
  - Fast-Forward 2x
  - Fast-Forward 4x
  - Fast-Forward 8x
  - Rewind 2x
  - Rewind 4x
  - Rewind 8x

- HSS
  - Fast-Forward 2x
  - Rewind 2x

DASH-HELPER Client MPD for HDS

A separate AdaptationSet is added to the DASH-HELPER client MPD to describe IDR-only ATS fragments. The AdaptationSet id attribute is set to i-frame.

```xml
<?xml version="1.0" encoding="utf-8"?>
<MPD xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
profiles="urn:com:cisco:profile:common-format:2012">
  <Period id="1">
    <AdaptationSet mimeType="video/mp2t" codecs="avc1.676400" segmentAlignment="false" startWithSAP="1" id="i-frame">
      <BaseURL>/1</BaseURL>
      <ContentComponent contentType="video" id="49"/>
      <SegmentTemplate timescale="90000" startNumber="27910"
media="$/RepresentationID/$Time$.ts">
        <SegmentTimeline>
          <S t="5028826778" d="180180" r="663"/>
        </SegmentTimeline>
      </SegmentTemplate>
    </AdaptationSet>
    <AdaptationSet mimeType="video/mp2t" codecs="mp4a.4c80" segmentAlignment="false" startWithSAP="1" id="video_seg_2">
      <BaseURL>/1</BaseURL>
      <!-- Representation info for additional segments -->
    </AdaptationSet>
  </Period>
</MPD>
```
Client Manifest for HDS

The i-frame streams are advertised in `media` with the `type` attribute set to `video-keyframe-only`.

```xml
<manifest xmlns="http://ns.adobe.com/f4m/1.0" version="2.0">
  <id>video_seg_2</id>
  <mimeType>video/x-flv</mimeType>
  <streamType>recorded</streamType>
  <drmAdditionalHeader>
  …
  </drmAdditionalHeader>
</manifest>
```
Sample cMPD I-Frame Request for HDS

```bash
--2013-08-08 22:07:45--
Resolving localhost... ::1, 127.0.0.1
Connecting to localhost|::1|:80... failed: Connection refused.
Connecting to localhost|127.0.0.1|:80... connected.
Proxy request sent, awaiting response... 200 OK
Length: 5011 (4.9K) [application/octet-stream]
Saving to: `MPD'
```

Sample Manifest I-Frame Request for HDS

```bash
--2013-08-08 22:07:55--
http://vos.ipndvr1.com/1886/ndvr/ip/172.22.98.58/hds/Manifest.f4m
Resolving localhost... ::1, 127.0.0.1
Connecting to localhost|::1|:80... failed: Connection refused.
Connecting to localhost|127.0.0.1|:80... connected.
Proxy request sent, awaiting response... 200 OK
Length: 13969 (14K) [application/f4m+xml]
Saving to: `Manifest.f4m'
```

Sample 2x Fast-Forward I-Frame Requests for HDS

The following sample shows that a DCM-produced asset was used with one IDR (random access point) per 2-second ATS fragment.
Sample 8x Fast-Forward I-Frame Requests for HDS

The following sample shows that a DCM-produced asset was used with one IDR (random access point) per 2-second ATS fragment.

Sample 2x Rewind I-Frame Requests for HDS

The following sample shows that a DCM-produced asset was used with one IDR (random access point) per 2-second ATS fragment.

Sample 8x Rewind I-Frame Requests for HDS

The following sample shows that a DCM-produced asset was used with one IDR (random access point) per 2-second ATS fragment.
Admission Control

Different VDS-OS usage scenarios consume different amounts of CPU and RAM. Resources can also vary drastically between similar scenarios.

System resources are influenced by unforeseen runtime events, such as a memory leak. As the leaked memory increases, the number of sessions that VDS-OS can admit decreases.

The admission control algorithm dynamically adapts to different usage scenarios, coding changes, and runtime events, as well as conditions in the Web Engine itself.

VDS-OS supports admission control for both DASH assets and ODE assets. Other assets are not directly accounted for in admission control statistics and are not blocked by admission control.

To account for all of these factors, admission control admits sessions based on new system-wide values, such as CPU utilization and RAM utilization. That is, admission control functions similar to the Service Monitor/Service Router.

The Web Engine already provides an admission control mechanism that performs a number of process-specific control checks, including the Web Engine process memory threshold, file descriptor usage, sessions-per-second ramp up, and total sessions. VDS-OS accepts these Web Engine criteria as both valid and complementary to its own new system-wide criteria.

Table 1-1 shows the admission control criteria.

<table>
<thead>
<tr>
<th>Table 1-1 Admission Control Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage</td>
</tr>
<tr>
<td>Memory Usage</td>
</tr>
<tr>
<td>HTTP Sessions</td>
</tr>
<tr>
<td>FD Usage</td>
</tr>
<tr>
<td>Ramp Up</td>
</tr>
<tr>
<td>Media Assets</td>
</tr>
</tbody>
</table>

There is some overlap between admission control and load threshold, since they factor in memory and CPU utilization when determining whether the system is overloaded. However, admission control uses a weighted moving average that provides a more dynamic and proactive approach to determining overload conditions.
System-Wide Admission Control Criteria

Initially, system-wide criteria are based off of two resource dimensions (average CPU usage and average RAM usage) and across two major Web Engine resources (HTTP Sessions and Media Assets). VDS-OS uses these criteria to determine admission in two ways.

- Admission control imposes a global usage threshold. If either CPU usage or RAM usage for a specific Web Engine resource (such as Sessions or Assets) crosses a utilization boundary (for example, 90% CPU utilization), further resources are not admitted.
- Admission control derives RAM and CPU weights for each resource, based on current usage and on the current number of “active” resources. Admission control uses these values to predict how many new resources can be admitted.

For example, if Web Engine is running with 20% CPU utilization and 100 sessions, admission control might assume that each session requires 0.2% CPU. If the system is configured with a 90% global CPU threshold, admission control allows up to \((90-20) / 0.2\) = 350 additional sessions.

For a low number of resources, resource weights might be too heavy. For example, a system with 20% memory usage and only one Media Asset might result in a 20% weight per asset. If the system had a 90% global threshold, that would mean that only three more assets could be admitted. To avoid that situation, admission control applies a “floor” threshold (for example, 50 assets), such that resource-weighting criteria are enabled only after the floor is exceeded.

Admission Control Averages

Admission control load averages are exponential moving averages (EMAs). EMAs are useful when calculating loads, and are used when calculating the familiar Unix load averages (for example, uptime). EMAs dampen sporadic instantaneous loads.

API Management

The VDS-OS provides HyperText Transport Protocol Secure (HTTPS) web services application programming interfaces (APIs) that comply with the REpresentational State Transfer (REST) standard, Java API for XML RESTful Web Services (JAX-RS), version JSR-311.

For more information, see the Cisco Videoscape Distribution Suite Origin Server Release 2.1.1 API Guide.

Asset Resolution

Each origin service is associated with an Asset Resolver configuration file. The Asset Resolver file contains a set of asset-based rules and actions for request processing. (All of the rules are asset-based, not user-based.) The Web Engine matches each incoming resource URL against the regex pattern defined in each rule in order to deliver assets to requestors.

The VDS-OS supports Asset Resolver for both DASH and ODE applications.

When creating an Asset Resolver, keep the following considerations in mind:

- The Asset Resolver performs CPU-intensive regular expression (regex) operations. Therefore, the number of rules and their order in the Asset Resolver file is critical. For better performance, we recommend that you use as few rules as possible, and make sure that the DASH or ODE rule is the first rule in the file.
The Asset Resolver uses the first matching regex rule. Therefore, rules that include specific regex patterns must come before more generic rules in the file.

For example, rules that include specific keywords must come before those with more generic ones. For HLS, rules for stream manifests must come before rules for variant manifests.

If there is an overlap in URL namespaces for different types of assets (HLS Live, ODE VOD, recording, and so on), which require different Asset Resolver rules, you must create different origin servers to handle the different types of assets. You can then define the rules in separate Asset Resolver files and upload them to different origin services.

If the default Asset Resolver ODE rules match those of native VOD assets, you must either replace the default Asset Resolver or deselect it from the origin service.

For sample Asset Resolver files, including the default Asset Resolver file, see the “Creating Asset Resolver Files” section on page A-1.

### Asset Resolution for ODE

When ODE is enabled, the SetTransformResource Directive contains SourceInfo and PublishInfo.

- SourceInfo provides parameters for the source of the transform.
- PublishInfo provides the publish manifest URL for client.

When an incoming HDS or HLS media request URL matches the regex, the Asset Resolver creates an ODE asset, based on the parameters specified in SourceInfo and PublishInfo. The mpdURL is sent to the DASH media application, and a DASH asset is also created.

- For HLS media assets, the VDS-OS supports either 2-second or 10-second segment durations. The Asset Resolver uses the segmentDuration to specify the expected segment duration, which must match the segment duration of the video source for the DASH application.
- For HDS media assets, the VDS-OS supports only 2-second segment durations.

### Default Asset Resolver File

The VDS-OS provides a default Asset Resolver. The VOSM automatically assigned the default Asset Resolver to an origin server when it is created.

If your URL format and asset storage structure differ from those in the default Asset Resolver, you must customize the Asset Resolver accordingly and reapply it to the origin service.

You can also assign a different Asset Resolver file as the default. For more information, see the “Set a File as the Default” section in the *Cisco Videoscape Distribution Suite Origin Server Release 2.1.1 API Guide*.

**Note**

The current default Asset Resolver file assumes that the CF content is stored on the NAS in the following directory structure for HLS playout: `/sharedDirectory/AssetDirectory/`

This is to identify the asset structure in variant manifest and stream manifest URLs.

Other NAS structures require a separate Asset Resolver file.

HDS and HSS play out correctly for all NAS structures with the default Asset Resolver file.
# Cache-Control Enhancements

- Cache-Control Headers Support, page 1-21
- Support for If-Modified-Since for Native ABR for HLS Live and for HDS, HLS, and HSS VOD, page 1-23
- Support for If-Modified-Since for ODE Playout from CF VOD on the NAS, page 1-25

## Cache-Control Headers Support

The cache-control general-header field is used to specify cache directives that must be obeyed by all caching mechanisms along the request/response chain. The directives specify behavior that prevents caches from adversely interfering with the request or response. These directives override the default caching algorithms. Cache directives are unidirectional, in that the presence of a directive in a request does not imply that the same directive is to be given in the response.

The VDS-OS supports the following tools to set the cache-control headers in the HTTP response for contents.

### Note

Only the **max-age** response cache directive is currently supported.

<table>
<thead>
<tr>
<th>Cache-Control Directive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Cache-Control for ABR VOD Asset</td>
<td>The default cache-control <strong>max-age</strong> is based on the <strong>Content Expiry</strong> field on the Origin Service General Settings page.</td>
</tr>
<tr>
<td>Set Cache-Control for Asset Class Using Asset Resolver</td>
<td>You can override the default cache-control directives using an Asset Resolver file with rules for asset classes.</td>
</tr>
<tr>
<td>Default Cache-Control for HLS Live Asset</td>
<td>For HLS Live assets, you must take special care when setting the cache-control <strong>max-age</strong> for manifest files, which are updated frequently. The following values are used for the different HLS Live files:</td>
</tr>
<tr>
<td></td>
<td>- Stream Manifest File—The stream manifest file is updated every time a segment is added, which is based on the Capture Resource <strong>Arrival Rate</strong> setting. The VDS-OS sets the <strong>Expiry</strong> header, based on when it expects the next update to take place, by adding the <strong>Arrival Rate</strong> to the <strong>Last Modified Time</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Variant Manifest File—The variant manifest file is updated only when a stream is added or removed due to a failure. The VDS-OS sets the <strong>Expiry</strong> header by adding the <strong>Arrival Rate</strong> to the <strong>Current Time</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Segment File—The life of a live segment file is the size of the <strong>Time Shift Window</strong>. The VDS-OS sets the <strong>Expiry</strong> header by adding the <strong>Time Shift Window</strong> to the <strong>Last Modified Time</strong>.</td>
</tr>
</tbody>
</table>
The following table shows the expected **max-age** in the cache-control header, based on the type of playout.

<table>
<thead>
<tr>
<th>Playout Type</th>
<th>Variant Manifest</th>
<th>Stream Manifest</th>
<th>Fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Republish Live (NAS)</td>
<td>Arrival rate</td>
<td>Arrival rate—time on disk</td>
<td>Remaining DVR window</td>
</tr>
<tr>
<td>Republish Live (InMemory)</td>
<td>Arrival rate</td>
<td>Arrival rate—time in disk</td>
<td>Remaining DVR window</td>
</tr>
<tr>
<td>Passthrough Live (NAS)</td>
<td>Arrival rate</td>
<td>Arrival rate—time on disk</td>
<td>Remaining DVR window</td>
</tr>
<tr>
<td>Passthrough Live (InMemory)</td>
<td>Arrival rate</td>
<td>Arrival rate—time in disk</td>
<td>Remaining DVR window</td>
</tr>
<tr>
<td>HLS VOD (Completed recording)</td>
<td>Content expiry</td>
<td>Content expiry</td>
<td>Content expiry</td>
</tr>
<tr>
<td>HLS VOD (InProgress)</td>
<td>Arrival rate</td>
<td>Arrival rate—time on disk</td>
<td>Content expiry</td>
</tr>
<tr>
<td>ODE VOD (Through content expiry)</td>
<td>Content expiry</td>
<td>Content expiry</td>
<td>Content expiry</td>
</tr>
<tr>
<td>ODE VOD (Through Asset Resolver)</td>
<td>Asset Resolver configured value</td>
<td>Asset Resolver configured value</td>
<td>Asset Resolver configured value</td>
</tr>
</tbody>
</table>

**Note**

When both configurations are present, the Asset Resolver configuration has priority.

For more information about configuring the **max-age** for a cache-control header using the VOSM, see the “General Settings” section on page 6-3.

To override the default cache-control directives using an Asset Resolver file, specify the **max-age**, in seconds, for a set of assets that match a set of regular-expression (regex) rules. The **max-age** can apply to an entire origin service (that is, it applies to all requests) or it can apply to a subset of requests, such as m3u8 index files or HLS fragment requests.

### Using Asset Resolver To Set Max-Age for an Origin Service Example 1

```xml
<Rule_Actions>
  <Rule_AssetResolve nametag="global_caching_headers_rule" matchGroup="grp1, grp2" protocol="http">  
    <SetMetaData>
      <DeliveryHeader>
        <SetCachingHeader>
          <Cache-Control>
            <Max-Age>300000</Max-Age>
          </Cache-Control>
        </SetCachingHeader>
      </DeliveryHeader>
    </SetMetaData>
  </Rule_AssetResolve>
</Rule_Actions>
```

### Using Asset Resolver To Set Max-Age for an Origin Service Example 2

**Note**

With the current Asset Resolver design, if you set **max-age** for HLS .ts alone, the same **max-age** also applies to all other HSS and HDS fragments. If that is unacceptable, you must set a specific **max-age** for HDS and HSS fragments.
Support for If-Modified-Since for Native ABR for HLS Live and for HDS, HLS, and HSS VOD

The If-Modified-Since HTTP header is sent by end-clients or caches to revalidate the request. The server responds with one of the following codes:

- 200 (OK) — If the page has been modified
- 304 (Not modified) — If the page has not been modified
The If-Modified-Since HTTP header is supported by the VDS-OS for the following types of ABR playout:

- Native HLS Live manifest and segments (pass-through or republish with NAS or In-Memory)
- Native HLS time-shift TV (TSTV) asset
- Native HLS, HSS, HDS VOD asset

An If-Modified-Since request can be sent in any type of HTTP requests, such as a GET request, a HEAD request, or a Range request. For each request, the VDS-OS compares the date and time specified in the If-Modified-Since to the Last-Modified date and time of the resource, and sends the appropriate 200 or 304 response.

**Sample If-Modified-Since HTTP Header 1**

The following header shows an HTTP GET request for which the If-Modified-Since time is greater than the Last-Modified time for the HLS segment file.


HTTP/1.1 304 Not Modified
Connection: Keep-Alive
Keep-Alive: timeout=15
Accept-Ranges: bytes
Cache-Control: max-age=500
Last-Modified: Wed, 22 May 2013 17:52:28 GMT
Content-Type: video/MP2T
Server: Cisco-VOS
Content-Length: 0
Date: Wed, 22 May 2013 17:46:58 GMT

**Sample If-Modified-Since HTTP Header 2**

The following header shows an HTTP GET Range request for which the If-Modified-Since time is greater than the Last-Modified time for the HLS stream manifest file.

debugshell# curl -i --header 'Range:bytes=10-20' --header 'If-Modified-Since: Tue, 21 May 2014 11:16:00 GMT' http://vos.ruixli.com/ruixli_hls/hls/high3000.m3u8

HTTP/1.1 304 Not Modified
Connection: Keep-Alive
Keep-Alive: timeout=15
Accept-Ranges: bytes
Cache-Control: max-age=4
Last-Modified: Wed, 22 May 2013 17:48:52 GMT
Content-Type: application/x-mpegURL
Server: Cisco-VOS
Content-Length: 0
Date: Wed, 22 May 2013 17:48:58 GMT

**Sample If-Modified-Since HTTP Header 3**

The following header shows an HTTP GET request for which the If-Modified-Since time is less than the Last-Modified time for the HLS manifest file.

debugshell# curl -i --header 'If-Modified-Since: Tue, 21 May 2013 11:16:00 GMT' http://vos.ruixli.com/ruixli_hls/hls/high3000.m3u8

HTTP/1.1 200 OK
Connection: Keep-Alive
Sample If-Modified-Since HTTP Header 4

The following header shows an HTTP GET request for which the If-Modified-Since time is greater that the Last-Modified time for a large HSS video file. (HSS audio and video fragment requests with If-Modified-Since are handled the same way.)

```
debugshell# curl -I --header 'If-Modified-Since: Wed, 30 May 2012 21:45:00 GMT' http://vos.ruixli.com/hssvod/BigBuckBunny_477.ismv
HTTP/1.1 304 Not Modified
Connection: Keep-Alive
Keep-Alive: timeout=15
Accept-Ranges: bytes
Content-Length: 47374020
Last-Modified: Sat, 29 Sep 2012 00:37:04 GMT
Content-Type: application/octet-stream
Server: Cisco-VOS
Date: Thu, 30 May 2013 22:44:24 GMT
```

Support for If-Modified-Since for ODE Playout from CF VOD on the NAS

For ODE HDS, HLS, and HSS resources from a CF VOD asset on the NAS, the Last-Modified time for the CF asset is compared to the If-Modified-Since time.

External Storage Devices—NAS

Network Attached Storage (NAS), a file-level storage connected to a network, is supported by VDS-OS. NAS file-systems can be accessed using the NFS protocol.

A NAS may be traditional or clustered. A clustered NAS is a NAS that uses a distributed file-system running simultaneously on multiple servers. The key difference between a clustered and traditional NAS is the ability to distribute (also known as stripe) data and metadata across the cluster nodes or storage devices. Clustered NAS, like a traditional one, still provides unified access to the files from any of the cluster nodes, unrelated to the actual location of the data. Any of the storage servers in the cluster can be used to mount a file-system volume.

Note

Performance and efficiency of the VDS-OS system may suffer if network storage is accessed using a high-latency or low-bandwidth wide-area network (WAN). To monitor storage latency and bandwidth, use the diagnostic counters and statistics pertaining to network storage.

The following assumptions are made about network storage topology for VDS-OS:

- There may be multiple independent NAS storage clusters in a VDS-OS deployment, spread across different locations.
- Storage clusters and VDS-OS nodes accessing storage within those clusters may be in different locations.
- Network storage cluster in one location may be accessible from VDS-OS nodes that are both co-located and in other locations.

**Note**

Network traffic performance can be impacted by too small a value for the TCP parameter: `net.inet.tcp.rexmit_slop`. If it is determined that network throughput performance is impacted, the `net.inet.tcp.rexmit_slop` value on the Network Storage Share server should be reviewed.

## High Availability—Resiliency and Redundancy

A VDS-OS that is designed with full redundancy and no single point of failure includes redundant VOSMs and Service Routers.

### Service Engine Redundancy

Keepalive messages from that Service Engine. When a new request comes in, the Service Router does not redirect the request to that Service Engine; instead, it redirects the request to other Service Engines within the same origin service. All the existing sessions on the failed Service Engine terminate and the affected end users must re-request the content.

### Service Router Redundancy

The VOSM can operate in two different roles: primary and standby. The primary role is the default. There can only be one primary active in the VDS-OS network; however, you can have any number of VOSMs operating in standby to provide redundancy and failover capability.

Primary and standby VOSMs must be running the same version of software. We recommend that the standby VOSM be upgraded first, followed by the primary VOSM.

The VOSM design principle is that the management device is never in the service playout path. When the VOSM fails, the rest of the VDS-OS continues to operate. A VOSM failure does not affect any services delivered to end users, and all content sourcing continues. The only negative effect is that the administrator cannot change configurations or monitor the VDS-OS. As soon as a failure to connect to the VOSM is noticed, the administrator can activate the standby VOSM. For information on making the standby VOSM the primary VOSM, see the “Changing a Standby to a Primary VOSM” section on page 4-12.

## Operational Enhancements

- Cross-Domain Policy File for HDS Playback, page 1-26
- Customized Asset URLs, page 1-27

### Cross-Domain Policy File for HDS Playback

The cross-domain policy file is an XML document that grants permission to a web client, such as the Adobe Flash Player or Adobe Reader, enabling the client to handle data across multiple domains.
When a client hosts content from a particular source domain, and that content directs requests toward a domain other than its own, the remote domain must host a cross-domain policy file in order to grant access to the source domain and allow the client to continue with the transaction. Cross-domain policy files grant read access to data, permit the client to include custom headers in cross-domain requests, and grant permission for socket-based connections.

During playback, the HDS player first initiates a request to the VDS-OS for the cross-domain policy file. To upload a cross-domain policy file for each origin service, select the **Cross-Domain File Registration** option on the VOSM **System > Configuration** page.

### Customized Asset URLs

The VDS-OS keeps a table of active assets for in-media applications (HDS, HLS, HSS, and DASH). Each asset has a unique asset URL that helps identify the asset to which the client request URL should attach.

The Asset Resolver `assetUrl` attribute identifies the asset URL, which is used as the base URL for the asset or profile and ODE. You can add an `assetUrl` attribute for `PublishInfo` to specify the asset URL for the client request URL.

**Note**

The generated asset URL must be unique for each asset.

For ODE, part of the asset URI is received as the `vm_id`. ODE then uses the `vm_id` to generate the variant manifest file.

### Sample URL for HLS

Given the following incoming manifest URL:

http://fqdn/rec_id.m3u8

The Manifest URL is:

http://fqdn/rec_id.m3u8

The AssetUrl URL can be:

http://fqdn/rec_id

The prefix ID `rec_id` is passed to the ODE, which generates the variant manifest with the following content:

rec_id/bitrate.m3u8

The client’s profile manifest URL is:

http://fqdn/rec_id/bitrate.m3u8

The profile manifest file contains the following media file:

bitrate/number.ts

The client’s media data URL is:

http://fqdn/rec_id/bitrate/number.ts

### Sample Asset Resolver Rule for HLS Media Data File for the Sample URL

```
<SetTransformResource matchRegex = "(.*/.*/(.*)/(.*).ts")>
```
Sample URL with Current VDS-OS Supported

Given the following incoming manifest URL:

http://fqdn/rec_id/anything/index.m3u8

The Manifest URL is:

http://fqdn/rec_id/anything/index.m3u8

The AssetUrl URL can be:

http://fqdn/rec_id/anything

No specified prefix ID is sent to the ODE. The ODE generates the variant manifest file, which contains the following content:

bitrate.m3u8

The client’s profile manifest URL is:

http://fqdn/rec_id/anything/bitrate.m3u8

The profile manifest file contains the following media file:

bitrate/number.ts

The client’s media data URL is:

http://fqdn/rec_id/anything/bitrate/number.ts

Sample URL for HDS

Given the following incoming manifest URL:

http://fqdn/rec_id.m3u8

The Manifest URL is:

http://fqdn/rec_id.f4m

The AssetUrl URL can be:

http://fqdn/rec_id

The prefix ID /rec_id is passed to the ODE, which generates the manifest with the following media_url template:

rec_id/media_file_template_prefix

The client’s media data URL is:

http://fqdn/rec_id/media_file_name
Display Usage for TMPFS and NSS Usage

The `show vos usage` command displays usage information for the VDS-OS, including:

- Network Storage Shares (NSS) usage for every Network File System (NFS) in the SE
- Temporary file storage (TMPFS) usage

For more information, see the description of the `show vos` command in the *Cisco Videoscape Distribution Suite Origin Server Release 2.1.1 Command Reference*.

Alarm Enhancements

Alarms 560015 (nas_threshold) and 1100002 (channel_failure) have been added.

Alarms 9000015 (WritingToNasHasFailed) and 1100001 (channel_partial_failure) have been enhanced.

For more information, see the alarm descriptions in the *Cisco Videoscape Distribution Suite Origin Server Release 2.1.1 Alarms and Error Messages Guide*.

Origin Services

Content origination is performed in the context of origin services. An origin service is a construct that is used to map the content and channels to a set of Service Engines that work together to originate content for the content distribution systems. Multiple origin services can coexist in the same VDS-OS system. The origin services are used to capture content (for example, fragments, streams, and so on) for playout to CDNs.

An origin service is restricted to a single location.

The built-in service routing and service definition capabilities of VDS-OS enable operators to manage services instead of servers. VDS-OS is used to provision, manage, and operate origin servers as a single unified service that has built-in fault tolerance and proximity-based server selection functions.

Following are the different properties of the origin services:

- **Service identification**—Each origin service is uniquely identified with an origin service name and a Service Routing Domain Name (SRDN), which is a fully-qualified domain name (FQDN). The names and the SRDNs must not overlap with other services in the system.
  
  The URL for all of the resources delivered from this service have the SRDN as the domain part. The template for the URL is: `http://<SRDN>/<Content_Specific_Identifiers>`

  For example, if the SRDN is `origin.tveverywhere.net`, then following are some URLs of resources that might be delivered from this service:

  `http://origin.tveverywhere.net/nbc/nbc1/live.m3u8`
  `http://origin.tveverywhere.net/nbc/nbc1.isml/Manifest`

- **Content types**—Any static HTTP resource that conforms to the HTTP specification can be delivered from an origin service. However, the service is optimized around Adaptive Media Streaming (HDS [VOD only], HLS, and HSS [VOD only]). The Media Delivery Applications are used to deliver the ABR content. For more information about Media Delivery Applications, see the “Media Delivery Applications” section on page 1-33.
Feature Support

Chapter 1      Product Overview

Note Each ABR content (VOD, live, or Live-to-VOD) is treated as a resource.

- **Content Resources**—Content resources consist of the following:
  - **Capture Resource**—Defines input streams the system should expect for a channel of every ABR type. VDS-OS supports HLS capture resources. The format-specific capture sources for the same channel have the same channel identification (there is a base URI that points to the channel).
  - **Linear Publish Resource**—Publishes the captured channel to the CDN systems. Multiple publish resources can use a common capture resource. For example, HLS Live streams for a channel (capture resource) can be published to the end users with two publish resources (for example, a smart-phone profile and a tablet-profile). The publish resource can use all or a subset of streams defined in the capture resource. The live channel publish resources also have settings that define the in-session time-shift windows and start and end times.
  - **VOD Publish Resource**—Publishes VOD content that is prerecorded into the authoritative storage (Network Storage Shares). There is no special configuration for this, the system automatically creates the VOD publish resource based on the client request.
  - **Time-Shift Recording and Publish Resources**—Records and publishes content in support of TSTV services. The TSTV publish resources are created based on operator-specified schedules (using the Capture Schedule XML file) or can be created dynamically on the Acquisition nodes based on a control command from an external session manager. When the end-time of a capture event has been reached, the content produced during the capture is converted to a VOD asset that can be delivered by the VOD publish resources. These schedules may change, so there is a polling interval specified to refresh the Capture Schedule XML file periodically.

- **Multi-Tenancy**—Multiple origin services can be provisioned in the system. The Service Engines assigned to an origin service can be shared with other origin services. The Service Engines are inherently multi-tenant and can host multiple origin services concurrently. The number of origin services that are supported by a Service Engine are dependent on the peak origination workflow requirements across the different services.

- **Service participants and routing**—Service Engines participate in the content origination workflows. One or more Service Engines can be assigned to an origin service

  The Service Routers are delegated to be the authoritative DNS server for the SRDN. Service Routers are primarily used to select origin server instances based on various policies such as proximity, server load, and availability thresholds.

  **Note** VDS-OS supports only DNS-based routing.

- **CDN integration**—VDS-OS can work with any CDN that can download content using HTTP as specified in RFC 2616. The CDN nodes do not know the difference between an origin service and an external origin server; both of them would export the same protocol interface.

- **Playout QoS settings**—During content playout, all resources played out from the VDS-OS system can be marked with specific DSCP markings. A configuration for QoS setting can be specified for each origin service.

- **Asset Resolver rules**—The Asset Resolver rules can help resolve incoming fragment, manifest, and other types of requests to the publish resource that can deliver the request. Given a URL, the action to be performed and the parameters associated with that action can be specified in the Asset Resolver XML file.
Live Channels

Each origin service can support the playout of one or more live channels. Each live channel describes the following:

- ABR format-specific publish resources
- Capture resources
- Pointer to the live Capture Schedules (for live-to-VOD conversion)
- Acquisition nodes that can acquire the live streams from external encapsulators

Each live channel is configured with at least one Acquisition node.

Network Storage Shares

The Network Storage Shares (NSS) define the external storage directories that are mounted by the Service Engines by way of the origin services. Each share is mapped to a mount point name that can be derived from the incoming request URLs. The NSSs are the export file systems from the NAS servers.

**Note**

At least one Network Storage Share must be assigned to an origin service and a live channel.

Content Sourcing

Content sourcing describes the process of acquiring content in the origin service. The sourcing setup workflows can differ based on the solution (linear, VOD, and TSTV).

Table 1-2 describes the different potential sources of content and the protocols and transports used for the different scenarios.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Sources</th>
<th>Signaling Protocol</th>
<th>Data Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed linear capture with external encapsulator (linear, TSTV)</td>
<td>External encapsulator</td>
<td>Not applicable</td>
<td>HLS</td>
</tr>
<tr>
<td>VOD content origination (NSS read)</td>
<td>External storage servers</td>
<td>NFS</td>
<td>NFS</td>
</tr>
</tbody>
</table>

VOD content origination (NSS read) is sourced from external storage servers and uses NFS as the signaling protocol and as the data protocol.

VOD content is packaged and stored in its native format (also known as post-encapsulated format) into Network Storage Shares along with the control and distribution metadata. The operator’s content management system is responsible for storing the content. The Service Engines can mount the NAS volumes and deliver the requested objects from the stored containers.

Live content is encapsulated for each playout technology and received by the VDS-OS Acquisition nodes by way of HTTP POST.

VDS-OS Acquisition nodes record content and publish it.
Content Playout

The playout process of the VDS-OS system delivers content to requesting clients (CDN nodes). All Service Engines that are part of the origin service are able to playout VOD content as long as the content is completely available as a recording. Live content is streamed by way of linear capture resources. For content playout, the origin service must be configured and the Service Router must be notified about the origin service and its participating Service Engines by way of the Coverage Zone file.

VOSM

The VDS-OS consists of a Virtual Origin System Manager (VOSM), one or more Service Engines (SEs), and one Service Router (SR). For full redundancy, a VDS-OS would include an additional VOSM and Service Router.

The VOSM is a secure Web browser-based user interface. It is a centralized system management device that allows an administrator to configure, manage, and monitor origin services as well as all devices in the VDS-OS.

APIs are provided for backoffice integration with the VOSM.

Authentication, Authorization, and Accounting

The VOSM uses HTTPS to secure the administrator's session. Multiple users can perform administrative operations by using the VOSM. The administrator can configure certain users to have either view-only rights for monitoring the VDS-OS, or full rights that allow configuration changes as well as monitoring capabilities.

User accounts and groups can be added to the VOSM and given roles and rights for accessing configuration information. It is also possible to segregate and group objects and give access to a limited group of users.

User authentication can be configured to use RADIUS and TACACS+ servers when available, otherwise the VOSM provides its own authentication server.

The VDS-OS-wide policy and status information is maintained in a relational database on the VOSM. This information is propagated and synchronized with all devices in the VDS-OS network.

As part of the network management process, the administrator can perform basic administration operations on the VOSM database, including backup and restore.

Device Management

The VOSM sends device configuration changes to the selected device or group of devices once the change has been submitted. The device sends any configuration changes that were made locally to the VOSM, and also provides periodic status information.

Devices can be organized into user-defined device groups, which allow administrators to apply configuration changes and perform other group operations on multiple devices simultaneously. Because a device can belong to multiple device groups, this reduces the management overhead of the administrator. Device groups allow for a single instance of management thus eliminating the need to repeat the same step for each device.

The VOSM also provides an automated workflow to apply software upgrades to the devices in a device group.
Origin Services Management

The VOSM provides the configuration and monitoring of origin services, which defines how content is sourced, recorded, and played out. The VOSM provides the Service Engines with information about the origin services and which Service Engines are participating in the origin service.

Service Engine (SE)

The Service Engine forms the basic building block for most of the content origination and distribution services. The Service Engine handles content sourcing, content distribution within the VDS-OS, and content playout.

Service Engines can be organized into user-defined device groups to allow administrators to apply configuration changes and perform other group operations on multiple devices simultaneously. One device may belong to multiple device groups.

Media Delivery Applications

Media Delivery Applications are software modules that are implemented on top of the Web Engine. The Media Delivery Applications perform the following functions:

- Source content and recording incoming linear streams
- Locate requested content from a stored location based on the requested URL
- Implement delivery technology specific behaviors (for example, fragment chaining, manifest creation, and so on)
- Implement Live-to-VOD content creation

The Media Delivery Application integrates and abstracts the functions such as content sourcing, recording, re-encapsulation, and playout. VDS-OS supports the following Media Delivery Applications:

- HDS Media Application (VOD)
- HLS Media Application (VOD, Live, and Live-to-VOD)
- HSS Media Application (VOD)

Linear Stream Acquisition

Linear stream acquisition is a function that is used to acquire the linear streams from the encapsulator.

Capture Controller

The Capture Controller is a software subsystem that controls the Web Engine Media Delivery Applications. It is used for all of the live content captures, including live-to-VOD conversion. The Web Engine implements the recording and playout of these captures.

The Capture Controller performs the following functions:

- Channel Management—Processes live channel configuration received from the VOSM and maintains the states of the live channels and capture resources.
- Interface Monitor—Examines the interfaces to obtain details about on-going and completed capture sessions.
Feature Support

- Capture Scheduler—Stores live and live-to-VOD events for all channels based on the Capture Schedule XML file and schedules these events to the Web Engine.
- Capture Life Cycle Management—Maintains the state of the live sessions, as well as live-to-VOD recording sessions.
- Channel Operation—Handles control messages to start, stop, or restart a publish resource or a capture resource.

Web Engine

The Web Engine is used to implement the recording and playout of the recorded assets.

All HTTP requests that are redirected to a Service Engine by the Service Router are handled by the Web Engine. The Web Engine, using HTTP, can serve the request from locally stored content in the VDS-OS.

An HTTP request that reaches the Service Engine can either be from a Service Router redirect or from a direct proxy request.

Note

The Web Engine supports the following:
- Optimization for small content objects
- Optimization of Adaptive Bitrate Streaming for Move, Apple iPhone, and Smooth HD
- MP3 live streaming
- Interoperation with Apple’s media stream segmenter, as well as Microsoft’s Internet Information Services 7.0 (IIS7.0) Smooth Streaming.
  - Apple’s media stream segmenter segments encoded media into separate files for streaming to iPhones.
  - Microsoft’s IIS Smooth Streaming offers adaptive streaming of high-definition (HD) content.
- HTTP GET, HTTP POST, and HEAD request methods.

Service Router (SR)

The Service Router for the VDS-OS system is used to load-balance incoming requests to different origin server instances. It is also used to provide redundancy within a VDS-OS service location as well as select between multiple sites.

The Service Router can be configured only as the Request Routing Engine.

Note

In describing the Service Router functions, the term “client” refers to the CDN Acquisition node.

Request Routing Engine

Request Routing Engine is used to load-balance incoming requests to different origin server instances. It is also used to provide redundancy within a VDS-OS Service location as well as select between multiple sites.
The Request Routing Engine supports DNS-based routing and RFQDN redirection. All the Service Engines registered and activated in the system send heartbeat messages to the Service Router for load monitoring purposes.

**Routing Redirection**

The Request Routing Engine uses DNS-based redirection as the routing method.

When DNS-based routing is configured, the Service Router routes the request based on the DNS proxy that is used by the downstream CDN Acquisition nodes. The IP address of the actual CDN node is not carried in the DNS request.

---

**Note**

When DNS-based redirection is used, for application-level requests, last-resort redirection is supported. However, on the DNS plane, an A record with the last-resort domain name or IP address is not returned.

DNS-based routing is enabled by default. When DNS-based redirection is enabled, the DNS proxy contacts the Request Routing Engine to resolve the requested URL, the Request Routing Engine determines which Service Engine to redirect the request to based on load, location, and other heuristics, and directly returns the appropriate Service Engine’s IP address instead of the Service Router’s IP address. The CDN Acquisition node then directly requests the content from the Service Engine instead of the Service Router.

---

**Note**

The TTL for the DNS proxy requests is one second. A one-second TTL ensures that the DNS proxy keeps sending requests to the Request Routing Engine, which in turn causes the Request Routing Engine to determine the best Service Engine at that point in time, and not to redirect the request to the same SE.

---

**Note**

There is a certain side effect in adopting this approach. When creating the Coverage Zone file, the IP address of the DNS proxy needs to be used for the CDN Acquisition node IP address range.

To configure DNS-based redirection, use the `service-router redirect-mode dns-redirect` command.

```
service-router redirect-mode dns-redirect {all | domain domain}
```

The following example enables DNS-based redirection with the voslive.com domain as the domain used to redirect all requests to:

```
SR(config)# service-router redirect-mode dns-redirect domain voslive.com
```

To display information about the redirect mode, use the `show service-router redirect-mode` command. To display the statistics, use the `show statistics service-router summary` command and the `show statistics service-router se` command. The output for the DNS-Based Redirection feature is listed as DNS Requests. In addition to these two show commands, there is also the `show statistics service-router dns` command.

**Routing Methods**

The Request Routing Engine chooses the best Service Engine based on whether the Service Engine is participating in the origin service for which the origin server matches that of the requested domain, and whether the Service Engine is assigned to serve the CDN Acquisition node’s network region, as defined in the Coverage Zone file.
If the CDN Acquisition node’s subnet is not defined in the Coverage Zone file, the Request Routing Engine checks the following routing methods to see if they are configured:

- **Load-Based Routing**
- **Zero-IP Based Configuration**
- **Last-Resort Routing**
- **Service Aware Routing**

**Note**

The keepalive messages between the Service Router and Service Engine are transmitted and received on port 2323. However, the software interoperates with older software releases that do not use port 2323 for keepalive messages. If a firewall is configured between the Service Engine and the Service Router, port 2323 (UDP) must be opened for the keepalive message to go through.

**Load-Based Routing**

Load-based routing is enabled by default and cannot be disabled. In load-based routing, the routing decision is made according to the capacity and load of the Service Engines.

The load of the Service Engine is determined by different parameters, such as processor usage, memory usage, disk usage, and so on. The current load is compared with the thresholds configured for the Service Engine. If a threshold has been exceeded for a Service Engine it is excluded from the routing table.

**Note**

Bursts of traffic (such as 800 connections per second) may cause the Web Engine to become disabled before it can transmit notification to the SR that the threshold has been reached.

**Zero-IP Based Configuration**

The zero-ip based configuration is a catch-all condition for routing. It can be used in combination with proximity-based routing and location-based routing. If an SE cannot be found through location-based routing or proximity-based routing, the zero-ip based configuration is taken into account for selecting an SE.

The zero-ip based configuration is a network entry in the Coverage Zone file defined as 0.0.0.0/0. It matches all client subnets. If the client subnet does not match any of the other network entries in the Coverage Zone file and a 0.0.0.0/0 network entry exists, then the SEs listed for that entry are considered for serving the client request.

**Last-Resort Routing**

Last-resort routing is useful when all Service Engines have exceeded their thresholds or all Service Engines in the domain are offline, or the client is unknown. If last-resort routing is configured, the Request Routing Engine redirects requests to a configurable alternate domain or translator response domain when all Service Engines serving a client network region are unavailable, or the client is unknown. A client is considered unknown if the client’s IP address is not part of a subnet range listed in the Coverage Zone file, or part of a defined geographical area (for location-based routing) listed in the Coverage Zone file.

**Note**

When DNS-based redirection is used, for application-level requests, last-resort redirection is supported. However, on the DNS plane, an A record with the last-resort domain name or IP address is not returned.
Last-resort routing works dynamically. When the load of one or more Service Engines in the original host domain is reduced below threshold limits or the Service Engines are reactivated, new requests are routed to the original host domain automatically.

Last-resort routing allows redirecting a request to an alternate domain or content origin (if Enable Origin Server Redirect is enabled) for one of the following conditions:

- All SEs in the origin service have exceeded their thresholds
- All SEs in the origin service are unavailable or no SEs are assigned to the origin service
- Client is unknown

**Note**

Unknown clients are only redirected to the alternate domain (last-resort domain) or translator response domain when the **Allow Redirect All Client Request** check box is checked or the equivalent `service-router last-resort domain <RFQDN> allow all` command is entered.

If the last-resort domain or the translator response domain are not configured and the Service Engine thresholds are exceeded, known client requests are redirected to a content origin and unknown clients either receive an error URL (if the Error Domain and Error Filename fields are configured), or a 404 “not found” message.

Last-resort routing could also be configured to redirect a client to an error domain and filename.

The URL translator provides a way to dynamically translate the client request URL in order to redirect the client to a different CDN. With the URL translator option, the following occurs if the SR uses last-resort routing for a client request:

1. The SR contacts the third-party URL translator through the Web Service API. The Web Service API is described in the *Cisco Videoscape Distribution Suite Origin Service 2.1.1 API Guide*.
2. The third-party URL translator sends the translated URL in the response to the SR.
3. The SR sends a 302 redirect message to the client with the translated URL it received from the third-party URL translator.

The timeout for connecting to the URL translator server is 500 milliseconds. There are no retries if the URL translator cannot be reached.

If there is no configuration on the URL translator for the requested domain or the connection timeout threshold has been reached, the SR last-resort routing falls back to the alternate domain configuration.

**Service Aware Routing**

Service-aware routing is enabled by default and cannot be disabled. In service aware routing, the Request Routing Engine redirects the request to the Service Engine that has not exceeded its threshold as configured. See the “Setting Service Monitor Thresholds” section on page 5-52 for more information.

When a request reaches the Service Router, the Request Routing Engine generates a hash from the URI. The Request Routing Engine first generates a list of Service Engines to best serve the request based on service aware routing. The Request Routing Engine then reorders the list based on the hash and selects the best Service Engine. Because the hash generated for the same URI is equal, typically the same Service Engine is selected. If the Service Engine is overloaded, the next Service Engine in the list is selected.

**Note**

For service aware routing, if a threshold is exceeded for all Service Engines, the Request Routing Engine redirects the client request to the origin server if a last-resort alternate domain is not configured. If a last-resort alternate domain is configured, the alternate domain takes precedence over the origin server.
Request Routing Engine Workflow of Coverage Zone Routing

Keepalive message to the Service Router on a periodic interval, which consists of information about the SE resources (such as disk, CPU, memory, and network interface usage). The Request Routing Engine uses the Service Engine’s load and liveness information for generating the routes.

VDS-OS can have more than one Service Router to support Service Router failover. In line with failover, the DNS server should be configured with multiple Service Routers for the same routed FQDN.

Note

DNS entries for all FQDNs must be delegated to the Service Router. In the DNS server’s database file, a name server record must be entered for each FQDN that routes to the Service Router.

Unified Routing Table

The unified routing table uses one global route context for all domains, with all SEs from the Coverage Zone file added to one set of route tables. This is a good option if the VDS-OS serves a number of different domains (configured as origin services), but uses the same set of SEs for the different origin services (domains). By enabling the unified routing table in this scenario, the memory usage on the SR is reduced.

If the VDS-OS is configured with fewer domains or the SEs are not all serving the same domains, then the memory usage is not impacted as much, and not enabling unified routing may be a better option.

The unified routing table option is disabled by default. To enable unified routing on the SR, enter the service-router unified-routing-table enable command.

Note

Not enabling the unified routing table increases the memory usage on the SR. Make sure the memory usage does not exceed the recommended limit, which is 1.5 GB when the SR is running with a load and no configuration changes are occurring.

Coverage Zone File

In Figure 1-4, all Service Engines serve Coverage Zone 1, and Service Engine 1 is specifically associated with Coverage Zone 2, a subset of Coverage Zone 1.

Figure 1-4  Coverage Zone Example
If a coverage zone is served by multiple Service Engines, all Service Engines are put in the routing table. The metric value, entered in the Coverage Zone file, indicates the proximity of the Service Engine to the client. When multiple Service Engines serving a coverage zone are on the same subnet and have the same metric value, and load-based routing is not enabled, the Request Routing Engine uses round-robin routing to redirect the client. If load-based routing is enabled, the load of the Service Engines are used to determine the best Service Engine to redirect the client.

**Device Modes**

The VDS-OS uses the device modes (VOSM, Service Engine, and Service Router) and applies the software functions that are required to perform content origination. The device mode configuration determines the set of software functions that can be activated in the device.

- **Virtual Origin System Manager**—Manages all the devices (Service Engines and Service Routers). In addition to the element management functions, the VOSM is also used to configure the system topology and services required for content origination. The VOSM supports a graphical user interface (GUI) and Web Services APIs for provisioning and monitoring VDS-OS. The VOSM provides device and service alarm information and reports statistical information on VDS-OS functionality.

- **Service Engine**—Provides all HTTP content origination functions, satisfying content requests from the CDN or directly from clients, sourcing live content from HTTP ABR encoders and encapsulators, and sourcing VOD or recorded content from the operator’s NAS subsystem. The Service Engine provides necessary ABR segmentation and fragmentation to satisfy requests for HTTP ABR content.

- **Service Router**—Provides optimal origin server selection and load-balancing enabling a highly resilient origin solution. Resolves DNS queries for the origin service domain names. The queries are resolved to the IP address of the Service Engines (SEs). The Service Router (SR) takes into account the device load, availability, and proximity of the SEs (with reference to the requesting DNS proxy) when resolving the DNS queries.

VDS-OS is implemented as a set of networked devices organized in a well-defined topology. The topology consists of a single location.

**System Topology**

The VDS-OS is a single-tier solution. The topology is defined as a set of stand-alone locations that are not inter-connected by way of the parent and child relationship.

Locations imply the topological proximity of the nodes that belong to that location. The relationship among locations guides the flow of content between the locations. Each location is configured with a unique-name that describes the location.

During the registration and activation process, all devices are assigned to a location. A device cannot be part of multiple locations.

For origin services, the locations are organized as a set of stand-alone locations. Each location can correspond to a data center (also known as a super headend, or SHE) location and these locations are not interconnected in the topology. There is no inter-location content movement through the VDS-OS nodes. Origin services cannot span more than one location in this release.

Based on the topology, different network zones can be created (manually) in the Service Router’s Coverage Zone file to indicate the subset of nodes that are exposed to the downstream CDN nodes and to associate a location based on the subnet and proximity of the downstream CDN nodes.
Figure 1-5 shows the major elements of a VDS-OS system. How content flows, from source to recording within the VDS-OS, to playout to CDNs, is dictated by the defined origin services. Live playout flows directly from the Acquisition nodes to the Playout nodes. VOD content is retrieved from the Network Storage Shares by the Playout nodes.

**Figure 1-5  High-Level View of the Cisco VDS-OS**

Service Engines have two roles:
- Acquisition nodes
- Playout nodes

**Acquisition Nodes**

Acquisition nodes receive content from live sources and facilitate redundancy within the origin tier for live and recording content.

Linear content is acquired by the Acquisition nodes from external encapsulators. The acquired linear content can be received into the Network Storage Share devices associated with the origin service. At least one Acquisition node must be assigned to a live channel.

VOD content is not acquired by the Acquisition nodes directly. Instead, the Cisco Media Suite (CMS) directly ingests the content into the Network Storage Shares.

At least one Network Storage Share must be assigned to an origin service and a live channel.

**Playout Nodes**

All nodes in an origin service that deliver content to the CDN are Playout nodes. An Acquisition node can also be a Playout node; however, the live channel redundancy capability is reduced. The Playout nodes are defined in the Coverage Zone file for the Service Router that resolves the DNS requests for that domain. The Playout nodes also mount the Network Storage Shares and can play the content out that is completely received and available in the storage system. For all content that is not completely received
(for example, Live-to-VOD captures that are not complete), the Playout nodes dynamically fetch the content from the Acquisition node. The set of Acquisition nodes for a Live-to-VOD capture and live channels are well known to all Service Engines participating in the origin service.

**Virtual Machine (VM) Support**

An SE can boot up as a VM in any hardware platform that meets the minimum resource requirements. VDS-OS support for VMs requires the following software programs and releases:

- VMware ESX hypervisor version 5.1 or later, running on the server
- VMware vCenter version 5.0 or later

  We recommend that you use vCenter to deploy VMs. Using vCenter to configure a static IP address, a VOSM primary management IP address, and other basic VM parameters prior to deployment ensures that the VM will be functional when it first boots up.

- VMware vSphere version 5.0 or later

  You can use vSphere to monitor and control basic features on the VM, but advanced features require vCenter.

Use the Open Virtual Appliance (OVA) to deploy the VM.

For more information about deploying a VM, including configuring the UCS B200 for load balancing, see the “Deploying the VDS-OS As a Virtual Machine” chapter.

**Provisioning of New Features**

- You can configure VDS-OS with multiple SEs.
- The Service Router coverage zone file is configured to include the SEs that are used to receive the request from the end-clients.
- The Asset Resolver configuration file includes a special directive that can derive the URL for the recordings or the URL for the recorder discovery function.
Figure 1-6 shows the sequence of operations to provision VDS-OS features.

**Figure 1-6  Provisioning Sequence of Operations**

![Provisioning Sequence of Operations Diagram](image)
CHAPTER 2

Installing the VDS-OS on UCS Platforms

This chapter provides detailed instructions for installing the VDS-OS software on Cisco Unified Computing System (UCS) platforms.

- Installing the Hardware, page 2-2
- Connecting a UCS Cisco Integrated Management Controller (CIMC) Port, page 2-2
- Configuring the CIMC, page 2-3
- Configuring the BIOS, page 2-5
- Configuring the BIOS to Boot from a CD-ROM, page 2-6
- Configuring Remote Presence, page 2-7
- Setting Up a UCS B200 for the VDS-OS Software using the GUI, page 2-8
- Installing the VDS-OS Software, page 2-25
  - Mounting a Virtual ISO and Rebooting the UCS, page 2-25
  - Connecting to a CIMC Serial Console and Installing the Software, page 2-27
  - Checking the BIOS Boot Order, page 2-27
  - Un-Mapping the ISO File, page 2-27
  - Exiting the VDS-OS Installer and Rebooting the UCS, page 2-27
  - Setting Up the VDS-OS Software, page 2-28

For information about deploying VDS-OS as a virtual machine (VM), see the “Deploying the VDS-OS As a Virtual Machine” chapter.

Note
Your screen shots might differ from those shown in this chapter, depending on the UCS platform that you are using.
Installing the Hardware

Install a UCS platform (blade or server).


  The UCS B200 blade server uses the backplane to connect the Ethernet NIC (eNIC) to the internal switch (IOM), and the hardware does not provide an LED to indicate that the NIC is up or connected. Therefore, the `show_mapping.sh nic` script does not make the port LED blink.

- If you are installing a UCS C200 in a rack, see the “Installing the Server” section in the Cisco UCS C200 Installation and Service Guide.

- If you are installing a UCS C210 in a rack, see the “Installing the Server” section of the Cisco UCS C210 Installation and Service Guide.

When installing a UCS C200 or C210, remember to:

- Populate disk bays with disk drives.
- Connect the power cable to the server.

Connecting a UCS Cisco Integrated Management Controller (CIMC) Port

The UCS CIMC is an integrated management functionality that enables you to perform the following tasks:

- Configure BIOS settings through HTTP.
- Remotely power-cycle the device.
- Control the keyboard, video, and mouse (KVM) through Java.
- Mount a virtual CD-ROM/block device/FDD to the system.
- Connect and perform various other operations.

The VDS-OS software installation requires a minimum of two IP configurations, each with an Ethernet cable attached to a switch—one to the CIMC UCS Management port and the other to one of the 6 NICs. The Gigabit Ethernet interfaces are shared between the CIMC and the UCS for UCS devices. Do not change the default values for duplex, speed, auto negotiation, and advertising.

**Step 1** Attach an Ethernet cable to the Management port of the UCS server. The Management port is labeled “M” (the port with the yellow Ethernet cable connection shown below).
Step 2  To bring up the CIMC, connect a USB keyboard and VGA monitor.
   a. Attach the USB keyboard cable to the USB port.
   b. Attach the VGA monitor cable to the monitor port.

Configuring the CIMC

Note  We recommend that you use Safari or Internet Explorer when working with the CIMC. Other browsers, such as Chrome or Internet Explorer, might experience problems when the CIMC executes random web-based Java code on your workstation.

Step 1  Turn on power to the UCS. When the Cisco splash screen appears, press F8.
The CIMC Configuration Utility screen is displayed.

```
NIC Properties
NIC mode
Dedicated: [X]
Shared LOM: [X]
Cisco Card: [X]
IPV4 (Basic)
DHCP enabled: [X]
CIMC IP: 172.22.68.39
Subnetmask: 255.255.255.128
Gateway: 172.22.68.1
ULAN (Advanced)
ULAN enabled: [X]
ULAN ID: 1
Priority: 0

......
```

**Step 2** On the CIMC configuration screen:
- a. Confirm that the NIC Mode and NIC Redundancy settings are correct. If they are not set correctly, the CIMC uses network ports other than the dedicated CIMC port, which can cause problems.
- b. Enter your IP, subnet mask, and gateway addresses.
- c. Enter and re-enter a default password.
- d. Press the **Space Bar** to apply the new IP configuration.

**Step 3** Verify that the CIMC interface can be reached by pinging the IP address associated with the CIMC port. If an error occurs, make sure the Ethernet cable is securely connected to the CIMC management port.

**Step 4** Verify that the CIMC Web Interface is available by pointing your Web browser to its IP address:

```
https://<CIMC IP>
```

**Step 5** When the CIMC login screen is displayed, log in using **admin** as the username and the default password you set in the “Configuring the CIMC” section.

**Step 6** When the CIMC Configuration Utility screen is displayed, press **F10** to save the configuration.
Configuring the BIOS

**Step 1**  On the CIMC login screen, log in using **admin** as the username and the default password you set in the “Configuring the CIMC” section. The Server Summary pane is displayed.

**Step 2**  Click **BIOS** in the left pane to display the BIOS pane.
Configuring the BIOS to Boot from a CD-ROM

**Step 1**  
In the BIOS pane, click **Configure Boot Order**.

**Step 2**  
When the Configure Boot Order popup is displayed:  
- Select **CD-ROM** and **HDD** in the Device Types box.  
- Click **Add** to add **CD-ROM** and **HDD** to the Boot Order box.  
- Use the Up and Down arrows to move the CD-ROM to the first position (the first device from which to boot).  
- Click **Apply**.
Step 3  Verify that CD-ROM and HDD appear in the Configured Boot Order pane in the correct order, then click Save Changes.

### Configuring Remote Presence

**Step 1**  In the left pane, click Remote Presence to display the Remote Presence screen.

**Step 2**  Select the Virtual KVM tab.

a. Check the Enabled check box.

b. Set Max Sessions to 4.

c. Set Remote Port to 2068.

d. Click Save Changes.

**Step 3**  Select the Virtual Media tab.

a. Check the Enabled check box.

b. Click Save Changes.

**Step 4**  Select the Serial over LAN tab.

a. Check the Enabled check box.

b. Select Baud Rate value of 9600 bps.

c. Click Save Changes.
Setting Up a UCS B200 for the VDS-OS Software using the GUI

Step 1  Connect the UCS to the Fabric Interconnect and power up all of the devices.
Step 2  Connect the UCS B200 to the Fabric Interconnect console port and assign the management IP address.
Step 3  Access the Cisco UCS Manager using your web browser and the IP address of the UCS Manager.

Step 4  Click Launch UCS Manager and log in with admin as the username and password as the password.
**Step 5** Configure the default adapter policy settings as shown in the following figure. To access the Ethernet Adapter Policy, choose **Servers > Policies > Root > Adapter Policies > Create Ethernet Adapter Policy**.

![Properties for Ethernet Adapter Policy default](image)

**Step 6** A blade server requires a service policy to achieve external communication through the mezzanine card. To configure a service pool policy, use the following procedure:

a. To use a server pool, associate the service profile with the pool. The UCS manager automatically selects an available compute node from the pool.

b. Set the **Filter** to **All**.

![UCS Manager interface](image)
c. Configure the server pool policy.

d. Name the server pool.
e. Add the server to the pool.
**Step 7** Configure the server port. Server ports allow communication between servers and the Fabric Interconnect.

**Step 8** Configure the uplink port. Uplink ports allow communication between the Fabric Interconnect and the backbone network.
Chapter 2  Installing the VDS-OS on UCS Platforms

Setting Up a UCS B200 for the VDS-OS Software using the GUI

Step 9  Configure the interface for the uplink port.

Step 10  Configure the service profile. Select Create Service Profile (expert) and define a profile name.
Step 11  Enter a name for the service profile and click **Create UUID Suffix Pool**.

Step 12  Enter a name for the UUID suffix pool.

Step 13  Click **Add UUID Blocks**.
Step 14  Create a block of UUID suffixes. UUIDs are globally unique identifiers for each compute node on a network.

Step 15  Add the newly created block of UUID suffixes.

Step 16  Add the UUID pool to the service profile.
Step 17 Configure the local disk policy. Click Storage.

Note The CMP application requires Windows 2008 on the local disk (bare metal installation).

Step 18 Click Create Local Disk Configuration Policy.

Step 19 Enter a name and select RAID 0 Striped as the Mode.

Step 20 Add the storage policy to the service profile. In the example in the following figure, the storage policy is VMS-Storage.

Step 21 Select no VHBA (the device is not connected to a SAN).
**Step 22** Click Networking.

**Step 23** For **How would you like to configure LAN connectivity**, select **Expert**.
Step 24  Click **Add** to create a virtual NIC (vNIC).

![Create vNIC](image1)

**Step 25**  Click **Create MAC Pool**. The vNIC uses MAC addresses from the MAC pool.

![Create MAC Pool](image2)

**Step 26**  Click **Add MAC Addresses** to assign a block of MAC addresses to the MAC pool.

![Add MAC Addresses](image3)
Step 27 Click **Add** to add the block of addresses.

Step 28 Assign the MAC addresses to the vNIC, then click **OK**.
The Networking page displays the MAC address pool.

Step 29  Click Server Boot Order.
Step 30  Configure the boot policy. The boot order is **CD-ROM then Local Disk**.

Step 31  Add the boot policy to the service profile.
Step 32 Click **Maintenance Policy** and select the default.

Step 33 Click **Server Assignment** to assign the server to the service profile. Apply the server policy to the service profile.
**Step 34**  
After the service profile is created, associate the service profile.
Chapter 2  Installing the VDS-OS on UCS Platforms

Setting Up a UCS B200 for the VDS-OS Software using the GUI
Installing the VDS-OS Software

Download the VDS-OS ISO file (rescue-cdrom.iso) to a workstation that is used to connect to the CIMC, then mount the ISO file as a Virtual Media. Once CIMC connectivity is established, you can install the software using the rescue-cdrom.iso file.

Mounting a Virtual ISO and Rebooting the UCS

Step 1  Access the CIMC Server Summary pane, then click Launch KVM Console. Accept any security warnings or certificate requests that are displayed.

Step 2  When the KVM console window is displayed, which can take up to 5 minutes, select the VM tab.

Step 3  Click Add Image, then browse your workstation's file system, select rescue image and click Open.
Step 4  Check the **Mapped** check box in the main table.

Note  Do not exit from the window. KVM must remain open to keep the virtual media mapped and to successfully boot from the virtual media.

Step 5  Reboot the UCS by accessing the CIMC Server Summary pane and clicking **Power Cycle Server**.
Connecting to a CIMC Serial Console and Installing the Software

The CIMC allows you to connect to a device’s serial console through a CIMC SSH session. This feature, known as Serial over LAN, eliminates the need for an external serial console server.

To connect to the CIMC serial console using SSH, use the following procedure:

**Step 1** Enter the IP address of the server, with admin as the username.
```
user1$ ssh -l admin 172.22.68.39
```

**Step 2** Enter the default password you set in the “Configuring the CIMC” section:
```
admin@172.22.68.39's password: XXXX
```
```
ucs-server#
```

**Step 3** Enter the following command:
```
ucs-server# connect host
```

**Step 4** When the VDS-OS installer launches, enter option 2 (Install all software) and press Enter.

**Step 5** Confirm that you wish to continue by entering Y. The software begins the installation process.

**Step 6** Do not select any of the options at this stage. Proceed to the “Checking the BIOS Boot Order” section.

Checking the BIOS Boot Order

In the CIMC BIOS pane, confirm that the BIOS boot order matches the order that you configured in the “Configuring the BIOS” and “Configuring the BIOS to Boot from a CD-ROM” sections. If you experience boot issues, you can change the boot order.

Un-Mapping the ISO File

**Step 1** In the KVM tab of the KVM console window, un-check the Mapped check box.

**Step 2** When prompted to confirm your request, select Yes.

**Step 3** Click Exit to close the KVM console window.

Exiting the VDS-OS Installer and Rebooting the UCS

Select option 3 on the Installer to exit the program and reboot the UCS.

After rebooting, information about the VDS-OS software is displayed.

You can also power-cycle the server by clicking Power Cycle Server in the CIMC Server Summary pane.
Chapter 2      Installing the VDS-OS on UCS Platforms

Setting Up the VDS-OS Software

**Step 1**  Keep the SSH connection open. If you are disconnected, use an SSH client to connect to the CIMC on the UCS with `admin` as the username.

```
ssh -l admin 172.22.68.39
```

**Step 2**  When prompted, enter the default password you set in the “Configuring the CIMC” section.

**Step 3**  Enter the following command:

```
ucs-server# connect host
```

The following message appears:

CISCO Serial Over LAN:
Close Network Connection to Exit
Press the 'Enter' key

**Step 4**  When prompted, enter `admin` as the username and the default password.

The VDS-OS application launches and the following prompt is displayed:

```
NO-HOSTNAME#
```

**Step 5**  Enter the `setup` command to launch the VDS-OS Setup utility:

```
NO-HOSTNAME# setup
```

The Setup utility takes you through the initial configuration settings for a VDS-OS device. You are prompted to specify the device mode (SE, SR, or VOSM) and to configure the interface to be used for VDS-OS communication.
Deploying the VDS-OS As a Virtual Machine

This chapter provides detailed instructions for deploying VDS-OS as a virtual machine (VM). VDS-OS provides the basic VM configuration automatically when you deploy through an OVA image using vSphere, PowerCLI, or similar software, connected through a vCenter or connected directly to an ESXi host.

- Deploying a VM Using vSphere, page 3-1
  - Deploying a VM Using vCenter (Recommended), page 3-1
  - Deploying a Stand-Alone VM Without vCenter, page 3-4
- Deploying a VM Using a Power CLI Script, page 3-6
- Configuring the UCS B200 for Load Balancing, page 3-7
  - Add a vNIC Adapter Policy, page 3-7
  - Add a vNIC to the Host, page 3-7
  - Configure the vNIC, page 3-7

Deploying a VM Using vSphere

Log in to vSphere using:

- The IP address, or hostname and domain, of the vCenter that manages the hypervisor host
- The IP address, or hostname and domain, of the hypervisor

Deploying a VM Using vCenter (Recommended)

Step 1 From the File menu, select Deploy OVF Template, then select the OVA file.
Step 2 Accept the license agreement.
Step 3 Enter the name of the VM, its location (data-center), and its data-store.
Step 4 Select the deployment configuration.
**Step 5** Select the disk format. We recommend *Thick Provision Eager Zeroed*, but consult your lab administrator if you are not sure.

**Step 6** Select the OVF properties to customize the VM deployment.

Configure the device:

- **a.** Enter the hostname.

  **Note** Do not enter the fully qualified domain name (FQDN) in the Hostname field. Enter only the local hostname. For example, if the FQDN is vosm.cisco.com, enter only *vosm*.

- **b.** Select a management role. This is required for VOSM mode.

- **c.** Enter the primary management IP (the VOSM IP address). This is required for VDS-OS mode and for the VOSM Standby role.

- **d.** Select the checkbox to enable CMS.

  If you do not select the checkbox, the property is ignored and the CLI takes precedence.

Configure the network parameters:

- **a.** Enter the IP address and subnet mask for **Network Adapter 1**.

  If you do not enter an IP address or subnet mask, the configuration on the first interface defaults to *ip address dhcp*.

  If you set the hostname of a device before powering it on, you can use DHCP to provide a specific IP address. When it powers up, the device can then communicate with a DHCP server and obtain the IP address.

- **b.** Enter the default gateway.

- **c.** Select the checkbox to set Network Adapter 1 as the primary interface.

  If you do not select the checkbox, the property is ignored and the CLI takes precedence.

  You can assign the first interface for which you assign an IP address as the primary interface.

  You cannot assign the primary interface if the first interface is configured for DHCP instead of static IP address.

**Step 7** Click **Finish** to deploy the OVA and create the VM.

**Note** It can take up to 15 minutes to create the VM.

After the VM has been successfully created, if you need to fine-tune the VM, right-click the VM, then select **Edit Settings** . . .
Step 8

Power on the VM.

The OVF properties are applied only when you first boot up. To modify the properties, use the CLI to customize the VM.

---

**Step 1**
Select Open Console and log in using *admin* as the username and the default password.

**Step 2**
Verify network connectivity by pinging the default gateway IP address.

**Step 3**
Verify that you can ping the VM from your workstation.

**Step 4**
Log in to the VM using *admin* as the username and the default password.

**Note**
To release the cursor, press CTRL+ALT (Windows) or CTRL+OPTION (Mac).

**Step 5**
Verify that the device mode is set to *virtual-origin-system-manager*, by entering the following commands:

```
vosm# show device-mode current
Current device mode: virtual-origin-system-manager
```

If it is not set to *virtual-origin-system-manager*, set it and reload the server, by entering the following commands:

```
vosm(config)# device mode virtual-origin-system-manager
vosm# reload
vosm# reload?[confirm]
```

**Step 6**
Verify that the primary interface is set to *tenGigabitEthernet 1/0* using the show run command.

**Note**
If you set Network Adapter 1 as the primary interface when you configured the network parameters, the primary interface should be set correctly.

**Step 7**
Set the NTP server and the DNS server.

```
vosm(config)# ntp server ?
Hostname or A.B.C.D or X:X:X:X: :X  NTP server name or IP address (maximum of 4)
```

```
vosm(config)# ip name-server ?
A.B.C.D or X:X:X:X: :X  Domain server IP address (maximum of 8)
```

**Step 8**
Verify that the CMS is running.

```
vosm# show cms processes
Service cms_httpd is running
Service cms_vosm is running
```

If it is not running, enable it.

```
vosm(config)# cms enable
vosm# show cms info
VDS-OS information :
Model              = GENERIC
Node Id            = 173
Device Mode        = vosm
Current VOSM role  = Primary
CMS services information :
```

---
Deploying a VM Using vSphere

Step 9 You can now access the GUI from your browser.

Step 10 Enter configuration mode.

Step 11 Enter the interface IP addresses.

To enable the DHCP server to choose the IP addresses, enter `ip address dhcp`.

For DHCP IP addresses obtained via DHCP client IDs, enter `ip address dhcp client-id id`, and configure the DHCP server to expect this DHCP client ID.

Step 12 Enter the default gateway: `ip default-gateway ip`

Step 13 Enable Telnet, if required.

Step 14 Enter the VOSM IP address.

Step 15 Select the checkbox to enable CMS.

Step 16 Enter the hostname.

Step 17 Enter the device mode.

Step 18 Restart the VM.

After the above steps, the VM is up and running and can be reached (via VOSM web interface/ telnet) for further application-level configuration.

Deploying a Stand-Alone VM Without vCenter

Step 1 From the File menu, select Deploy OVF Template, then select the OVA file.

Step 2 Accept the license agreement.

Step 3 Enter the name of the VM, its location (data-center), and its data-store.

Step 4 Select the deployment configuration.

<table>
<thead>
<tr>
<th>VM Product</th>
<th>Cores</th>
<th>RAM</th>
<th>Hard Disk</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal VDS-OS</td>
<td>4</td>
<td>16 GB</td>
<td>64 GB</td>
<td>Ten 10GEthernet</td>
</tr>
<tr>
<td>Standard VDS-OS</td>
<td>8</td>
<td>28 GB</td>
<td>64 GB</td>
<td>Ten 10GEthernet</td>
</tr>
<tr>
<td>VOSM</td>
<td>4</td>
<td>4 GB</td>
<td>64 GB</td>
<td>Ten 10GEthernet</td>
</tr>
</tbody>
</table>

Step 5 Select the disk format. We recommend Thick Provision Eager Zeroed, but consult your lab administrator if you are not sure.

Step 6 Click Finish to deploy the OVA and create the VM.

Note It can take up to 15 minutes to create the VM.

After the VM has been successfully created, if you need to fine-tune the VM, right-click the VM, then select Edit Settings . . .
Step 7 Power on the VM.

To modify the properties the first time, use the CLI to customize the VM.

Step 1 Select Open Console and log in using admin as the username and the default password.
Step 2 Verify network connectivity by pinging the default gateway IP address.
Step 3 Verify that you can ping the VM from your workstation.
Step 4 Log in to the VM using admin as the username and the default password.

Note To release the cursor, press CTRL+ALT (Windows) or CTRL+OPTION (Mac).

Step 5 Verify that the device mode is set to virtual-origin-system-manager. If it is not set to virtual-origin-system-manager, set it and reload the server.
Step 6 Verify that the primary interface is set to tenGigabitEthernet 1/0 using the show run command.

Note If you set Network Adapter 1 as the primary interface when you configured the network parameters, the primary interface should be set correctly.

Step 7 Set the NTP server and the DNS server.
Step 8 Verify that the CMS is running. If it is not running, enable it.
Step 9 You can now access the GUI from your browser.
Step 10 Enter configuration mode.
Step 11 Enter the interface IP addresses.
   To enable the DHCP server to choose the IP addresses, enter ip address dhcp.
   For DHCP IP addresses obtained via DHCP client IDs, enter ip address dhcp client-id id, and configure the DHCP server to expect this DHCP client ID.
Step 12 Enter the default gateway: ip default-gateway ip
Step 13 Enable Telnet, if required.
Step 14 Enter the VOSM IP address.
Step 15 Select the checkbox to enable CMS.
Step 16 Verify that the default gateway can be reached.

After the above steps, the VM is up and running and can be reached (via VOSM web interface/ telnet) for further application-level configuration.

You can further modify the configuration, through the console or via Telnet into the VM, by entering the appropriate configuration in configuration mode.
Deploying a VM Using a Power CLI Script

You can use PowerCLI scripts to customize the VM properties. For example, the following script sets the device-mode property to SE. You can use similar scripts to set other properties.

```powershell
# Sample Script for setting OVA properties

Function Wait-vShieldBoot {
    do {
        $VM = Get-VM $VosHostName
        Sleep 5
    } until ($VM.ToolsStatus -eq "toolsOK")
}

$Newproperty = New-VIProperty -Name ToolsStatus -ObjectType VirtualMachine -Value {
    param($vm)
    $vm.ExtensionData.Guest.ToolsStatus
} -Force

# Set parameters
$VosOVA = "C:\Users\bhagatyj\Documents\work\vmware\packaging\ovfs\vos_ovf.ova"
$VosHostName = "Vos-120"
vShieldFQDN = "vshield.virtu-al.local"
$VosDS = "phy-ds-2"
$VosUser = "admin"
$VosPass = "default"
vCenter = "deming-vc.cisco.com"
vCUsername = "root"
vCPass = "vmware"

# Execution starts here
Write-Host "Connecting to vCenter"
$Connect = Connect-VIServer $vCenter -User $vcUsername -Password $vcPass
Write-Host "Importing the OVF file"
$va = Import-VApp -Name $VosHostName -Datastore $VosDS -VMHost bhagatyj-ucs2.cisco.com -Source $VosOVA
$Vm = Get-VM -Name $VosHostName
$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.VAppConfig = New-Object VMWare.Vim.VmConfigSpec
$newProp = New-Object VMWare.Vim.VAppPropertySpec
$newProp.Operation = "edit"
$prop = $Vm.ExtensionData.Config.VAppConfig.Property | where {$_.Id -eq "devicemode"}
$prop.Value = "se"
$newProp.Info = $prop
$spec.VAppConfig.Property += $newProp
$Vm.ExtensionData.ReconfigVM($spec)
Write-Host "Starting the vShield VM"
$Start = Start-VM $VosHostName -Confirm:$false
#Write-Host "Waiting until the vShield VM has started"
#Wait-vShieldBoot

Write-Host "Configuration Complete"
```
Configuring the UCS B200 for Load Balancing

To enable adapter load balancing, use the UCSM GUI to configure the UCS B200 to expose the vNICs to the host server.

Note
This procedure applies whether the UCSB is stand-alone or is communicating with the Fabric Interconnect using the GUI.

Add a vNIC Adapter Policy

To optimize load balancing among all virtual CPU cores, you must first create a new adapter policy.

Step 1 Select the Servers tab.
Step 2 In the left pane, expand Servers > Policies > root > Adapter Policies.
Step 3 In the right pane, click Add. The Create Ethernet Adapter Policy window is displayed.
Step 4 Enter a name for the adapter policy, such as Load-Balanced_32.
Step 5 Under Resources, set the following values for the policy:
   a. Set Transient Queues to 1.
   b. Set the number of Receive Queues to \( n \), where \( n \) is the number of virtual CPU cores. For example, for 32 virtual CPU cores, set Receive Queues to 32.
   c. Set Completion Queues to \( n+1 \), or 33 in our example.
   d. Set Interrupts to \( n+3 \), or 35 in our example.
Step 6 Under Options, enable Received Side Scaling and set the Fallback Timeout to 2 seconds.

Add a vNIC to the Host

Step 1 Select the Servers tab.
Step 2 In the left pane, select the vNICs entry under the service profile of the host server.
Step 3 In the right pane, click Add.

Configure the vNIC

Step 1 On the Create vNIC page, enter a name for the vNIC.
Step 2 Enter a MAC address.
Step 3 At the bottom of the page, select the Adapter Policy that you created earlier, such as Load-Balanced_32.
Step 4  Save the policy changes and reboot when prompted to do so.
Getting Started with Configuration

This chapter discusses initial device configuration, logging into and navigating the Virtual Origin System Manager (VOSM), and a typical VDS-OS configuration workflow. This chapter presents the following major topics:

- Initial Device Configuration, page 4-1
- Logging In To the VOSM, page 4-1
- Activating and Synchronizing the Devices, page 4-3
- Navigating the VOSM, page 4-7
- Configuring Primary and Standby VOSMs, page 4-11
- Typical Configuration Workflow, page 4-13

Initial Device Configuration

You must initially configure the Cisco hardware models that run the VDS-OS software before they can participate in the VDS-OS network. The Cisco hardware model that runs the VOSM must be initialized first so that the hardware models running the Service Engine (SE) and Service Router (SR) can register with it. For more information about initially configuring the hardware models, see the Release Notes for the Cisco Media Origination Suite Release 2.0. See the “Related Publications” section on page xii.

After you have initially configured your hardware, you must activate the SEs and SRs and configure the internal clocks by using the VOSM. See the “Activating and Synchronizing the Devices” section on page 4-3 for more information.

Logging In To the VOSM

To log in to the VOSM, do the following:

**Step 1**
Using your web browser, enter the IP address of your VOSM and port 8443.

>Note VDS-OS supports Internet Explorer version 6 or higher, and Mozilla Firefox version 3.6 or higher.

For example, if the IP address of your VOSM is 192.168.0.236, enter:
https://192.168.0.236:8443

The Security Alert message is displayed.

**Note** If you are using Mozilla Firefox version 3.6 or higher as your web browser, you need to add the VOSM IP address to the exception list. After entering the VOSM IP address with port 8443, Firefox displays a Secure Connection Failed message with a link stating “Or you can add an exception.” Click this link, then click Add Exception. The Add Security Exception dialog box is displayed. Click Get Certificate, and then click Confirm Security Exception. The VOSM IP address has been added to the exception list and you no longer get the Secure Connection Failed message.

Sometimes the VOSM is not initially accessible from a web browser. If this occurs you must disable and re-enable the Centralized Management System (CMS). Log in to the CLI for the VOSM, and enter the global configuration command `no cms enable` followed by `cms enable`.

**Step 2** Click Yes to accept the security certificate. The Login page is displayed (Figure 4-1).

**Figure 4-1 VOSM Login Page**

Step 3 Enter the username and password and click Login. The VOSM home page is displayed.

The built-in username is `admin` and the initial password is `default`.

**Note** We strongly recommend that you change the built-in admin password as soon as possible. To do so, log in to the CLI of the VOSM device, and use the `username admin password password` global configuration command.

**Note** If the default username and password have been changed by another VOSM administrator, you need to get the new username and password.
Activating and Synchronizing the Devices

The VDS-OS administrator approves a device by making it active. This security feature prevents unauthorized devices from joining the VDS-OS.

Caution

All devices must be synchronized with each other for the VDS-OS to function properly.

Synchronization ensures accurate timestamps in all the logs and accuracy in caching decisions determined by If Modified Since (IMS) lookups. Using Network Time Protocol (NTP) to synchronize the devices in the VDS-OS is the best practice.

Note

If the network is not configured with NTP, then every device in the VDS-OS must be configured with exactly the same time and time zone. We recommend that you use an NTP server for network synchronization.

Activating and Setting NTP for Each Device

Tip

To navigate within the VOSM, click one of the tabs (for example, Devices) and then one of the tab options (for example Locations). Navigational directions in procedures are written in the following way: Devices > Devices > Assignments > Device Groups

Note

From the Devices table, you can activate all inactive devices by clicking the Activate All Inactive SEs icon. See the “Activating All Inactive Service Engines” section on page 4-5.

To activate and synchronize a Service Engine (SE) or Service Router (SR), do the following:

Step 1

From the VOSM home page, choose Devices > Devices. The Devices table is displayed (Figure 4-2) listing all of the registered SEs and SRs.
Step 2  Click the **Edit** icon next to the device name. The Devices home page is displayed.

**Note**  If the device you want to activate is not listed in the Devices Table, restart the CMS for that device by telnetting to it and entering `no cms enable` followed by `cms enable` in global configuration mode.

Step 3  Click **Activate** in the Devices home page. The Location dialog box is displayed (Figure 4-3).

Step 4  Create or choose a location. To activate an SE, you need to assign it to a location.

Because the standby VOSM is global to the VDS-OS network, it does not need to be assigned to a location.

You have the following options in creating or choosing a location:

a. If you have already created locations, you can choose a location from the **Location** drop-down list.
b. To create a default location, which can be edited later, check the Create a New location check box. A default location is created with the following name: <SE-name>-location. From the Parent of the New Location drop-down list, choose a parent for this location.

For information about creating locations, see the “Configuring Locations” section on page 5-1.

Step 5  Click Apply and Activate.

The Status of the device shows “pending” until the device is fully activated. This may take a few minutes.

Step 6  To display the top-level Table of Contents, click the Show All button above the Contents pane.

Step 7  From the left-panel menu, select General Settings > Network > NTP. The NTP Settings page is displayed.

Step 8  Check the Enable check box and enter the IP address or hostname of each NTP server. Use a space to separate each server.

Step 9  Click Submit to save your settings.

The activation and NTP server settings must be completed for each SE, SR, and standby VOSM.

Tip
For a quick way to get to other SEs, click the Display All Devices icon located to the left of the Expand All button. This icon toggles between the Display All Devices and Menu icons.

For more detailed information about configuring locations, activating devices, and configuring NTP servers, see the following sections:

- Configuring Locations, page 5-1
- Activating a Service Engine, page 5-9
- Configuring NTP, page 5-35

Activating All Inactive Service Engines

To activate all inactive SEs, do the following:

Step 1  From the VOSM home page, choose Device > Devices and click the Activate All Inactive SEs icon. See Figure 4-4.

Figure 4-4  Devices Table Page—Activate All Inactive Service Engines
The Location Choice page is displayed (Figure 4-5).

**Figure 4-5 Location Choice Page**

![Location Choice Page](image)

**Step 2** In the Location Choice page, click either **Select an Existing Location for All Inactive SEs** or **Create a New Location for Each Inactive SE**.

If you are creating a new location, you can select a parent location, or leave the default of “none.”

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

The Status in the Devices Table for all the inactive SEs shows “pending” until the devices have been fully activated.

**Note** All devices activated in this way need to have the NTP settings configured. See Step 6 through Step 9 in the “Activating and Setting NTP for Each Device” section on page 4-3.
Navigating the VOSM

Figure 4-6 shows the different elements of the VOSM.

Figure 4-6  VOSM User Interface

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Left panel menu</td>
<td><strong>5</strong></td>
<td>System Status bar</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Tab options</td>
<td><strong>6</strong></td>
<td>Page</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Tabs</td>
<td><strong>7</strong></td>
<td>Submit and Cancel buttons</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Task bar</td>
<td><strong>8</strong></td>
<td>Tools (Home, Help, and Logout)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The System Status bar, tabs, tab options, and tools are accessible from any page in the VOSM. The left panel menu changes depending on which tab and tab option you choose.

Devices, Services, and Other Tables

The Devices Table page shows all the devices registered in the VOSM. Figure 4-7 shows an example of the Devices Table page. A table is displayed for each of the following tab options:

- Devices (from Devices tab)
- Device Groups (from Devices tab)
- Locations (from Devices tab)
• Virtual Origin Services (from Services tab)
• Live Video (from Services tab)

**Figure 4-7 Devices Table Page**

![Devices Table Page](image)

You can sort the information in the table by clicking on any column title. The table can be sorted in ascending or descending order for each column. The task bar options provide other table manipulations, including filtering, refreshing the table, viewing all items, and printing.

The bottom of the table lists the page number and the total number of pages, as well as how many items are showing out of the total number of items.

The table defaults to listing ten rows. You can change the number of rows shown by clicking the Rows drop-down list.

To get more information on an item or to configure an item, click the **Edit** icon to the left of the item name. To create a new item, click the **Create New** icon in the task bar.

**Devices Home Page**

The Devices home page provides information about the device, as well as the ability to perform the following tasks:

• Activate the device
• Update the device software
• Assign the device to baseline groups

From the Devices home page you can access the origin services and device groups the device is assigned to, by clicking the appropriate link. All origin services, or device groups (depending on which link you clicked), configured in your VDS-OS are displayed. Through this page, you can assign the device to additional origin services or device groups by clicking the icon next to the applicable origin services or device groups and submitting your selection.

The Devices home page offers detailed bandwidth and bytes-served graphs with detailed reports for each.
The left panel menu has two toggle buttons: Show Basic/Show All and Expand All/Collapse All.

- **Show All**  
  Shows all the menu items in the menu.

- **Show Basic**  
  Shows only the Device home menu item.

- **Expand All**  
  Shows every menu and submenu.

- **Collapse All**  
  Shows only the top-level menu items.

**Task Bar**

The task bar displays information about the page you are on and provides associated tasks. All task bar icons, as well as other icons, have labels that are displayed when you roll over the icon with your mouse pointer.

Any icon used in a procedure is referenced by the rollover label; for example, **Create New** is the rollover label for the following icon:

Table 4-1 describes the icons available in the VOSM.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Activates all inactive Service Engines." /></td>
<td>Activates all inactive Service Engines.</td>
</tr>
<tr>
<td><img src="image" alt="Displays devices." /></td>
<td>Displays devices.</td>
</tr>
<tr>
<td><img src="image" alt="Displays left-panel menu." /></td>
<td>Displays left-panel menu.</td>
</tr>
<tr>
<td><img src="image" alt="Deactivate the device." /></td>
<td>Deactivates the device.</td>
</tr>
<tr>
<td><img src="image" alt="Updates application statistics." /></td>
<td>Updates application statistics.</td>
</tr>
<tr>
<td><img src="image" alt="Forces refresh of replication information or process content changes." /></td>
<td>Forces refresh of replication information or process content changes.</td>
</tr>
<tr>
<td><img src="image" alt="Goes back to Replication Status page." /></td>
<td>Goes back to Replication Status page.</td>
</tr>
<tr>
<td><img src="image" alt="Forces full database update." /></td>
<td>Forces full database update.</td>
</tr>
<tr>
<td><img src="image" alt="Forces settings on SEs in group." /></td>
<td>Forces settings on SEs in group.</td>
</tr>
<tr>
<td><img src="image" alt="Forces the group settings." /></td>
<td>Forces the group settings.</td>
</tr>
</tbody>
</table>
### Chapter 4      Getting Started with Configuration

Table 4-1  **VOSM Icons (continued)**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Views read-only items.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>Creates a new item.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>Edits an item.</td>
</tr>
<tr>
<td><img src="image4" alt="Icon" /></td>
<td>Deletes an item.</td>
</tr>
<tr>
<td><img src="image5" alt="Icon" /></td>
<td>Adds a content item for acquisition.</td>
</tr>
<tr>
<td><img src="image6" alt="Icon" /></td>
<td>Deletes a selected item.</td>
</tr>
<tr>
<td><img src="image7" alt="Icon" /></td>
<td>Manages between host and proxy servers for content acquisition.</td>
</tr>
<tr>
<td><img src="image8" alt="Icon" /></td>
<td>Saves to disk.</td>
</tr>
<tr>
<td><img src="image9" alt="Icon" /></td>
<td>Views complete URL (+) or view (-) partial URL that is used to acquire content.</td>
</tr>
<tr>
<td><img src="image10" alt="Icon" /></td>
<td>Exports a table to a comma-separated value (CSV) file.</td>
</tr>
<tr>
<td><img src="image11" alt="Icon" /></td>
<td>Creates a filtered table. Filter the table based on the field values.</td>
</tr>
<tr>
<td><img src="image12" alt="Icon" /></td>
<td>Displays a graph.</td>
</tr>
<tr>
<td><img src="image13" alt="Icon" /></td>
<td>Applies the default settings to the device.</td>
</tr>
<tr>
<td><img src="image14" alt="Icon" /></td>
<td>Overrides the group settings on the device.</td>
</tr>
<tr>
<td><img src="image15" alt="Icon" /></td>
<td>Views all table entries. Click this icon to view all entries after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image16" alt="Icon" /></td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td><img src="image17" alt="Icon" /></td>
<td>Reboots the device.</td>
</tr>
<tr>
<td><img src="image18" alt="Icon" /></td>
<td>Prints the current window.</td>
</tr>
<tr>
<td><img src="image19" alt="Icon" /></td>
<td>Assigns all items to the entity.</td>
</tr>
</tbody>
</table>
Configuring Primary and Standby VOSMs

The VOSM can operate in two different roles: primary and standby. The primary role is the default. You can have only one primary VOSM active in your network; however, you can have any number of VOSMs operating in a standby role to provide redundancy and failover capacity. You must configure the primary VOSM first.

Note

The primary and standby VOSMs must be running the same version of software. You must upgrade your standby VOSM first, and then upgrade your primary VOSM.

If the primary VOSM is down, the devices (SEs and SRs) cannot send regular reports and events to it, so the data is sent to the standby VOSM. After the primary VOSM is online, the database on the standby VOSM is synchronized with the database on the primary VOSM.

To configure a standby VOSM, do the following using the CLI:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Follow the instructions for configuring a VOSM using the setup utility, except do not enter the IP address of the VOSM. The instructions can be found in the Release Notes for the Cisco Media Origination Suite Release 2.0.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure the standby VOSM.</td>
</tr>
<tr>
<td>SE(config)# VOSM role standby</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Identify the IP address of the primary VOSM.</td>
</tr>
<tr>
<td>SE(config)# VOSM ip 10.1.1.90</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Start the Centralized Management System (CMS).</td>
</tr>
<tr>
<td>SE(config)# cms enable</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Save the configuration.</td>
</tr>
<tr>
<td>SE# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Activate the standby VOSM by using the web interface of the primary VOSM.</td>
</tr>
<tr>
<td>The primary VOSM notifies all registered devices that a standby VOSM exists and sends each device the information it needs to contact the standby should the primary fail or become inactive.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Primary and Standby VOSMs

#### Note
You cannot log in to the web interface of the standby VOSM. Its function is to maintain an up-to-date copy of the primary’s database.

---

### Changing a Standby to a Primary VOSM

#### Note
If your primary VOSM is still operating, you must change its role to standby by executing the `VOSM role standby` command before following these steps. You can only have one primary VOSM operating at any given time.

To change the standby VOSM to become the primary, do the following:

1. **Step 1**
   - If your primary VOSM has failed, enter the following command:
     ```
     SE(config)# VOSM role primary
     ```

2. **Step 2**
   - Save the configuration.
     ```
     SE# copy running-config startup-config
     ```

3. **Step 3**
   - Restore the old primary VOSM, if possible.

4. **Step 4**
   - When the old primary VOSM is restored, change its role to standby.
     ```
     VOSM role standby
     ```

5. **Step 5**
   - Reconnect the old primary VOSM (now standby VOSM) into the VDS-OS network.

6. **Step 6**
   - Wait at least one polling interval to allow the data from the primary VOSM to be copied to the standby VOSM.

   #### Note
   During this period, do not make any configuration changes.

7. **Step 7**
   - When the new primary VOSM and the new standby VOSM have synchronized, you can change the roles of the VOSMs back to their original roles.

   #### Note
   There can only be one primary VOSM in a VDS-OS at one time. If there are two primary VOSMs, both VOSMs are halted.

To change the roles back, do the following:

- a. Change the role of the primary VOSM to standby.
   ```
   VOSM role standby
   ```

- b. Change the role of the standby VOSM to primary.
   ```
   VOSM role primary
   ```
Note

If you have recently made configuration changes to the primary VOSM, wait at least the polling interval before changing roles to ensure that the standby has a record of the most recent configuration changes.

Recovering from Two Primary VOSMs

If you did not change the primary VOSM to standby before you changed the standby VOSM to primary, you will have two primary VOSMs in your VDS-OS and both will be halted. To restore both VOSMs, do the following:

Step 1
Make sure the VOSM that is to be designated as the standby is in fact the standby by entering the VOSM role standby command.

Step 2
Initiate the CMS on the standby VOSM by entering the cms enable command.

Step 3
Make sure the VOSM that is to be designated as the primary is in fact the primary by entering the VOSM role primary command.

Step 4
Initiate the CMS on the primary VOSM by entering the cms enable command.

Step 5
Make sure the standby VOSM is activated by using the web interface of the primary VOSM.

Typical Configuration Workflow

Once you have completed activating and configuring the NTP servers for all the devices in the VOSM, you are ready to configure the VDS-OS for content playout. For information about activating and configuring the NTP servers for a device, see the “Activating and Setting NTP for Each Device” section on page 4-3.

Table 4-2 lists the basic tasks for configuring the VDS-OS for content playout, with references to the associated sections in each chapter.
**Table 4-2 Configuration Workflow**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change admin password</td>
<td>Change the administrator password on each device, including the VOSM, and change the administrator password for the system</td>
<td>Log in to the CLI for the device and use the <code>username admin password password</code> global configuration command. The password strength must be a combination of alphabetic characters, at least one number, at least one special character, and at least one uppercase character. To change the password for the VOSM GUI and CLI, go to “Creating, Editing, and Deleting Users,” page 7-2</td>
</tr>
<tr>
<td>Create Device Groups</td>
<td>Group like devices to speed up configuration</td>
<td>“Configuring Device Groups,” page 5-3</td>
</tr>
<tr>
<td>Define Network Storage Shares</td>
<td>Each origin service and live channel must have at least one Network Storage Share assigned.</td>
<td>Defining Network Storage Shares, page 7-13</td>
</tr>
<tr>
<td>Create optional mount profiles</td>
<td>If the default mount profile is not sufficient, create new mount profiles.</td>
<td>Creating Mount Option Profiles for Network Storage Shares, page 7-14</td>
</tr>
<tr>
<td>Configure RCP</td>
<td>Configure Remote Copy Protocol (RCP) to listen for requests on TCP port 514</td>
<td>“Enabling RCP,” page 5-35</td>
</tr>
<tr>
<td>Configure FTP</td>
<td>Enable FTP services to listen for connection requests</td>
<td>“Enabling FTP Services,” page 5-34</td>
</tr>
<tr>
<td>Configure Web Engine</td>
<td>For all SEs participating in delivering content</td>
<td>“Configuring Web Engine HTTP Cache Freshness,” page 5-18</td>
</tr>
<tr>
<td>Create Coverage Zone File</td>
<td>Map SEs to client service areas by IP address or geographic location</td>
<td>Appendix B, “Creating Coverage Zone Files”</td>
</tr>
<tr>
<td>Import or Upload Coverage Zone File</td>
<td>Apply Coverage Zone mappings to VDS-OS</td>
<td>“Coverage Zone File Registration,” page 7-10</td>
</tr>
<tr>
<td>Configure Global Routing Method</td>
<td>Set the Coverage Zone file</td>
<td>“Configuring Global Routing,” page 7-12</td>
</tr>
<tr>
<td>Configure Routing Method</td>
<td>Configure the routing method used by SRs to be DNS-based routing</td>
<td>“Routing Redirection,” page 1-35</td>
</tr>
<tr>
<td>Create Origin Service Definitions</td>
<td>Create origin services for both prefetched or cached content and live programs</td>
<td>“Configuring Origin Services,” page 6-1</td>
</tr>
<tr>
<td>Create Live Channels</td>
<td>Create live channels and schedules</td>
<td>“Creating Live Channels,” page 6-7</td>
</tr>
</tbody>
</table>
Configuring Devices

This chapter discusses configuring locations and device groups for devices, and detailed instructions on configuring the different types of devices—SEs, SRs, and VOSMs. This chapter presents the following major topics:

- Configuring Locations, page 5-1
- Configuring Device Groups, page 5-3
- Configuring the Service Engine, page 5-9
- Configuring the Service Router, page 5-66
- Configuring the VOSM, page 5-72

Configuring Locations

Locations are set up in the VOSM to organize and group SEs into virtual networks for distribution of content through origin services.

Locations need to be configured before you can activate SEs and SRs and bring them online in the VDS-OS network. Table 5-1 describes the icons for the Locations Table page.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Create" /></td>
<td>Create a new location.</td>
</tr>
<tr>
<td><img src="image" alt="Filtered" /></td>
<td>Create a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="View" /></td>
<td>View all locations.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refresh the table.</td>
</tr>
<tr>
<td><img src="image" alt="Print" /></td>
<td>Print the current window.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit a location.</td>
</tr>
</tbody>
</table>
To create a new location or edit an existing one, do the following:

**Step 1** Choose Devices > Locations. The Locations Table page is displayed (Figure 5-1).

The table is sortable by clicking the column headings.

**Figure 5-1 Locations Table Page**

```
<table>
<thead>
<tr>
<th>Location</th>
<th>Parent</th>
<th>Level</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>None</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
```

**Step 2** In the task bar, click the Create New Location icon. The Creating New Location page is displayed (Figure 5-2).

To edit a location, click the Edit icon next to the location name.

**Figure 5-2 Creating New Location Page**

**Step 3** Enter the settings as appropriate. See Table 5-2 for a description of the fields.
Table 5-2  Location Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the location.</td>
</tr>
<tr>
<td>Parent Location</td>
<td>Choose a location from the drop-down list. A location with no parent, None, is level 1. The location level is displayed after you choose a parent location.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter any information about the location.</td>
</tr>
</tbody>
</table>

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

To delete a location, from the Locations Table page, click the **Edit** icon next to the location you want to delete, and click the **Delete** icon in the task bar.

To view the location tree, click the **Location Trees** icon in the task bar. The location tree represents the network topology you configured when you assigned a parent to each location.

## Configuring Device Groups

The VOSM allows you to configure SEs into device groups so that the entire group of SEs is configured at one time. Device groups and SEs share the same configuration features and options.

Table 5-3 describes the icons for the Device Groups Table page.

Table 5-3  Device Group Table Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Creates a new device group.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Creates a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Views all device groups.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Prints the current window.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Edits a device group.</td>
</tr>
</tbody>
</table>

This section covers creating, editing, and deleting device groups. All other configuration pages for a device group are covered in the “Configuring the Service Engine” section on page 5-9.
To create or edit a device group, do the following:

**Step 1** Choose **Devices > Device Groups**. The Device Groups Table page is displayed (Figure 5-3). The table is sortable by clicking the column headings.

![Device Groups Table Page](image)

**Step 2** In the task bar, click the **Create New Device Group** icon. The Creating New Device Group page is displayed (Figure 5-4).

To edit a device group, click the **Edit** icon next to the device group name.

![Creating New Device Group Page](image)

**Step 3** In the Name field, enter the name of the device group. The name must be unique and should be a name that is useful in distinguishing the device group from the others in the VDS-OS.

**Step 4** Check the **Automatically assign all newly activated devices to this group** check box if applicable.

**Step 5** Choose **Regular Group** to indicate this group is not used as a baseline for all SEs or choose **Baseline Group** and select the baseline type to define this group as a baseline for all SEs.
A baseline group is a special type of device group that denotes a group of devices for a particular service. There are three baseline groups:

- Web Baseline Group—Used for web-based content
- Video Baseline Group—Used for video content
- Platform Baseline Group—Used for platform-specific configurations

A device group can be configured as a baseline group. A device can be assigned to a baseline group in the following two ways:

- From the Devices home page.
- From the Device Group Assignment page.

**Step 6**
To customize the left panel menu for this device group, click the **Select pages to hide from the menu for this device group** arrow, and check the pages you want to hide. To collapse these settings, click the arrow again.

Use this feature to remove from view any configuration pages that you do not need for the device group.

**Step 7**
In the Comments field, enter any information about the device group.

**Step 8**
Click **Submit** to save the settings.

If you are editing this device group, you can view a list of all settings configured for this device group by clicking the **Pages configured for this device group** arrow. To collapse this information list, click the arrow again.

To delete a device group, click the **Delete** icon in the task bar.

**Step 9**
To assign SEs to the device group, choose **Assignments > Devices**. The Assignment table is displayed listing all SEs in the VDS-OS.

**Note**
From this point forward, the steps to get to a configuration page are combined into one step using notation similar to the following: **Device Group > Assignments > Devices**.

**Step 10**
Click the **Assign** icon (blue cross mark) next to each SE name you want to assign to this group.

To assign all SEs, click **Assign all Service Engines** in the task bar.

**Step 11**
Click **Submit** to add the selected SEs to the device group.

To remove an SE from the device group, click the **Unassign** icon (green check mark) next to the name of the SE, and click **Submit**.

To remove all SEs from the device group, click the **Unassign all Service Engines** icon in the task bar, and click **Submit**.

**Working with Device Groups**

When you first create a device group, all settings you configure for the device group are automatically propagated to all the SEs assigned to that group.
Note
All SE settings in the “Configuring the Service Engine” section on page 5-9, except those listed below, can also be configured for a device group. The following pages are not available for device group configuration:

- **Devices > General Settings > Network > Network Interfaces.** See the “Viewing Network Interfaces” section on page 5-39 for more information.
- **Devices > General Settings > Network > External IP.** See the “Configuring External IP Addresses” section on page 5-39 for more information.
- **Devices > General Settings > Network > IP ACL.** See the “Configuring IP ACL for IPv4” section on page 5-40 for more information.

After configuring the device group settings, the task bar for the corresponding configuration page for an individual SE that is part of that device group displays the Override Group Settings icon and the Device Group drop-down list with the device group name displayed.

When an SE is associated with one or many device groups, the name of the device group whose settings were applied last are displayed.

To configure individual settings for an SE in a device group, click the Override Group Settings icon in the task bar. You can then edit the fields on the page and click Submit. The Device Group drop-down list displays “Select a Device Group.”

To reapply the settings for the device group, select the device group from the Device Group drop-down list and click Submit. Alternatively, you can go to the corresponding device group configuration page and click the Force Settings on SEs in Group. The Force Settings on SEs in Group only displays for a device group configuration page when an SE’s individual settings override the group settings.

Note
The individual SE configuration page does not display the Override Group Settings icon and Device Group drop-down list in the task bar if the settings have not been configured for the corresponding device group configuration page.

Note
When adding an SE to an existing device group, the new SE does not automatically inherit the device group settings. Use the Force Group Settings option for the device group to force the group settings to all SEs in the group.

Alternatively, you can go to each device group configuration page and click the Force Settings on SEs in Group. A dialog box lists all the SEs that have different configuration settings than the device group settings. The Force Settings on SEs in Group only displays for a device group configuration page when an SE’s individual settings override the group settings.

To force all device group settings to all assigned SEs, go to the Device Group Home page and click the Force Group Settings icon in the task bar.

Note
The last configuration submitted for the device, whether it is the device group configuration or the individual device configuration, is the configuration the device uses.

Table 5-4 describes the icons for the Device Groups configuration pages.
Table 5-4  Device Group Configuration Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Trash Can]</td>
<td>Deletes a device group.</td>
</tr>
<tr>
<td>![File Exclamation]</td>
<td>Updates application statistics.</td>
</tr>
<tr>
<td>![Database]</td>
<td>Forces full database update.</td>
</tr>
<tr>
<td>![Reboot]</td>
<td>Reboots all devices in device group.</td>
</tr>
<tr>
<td>![Group Settings]</td>
<td>Forces the group settings. Forces the complete set of configurations made for a device group to all devices associated with that group.</td>
</tr>
<tr>
<td>![SE Settings]</td>
<td>Forces settings on SEs in a device group. Forces the configuration of the displayed page to all SEs in the device group.</td>
</tr>
<tr>
<td>![Override]</td>
<td>Overrides the group settings on the device.</td>
</tr>
<tr>
<td>![Print]</td>
<td>Prints the current window.</td>
</tr>
</tbody>
</table>

Aggregate Settings

The following device and device group configuration pages have aggregate settings:

- **Service Control > URL Signing.** See the “Configuring Transaction Logs” section on page 5-15 for more information.

- **General Settings > Login Access Control > Users > Usernames.** See the “Creating, Editing, and Deleting Users—Usernames” section on page 5-26 for more information.

To access these pages, first choose Devices > Devices or Devices > Device Groups, followed by the **Edit** icon next to the device or device group you want to configure.

Aggregate Settings is set to **Yes** by default. When Aggregate Settings is set to **Yes**, the settings for the device group are aggregated with the settings for the SE. This means you can configure settings for all SEs in a device group, then configure individual settings for each SE, and the combined settings for the device group and individual SE are apply to the SE. Any settings for the device group are listed with the **View** icon and any settings for the individual SE are listed with the **Edit** icon on the individual SE configuration page.

If Aggregate Settings is set to **No**, only the individual SE settings are applied to the SE and the device group settings do not apply to the SE.

To edit the device group settings, or configure new settings for the device group, you must go to the device group corresponding configuration page.

If you remove all device group settings, all device settings displayed with Aggregate Settings enabled are removed as well.
Note
The last configuration submitted for the device, whether it is the device group configuration or the individual device configuration, is the configuration the device uses.

Table 5-5 describes the icons for the configuration pages that have aggregate settings.

Table 5-5 Aggregate Settings Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Create" /></td>
<td>Creates a new entry.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edits an entry.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Deletes an entry.</td>
</tr>
<tr>
<td><img src="image" alt="View" /></td>
<td>Views read-only entry.</td>
</tr>
<tr>
<td><img src="image" alt="Create Filtered Table" /></td>
<td>Creates a filtered table. Filter the table based on the field values.</td>
</tr>
<tr>
<td><img src="image" alt="View All Table Entries" /></td>
<td>Views all table entries. Click this icon to view all entries after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td><img src="image" alt="Print" /></td>
<td>Prints the current window.</td>
</tr>
</tbody>
</table>

Device Group Overlap

If you want the ability to assign a device to more than one device group, you must enable device group overlap. Device group overlap is enabled by default.

To enable or disable device group overlap, do the following:

Step 1 Choose **System > Configuration**. The Configuration Properties page is displayed.

Step 2 Click the **Edit** icon next to the **DeviceGroup.overlap** property. The Modifying Config Property page is displayed.

Step 3 To enable device group overlap, choose **true** from the **Value** drop-down list.

To disable device group overlap, choose **false** from the **Value** drop-down list.

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

You cannot disable device group overlap after you have assigned devices to multiple device groups.
Chapter 5 Configuring Devices

Configuring the Service Engine

This section walks you through the different configuration pages available for a Service Engine. The main configuration groups are described as follows:

- **Service Control**—Settings for access control by way of URL signing and transaction logs are configured to monitor traffic
- **Application Control**—Settings for HTTP cache freshness
- **General Settings**—Settings for access control of the device, maintenance, network connectivity, and monitoring

The first two pages, Device Activation and Assignment, cover activating an SE in the VOSM and assigning it to a location, and assigning device groups and origin services to the SE.

Activating a Service Engine

Activating a device (Service Engine, Service Router, or standby VOSM) can be done through the Devices home page initially, or through the Device Activation page.

To activate a device from the Device Activation page, do the following:

**Step 1** Choose Devices > Devices. The Devices Table page is displayed (Figure 5-5).

**Figure 5-5 Devices Table Page**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Type</th>
<th>IP Address</th>
<th>Status</th>
<th>Location</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VS4-USOS1-ESD1</td>
<td>Service Engine</td>
<td>140.14.194</td>
<td>Online</td>
<td>root</td>
<td>1.0.0.43</td>
</tr>
<tr>
<td>VS4-USOS1-ESD2</td>
<td>Service Engine</td>
<td>140.14.195</td>
<td>Online</td>
<td>root</td>
<td>1.0.0.45</td>
</tr>
<tr>
<td>VS4-USOS1-ESD3</td>
<td>Service Engine</td>
<td>140.14.196</td>
<td>Online</td>
<td>root</td>
<td>1.0.0.44</td>
</tr>
<tr>
<td>VS4-USOS1-ESD4</td>
<td>Service Engine</td>
<td>140.14.197</td>
<td>Online</td>
<td>root</td>
<td>1.0.0.43</td>
</tr>
<tr>
<td>VS4-USOS1-ESD5</td>
<td>Service Engine</td>
<td>140.14.185</td>
<td>Online</td>
<td>root</td>
<td>1.0.0.43</td>
</tr>
<tr>
<td>VS4-USOS1-ESD6</td>
<td>Service Engine</td>
<td>140.14.186</td>
<td>Online</td>
<td>root</td>
<td>1.0.0.44</td>
</tr>
<tr>
<td>VS4-USOS2-ESD4</td>
<td>Virtual Origin System Manager (Primary)</td>
<td>15.14.0.222</td>
<td>Online</td>
<td>root</td>
<td>1.0.0.44</td>
</tr>
<tr>
<td>VS4-USOS2-ESD3</td>
<td>Service Router</td>
<td>15.14.0.204</td>
<td>Online</td>
<td>root</td>
<td>1.0.0.44</td>
</tr>
</tbody>
</table>

**Step 2** Click the Edit icon next to the device you want to configure. The Devices home page is displayed.

**Step 3** Click Show All to display the top-level menu options, and click Device Activation. The Device Activation page is displayed (Figure 5-6).
Step 4  Enter the settings as appropriate. See Table 5-6 for a description of the fields.

**Table 5-6  Device Activation Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Location</td>
<td>Lists all the locations configured for the VDS-OS.</td>
</tr>
<tr>
<td>Activate</td>
<td>To activate or deactivate the device, check or uncheck the <strong>Activate</strong> check box. Alternatively, you can click the <strong>Deactivate Device</strong> icon in the task bar. <strong>Note</strong> You cannot deactivate an SE if it is the only active Acquisition node for a live channel. When you uncheck the <strong>Activate</strong> check box and click <strong>Submit</strong>, the <strong>Replaceable</strong> check box is displayed. Check the <strong>Replaceable</strong> check box when you need to replace the device or recover lost registration information. For more information, see the “Recovering VDS-OS Network Device Registration Information” section on page 9-24.</td>
</tr>
</tbody>
</table>
Table 5-6  Device Activation Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Offload</td>
<td>To offload this device for maintenance or a software upgrade, check the <strong>Server Offload</strong> check box. When checked, the Service Router stops sending requests to this device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If a client paused a program at that moment <strong>Server Offload</strong> is enabled, most likely resuming the program will fail.</td>
</tr>
<tr>
<td></td>
<td>To monitor the current streams on an SE during the Server Offload state, use the <code>show interface</code> command. If the packets received or packets sent is increasing then the SE is streaming. The number of packets received is high if there is an incoming stream.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>We recommend separating the management traffic from the streaming traffic by using the port channel configuration, see the “Configuring Port Channel” section on page D-1 for more information.</td>
</tr>
<tr>
<td></td>
<td>• If management and streaming traffic are separated, the <code>show interface</code> command for the streaming port channel displays information on active sessions.</td>
</tr>
<tr>
<td></td>
<td>• If management and streaming traffic are not separated, the <code>show interface</code> command shows very low traffic; the packets received and packets sent are lower than a client streaming session.</td>
</tr>
<tr>
<td></td>
<td>Once the SE has finished streaming, you can perform maintenance or upgrade the software on the device. For information about upgrading the software, see the “Software Upgrade” section on page 9-1.</td>
</tr>
<tr>
<td></td>
<td>The Status field on the Device Activation page and the Devices Table page displays “offloading” when <strong>Server Offload</strong> is checked.</td>
</tr>
<tr>
<td></td>
<td>Once the software upgrade or maintenance is complete, you need to uncheck the <strong>Server Offload</strong> check box so that the device can again participate in the system.</td>
</tr>
<tr>
<td>Content Cache</td>
<td>Informational only. The content cache size is the total disk space on the content delivery network file system (CDNFS) on the SE that is designated for cache. The Content Cache represents the unused cache space. The used cache space is the disk space allotted for all the origin services to which the SE is assigned. To view the used cache space, choose Services &gt; Service Definition &gt; Virtual Origin Services &gt; Assign Service Engines.</td>
</tr>
<tr>
<td>Mount Option Profile</td>
<td>Lists all the mount option profiles for mounting a Network Storage Share. If a mount option profile is not selected, the SE uses the VDS-OS default mount profile. For more information, see the “Creating Mount Option Profiles for Network Storage Shares” section on page 7-14.</td>
</tr>
</tbody>
</table>
To make sure the SE is binding to the primary interface (or management IP address if configured) as the source IP address when sending management traffic to the VOSM, create a static route from the SE to the VOSM. To configure a static IPv4 route from the SE, see the “Configuring Static IPv4 Routes” section on page 5-49. Alternatively, you can use the `ip route` command on the VDS-OS device.

**Table 5-6 Device Activation Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Default Coverage Zone File</td>
<td>When checked, which is the default setting, a default Coverage Zone file is generated with the SE serving the local subnet it resides on. The coverage zone is a VDS-OS network-wide mapping of client IP addresses to SE IP addresses that should respond to client requests. For more information, see the “Coverage Zone File Registration” section on page 7-10. The default coverage zone can be disabled and you can create and assign custom coverage zones using the Coverage Zone file import or upload. Uncheck the <strong>Set Default Coverage Zone File</strong> check box to use a user-defined Coverage Zone file that was imported or uploaded.</td>
</tr>
<tr>
<td>Use SE’s primary IP address</td>
<td>Enables the VOSM to use the IP address on the primary interface of the SE for management communications. Note: If the <strong>Use SE’s primary IP Address for Management Communication</strong> check box is checked and the Management Communication Address and Port are configured, the VOSM uses the SE’s primary IP address for communication. Note: Do not check the <strong>Use SE’s primary IP Address for Management Communication</strong> check box if you want to separate management and streaming traffic. Instead, use the Management Communication Address and Port fields to specify where management traffic should be sent.</td>
</tr>
<tr>
<td>Management Communication Address</td>
<td>Manually configures a management IP address for the VOSM to communicate with the SE. Manual configuration of the management IP address and port are used when using port channel configuration to separate management and streaming traffic. For more information about port channel configuration see the “Configuring Port Channel and Load Balancing Settings” section on page 5-39 and the “Configuring Port Channel” section on page D-1.</td>
</tr>
<tr>
<td>Management Communication Port</td>
<td>Port number to enable communication between the VOSM and the SE.</td>
</tr>
<tr>
<td>Comments</td>
<td>Information about the settings.</td>
</tr>
</tbody>
</table>

**Step 5**  Click **Submit** to save the settings.
Assigning Devices to Device Groups

You can assign devices to device groups in three ways:

- Through the Device Group Assignment page
- Through the device Assignment page
- Through the Devices home page, if the device group is a baseline group

To assign devices to device groups through the Assignment page, do the following:

**Step 1** Choose Devices > Devices, and click the Edit icon next to the device you want to assign.

**Step 2** Click Show All, and then choose Assignments > Device Groups. The Device Group Table page is displayed with all of the configured device groups listed (Figure 5-7).

**Note** From this point forward, the beginning steps in the procedures are combined into one step using notation similar to the following: Devices > Devices > Assignments > Device Groups.

**Figure 5-7 Device Group Assignment Page**

**Step 3** Click the Assign icon (blue cross mark) next to the device group you want to assign to this SE. Alternatively, click the Assign All Device Groups icon in the task bar.

A green arrow wrapped around the blue X indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon. The SE assignment states are described in Figure 5-8.

**Figure 5-8 SE Assignment State**

**Step 4** Click Submit to save the settings.
A green circle with a check mark indicates a device group is assigned to this SE. To unassign the device group, click this icon, or click the Remove All Device Groups icon in the task bar. Click Submit to save the changes.

Additionally, the Filter Table icon and View All Device Groups icon allow you to first filter a table and then view all device groups again.

### Assigning Devices to Origin Services

You can assign devices to origin services in two ways:

- Through the Origin Services Assignment page (Services > Virtual Origin Services > Service Definition > Assign Service Engines)
- Through the device Assignment page (Devices > Devices > Assignments > Origin Services)

To assign devices to origin services through the Assignment page, do the following:

**Step 1** Choose Devices > Devices, and click the Edit icon next to the device you want to assign.

**Step 2** Click Show All, and then choose Assignments > Origin Services. The Origin Services Table page is displayed with all of the configured device groups listed (Figure 5-9).

**Figure 5-9 Origin Service Assignment Page**

![Origin Service Assignment Page](image)

**Step 3** Click the Assign icon (blue cross mark) next to the origin service you want to assign. Alternatively, click the Assign All Origin Services icon in the task bar.

A green arrow wrapped around the blue X indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon. The SE assignment states are described in Figure 5-8.

**Step 4** Click Submit to save the settings.
A green circle with a check mark indicates an origin service is assigned to this SE. To unassign the origin service, click this icon, or click the Remove All Origin Services icon in the task bar. Click Submit to save the changes.

Additionally, the Filter Table icon and View All Origin Services icon allow you to first filter a table and then view all device groups again.

Service Control

The Service Control pages provide settings for client request filtering, URL signing, and Authorization Server settings. Additionally, transaction logs that monitor traffic are configured under the Service Control. Configuring service control consists of the Configuring Transaction Logs page. Table 5-7 describes the icons for the Service Control pages.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refreshes the table or page.</td>
</tr>
<tr>
<td><img src="image" alt="Apply" /></td>
<td>Applies the default settings to the device.</td>
</tr>
<tr>
<td><img src="image" alt="New Item" /></td>
<td>Creates a new item.</td>
</tr>
<tr>
<td><img src="image" alt="New Filter" /></td>
<td>Creates a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="View All" /></td>
<td>Views all data. Click this icon to view all data after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="Print" /></td>
<td>Prints the current window.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edits an item.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Deletes an item. To delete an item, click the Edit icon and then click this icon.</td>
</tr>
</tbody>
</table>

Configuring Transaction Logs

Transaction logs allow administrators to view the traffic that has passed through the SE. Typical fields in the transaction log are the date and time when a request was made, the URL that was requested, whether it was a cache hit or a cache miss, the type of request, the number of bytes transferred, and the source IP address. For more information about transaction logs and their formats, see the “Transaction Logs” section on page 8-23.
To enable transaction logging, do the following:

**Step 1** Choose **Devices > Devices > Service Control > Transaction Logging**. The Transaction Log Settings page is displayed.

**Step 2** Enter the settings as appropriate. See **Table 5-8** for a description of the fields.

### Table 5-8  Transaction Log Settings 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>Transaction Log Enable</td>
<td>Enables transaction logging.</td>
</tr>
<tr>
<td>Log Windows Domain</td>
<td>If NTLM authentication is configured, you can record the Windows domain name and username in the “authenticated username” field of the transaction log by checking this check box.</td>
</tr>
<tr>
<td>Compress Files before Export</td>
<td>When this check box is checked, archived log files are compressed into gzip format before being exported to external FTP servers</td>
</tr>
<tr>
<td>Log File Format</td>
<td>Log file format choices are <strong>extended-squid</strong> or <strong>apache</strong>. The default is <strong>apache</strong>. For more information, see the “Transaction Log Formats for Web Engine” section on page 8-23. Or, choose <strong>Log Format Custom</strong> and enter a custom format string. For more information, see the “Custom Format” section on page 8-26.</td>
</tr>
<tr>
<td>Log Format Custom</td>
<td></td>
</tr>
<tr>
<td><strong>Archive Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Max size of Archive File</td>
<td>Maximum size (in kilobytes) of the archive file to be maintained on the local disk. The range is from 1000 to 2000000. The default is 500000.</td>
</tr>
<tr>
<td>Max number of files to be archived</td>
<td>Maximum number of files to be maintained on the local disk. The range is from 1 to 10000. The default is 10.</td>
</tr>
</tbody>
</table>
| Archive occurs         | How often the working log is archived and the data is cleared from the working log. Choose one of the following:  
  - Choose **every** to archive every so many seconds, and enter the number of seconds for the interval. The range is from 120 to 604800.  
  - Choose **every hour** to archive using intervals of one hour or less, and choose one of the following:  
    - **at**—Specifies the minute in which each hourly archive occurs  
    - **every**—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30)  
  - Choose **every day** to archive using intervals of one day or less, and choose one of the following:  
    - **at**—Specifies the hour in which each daily archive occurs  
    - **every**—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24)  
  - Choose **every week on** to archive at intervals of one or more times a week, choose the days of the week, and choose what time each day. |
Table 5-8  Transaction Log Settings Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Export</td>
<td>Enables exporting of the transaction log to an FTP server.</td>
</tr>
<tr>
<td>Export occurs</td>
<td>How often the working log is sent to the FTP server and the data is cleared from the working log. Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Choose every to export every so many minutes, and enter the number of minutes for the interval. The range is from 1 to 10080.</td>
</tr>
<tr>
<td></td>
<td>• Choose every hour to export using intervals of one hour or less, and choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>– at—Specifies the minute in which each hourly export occurs</td>
</tr>
<tr>
<td></td>
<td>– every—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30)</td>
</tr>
<tr>
<td></td>
<td>• Choose every day to export using intervals of one day or less, and choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>– at—Specifies the hour in which each daily export occurs</td>
</tr>
<tr>
<td></td>
<td>– every—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24)</td>
</tr>
<tr>
<td></td>
<td>• Choose every week on to export using intervals of one or more times a week, choose the days of the week, and what time each day.</td>
</tr>
<tr>
<td>FTP Export Server</td>
<td>IP address or hostname of the FTP server.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the user.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirms the password for the user.</td>
</tr>
<tr>
<td>Directory</td>
<td>Name of the directory used to store the transaction logs on the FTP server.</td>
</tr>
<tr>
<td>SFTP</td>
<td>Check the SFTP check box, if you are using an SFTP server.</td>
</tr>
</tbody>
</table>

Step 3  Click Submit to save the settings.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

Application Control

The Application Control pages provide settings for HTTP cache freshness.

Note  Application Control is not supported in VDS-OS 2.1.1.
Configuring Web Engine HTTP Cache Freshness

To configure the web engine HTTP cache freshness, do the following:

**Step 1**  
Choose Devices > Devices > Application Control > Web > HTTP > HTTP Cache Freshness. The HTTP Cache Freshness page is displayed (Figure 5-10).

![HTTP Cache Freshness Page](image)

**Figure 5-10  HTTP Cache Freshness Page**

**Step 2**  
Enter the settings as appropriate. See Table 5-9 for a description of the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>When checked, HTTP cache freshness is enabled.</td>
</tr>
<tr>
<td>Object Age Multiplier</td>
<td>The age multiplier value (as a percentage) enables the SE to guess the life of an object by multiplying the time since the object was last modified by a percentage to obtain an approximate expiration date. After this date, the object is considered stale, and subsequent results cause a fresh retrieval by the SE. The range is from 0 to 100. The default value is 30.</td>
</tr>
<tr>
<td>Max TTL Scale</td>
<td>The scale (seconds, hours, minutes, or days) to use for the Max Object TTL. The time-to-live (TTL) sets a ceiling on estimated expiration dates. If an object has an explicit expiration date, this takes precedence over the configured TTL. The default is days.</td>
</tr>
</tbody>
</table>
Step 3  Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

**General Settings**

The General Settings pages provide settings for access control of the device, maintenance, network connectivity, and monitoring. The configuring of general settings consists of the following procedures:

- Login Access Control
- Authentication
- Scheduling Database Maintenance
- Setting Storage Handling
- Network Settings
- Configuring Notification and Tracking
- Configuring Troubleshooting
- Configuring Service Router Settings

---

**Login Access Control**

Login authentication and authorization are used to control user access and configuration rights to SEs, SRs, and VOSMs. Login authentication is the process by which the devices verify whether the person who is attempting to log in to the device has a valid username and password. The person logging in must have a user account registered with the device. User account information serves to authorize the user for login and configuration privileges. The user account information is stored in an authentication, authorization, and accounting (AAA) database, and the devices must be configured to access the particular authentication server (or servers) where the AAA database is kept.

In a VDS-OS network, user accounts can be created for access to the VOSM and, independently, for access to the SEs and SRs that are registered to the VOSM. For user accounts that access the VOSM, see the “Configuring AAA” section on page 7-1.

---

**Table 5-9  HTTP Cache Freshness Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Max Object TTL    | The maximum time-to-live (TTL) for objects in cache. The ranges are as follows:  
|                   | 1 to 1825 days     
|                   | 1 to 43800 hours   
|                   | 1 to 2628000 minutes 
|                   | 1 to 157680000 seconds 
|                   | The default is 61 day. |
| Minimum TTL       | The minimum time-to-live (in minutes) for objects in the cache. The range is from 0 to 86400. The default value is 60. |
Login Authentication

Login authentication provides the configuration for independent logins; in other words, login access to the device only.

Login authentication can also be used to log in to the VOSM GUI. When logging in to the VOSM GUI with an external user account (RADIUS or TACACS+), the user is authenticated by the external database. After the external user is authenticated, its role depends on the privilege configured in the external database (zero [0] means a normal user and 15 means a super user). The privilege level of 0 or 15 is mapped to the read-only or admin user role in the VOSM GUI. No VOSM local user is created in the VOSM database for the external user that logs in, so the external user cannot be managed by the VOSM GUI.

**Note**
If you plan to use a RADIUS server or a TACACS+ server for authentication, you must configure the server settings before you configure and submit these settings. See the “Configuring RADIUS Server Settings” section on page 5-27 and the “Configuring TACACS+ Server Settings” section on page 5-28 for more information.

When the primary login server and the primary enable server are set to local, usernames and passwords are local to each device. Local authentication and authorization uses locally configured login and passwords to authenticate login attempts.

**Note**
If the Enable Failover Server Unreachable option is enabled, it applies to both the login authorization methods and the exec authentication methods.

If you are going to use different servers for login authentication and enable authentication (for example, local for login authentication and RADIUS for the enable authentication), then the username and password must be the same for both servers.

By default, local login authentication is enabled. You can disable local login authentication only after enabling one or more of the other login authentication servers. However, when local login authentication is disabled, if you disable all other login authentication methods, a warning message is displayed stating “At least one authentication method is required to select for login.”

**Caution**
Make sure that RADIUS or TACACS+ authentication is configured and operating correctly before disabling local authentication and authorization. If you disable local authentication and RADIUS or TACACS+ is not configured correctly, or if the RADIUS or TACACS+ server is not online, you may be unable to log in to the device.

To configure the login authentication and enable authentication schemes for the device, do the following:

**Step 1** Choose Devices > Devices > General Settings > Login Access Control > Login Authentication. The Login Authentication page is displayed.

**Step 2** Enter the settings as appropriate. See Table 5-10 for a description of the fields.
Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

**Exec Authorization**

Exec authorization provides the configuration for determining the services allowed for each user that logs in to the device.

Exec authorization can also be used to determine the services the user has for the VOSM GUI. When logging in to the VOSM GUI with an external user account (RADIUS or TACACS+), the user is authenticated by the external database. After the external user is authenticated, its role depends on the privilege configured in the external database (zero [0] means a normal user and 15 means a super user). The privilege level of 0 or 15 is mapped to the read-only or admin user role in the VOSM GUI. No VOSM local user is created in the VOSM database for the external user that logs in, so the external user cannot be managed by the VOSM GUI.

**Note**

If you plan to use a TACACS+ server for authorization, you must configure the server settings before you configure and submit these settings. See the “Configuring RADIUS Server Settings” section on page 5-27 and the “Configuring TACACS+ Server Settings” section on page 5-28 for more information.

When the primary authorization server is set to local, usernames and passwords are local to each device. Local authorization uses locally configured login and passwords to authorize services for the user.

**Note**

If the **Enable Failover Server Unreachable** option is enabled, it applies to both the login authorization methods and the exec authentication methods.

If you are going to use different servers for login authentication and enable authentication (for example, local for login authentication and RADIUS for the enable authentication), then the username and password must be the same for both servers.

---

**Caution**

Make sure that RADIUS or TACACS+ authentication is configured and operating correctly before disabling local authentication and authorization. If you disable local authentication and RADIUS or TACACS+ is not configured correctly, or if the RADIUS or TACACS+ server is not online, you may be unable to log in to the device.

To configure the exec authorization schemes for the device, do the following:

**Step 1** Choose **Devices > Devices > General Settings > Login Access Control > Exec Authorization**. The Exec Authorization page is displayed.

**Step 2** Enter the settings as appropriate. See Table 5-11 for a description of the fields.
### Table 5-11  Exec Authorization Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Authorization Exec Servers | When enabled, authorization exec servers are used to authorize services for logged in users.  
Check this option and set one or more servers for exec authorization. By clearing this option, local authentication is used by default. Three servers can be configured.  
**Note** If a user encounters failure during EXEC shell startup authorization, the user fails to log in to the SE even if the user passed the login authentication. |
| Primary Exec Server    | Choose local, RADIUS, or TACACS+.                                                                                                               |
| Secondary Exec Server  | Choose local, RADIUS, or TACACS+.                                                                                                              |
| Tertiary Exec Server   | Choose local, RADIUS, or TACACS+.                                                                                                              |
| Primary Enable Server  | The enable server determines if the normal user can enter the privileged EXEC mode. Choose local, RADIUS, or TACACS+.                           |
| Normal User Commands   | Choose **Enable** or **Enable if Authenticated**.  
The **Enable if Authenticated** option turns off authorization on the TACACS+ server and authorization is granted to any Normal user who is authenticated. |
| Super User Commands    | Choose **Enable** or **Enable if Authenticated**.  
The **Enable if Authenticated** option turns off authorization on the TACACS+ server and authorization is granted to any Super user who is authenticated. |
| Enable Config Commands | Check the **Enable Config Commands** check box to enable authorization of the configuration mode commands.  
By default, this option is disabled, which means all configuration commands issued are allowed. |
| Enable Console Config  | Check the **Enable Console Commands** check box to enable authorization of all commands issued on a console TTY connection.  
By default, this option is disabled, which means commands issued through a console TTY connection always succeed. |

**Note** The following commands bypass authorization and accounting: CTRL+C, CTRL+Z, `exit`, `end`, and all of configuration commands for entering submode (for example, `interface GigabitEthernet 1/0`).

**Step 3**  
Click **Submit** to save the settings.  
To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.  
To remove the settings from the device, click the **Remove Settings** icon in the task bar.
Configuring SSH

Secure Shell (SSH) consists of a server and a client program. Like Telnet, you can use the client program to remotely log in to a machine that is running the SSH server. However, unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

The SSH page allows you to specify the key length and login grace time.

To enable the SSH daemon, do the following:

**Step 1** Choose Devices > Devices > General Settings > Login Access Control > SSH. The SSH page is displayed.

**Step 2** Check Enable to enable the SSH feature. SSH enables login access to the device through a secure and encrypted channel.

**Step 3** In the Length of Key field, specify the number of bits needed to create an SSH key. The default is 2048.

**Step 4** In the Login Grace Time field, specify the number of seconds the server waits for the user to successfully log in before it ends the connection. The authentication procedure must be completed within this time limit. The default is 300 seconds.

**Note** When changing the Login Grace Time, you need to first uncheck the Enable check box and click Submit. Enter the new Login Grace Time, check Enable, and click Submit.

**Step 5** Select the SSH version.

a. To allow clients to connect using SSH protocol version 1, check the Enable SSHv1 check box.

b. To allow clients to connect using SSH protocol version 2, check the Enable SSHv2 check box.

**Note** You can enable both SSHv1 and SSHv2, or you can enable one version and not the other. You cannot disable both versions of SSH unless you disable the SSH feature by clearing the Enable check box.

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

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.

Enabling Telnet

To enable the Telnet service, do the following:

**Step 1** Choose Devices > Devices > General Settings > Login Access Control > Telnet. The Telnet page is displayed.

**Step 2** Check Telnet Enable to enable the terminal emulation protocol for remote terminal connections.

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

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.
Configuring the Service Engine

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

### Setting the Message of the Day

The Message of the Day (MOTD) feature enables you to provide information bits to the users when they log in to a device. There are three types of messages that you can set up:

- MOTD banner
- EXEC process creation banner
- Login banner

To configure the Message of the Day settings, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Devices &gt; Devices &gt; General Settings &gt; Login Access Control &gt; Message of the Day</strong>. The MOTD page is displayed.</td>
</tr>
<tr>
<td>2</td>
<td>Check <strong>Enable</strong> to enable the MOTD settings. The Message of the Day (MOTD) banner, EXEC process creation banner, and Login banner fields become enabled.</td>
</tr>
<tr>
<td>3</td>
<td>In the <strong>Message of the Day (MOTD) Banner</strong> field, enter a string that you want to display as the MOTD banner when a user attempts to log in to the device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In the Message of the Day (MOTD) Banner, EXEC Process Creation Banner, and Login Banner fields, you can enter a maximum of 980 characters. A new line character (or <strong>Enter</strong>) is counted as two characters, as it is interpreted as \n by the system. You cannot use special characters such as `, %, ^, and “ in the MOTD text.</td>
</tr>
<tr>
<td>4</td>
<td>In the <strong>EXEC Process Creation Banner</strong> field, enter a string to be displayed as the EXEC process creation banner when a user enters into the EXEC shell of the device.</td>
</tr>
<tr>
<td>5</td>
<td>In the <strong>Login Banner</strong> field, enter a string to be displayed after the MOTD banner when a user attempts to log in to the device.</td>
</tr>
<tr>
<td>6</td>
<td>Click <strong>Submit</strong> to save the settings.</td>
</tr>
</tbody>
</table>

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

### Changing the CLI Session Time

To change the CLI session time, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Devices &gt; Devices &gt; General Settings &gt; Login Access Control &gt; CLI Session Time</strong>. The CLI Session Time page is displayed.</td>
</tr>
<tr>
<td>2</td>
<td>In the <strong>CLI Session Time</strong> field, enter the time (in minutes) that the device waits for a response before ending the session.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Submit</strong> to save the settings.</td>
</tr>
</tbody>
</table>

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
Chapter 5      Configuring Devices

Configuring the Service Engine

To remove the settings from the device, click the Remove Settings icon in the task bar.

Changing Users—Admin Password

Every device (SE, SR, and VOSM) has a built-in user account. The username is admin and the default password is default. This account allows access to all services and entities in the VDS-OS. Any user that can access the Admin Password page in the VOSM can configure a new password for the administrator user account on individual SEs and SRs.

To change the Admin password, do the following:

Step 1  Choose Devices > Devices > General Settings > Login Access Control > Users > Admin Password. The Admin Password page is displayed.
Step 2  In the Password field, enter a new password.
Step 3  In the Confirm Password field, re-enter the password.
Step 4  Click Submit to save the settings.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.
To remove the settings from the device, click the Remove Settings icon in the task bar.

Creating, Editing, and Deleting Users—Usernames

You can create, edit, and delete user accounts for login access to individual devices or device groups. A privilege profile must be assigned to each new user account. The Usernames page uses privilege profiles to determine which tasks a user can perform and the level of access provided. Users with administrative privileges can add, delete, or modify user accounts through the VOSM or the device CLI.

To create, edit, or delete a user account, do the following:

Step 1  Choose Devices > Devices > General Settings > Login Access Control > Users > Usernames. The User Table page is displayed.
Step 2  Click the Create New icon in the task bar. The Local User page is displayed.
Step 3  Enter the settings as appropriate. See Table 5-12 for a description of the fields.

Table 5-12       Local User Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Name of user.</td>
</tr>
<tr>
<td>Password</td>
<td>User password.</td>
</tr>
</tbody>
</table>
Configuring Devices

Chapter 5

Configuring the Service Engine

Configuring the Service Engine

Step 4
Click Submit to save the settings.

To delete a user, click the Edit icon for the user, then click the Delete icon in the task bar.

Authentication

User authentication and authorization (configuration rights) data can be maintained in any combination of these three databases:

- Local database (located on the device)
- RADIUS server (external database)
- TACACS+ server (external database)

The Login Authentication page allows you to choose an external access server or the internal (local) device-based authentication, authorization, and accounting (AAA) system for user access management. You can choose one method or a combination of the three methods. The default is to use the local database for authentication.

Configuring RADIUS Server Settings

Note
The VOSM does not cache user authentication information. Therefore, the user is reauthenticated against the Remote Authentication Dial In User Service (RADIUS) server for every request. To prevent performance degradation caused by many authentication requests, install the VOSM in the same location as the RADIUS server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure the RADIUS server settings, do the following:

Step 1
Choose Devices > Devices > General Settings > Authentication > RADIUS Server. The RADIUS Server Settings page is displayed.

Step 2
Enter the settings as appropriate. See Table 5-13 for a description of the fields.

Table 5-12 Local User Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Password</td>
<td>Re-enter user password.</td>
</tr>
<tr>
<td>Privilege</td>
<td>There are two types of predefined privilege profiles:</td>
</tr>
<tr>
<td></td>
<td>• Normal user—User has read access and can see some of the SE, SR, or VOSM settings.</td>
</tr>
<tr>
<td></td>
<td>• Superuser—User has administrative privileges such as creating new users and modifying the SE, SR, or VOSM settings.</td>
</tr>
</tbody>
</table>

Table 5-12 Local User Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Password</td>
<td>Re-enter user password.</td>
</tr>
<tr>
<td>Privilege</td>
<td>There are two types of predefined privilege profiles:</td>
</tr>
<tr>
<td></td>
<td>• Normal user—User has read access and can see some of the SE, SR, or VOSM settings.</td>
</tr>
<tr>
<td></td>
<td>• Superuser—User has administrative privileges such as creating new users and modifying the SE, SR, or VOSM settings.</td>
</tr>
</tbody>
</table>
Chapter 5 Configuring Devices

Configuring Devices

Configuring the Service Engine

Step 3
Click Submit to save the settings.
To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.
To remove the settings from the device, click the Remove Settings icon in the task bar.

To use RADIUS for login authentication and authorization, see the “Login Authentication” section on page 5-20.

Configuring TACACS+ Server Settings

The VOSM does not cache user authentication information. Therefore, the user is reauthenticated against the Terminal Access Controller Access Control System Plus (TACACS+) server for every request. To prevent performance degradation caused by many authentication requests, install the VOSM in the same location as the TACACS+ server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure the TACACS+ server settings, do the following:

Step 1 Choose Devices > Devices > General Settings > Authentication > TACACS+ Server. The TACACS+ Server Settings page is displayed.
Step 2 Enter the settings as appropriate. See Table 5-14 for a description of the fields.

Table 5-13 RADIUS Server Settings Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Radius</td>
<td>Enables RADIUS authentication.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Number of seconds to wait for a response before timing out on a connection to a RADIUS server. The range is from 1 to 20. The default is 5.</td>
</tr>
<tr>
<td>Number of retransmits</td>
<td>Number of attempts allowed to connect to a RADIUS server. The default is 2.</td>
</tr>
<tr>
<td>Enable redirect</td>
<td>Redirects an authentication response to a different authentication server if an authentication request using the RADIUS server fails.</td>
</tr>
<tr>
<td>Redirect Message</td>
<td>Message sent to the user if redirection occurs.</td>
</tr>
<tr>
<td>[1-3]</td>
<td>Note If the redirect message has a space, it must be in quotes (“ “).</td>
</tr>
<tr>
<td>Location [1-3]</td>
<td>Sets an HTML page location. This is the URL destination of the redirect message that is sent when authentication fails.</td>
</tr>
<tr>
<td>Shared Encryption Key</td>
<td>Encryption key shared with the RADIUS server. The maximum number of characters allowed is 15.</td>
</tr>
<tr>
<td>Server Name [1-5]</td>
<td>IP address or hostname of the RADIUS server.</td>
</tr>
<tr>
<td>Server Port [1-5]</td>
<td>Port number on which the RADIUS server is listening. The default is 1645.</td>
</tr>
</tbody>
</table>
Chapter 5  Configuring Devices

Configuring the Service Engine

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

To use TACACS+ for login authentication and authorization, see the “Login Authentication” section on page 5-20.

### Configuring AAA Accounting

Accounting tracks all user actions and when the action occurred. It can be used for an audit trail or for billing for connection time or resources used (bytes transferred).

The VDS-OS accounting feature uses TACACS+ server logging. Accounting information is sent to the TACACS+ server only, not to the console or any other device. The syslog file on the SE logs accounting events locally. The format of events stored in the syslog is different from the format of accounting messages.

The TACACS+ protocol allows effective communication of AAA information between SEs and a central TACACS+ server. It uses TCP for reliable connections between clients and servers. SEs send authentication and authorization requests, as well as accounting information to the TACACS+ server.

#### Table 5-14  TACACS+ Server Settings Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable TACACS+ Servers</td>
<td>Enables TACACS+ authentication.</td>
</tr>
<tr>
<td>Use ASCII Password</td>
<td>Changes the default password type from Password Authentication Protocol (PAP) to ASCII clear text format.</td>
</tr>
<tr>
<td>Time to wait</td>
<td>Number of seconds to wait for a response before timing out on a connection to a TACACS+ server. The range is from 1 to 20. The default is 5.</td>
</tr>
<tr>
<td>Number of retransmits</td>
<td>Number of attempts allowed to connect to a TACACS+ server. The default is 2.</td>
</tr>
<tr>
<td>Security Word</td>
<td>Encryption key shared with the TACACS+ server. The range is from 1 to 99. An empty string is the default.</td>
</tr>
<tr>
<td>Primary Server</td>
<td>IP address or hostname of the primary TACACS+ server.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>IP address or hostname of the backup TACACS+ server. Up to two backup servers are allowed.</td>
</tr>
<tr>
<td>Tertiary Server</td>
<td>IP address or hostname of the backup TACACS+ server. Up to two backup servers are allowed.</td>
</tr>
</tbody>
</table>

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

Before you can configure the AAA accounting settings for a device, you must first configure a TACACS+ server for the device. See the “Configuring TACACS+ Server Settings” section on page 5-28.
The VOSM does not cache user authentication information. Therefore, the user is reauthenticated against the Terminal Access Controller Access Control System Plus (TACACS+) server for every request. To prevent performance degradation caused by many authentication requests, install the VOSM in the same location as the TACACS+ server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure the AAA accounting settings, do the following:

**Step 1** Choose Devices > Devices > General Settings > Authentication > AAA Accounting. The AAA Accounting Settings page is displayed.

**Step 2** Enter the settings as appropriate. See Table 5-14 for a description of the fields.

**Table 5-15 AAA Accounting Settings Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Events</td>
<td>Enables accounting records on the TACACS+ server about system events; such as system reboot, interface up or down states, and accounting configuration enabled or disabled. From the System Events drop-down list choose start-stop or stop-only. The start-stop option records events when they start and when they stop. The stop-only option records events when they stop.</td>
</tr>
<tr>
<td>Exec Shell Events</td>
<td>Enables accounting records on the TACACS+ server about user EXEC terminal sessions, including username, date, and start and stop times. From the Exec Shell Events drop-down list choose start-stop or stop-only. The start-stop option records events when they start and when they stop. The stop-only option records events when they stop.</td>
</tr>
<tr>
<td>Normal User Commands</td>
<td>Enables accounting records on the TACACS+ server for Normal users using commands in the EXEC mode. From the Normal User Commands drop-down list choose start-stop or stop-only. The start-stop option records events when they start and when they stop. The stop-only option records events when they stop.</td>
</tr>
<tr>
<td>Super User Commands</td>
<td>Enables accounting records on the TACACS+ server for Super users using commands in the EXEC mode. From the Super User Commands drop-down list choose start-stop or stop-only. The start-stop option records events when they start and when they stop. The stop-only option records events when they stop.</td>
</tr>
</tbody>
</table>

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

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar. To remove the settings from the device, click the Remove Settings icon in the task bar.
Configuring an Access Control List

To configure an access control list (ACL) for group authorization, do the following:

Step 1
Choose Devices > Devices > General Settings > Authentication > Access Control List > Configure Access Control List. The Access Control List Table page is displayed.

The table is sortable by clicking the column headings.

Step 2
Click the Create New icon in the task bar. The Configure Access Control List page is displayed.

To edit a group, click the Edit icon next to the name you want to edit.

Step 3
Enter the settings as appropriate. See Table 5-16 for a description of the fields.

Step 4
Click Submit to save the settings.

To delete a group, click the Edit icon for the group, then click the Delete icon in the task bar.

Step 5
From the left-panel menu, choose Enable Access Control List. The Enable Access Control List page is displayed.

Step 6
Check the Enable Access Control List check box and click Submit.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.

To move a group up or down in the Access Control List table, click the Up arrow or Down arrow in the Move column.

The ACL can be applied from the device or from a device group. The source of the currently applied settings is shown in the Access Control List Table page.

Scheduling Database Maintenance

The database maintenance runs at the scheduled time only when the following three conditions are satisfied:

- Last vacuum process happened more than 30 minutes in the past.
- Percent increase in disk space usage is greater than 10 percent.
- Available free disk space is greater than 10 percent of the total disk space.

If any of these conditions are not satisfied, the database maintenance does not run at the scheduled time.
To schedule a database cleaning or reindexing, do the following:

**Step 1** Choose Devices > Devices > General Settings > Database Maintenance. The Database Maintenance Settings page is displayed.

**Step 2** Enter the settings as appropriate. See Table 5-17 for a description of the fields.

**Table 5-17 Database Maintenance Settings Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Database Maintenance Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>When enabled, a full database maintenance routine is performed on the device.</td>
</tr>
<tr>
<td>Every Day</td>
<td>The days of the week when the maintenance is performed</td>
</tr>
<tr>
<td>Sun-Sat</td>
<td>When Every Day is enabled, all days of the week are also enabled.</td>
</tr>
<tr>
<td>At (time)</td>
<td>Time of day the maintenance is performed. Time is entered in 24-hour format as hh:mm. The default is 04:00.</td>
</tr>
<tr>
<td><strong>Regular Database Maintenance Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>When enabled, a re-indexing routine is performed on the device.</td>
</tr>
<tr>
<td>Every Day</td>
<td>The days of the week when the maintenance is performed.</td>
</tr>
<tr>
<td>Sun-Sat</td>
<td>When Every Day is enabled, all days of the week are also enabled.</td>
</tr>
<tr>
<td>At (time)</td>
<td>Time of day the maintenance is performed. Time is entered in 24-hour format as hh:mm. The default is 02:00.</td>
</tr>
</tbody>
</table>

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

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.

**Setting Storage Handling**

The Storage option offers disk error-handling settings.

**Enabling Disk Error Handling**

The Disk Error Handling page allows you to configure how disk errors are handled, and to define disk error-handling thresholds for bad sectors and disk errors (I/O errors).

The **Threshold for Bad Sectors** and the **Threshold for Disk Errors** counts only apply to bad sectors and disk errors detected since the last reboot of the device. These counts do not persist across a device reboot (reload).

If the **Enable Disk Error Handling Reload** option is enabled and a SYSTEM disk drive is marked bad because the disk error-handling threshold (bad sectors or disk errors) was reached, the device is automatically reloaded. Following the device reload, the bad sector and disk error threshold counts are reset, and a syslog message and an SNMP trap are generated.
If a critical disk drive is marked bad, the redundancy of the system disks for this device is affected. Critical disks are disks with SYSTEM partitions. However, drives with SYSTEM partitions use RAID1. With the RAID system, if the critical primary disk fails, the other mirrored disk (mirroring only occurs for SYSTEM partitions) seamlessly continues operation. There is a separate alarm for bad RAID. The SMART statistics that are returned by the `show disks SMART-info detail` command include sector errors directly reported by the drive itself.

**Note**
We do not recommend enabling the **Enable Disk Error Handling Reload** option, because the software state may be lost when the device is reloaded.

To configure a disk error-handling method, do the following:

**Step 1**
Choose **Devices > Devices > General Settings > Storage > Disk Error Handling**. The Disk Error Handling Settings page is displayed.

**Step 2**
Check the **Enable** check box.

**Step 3**
Check the **Enable Disk Error Handling Reload** check box if you want the device to reload when a critical disk (SYSTEM) has problems.

**Step 4**
Check the **Enable Disk Error Handling Threshold** check box if you want to set the number of disk errors allowed before the disk is marked bad, and enter the following:

- **a.** In the **Threshold for Bad Sectors** field, enter the number of allowed bad sectors before marking the disk bad. This threshold only applies to bad sectors detected since the last reboot of the device. The range is 0 to 100. The default threshold is 30.

- **b.** In the **Threshold for Disk Errors** field, enter the number of allowed disk errors (I/O errors) before marking the disk bad. This threshold only applies to disk and sector errors detected since the last reboot of the device. The range is from 0 to 100,000. The default is 500.

**Note**
When both **Threshold for Bad Sectors** and **Threshold for Disk Errors** are set to 0, it means never mark the disk bad when it detects bad sectors or disk errors, and the disk_failure alarm is not raised. A disk with SYSTEM partitions uses RAID1. There is a separate alarm for bad RAID.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

When a sector I/O error is detected, a “badsector” alarm is raised against the corresponding disk, which occurs during the lifetime of a disk. A “badsector” alarm is raised when the number of bad sectors for a specific disk exceeds the “badsector” alarm threshold. The default threshold for bad sector alarms is set to 15 errored sectors. See the *Cisco Videoscape Distribution Suite Origin Server Release 2.1.1 Command Reference* for information on setting the threshold for bad sector alarms and remapped sector alarms, by using the following commands:

```
(config)# disk error-handling threshold alarm-bad-sectors <threshValue>
(config)# disk error-handling threshold alarm-remapped-sectors <threshValue>
(config)# disk error-handling bad-sectors-mon-period <minutes>
```
The **Disk Failure Percentage Threshold** field on the Service Monitor page sets the overall percentage of CDNFS disk failures. When the percentage of failed disks (default is 75) exceeds this threshold, no further requests are sent to this device. The **Disk Failure Threshold** setting is only for the CDNFS disks. For more information, see the “Setting Service Monitor Thresholds” section on page 5-52.

**Network Settings**

The Network pages provide settings for network connectivity. Configuring network settings consist of the following procedures:

- Enabling FTP Services
- Enabling DNS
- Enabling RCP
- Configuring NTP
- Setting the Time Zone
- Viewing Network Interfaces
- Configuring External IP Addresses
- Configuring Port Channel and Load Balancing Settings
- Configuring IP General Settings
- Configuring IP ACL for IPv4
- Configuring Static IPv4 Routes
- Configuring DSR VIP

**Enabling FTP Services**

To enable FTP services to listen for connection requests, do the following:

**Step 1**  
Choose **Devices > Devices > General Settings > Network > FTP**. The FTP Settings page is displayed.

**Step 2**  
Check the **Enable FTP Services** check box.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

**Enabling DNS**

DNS Settings are required on all SEs, SRs, and VOS Ms. The SEs need to be able to resolve the content origin server host name, the SRs need to be able to communicate with the DNS servers, and the VOSMs need to resolve host names.

To configure Domain Name System (DNS) servers, do the following:

**Step 1**  
Choose **Devices > Devices > General Settings > Network > DNS**. The DNS Settings page is displayed.

**Step 2**  
Enter the settings as appropriate. See **Table 5-18** for a description of the fields.
Enabling RCP

Remote Copy Protocol (RCP) lets you download, upload, and copy configuration files between remote hosts and a switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection oriented. This service listens for requests on TCP port 514.

To enable RCP services, do the following:

1. Choose Devices > Devices > General Settings > Network > RCP. The RCP page is displayed.
2. Check the RCP Enable check box to have the RCP services listen for RCP requests.
3. Click Submit to save the settings.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.

Configuring NTP

To configure the device to synchronize its clock with an NTP server, do the following:

1. Choose Devices > Devices > General Settings > Network > NTP. The NTP page is displayed.
2. Check Enable to enable NTP.
3. In the NTP Server field, enter the IP address or hostname of up to four NTP servers. Use a space to separate the entries.
4. Click Submit to save the settings.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.
To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

### Setting the Time Zone

If you have an outside source on your network that provides time services, such as an NTP server, you do not need to set the system clock manually. When manually setting the clock, enter the local time. The device calculates Coordinated Universal Time (UTC) based on the time zone set.

---

**Note**

Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at startup to initialize the software clock.

---

**Caution**

We highly recommend that you use NTP servers to synchronize the devices in your VDS-OS network. If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

To manually configure the time zone, do the following:

---

**Step 1**

Choose **Devices > Devices > General Settings > Network > Time Zone**. The Time Zone page is displayed with the default settings of UTC (offset = 0) and no daylight savings time configured.

**Step 2**

To configure a standard time zone, do the following:

- a. Click the **Standard Time Zone** radio button.

  The standard convention for time zones uses a **Location/Area** format in which **Location** is a continent or a geographic region of the world and **Area** is a time zone region within that location. For a list of standard time zones that can be configured and their UTC offsets, see **Table 5-19** on page 5-37.

- b. From the **Standard Time Zone** drop-down list, choose a location for the time zone. The page refreshes, displaying all area time zones for the chosen location in the second drop-down list.

- c. Choose an area for the time zone.

  The UTC offset (hours and minutes ahead or behind UTC) for the corresponding time zone is displayed. During summer time savings, the offset may differ and is displayed accordingly.

**Note**

Some of the standard time zones (mostly time zones within the United States) have daylight savings time zones configured automatically.

**Step 3**

To configure a customized time zone, do the following:

- a. Click the **Customized Time Zone** radio button.

- b. In the **Customized Time Zone** field, enter a name to for the time zone. The time zone entry is case sensitive and can contain up to 40 characters. Spaces are not allowed. If you specify any of the standard time zone names, an error message is displayed when you click **Submit**.
c. For UTC offset, choose + or – from the UTC Offset drop-down list to indicate whether the configured time zone is ahead or behind UTC. Also, choose the number of hours (0 to 23) and minutes (0 to 59) offset from UTC for the customized time zone. The range for the UTC offset is from –23:59 to 23:59, and the default is 0:0.

Step 4 To configure customized summer time savings, do the following:

Note Customized summer time can be specified for both standard and customized time zones.

The start and end dates for summer time can be configured in two ways: absolute dates or recurring dates. Absolute dates apply once and must be reset every year. Recurring dates apply every year.

a. Click the Absolute Dates radio button to configure summer settings once.

b. In the Start Date and End Date fields, specify the month, day, and year that the summer time savings starts and ends in mm/dd/yyyy format. Alternatively, click the Calendar icon and select a date. The chosen date is highlighted in blue. Click Apply.

c. Click the Recurring Dates radio button to configure a recurring summer setting.

d. Using the drop-down lists, choose the start day, week, and month when the summer time savings starts. For example, if the summer time savings begins the first Sunday in March, you would select Sunday, 1st, March from the drop-down lists.

e. Using the drop-down lists, choose the start day, week, and month when the summer time savings ends.

Step 5 Using the Start Time drop-down lists and the End Time drop-down lists, choose the hour (0 to 23) and minute (0 to 59) at which daylight savings time starts and ends.

Start Time and End Time fields for summer time are the times of the day when the clock is changed to reflect summer time. By default, both start and end times are set at 00:00.

Step 6 In the Offset field, specify the minutes offset from UTC (0 to 1439). (See Table 5-19 on page 5-37.) The summer time offset specifies the number of minutes that the system clock moves forward at the specified start time and backward at the end time.

Step 7 To not specify a summer or daylight savings time for the corresponding time zone, click the No Customized Summer Time Configured radio button.

Step 8 Click Submit to save the settings.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.

Table 5-19 lists the UTC offsets for the different locations around the world.

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Offset from UTC (in hours)</th>
<th>Time Zone</th>
<th>Offset from UTC (in hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa/Algiers</td>
<td>+1</td>
<td>Asia/Vladivostok</td>
<td>+10</td>
</tr>
<tr>
<td>Africa/Cairo</td>
<td>+2</td>
<td>Asia/Yekaterinburg</td>
<td>+5</td>
</tr>
<tr>
<td>Africa/Casablanca</td>
<td>0</td>
<td>Asia/Yakutsk</td>
<td>+9</td>
</tr>
</tbody>
</table>
Table 5-19  Time Zone—Offset from UTC (continued)

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Offset from UTC (in hours)</th>
<th>Time Zone</th>
<th>Offset from UTC (in hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa/Harare</td>
<td>+2</td>
<td>Australia/Adelaide</td>
<td>+9.30</td>
</tr>
<tr>
<td>Africa/Johannesburg</td>
<td>+2</td>
<td>Australia/Brisbane</td>
<td>+10</td>
</tr>
<tr>
<td>Africa/Nairobi</td>
<td>+3</td>
<td>Australia/Darwin</td>
<td>+9.30</td>
</tr>
<tr>
<td>America/Buenos_Aires</td>
<td>–3</td>
<td>Australia/Hobart</td>
<td>+10</td>
</tr>
<tr>
<td>America/Caracas</td>
<td>–4</td>
<td>Australia/Perth</td>
<td>+8</td>
</tr>
<tr>
<td>America/Mexico_City</td>
<td>–6</td>
<td>Australia/Sydney</td>
<td>+10</td>
</tr>
<tr>
<td>America/Lima</td>
<td>–5</td>
<td>Canada/Atlantic</td>
<td>–4</td>
</tr>
<tr>
<td>America/Santiago</td>
<td>–4</td>
<td>Canada/Newfoundland</td>
<td>–3.30</td>
</tr>
<tr>
<td>Atlantic/Azores</td>
<td>–1</td>
<td>Canada/Saskatchewan</td>
<td>–6</td>
</tr>
<tr>
<td>Atlantic/Cape_Verde</td>
<td>–1</td>
<td>Europe/Athens</td>
<td>+2</td>
</tr>
<tr>
<td>Asia/Almaty</td>
<td>+6</td>
<td>Europe/Berlin</td>
<td>+1</td>
</tr>
<tr>
<td>Asia/Baghdad</td>
<td>+3</td>
<td>Europe/Bucharest</td>
<td>+2</td>
</tr>
<tr>
<td>Asia/Baku</td>
<td>+4</td>
<td>Europe/Helsinki</td>
<td>+2</td>
</tr>
<tr>
<td>Asia/Bangkok</td>
<td>+7</td>
<td>Europe/London</td>
<td>0</td>
</tr>
<tr>
<td>Asia/Colombo</td>
<td>+6</td>
<td>Europe/Moscow</td>
<td>+3</td>
</tr>
<tr>
<td>Asia/Dacca</td>
<td>+6</td>
<td>Europe/Paris</td>
<td>+1</td>
</tr>
<tr>
<td>Asia/Hong_Kong</td>
<td>+8</td>
<td>Europe/Prague</td>
<td>+1</td>
</tr>
<tr>
<td>Asia/Irkutsk</td>
<td>+8</td>
<td>Europe/Warsaw</td>
<td>+1</td>
</tr>
<tr>
<td>Asia/Jerusalem</td>
<td>+2</td>
<td>Japan</td>
<td>+9</td>
</tr>
<tr>
<td>Asia/Kabul</td>
<td>+4.30</td>
<td>Pacific/Auckland</td>
<td>+12</td>
</tr>
<tr>
<td>Asia/Karachi</td>
<td>+5</td>
<td>Pacific/Fiji</td>
<td>+12</td>
</tr>
<tr>
<td>Asia/Katmandu</td>
<td>+5.45</td>
<td>Pacific/Guam</td>
<td>+10</td>
</tr>
<tr>
<td>Asia/Krasnoyarsk</td>
<td>+7</td>
<td>Pacific/Kwajalein</td>
<td>–12</td>
</tr>
<tr>
<td>Asia/Magadan</td>
<td>+11</td>
<td>Pacific/Samoan</td>
<td>–11</td>
</tr>
<tr>
<td>Asia/Muscat</td>
<td>+4</td>
<td>US/Alaska</td>
<td>–9</td>
</tr>
<tr>
<td>Asia/New Delhi</td>
<td>+5.30</td>
<td>US/Central</td>
<td>–6</td>
</tr>
<tr>
<td>Asia/Rangoon</td>
<td>+6.30</td>
<td>US/Eastern</td>
<td>–5</td>
</tr>
<tr>
<td>Asia/Riyadh</td>
<td>+3</td>
<td>US/East–Indiana</td>
<td>–5</td>
</tr>
<tr>
<td>Asia/Seoul</td>
<td>+9</td>
<td>US/Hawaii</td>
<td>–10</td>
</tr>
<tr>
<td>Asia/Singapore</td>
<td>+8</td>
<td>US/Mountain</td>
<td>–7</td>
</tr>
<tr>
<td>Asia/Taipei</td>
<td>+8</td>
<td>US/Pacific</td>
<td>–8</td>
</tr>
<tr>
<td>Asia/Tehran</td>
<td>+3.30</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The offset time (number of hours ahead or behind UTC) as displayed in the table is in effect during winter time. During summer time or daylight savings time, the offset may be different from the values in the table and is calculated and displayed accordingly by the system clock.
**Viewing Network Interfaces**

The Network Interfaces page is informational only. To view this information, choose **Devices > Devices > General Settings > Network > Network Interfaces**. Information about the network interfaces configured for the device is displayed.

**Configuring External IP Addresses**

The External IP page allows you to configure up to eight Network Address Translation (NAT) IP addresses. This allows a router to translate up to eight internal addresses to registered unique addresses and translate external registered addresses to addresses that are unique to the private network.

To configure NAT IP addresses, do the following:

**Step 1** Choose **Devices > Devices > General Settings > Network > External IP**. The External IP Settings page is displayed.

**Step 2** Check the **Enable** check box.

**Step 3** In the External IP Address fields (1–8), enter up to eight IP addresses.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

**Configuring Port Channel and Load Balancing Settings**

For information about configuring port channels using the CLI, see the “Redundant Dedicated Management Ports” section on page D-1.

To configure load balancing on port channels, do the following:

**Step 1** Choose **Devices > Devices > General Settings > Network > Port Channel Settings**. The Port Channel Settings page is displayed.

**Step 2** From the **Load Balancing Method** drop-down list, choose one of the following load balancing methods:

- **dst-ip**—Destination IP address
- **dst-mac**—Destination MAC address
- **dst-mixed-ip-port**—Destination IP address and TCP/UDP port
- **dst-port**—Destination port
- **round robin**—Each interface in the channel group
- **src-dst-ip**—Source and destination IP address
- **src-dst-mac**—Source and destination MAC address
- **src-dst-mixed-ip-port**—Source destination IP address and source destination port
- **src-dst-port**—Source and destination port
- **src-mixed-ip-port**—Source IP address and source destination port
- **src-port**—Source port
Configuring the Service Engine

Round robin allows traffic to be distributed evenly among all interfaces in the channel group. The other balancing options give you the flexibility to choose specific interfaces (by IP address, MAC address, port) when sending an Ethernet frame.

The source and destination options mean that while calculating the outgoing interface, take into account both the source and destination (MAC address or port).

**Note**  
Round-robin load-balancing mode is not supported when Link Aggregation Control Protocol (LACP) is enabled on the port channel.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

**Configuring IP General Settings**

The Path Maximum Transmission Unit (MTU) Discovery discovers the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By using the largest MTU the links can support, the sending device can minimize the number of packets it must send.

**Note**  
The Path MTU Discovery is a process initiated by the sending device. If a server does not support IP Path MTU Discovery, the receiving device has no mechanism available to avoid fragmenting datagrams generated by the server.

To enable Path MTU Discovery, do the following:

**Step 1**  
Choose **Devices > Devices > General Settings > Network > IP General Settings**. The IP General Settings page is displayed.

**Step 2**  
Check **Enable Path MTU Discovery**.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

**Configuring IP ACL for IPv4**

Access control lists (ACLs) provide a means to filter packets by allowing a user to permit or deny IP packets from crossing specified interfaces. Packet filtering helps to control packet movement through the network. Such control can help limit network traffic and restrict network use by certain users or devices.

You can also apply ACLs to management services such as SNMP, SSH, HTTPS, Telnet, and FTP. ACLs can be used to control the traffic that these applications provide by restricting the type of traffic that the applications handle.
In a managed VDS-OS network environment, administrators need to be able to prevent unauthorized access to various devices and services. VDS-OS supports standard and extended ACLs that allow administrators to restrict access to or through a VDS-OS network device, such as the SE. Administrators can use ACLs to reduce the infiltration of hackers, worms, and viruses that can harm the network.

ACLs provide controls that allow various services to be tied to a particular interface. For example, the administrator can use IP ACLs to define a public interface on the Service Engine for content serving and a private interface for management services (for example, Telnet, SSH, SNMP, HTTPS, and software upgrades). A device attempting to access one of the services must be on a list of trusted devices before it is allowed access. The implementation of ACLs for incoming traffic on certain ports for a particular protocol type is similar to the ACL support for the Cisco Global Site Selector and Cisco routers.

To use ACLs, the system administrator must first configure ACLs and then apply them to specific services. The following are some examples of how IP ACLs can be used in various enterprise deployments:

- Application layer proxy firewall with a hardened outside interface has no ports exposed. (Hardened means that the interface carefully restricts which ports are available for access primarily for security reasons. Because the interface is outside, many types of attacks are possible.) The device’s outside address is globally accessible from the Internet, while its inside address is private. The inside interface has an ACL to limit Telnet, SSH, and VOSM traffic.

- Device is deployed anywhere within the enterprise. Like routers and switches, the administrator wants to limit Telnet, SSH, and VOSM access to the IT source subnets.

- Device is deployed as a reverse proxy in an untrusted environment, and the administrator wishes to allow only port 80 inbound traffic on the outside interface and outbound connections on the back-end interface.

**Note**

IP ACLs are defined for individual devices only. IP ACLs cannot be managed through device groups.

When you create an IP ACL, you should note the following constraints:

- IP ACL names must be unique within the device.
- IP ACL names must be limited to 30 characters and contain no spaces or special characters.
- VOSM can manage up to 50 IP ACLs and a total of 500 conditions per device.
- When the IP ACL name is numeric, numbers 1 through 99 denote standard IP ACLs and numbers 100 through 199 denote extended IP ACLs. IP ACL names that begin with a number cannot contain nonnumeric characters.
- Extended IP ACLs cannot be used with SNMP applications.

**Creating a New IP ACL**

To create a new IP ACL, do the following:

**Step 1** Choose Devices > Devices > General Settings > Network > IP ACL for IPv4 addressing. The IP ACL Table page is displayed. The table is sortable by clicking the column headings.

**Step 2** Click the Create New icon in the task bar. The IP ACL page is displayed. To edit an ACL, click the Edit icon next to the name you want to edit.

**Step 3** In the Name field, enter a name, observing the naming rules for IP ACLs.
Step 4 From the ACL Type drop-down list, choose an IP ACL type (Standard or Extended). The default is Standard.

Step 5 Click Submit. The page refreshes and the Modifying IP ACL page for a newly created IP ACL is displayed.

Note Clicking Submit at this point merely saves the IP ACL; IP ACLs without any conditions defined do not appear on the individual devices.

Adding Conditions to an IP ACL
To add conditions to an IP ACL, do the following:

Step 1 Choose Devices > Devices > General Settings > Network > IP ACL for IPv4 addressing. The IP ACL Table page is displayed.

Step 2 Click the Edit icon next to the name of the IP ACL you want to add a condition to. The Modifying IP ACL page is displayed.

Step 3 Click the Create New icon in the task bar. The Condition page is displayed.

To edit a condition, click the Edit icon next to the name you want to edit.

Note The number of available fields for creating IP ACL conditions depends on whether the IP ACL type is standard or extended.

Step 4 Enter values for the properties that are enabled for the type of IP ACL that you are creating.
- To create a standard IP ACL, go to Step 5.
- To create an extended IP ACL, go to Step 6.

Step 5 To set up conditions for a standard IP ACL, do the following:

a. From the Purpose drop-down list, choose a purpose (Permit or Deny).

b. In the Source IP field, enter the source IP address.

c. In the Source IP Wildcard field, enter a source IP wildcard address.

d. Click Submit. The Modifying IP ACL page is displayed showing the new condition and its configuration.

e. To add another condition to the IP ACL, repeat the steps.

f. To reorder your list of conditions in the Modifying IP ACL page, use the Up arrow or Down arrow in the Order column, or click a column heading to sort by any configured parameter.

Note The order of the conditions listed becomes the order in which IP ACLs are applied to the device.

g. When you have finished adding conditions to the IP ACL, and you are satisfied with all your entries and the order in which the conditions are listed, click Submit in the Modifying IP ACL page to commit the IP ACL to the device database.
A green “Change submitted” indicator appears in the lower right corner of the Modifying IP ACL page to indicate that the IP ACL is being submitted to the device database.

Table 5-20 describes the fields in a standard IP ACL.

### Table 5-20  Standard IP ACL Conditions

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Permit</td>
<td>Specifies whether a packet is to be passed (Permit) or dropped (Deny).</td>
</tr>
<tr>
<td>Source IP</td>
<td>0.0.0.0</td>
<td>IP address of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4.</td>
</tr>
<tr>
<td>Source IP</td>
<td>255.255.255.255</td>
<td>Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.</td>
</tr>
</tbody>
</table>

1. Required field.

#### Step 6

To set up conditions for an extended IP ACL, do the following:

a. From the Purpose drop-down list, choose a purpose (Permit or Deny).

b. From the Extended Type drop-down list, choose Generic, TCP, UDP, or ICMP.

After you choose a type of extended IP ACL, various options become available depending on what type you choose.

c. Enter the settings as appropriate. See Table 5-21 for descriptions of the extended IP ACL fields.

d. Click Submit. The Modifying IP ACL page is displayed showing the new condition and its configuration.

e. To add another condition to the IP ACL, repeat the steps.

f. To reorder your list of conditions from the Modifying IP ACL page, use the Up arrow or Down arrow in the Order column, or click a column heading to sort by any configured parameter.

**Note**  The order of the conditions listed becomes the order in which IP ACLs are applied to the device.

g. When you have finished adding conditions to the IP ACL, and you are satisfied with all your entries and the order in which the conditions are listed, click Submit in the Modifying IP ACL page to commit the IP ACL to the device database.

A green “Change submitted” indicator appears in the lower-left corner of the Modifying IP ACL page to indicate that the IP ACL is being submitted to the device database.
**Table 5-21  Extended IP ACL Conditions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Description</th>
<th>Extended Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong>&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Permit</td>
<td>Specifies whether a packet is to be passed (<strong>Permit</strong>) or dropped (<strong>Deny</strong>).</td>
<td>Generic, TCP, UDP, ICMP</td>
</tr>
<tr>
<td>Protocol</td>
<td>ip</td>
<td>Internet protocol (<strong>gre, icmp, ip, tcp, or udp</strong>) To match any Internet protocol, use the <strong>ip</strong> keyword.</td>
<td>Generic</td>
</tr>
<tr>
<td>Established</td>
<td>Unchecked (false)</td>
<td>When checked, a match with the ACL condition occurs if the TCP datagram has the ACK or RST bits set, indicating an established connection. Initial TCP datagrams used to form a connection are not matched.</td>
<td>TCP</td>
</tr>
<tr>
<td>Source IP&lt;sup&gt;1&lt;/sup&gt;</td>
<td>0.0.0.0</td>
<td>IP address of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4.</td>
<td>Generic, TCP, UDP, ICMP</td>
</tr>
<tr>
<td>Source IP Wildcard&lt;sup&gt;1&lt;/sup&gt;</td>
<td>255.255.255.255</td>
<td>Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.</td>
<td>Generic, TCP, UDP, ICMP</td>
</tr>
<tr>
<td>Source Prefix</td>
<td>255.255.255.255</td>
<td>Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.</td>
<td>Generic, TCP, UDP, ICMP</td>
</tr>
<tr>
<td>Source Port 1</td>
<td>0</td>
<td>Decimal number or name of a port. Valid port numbers are 0 to 65535. See <strong>Table 5-22</strong> and <strong>Table 5-23</strong> for port name descriptions and associated port numbers.</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Source Port 2</td>
<td>65535</td>
<td>Decimal number or name of a port. See Source Port 1.</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Source Operator</td>
<td>range</td>
<td>Specifies how to compare the source ports against incoming packets. Choices are &lt;, &gt;, ==, !=, or <strong>range</strong>.</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Destination IP</td>
<td>0.0.0.0</td>
<td>IP address of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4.</td>
<td>Generic, TCP, UDP, ICMP</td>
</tr>
<tr>
<td>Destination IP Wildcard</td>
<td>255.255.255.255</td>
<td>Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.</td>
<td>Generic, TCP, UDP, ICMP</td>
</tr>
<tr>
<td>Destination Prefix</td>
<td>255.255.255.255</td>
<td>Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.</td>
<td>Generic, TCP, UDP, ICMP</td>
</tr>
</tbody>
</table>

**Valid TCP port names are as follows:**
- domain
- exec
- ftp
- ftp-data
- https
- nfs
- rtsp
- ssh
- telnet
- www

**Valid UDP port names are as follows:**
- bootpc
- bootps
- domain
- netbios-dgm
- netbios-ns
- netbios-ss
- nfs
- ntp
- snmp
- snmptrap
### Table 5-21  Extended IP ACL Conditions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Description</th>
<th>Extended Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Port 1</td>
<td>0</td>
<td>Decimal number or name of a port. Valid port numbers are 0 to 65535.</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Table 5-22 and Table 5-23 for port name descriptions and associated port numbers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid TCP port names are as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• exec</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ftp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ftp-data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• https</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• nfs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• rtsp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ssh</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• telnet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• www</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid UDP port names are as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bootpc</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bootps</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• netbios-dgm</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• netbios-ns</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• netbios-ss</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• nfs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ntp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• snmp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• snmptrap</td>
<td></td>
</tr>
<tr>
<td>Destination Operator</td>
<td>range</td>
<td>Specifies how to compare the destination ports against incoming packets.</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Choices are &lt;, &gt;, ==, !=, or range.</td>
<td></td>
</tr>
<tr>
<td>Destination Port 2</td>
<td>65535</td>
<td>Decimal number or name of a port. Valid port numbers are 0 to 65535.</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Destination Port 1.</td>
<td></td>
</tr>
<tr>
<td>ICMP Param Type¹</td>
<td>None</td>
<td>Choices are None, Type/Code, or Msg.</td>
<td>ICMP</td>
</tr>
<tr>
<td>ICMPv6 Param Type</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP Message¹</td>
<td>administratively-prohibited</td>
<td>Allows a combination of ICMP type and code to be specified using a keyword chosen from the drop-down list.</td>
<td>ICMP</td>
</tr>
<tr>
<td>ICMPv6 Message</td>
<td></td>
<td>See Table 5-24 for descriptions of the ICMP messages.</td>
<td></td>
</tr>
<tr>
<td>ICMP Type¹</td>
<td>0</td>
<td>Number from 0 to 255. This field is enabled when you choose Type/Code.</td>
<td>ICMP</td>
</tr>
<tr>
<td>ICMPv6 Type</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use ICMP Code¹</td>
<td>Unchecked</td>
<td>When checked, enables the ICMP Code field.</td>
<td>ICMP</td>
</tr>
<tr>
<td>Use ICMPv6 Code</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP Code¹</td>
<td>0</td>
<td>Number from 0 to 255. Message code option that allows ICMP messages of a particular type to be further filtered by an ICMP message code.</td>
<td>ICMP</td>
</tr>
<tr>
<td>ICMPv6 Code</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹. Required field.
Table 5-22 lists the UDP keywords that you can use with extended access control lists.

**Table 5-22   UDP Keywords and Port Numbers**

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Description</th>
<th>UDP Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootpc</td>
<td>Bootstrap Protocol (BOOTP) client service</td>
<td>68</td>
</tr>
<tr>
<td>bootps</td>
<td>Bootstrap Protocol (BOOTP) server service</td>
<td>67</td>
</tr>
<tr>
<td>domain</td>
<td>Domain Name System (DNS) service</td>
<td>53</td>
</tr>
<tr>
<td>netbios-dgm</td>
<td>NetBIOS datagram service</td>
<td>138</td>
</tr>
<tr>
<td>netbios-ns</td>
<td>NetBIOS name resolution service</td>
<td>137</td>
</tr>
<tr>
<td>netbios-ss</td>
<td>NetBIOS session service</td>
<td>139</td>
</tr>
<tr>
<td>nfs</td>
<td>Network File System service</td>
<td>2049</td>
</tr>
<tr>
<td>ntp</td>
<td>Network Time Protocol settings</td>
<td>123</td>
</tr>
<tr>
<td>snmp</td>
<td>Simple Network Management Protocol service</td>
<td>161</td>
</tr>
<tr>
<td>snmptrap</td>
<td>SNMP traps</td>
<td>162</td>
</tr>
</tbody>
</table>

Table 5-23 lists the TCP keywords that you can use with extended access control lists.

**Table 5-23   TCP Keywords and Port Numbers**

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Description</th>
<th>TCP Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>Domain Name System service</td>
<td>53</td>
</tr>
<tr>
<td>exec</td>
<td>Remote process execution</td>
<td>512</td>
</tr>
<tr>
<td>ftp</td>
<td>File Transfer Protocol service</td>
<td>21</td>
</tr>
<tr>
<td>ftp-data</td>
<td>FTP data connections (used infrequently)</td>
<td>20</td>
</tr>
<tr>
<td>https</td>
<td>Secure HTTP service</td>
<td>443</td>
</tr>
<tr>
<td>nfs</td>
<td>Network File System service applications</td>
<td>2049</td>
</tr>
<tr>
<td>rtsp</td>
<td>Real-Time Streaming Protocol applications</td>
<td>554</td>
</tr>
<tr>
<td>ssh</td>
<td>Secure Shell login</td>
<td>22</td>
</tr>
<tr>
<td>telnet</td>
<td>Remote login using Telnet</td>
<td>23</td>
</tr>
<tr>
<td>www</td>
<td>World Wide Web (HTTP) service</td>
<td>80</td>
</tr>
</tbody>
</table>

Table 5-24 lists the keywords that you can use to match specific ICMP message types and codes.

**Table 5-24   Keywords for ICMP Message Type and Code**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>administratively-prohibited</td>
<td>Messages that are administratively prohibited from being allowed access.</td>
</tr>
<tr>
<td>alternate-address</td>
<td>Messages that specify alternate IP addresses.</td>
</tr>
<tr>
<td>conversion-error</td>
<td>Messages that denote a datagram conversion error.</td>
</tr>
<tr>
<td>dod-host-prohibited</td>
<td>Messages that signify a Department of Defense (DoD) protocol Internet host denial.</td>
</tr>
</tbody>
</table>
### Table 5-24 Keywords for ICMP Message Type and Code (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dod-net-prohibited</td>
<td>Messages that specify a DoD protocol network denial.</td>
</tr>
<tr>
<td>echo</td>
<td>Messages that are used to send echo packets to test basic network connectivity.</td>
</tr>
<tr>
<td>echo-reply</td>
<td>Messages that are used to send echo reply packets.</td>
</tr>
<tr>
<td>general-parameter-problem</td>
<td>Messages that report general parameter problems.</td>
</tr>
<tr>
<td>host-isolated</td>
<td>Messages that indicate that the host is isolated.</td>
</tr>
<tr>
<td>host-precedence-unreachable</td>
<td>Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable). This is the most common response. Large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions.</td>
</tr>
<tr>
<td>host-redirect</td>
<td>Messages that specify redirection to a host.</td>
</tr>
<tr>
<td>host-tos-redirect</td>
<td>Messages that specify redirection to a host for type of service-based (ToS) routing.</td>
</tr>
<tr>
<td>host-tos-unreachable</td>
<td>Messages that denote that the host is unreachable for ToS-based routing.</td>
</tr>
<tr>
<td>host-unknown</td>
<td>Messages that specify that the host or source is unknown.</td>
</tr>
<tr>
<td>host-unreachable</td>
<td>Messages that specify that the host is unreachable.</td>
</tr>
<tr>
<td>information-reply</td>
<td>Messages that contain domain name replies.</td>
</tr>
<tr>
<td>information-request</td>
<td>Messages that contain domain name requests.</td>
</tr>
<tr>
<td>mask-reply</td>
<td>Messages that contain subnet mask replies.</td>
</tr>
<tr>
<td>mask-request</td>
<td>Messages that contain subnet mask requests.</td>
</tr>
<tr>
<td>mobile-redirect</td>
<td>Messages that specify redirection to a mobile host.</td>
</tr>
<tr>
<td>net-redirect</td>
<td>Messages that are used for redirection to a different network.</td>
</tr>
<tr>
<td>net-tos-redirect</td>
<td>Messages that are used for redirection to a different network for ToS-based routing.</td>
</tr>
<tr>
<td>net-tos-unreachable</td>
<td>Messages that specify that the network is unreachable for the ToS-based routing.</td>
</tr>
<tr>
<td>net-unreachable</td>
<td>Messages that specify that the network is unreachable.</td>
</tr>
<tr>
<td>network-unknown</td>
<td>Messages that denote that the network is unknown.</td>
</tr>
<tr>
<td>no-room-for-option</td>
<td>Messages that specify the requirement of a parameter, but that no room is available for it.</td>
</tr>
<tr>
<td>option-missing</td>
<td>Messages that specify the requirement of a parameter, but that parameter is not available.</td>
</tr>
<tr>
<td>packet-too-big</td>
<td>Messages that specify that the ICMP packet requires fragmentation but the Do Not Fragment (DF) bit is set.</td>
</tr>
<tr>
<td>parameter-problem</td>
<td>Messages that signify parameter-related problems.</td>
</tr>
<tr>
<td>port-unreachable</td>
<td>Messages that specify that the port is unreachable.</td>
</tr>
<tr>
<td>precedence-unreachable</td>
<td>Messages that specify that host precedence is not available.</td>
</tr>
</tbody>
</table>
Configuring the Service Engine

Chapter 5  Configuring Devices

Configuring the Service Engine

Applying an IP ACL to an Interface

The IP ACLs can be applied to a particular interface (such as management services to a private IP address) so that the device can have one interface in a public IP address space that serves content and another interface in a private IP address space that the administrator uses for management purposes. This feature ensures that clients can access the Service Engine only in the public IP address space for serving content and not access it for management purposes. A device attempting to access one of these applications that is associated with an IP ACL must be on the list of trusted devices to be allowed access.

To apply an IP ACL to an interface from the CLI, use the following interface configuration command:

```
interface {GigabitEthernet | Portchannel | Standby | TenGigabitEthernet} slot/port [ip]
access-group {accesslistnumber | accesslistname} {in | out}
```
Deleting an IP ACL

You can delete an IP ACL, including all conditions and associations with network interfaces, or you can delete only the IP ACL conditions. Deleting all conditions allows you to change the IP ACL type if you choose to do so. The IP ACL entry continues to appear in the IP ACL listing; however, it is in effect nonexistent.

To delete an IP ACL, do the following:

**Step 1** Choose Devices > Devices > General Settings > Network > IP ACL for IPv4 addressing. The IP ACL Table page is displayed.

**Step 2** Click the Edit icon next to the name of the IP ACL that you want to delete. The Modifying IP ACL page is displayed. If you created conditions for the IP ACL, you have three options for deletion:

- **Delete ACL**—This option removes the IP ACL, including all conditions and associations with network interfaces and applications.
- **Delete All Conditions**—This option removes all the conditions, while preserving the IP ACL name.
- **Delete IP ACL Condition**—This option removes one condition from the ACL.

**Step 3** To delete the entire IP ACL, click Delete ACL in the task bar. You are prompted to confirm your action. Click OK. The record is deleted.

**Step 4** To delete only the conditions, click Delete All Conditions in the task bar. You are prompted to confirm your action. Click OK. The window refreshes, conditions are deleted, and the ACL Type field becomes available.

**Step 5** To delete one condition, do the following:

a. Click the Edit icon next to the condition. The condition settings are displayed.

b. Click the Delete IP ACL Condition icon in the task bar. The IP ACL table is displayed.

c. Click Submit to save the IP ACL table to the database.

Configuring Static IPv4 Routes

The Static IP Routes page allows you to configure a static IPv4 route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure a static IP route, do the following:

**Step 1** Choose Devices > Devices > General Settings > Network > Static IP Routes. The IP Route Table page is displayed.

The table is sortable by clicking the column headings.

**Step 2** Click the Create New icon in the task bar. The IP Route page is displayed.

To edit a static route, click the Edit icon next to the name you want to edit.

**Step 3** In the Destination Network Address field, enter the destination network IP address.

**Step 4** In the Netmask field, enter the destination host netmask.

**Step 5** In the Gateway’s IP Address field, enter the IP address of the gateway interface.

**Step 6** Click Submit to save the settings.
To delete a route, click the **Edit** icon for the route, then click the **Delete** icon in the task bar.

---

**Configuring DSR VIP**

The VDS-OS supports Virtual IP (VIP) configuration for Direct Server Return (DSR) when working with networks that use load balancers. DSR bypasses the load balancer for all server responses to client requests by using MAC Address Translation (MAT).

The VDS-OS allows for the configuration of up to four VIPs (on loopback interfaces).

Client requests are sent to the load balancer and the load balancer sends the requests on to the Service Router. If DSR VIP is configured on the VDS-OS (and supported on the load balancer), all VDS-OS responses to the client are sent directly to the client, bypassing the load balancer.

---

**Note**

If DSR VIP is configured on an SE, the DSR VIP IP address cannot be the same as the origin service FQDN (OFQDN).

To configure a DSR VIP, do the following:

---

**Step 1** Choose Devices > Devices > General Settings > Network > DSR VIP. The DSR VIP page is displayed.

**Step 2** In the **Direct Server Return VIP 1** field, enter the IPv4 address of the Direct Server Return VIP.

**Step 3** Enter any additional DSR VIPs in the remaining fields (Direct Server Return VIP 2 to 4).

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

**Configuring Notification and Tracking**

The Notification and Tracking pages provide settings for alarms, thresholds, SNMP connectivity, and device monitoring. Configuring notification and tracking consists of the following procedures:

- Enabling Alarm Overload Detection
- Setting Service Monitor Thresholds
- Configuring SNMP
- Enabling System Logs

**Alarm Settings**

The Alarm Settings page covers the following configuration settings:

- Enabling Alarm Overload Detection
- Alarms for Admin Shutdown Interface
Enabling Alarm Overload Detection

The device tracks the rate of incoming alarms from the Node Health Manager. If the rate of incoming alarms exceeds the high-water mark (HWM) threshold, the device enters an alarm overload state. This condition occurs when multiple applications raise alarms at the same time. When a device is in an alarm overload state, the following events occur:

- Traps for the raise alarm-overload alarm and clear alarm-overload alarm are sent. SNMP traps for subsequent alarm raise-and-clear operations are suspended.
- Traps for alarm operations that occur between the raise-alarm-overload alarm and the clear-alarm-overload alarm operations are suspended, but individual device alarm information is still collected and available using the CLI.
- Device remains in an alarm overload state until the rate of incoming alarms decreases to less than the low-water mark (LWM).
- If the incoming alarm rate falls below the LWM, the device comes out of the alarm overload state and begins to report the alarm counts to the SNMP servers and the VOSM.

Alarms that have been raised on a device can be listed by using the CLI commands shown in Table 5-25. These CLI commands allow you to systematically drill down to the source of an alarm.

Table 5-25 Viewing Device Alarms

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show alarms</td>
<td></td>
<td>Displays a list of all currently raised alarms (critical, major, and minor alarms) on the device.</td>
</tr>
<tr>
<td>show alarms critical</td>
<td></td>
<td>Displays a list of only currently raised critical alarms on the device.</td>
</tr>
<tr>
<td>show alarms major</td>
<td></td>
<td>Displays a list of only currently raised major alarms on the device.</td>
</tr>
<tr>
<td>show alarms minor</td>
<td></td>
<td>Displays a list of only currently raised minor alarms on the device.</td>
</tr>
<tr>
<td>show alarms detail</td>
<td></td>
<td>Displays detailed information about the currently raised alarms.</td>
</tr>
<tr>
<td>show alarms history</td>
<td></td>
<td>Displays a history of alarms that have been raised and cleared on the device. The CLI retains the last 100 alarm raise and clear events only.</td>
</tr>
<tr>
<td>show alarms status</td>
<td></td>
<td>Displays the counts for the currently raised alarms on the device. Also lists the alarm-overload state and the alarm-overload settings.</td>
</tr>
</tbody>
</table>

To configure the alarm overload detection, do the following:

**Step 1** Choose Devices > Devices > General Settings > Notification and Tracking > Alarm Settings. The Alarm Settings page is displayed.

**Step 2** Uncheck the Enable Alarm Overload Detection check box if you do not want to configure the device to suspend alarm raise and clear operations when multiple applications report error conditions. Alarm overload detection is enabled by default.

**Step 3** In the Alarm Overload Low Water Mark field, enter the number of alarms per second for the clear alarm overload threshold. The low water mark is the level to which the number of alarms must drop below before alarm traps can be sent. The default value is 1.

**Step 4** In the Alarm Overload High Water Mark field, enter the number of alarms per second for the raise alarm-overload threshold. The high-water mark is the level the number of alarms must exceed before alarms are suspended. The default value is 10.
Step 5  Click **Submit** to save the settings.
To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

**Alarms for Admin Shutdown Interface**

When the **Alarms for Admin Shutdown Interface** check box is checked, the interface alarm is shutdown. If there is already an alarm raised when the setting is submitted, clearing the option and submitting the change does not clear the outstanding alarm. There are two ways to avoid this situation:

1. Clear the outstanding alarm first before disabling this option.
2. Disable this option and reboot. The alarm is cleared during reboot.

---

**Note**

The **Alarms for Admin Shutdown Interface** option should be enabled before any of the above for the alarm to take effect.

To enable the **Alarms for Admin Shutdown Interface** option, do the following:

**Step 1**  Choose **Devices > Devices > General Settings > Notification and Tracking > Alarm Settings**. The Alarm Settings page is displayed.

**Step 2**  Check the **Alarms for Admin Shutdown Interface** check box to enable this option.

**Step 3**  Click **Submit** to save the settings.
To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

**Setting Service Monitor Thresholds**

The Service Monitor page is where you configure workload thresholds for the device.

In load-based routing, these thresholds are used to determine the best device to serve requested content. For more information about load-based routing, see the “Configuring the Service Router” section on page 5-66.

---

**Note**

Threshold monitoring is performed on each device in the VDS-OS. The NIC bandwidth thresholds are only monitored on the SE. They are not monitored on the SR and VOSM.

---

**Note**

The base license limit is set to 200 sessions and 200 Mbps bandwidth.

- The burst count, which indicates the number of days after which a major alarm is raised, is configurable. On the Service Engine, use the **service-router service-monitor threshold burstcnt** command to configure the burst count. The default setting is one (1), which means all the minor alarms that occur in a single day (24-hour interval) are counted as one single alarm. If the **service-router service-monitor threshold burstcnt** command is set to two, all minor alarms that occur in two days (48-hour interval) are counted as a single alarm.
To configure workload thresholds, do the following:

**Step 1** Choose Devices > Devices > General Settings > Notification and Tracking > Service Monitor. The Service Monitor page is displayed.

**Step 2** Enter the settings as appropriate. See Table 5-26 for a description of the fields.

### Table 5-26 Service Monitor Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Allows the SR to collect CPU load information from the device.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Value (as a percentage) that determines when the device is overloaded. The threshold determines the extent of CPU usage allowed. The range is from 1 to 100. The default is 80.</td>
</tr>
<tr>
<td>Sample Period</td>
<td>Time interval (in seconds) between two consecutive samples. The sample period is the time during which the devices exchange keepalive messages that contain the device load information. The range is from 1 to 60. The default is 1.</td>
</tr>
<tr>
<td>Number of Samples</td>
<td>Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.</td>
</tr>
<tr>
<td><strong>Disk Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Allows the SR to collect disk transaction information from the device.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The threshold, as a percentage, determines the extent of disk I/O load allowed. The disk threshold is a disk I/O load threshold setting. It is not used to monitor disk usage, it is calculated using the kernel’s diskstats status. This represents how much disk I/O capacity the device is using. It is calculated across all disks on the device. The range is from 1 to 100. The default is 80.</td>
</tr>
<tr>
<td>Sample Period</td>
<td>Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.</td>
</tr>
<tr>
<td>Number of Samples</td>
<td>Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.</td>
</tr>
<tr>
<td><strong>Memory Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Allows the SR to collect memory usage information from the device.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The threshold (in percent) determines the extent of memory usage allowed. The range is from 1 to 100. The default is 80.</td>
</tr>
<tr>
<td>Sample Period</td>
<td>Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.</td>
</tr>
<tr>
<td>Number of Samples</td>
<td>Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.</td>
</tr>
<tr>
<td><strong>KMemory Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Allows the SR to collect kernel memory usage information from the device.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The threshold (in percent) determines the extent of kernel memory usage allowed. The range is from 1 to 100. The default is 50.</td>
</tr>
<tr>
<td>Sample Period</td>
<td>Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.</td>
</tr>
</tbody>
</table>
Chapter 5  Configuring Devices

Step 3  Click Submit to save the settings.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.
Augmentation Alarms

Augmentation alarms are soft alarms that send alerts before the threshold is reached. These alarms are applicable to all devices—Service Engines, Service Routers, and VOSMs. Augmentation thresholds apply to device parameters.

A different augmentation alarm is supported for each of the device-level thresholds. Based on the device parameters monitored by Service Monitor, the following minor alarms could be raised for device-level thresholds:

- CpuAugThreshold—Service Monitor CPU augmentation alarm.
- MemAugThreshold—Service Monitor memory augmentation alarm.
- KmemAugThreshold—Service Monitor kernel memory augmentation alarm.
- DiskAugThreshold—Service Monitor disk augmentation alarm.
- DiskFailCntAugThreshold—Service Monitor disk failure count augmentation alarm.
- NicAugThreshold—Service Monitor NIC augmentation alarm.

Check the augmentation threshold, device-level threshold, and average load for the above alarm instance. Add more devices if necessary. A useful command is the `show service-router service-monitor` command. The augmentation alarms raised are displayed in the `show alarms detail` command. The alarms are cleared when the load goes below the augmentation threshold.

Note

For system disks (disks that contain SYSTEM partitions), only when all system disks are bad is the diskfailure augmentation and threshold alarms raised. The diskfailcnt threshold does not apply to system disks. The threshold only applies to CDNFS disks, which is also the case for the augmentation thresholds. This is because the system disks use RAID1. There is a separate alarm for bad RAID. With the RAID system, if the critical primary disk fails, the other mirrored disk (mirroring only occurs for SYSTEM partitions) seamlessly continues operation. However, if the disk drive that is marked bad is a critical disk drive, the redundancy of the system disks for this device is affected. For more information on disk error handling and threshold recommendations, see the “Enabling Disk Error Handling” section on page 5-32.

As the `show disk details` command output reports, if disks have both SYSTEM and CDNFS partitions, they are treated as only system disks, which means they are not included in the accounting of the CDNFS disk calculation.

Note

The NIC augmentation alarm is only applicable if the device is an SE.

Configuring SNMP

The VDS-OS supports the following versions of SNMP:

- Version 1 (SNMPv1)—A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
- Version 2 (SNMPv2c)—The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.
Version 3 (SNMPv3)—An interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- Message integrity—Ensuring that a packet has not been tampered with in-transit.
- Authentication—Determining the message is from a valid source.
- Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

Table 5-27 identifies what the combinations of security models and levels mean.

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>noAuthNoPriv</td>
<td>Community String</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v2c</td>
<td>noAuthNoPriv</td>
<td>Community String</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>noAuthNoPriv</td>
<td>Username</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>authNoPriv</td>
<td>MD5 or SHA</td>
<td>No</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.</td>
</tr>
<tr>
<td>v3</td>
<td>authPriv</td>
<td>MD5 or SHA</td>
<td>DES</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.</td>
</tr>
</tbody>
</table>

The SNMPv3 agent can be used in the following modes:

- noAuthNoPriv mode (that is, no security mechanisms turned on for packets)
- AuthNoPriv mode (for packets that do not need to be encrypted using the privacy algorithm [DES 56])
- AuthPriv mode (for packets that must be encrypted; privacy requires that authentication be performed on the packet)

Using SNMPv3, users can securely collect management information from their SNMP agents without worrying that the data has been tampered with. Also, confidential information, such as SNMP set packets that change a Content Engine’s configuration, can be encrypted to prevent their contents from being exposed on the wire. Also, the group-based administrative model allows different users to access the same SNMP agent with varying access privileges.

Note the following about SNMPv3 objects:

- Each user belongs to a group.
- Group defines the access policy for a set of users.
- Access policy is what SNMP objects can be accessed for reading, writing, and creating.
Group determines the list of notifications its users can receive.
Group also defines the security model and security level for its users.

To configure the SNMP settings, do the following:

**Step 1** Choose Devices > Devices > General Settings > Notification and Tracking > SNMP > General Settings. The SNMP General Settings page is displayed.

**Step 2** Enable the settings as appropriate. See Table 5-28 for a description of the fields.

**Table 5-28 SNMP General Settings Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traps</td>
<td></td>
</tr>
<tr>
<td>Enable SNMP Settings</td>
<td>Enables the SNMP agent to transmit traps to the SNMP server.</td>
</tr>
<tr>
<td>Service Engine</td>
<td>Enables the Disk Fail trap, which is the disk failure error trap.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Enables SNMP-specific traps:</td>
</tr>
<tr>
<td></td>
<td>• Authentication—Enables authentication trap.</td>
</tr>
<tr>
<td></td>
<td>• Cold Start—Enables cold start trap.</td>
</tr>
<tr>
<td>SE Alarm</td>
<td>Enables alarm traps:</td>
</tr>
<tr>
<td></td>
<td>• Raise Critical—Enables raise-critical alarm trap.</td>
</tr>
<tr>
<td></td>
<td>• Clear Critical—Enables clear-critical alarm trap.</td>
</tr>
<tr>
<td></td>
<td>• Raise Major—Enables raise-major alarm trap.</td>
</tr>
<tr>
<td></td>
<td>• Clear Major—Enables clear-major alarm trap.</td>
</tr>
<tr>
<td></td>
<td>• Raise Minor—Enables raise-minor alarm trap.</td>
</tr>
<tr>
<td></td>
<td>• Clear Minor—Enables clear-minor alarm trap.</td>
</tr>
<tr>
<td>Entity</td>
<td>Enables SNMP entity traps.</td>
</tr>
<tr>
<td>Config</td>
<td>Enables CiscoConfigManEvent error traps.</td>
</tr>
<tr>
<td>Miscellaneous Settings</td>
<td></td>
</tr>
<tr>
<td>Notify Inform</td>
<td>Enables the SNMP notify inform request.</td>
</tr>
</tbody>
</table>

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

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.
To remove the settings from the device, click the Remove Settings icon in the task bar.

**Step 4** From the left-panel menu, click Community. The SNMP Community Table page is displayed.
The table is sortable by clicking the column headings. The maximum number of community strings that can be created is ten.

**Step 5** Click the Create New icon in the task bar. The SNMP Community page is displayed.
Click the Edit icon next to the community name to edit a community setting.
Note
Each community is associated with a group. Each group has a view and users are assigned to a group. If the group does not have a view associated with it, then users associated that group cannot access any MIB entry.

Step 6 Enter the settings as appropriate. See Table 5-29 for a description of the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community</td>
<td>Community string used as a password for authentication when you access the SNMP agent of the device using SNMPv1 or SNMPv2. The “Community Name” field of any SNMP message sent to the device must match the community string defined here to be authenticated. You can enter a maximum of 64 characters in this field.</td>
</tr>
<tr>
<td>Group name/rw</td>
<td>Group to which the community string belongs. The Read/Write option allows a read or write group to be associated with this community string. The Read/Write option permits access to only a portion of the MIB subtree. Choose one of the following three options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• None—Choose this option if you do not want to specify a group name to be associated with the community string.</td>
</tr>
<tr>
<td></td>
<td>• Read/Write—Choose this option if you want to allow read-write access to the group associated with this community string.</td>
</tr>
<tr>
<td></td>
<td>• Group—Choose this option if you want to specify a group name.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Name of the group to which the community string belongs. You can enter a maximum of 64 characters in this field. This field is available only if you have chosen the Group option in the Group name/rw field.</td>
</tr>
</tbody>
</table>

Step 7 Click Submit to save the settings.

To delete an SNMP community, click the Edit icon for the community, then click the Delete icon in the task bar.

Step 8 From the left-panel menu, click Group. The SNMP Group Table page is displayed.

The table is sortable by clicking the column headings. The maximum number of groups that can be created is ten.

Step 9 Click the Create New icon in the task bar. The SNMP Group page is displayed.

Click the Edit icon next to the Group Name to edit a group.

Step 10 Enter the settings as appropriate. See Table 5-30 for a description of the fields.
Chapter 5 Configuring Devices

Configuring the Service Engine

Table 5-30 SNMP Group Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the SNMP group. You can enter a maximum of 256 characters. A group defines a set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive. An SNMP group is a collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of the attributes defined by the group.</td>
</tr>
<tr>
<td>Security Model</td>
<td>Security model for the group. Choose one of the following options from the drop-down list:</td>
</tr>
<tr>
<td>v1</td>
<td>Version 1 security model (SNMP Version 1 [noAuthNoPriv]).</td>
</tr>
<tr>
<td>v2c</td>
<td>Version 2c security model (SNMP Version 2 [noAuthNoPriv]).</td>
</tr>
<tr>
<td>v3-auth</td>
<td>User security level SNMP Version 3 (AuthNoPriv).</td>
</tr>
<tr>
<td>v3-noauth</td>
<td>User security level SNMP Version 3 (noAuthNoPriv).</td>
</tr>
<tr>
<td>v3-priv</td>
<td>User security level SNMP Version 3 (AuthPriv).</td>
</tr>
</tbody>
</table>

The Security Model you choose determines which of the following three security algorithms is used on each SNMP packet:

- noAuthNoPriv—Authenticates a packet by a string match of the username.
- AuthNoPriv—Authenticates a packet by using either the HMAC MD5 or SHA algorithms.
- AuthPriv—Authenticates a packet by using either the HMAC MD5 or SHA algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.

<table>
<thead>
<tr>
<th>Read View</th>
<th>Name of the view (a maximum of 64 characters) that enables you only to view the contents of the agent. By default, no view is defined. To provide read access to users of the group, a view must be specified. A read view defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write View</td>
<td>Name of the view (a maximum of 64 characters) that enables you to enter data and configure the contents of the agent. By default, no view is defined. A write view defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.</td>
</tr>
<tr>
<td>Notify View</td>
<td>Name of the view (a maximum of 64 characters) that enables you to specify a notify, inform, or trap. By default, no view is defined. A notify view defines the list of notifications that can be sent to each user in the group.</td>
</tr>
</tbody>
</table>

Step 11 Click Submit to save the settings.

To delete an SNMP group, click the Edit icon for the group, then click the Delete icon in the task bar.

Step 12 From the left-panel menu, click User. The SNMP User Table page is displayed.
The table is sortable by clicking the column headings. The maximum number of users that can be created is ten.

**Step 13** Click the **Create New** icon in the task bar. The SNMP User page is displayed.

Click the **Edit** icon next to the username to edit a user.

**Step 14** Enter the settings as appropriate. See Table 5-31 for a description of the fields.

**Table 5-31 SNMP User Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String representing the name of the user (256 characters maximum) who can access the device. An SNMP user is a person for which an SNMP management operation is performed.</td>
</tr>
<tr>
<td>Group</td>
<td>Name of the group (256 characters maximum) to which the user belongs.</td>
</tr>
<tr>
<td>Remote SNMP ID</td>
<td>Globally unique identifier for a remote SNMP entity. To send an SNMPv3 message to the device, at least one user with a remote SNMP ID must be configured on the device. The SNMP ID must be entered in octet string format. For example, if the IP address of a remote SNMP entity is 192.147.142.129, then the octet string would be 00:00:63:00:00:00:a1:c0:93:8e:81.</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>Authentication algorithm that ensures the integrity of SNMP packets during transmission. Choose one of the following three options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>No-auth</strong>—Requires no security mechanism to be turned on for SNMP packets.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MD5</strong>—Provides authentication based on the hash-based Message Authentication Code Message Digest 5 (HMAC-MD5) algorithm.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SHA</strong>—Provides authentication based on the hash-based Message Authentication Code Secure Hash (HMAC-SHA) algorithm.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>String (256 characters maximum) that configures the user authentication (HMAC-MD5 or HMAC-SHA) password. The number of characters is adjusted to fit the display area if it exceeds the limit for display. This field is optional if the <strong>no-auth</strong> option is chosen for the authentication algorithm. Otherwise, this field must contain a value.</td>
</tr>
<tr>
<td>Confirmation Password</td>
<td>Authentication password for confirmation. The re-entered password must be the same as the one entered in the Authentication Password field.</td>
</tr>
<tr>
<td>Private Password</td>
<td>String (256 characters maximum) that configures the authentication (HMAC-MD5 or HMAC-SHA) parameters to enable the SNMP agent to receive packets from the SNMP host. The number of characters is adjusted to fit the display area if it exceeds the limit for display.</td>
</tr>
<tr>
<td>Confirmation Password</td>
<td>Private password for confirmation. The re-entered password must be the same as the one entered in the Private Password field.</td>
</tr>
</tbody>
</table>

**Step 15** Click **Submit** to save the settings.

To delete an SNMP user, click the **Edit** icon for the user, then click the **Delete** icon in the task bar.

**Step 16** To define a SNMPv2 MIB view, click **View** from the left-panel menu. The SNMP View Table page is displayed.
The table is sortable by clicking the column headings. The maximum number of SNMPv2 views that can be created is ten.

SNMP view—A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

**Step 17** Click the **Create New** icon in the task bar. The SNMP View page is displayed.

Click the **Edit** icon next to the username to edit a view.

**Step 18** Enter the settings as appropriate. See Table 5-32 for a description of the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String representing the name of this family of view subtrees (256 characters maximum). The family name must be a valid MIB name such as ENTITY-MIB.</td>
</tr>
<tr>
<td>Family</td>
<td>Object identifier (256 characters maximum) that identifies a subtree of the MIB.</td>
</tr>
<tr>
<td>View Type</td>
<td>View option that determines the inclusion or exclusion of the MIB family from the view. Choose one of the following two options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Included</strong>—The MIB family is included in the view.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Excluded</strong>—The MIB family is excluded from the view.</td>
</tr>
</tbody>
</table>

**Note** When configuring an SNMP View with Excluded, the specified MIB that is excluded is not accessible for the community associated with the group that has that view.

**Step 19** Click **Submit** to save the settings.

To delete an SNMP view, click the **Edit** icon for the view, then click the **Delete** icon in the task bar.

**Step 20** From the left-panel menu, click **Host**. The SNMP Host Table page is displayed.

The table is sortable by clicking the column headings. The maximum number of hosts that can be created is four.

**Step 21** Click the **Create New** icon in the task bar. The SNMP Host page is displayed.

Click the **Edit** icon next to the hostname to edit a host.

**Step 22** Enter the settings as appropriate. See Table 5-33 for a description of the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Host</td>
<td>Hostname or IP address an SNMP entity to which notifications (traps and informs) are to be sent.</td>
</tr>
<tr>
<td>Community/User</td>
<td>Name of the SNMP community or user (256 characters maximum) that is sent in SNMP trap messages from the device.</td>
</tr>
</tbody>
</table>
Table 5-33 \textit{SNMP Host Fields (continued)}

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Security model to use for sending notification to the recipient of an SNMP trap operation. Choose one of the following options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>\begin{itemize} \item \textbf{No-auth}—Sends notification without any security mechanism. \item \textbf{v2c}—Sends notification using Version 2c security. \item \textbf{Model v3-auth}—Sends notification using SNMP Version 3 (AuthNoPriv). \item \textbf{Security Level v3-noauth}—Sends notification using SNMP Version 3 (NoAuthNoPriv security). \item \textbf{Level v3-priv}—Sends notification using SNMP Version 3 (AuthPriv security). \end{itemize}</td>
</tr>
<tr>
<td>Retry</td>
<td>Number of retries (1 to 10) allowed for the inform request. The default is 2.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout for the inform request in seconds (1 to 1000). The default is 15.</td>
</tr>
</tbody>
</table>

\textbf{Step 23} Click \textit{Submit} to save the settings.

To delete an SNMP host, click the \textit{Edit} icon for the host, then click the \textit{Delete} icon in the task bar.

\textbf{Step 24} From the left-panel menu, click \textit{Asset Tag}. The SNMP Asset Tag page is displayed.

\textbf{Step 25} In the \textit{Asset Tag Name} field, enter a name for the asset tag and click \textit{Submit}.

To apply the factory default settings for the device, click the \textit{Apply Defaults} icon in the task bar.

To remove the settings from the device, click the \textit{Remove Settings} icon in the task bar.

\textbf{Step 26} From the left-panel menu, click \textit{Contact}. The SNMP Contact page is displayed.

\textbf{Step 27} In the \textit{Contact} field, enter a name of the contact person for this device.

\textbf{Step 28} In the \textit{Location} field, enter a location of the contact person for this device.

\textbf{Step 29} Click \textit{Submit} to save the settings.

To apply the factory default settings for the device, click the \textit{Apply Defaults} icon in the task bar.

To remove the settings from the device, click the \textit{Remove Settings} icon in the task bar.

\textbf{Supported MIBs}

The SNMP agent supports the following MIBs:

\begin{itemize} \item ENTITY-MIB (RFC 2037 Revision 199610310000Z)) \item MIB-II (RFC 1213) \item HOST-RESOURCES-MIB (RFC 2790, hrSWInstalled and hrPrinterTable subgroups are not supported) \item BGP-4-MIB (RFC-4274) \item UCD-SNMP-MIB \item CISCO-ENTITY-ASSET-MIB \item CISCO-CONFIG-MAN-MIB (Revision 9511280000Z) \item CISCO-SERVICE-ENGINE-MIB (supports streaming media-related MIB objects) \end{itemize}
ENTITY-MIB, MIB-II, HOST-RESOURCES-MIB, BGP-4-MIB, and UCD-SNMP-MIB are public-available MIBs.

To download a copy of the CISCO-SERVICE-ENGINE-MIB, do the following:

---

**Step 1**
Choose **System > Files > SNMP MIB.** The CISCO_SERVICE-ENGINE-MIB.my is listed.

**Step 2**
Click one of the following links:
- CISCO_SERVICE-ENGINE-MIB.my
- CISCO_CDS_SERVICE_ROUTING_MIB.my

Your browser program displays a dialog box asking if you want to open or save the file.

**Step 3**
Choose the appropriate option; either open or save the file.

---

For each 64-bit counter MIB object in the CISCO-SERVICE-ENGINE-MIB, a 32-bit counter MIB object is implemented so that SNMP clients using SNMPv1 can retrieve data associated with 64-bit counter MIB objects. The MIB objects of each of these groups are read-only.

The CISCO_CDS_SERVICE_ROUTING_MIB.my provides some object identifiers (OIDs) for Service Router statistics. All the OIDs in the MIB are only for querying purposes; no traps have been added to this MIB. The Service Router MIB provides two groups, cdssrStatsGroup and cdssrServiceMonitorGroup, which contain OIDs for the statistics from the `show statistics service-router summary/dns/history/se/content-origin` command and the `show service-router service-monitor` command.

Use the following link to access the CISCO-ENTITY-ASSET-MIB and the CISCO-CONFIG-MAN-MIB:


---

**Note**
If your browser is located behind a firewall or you are connecting to the Internet with a DSL modem and you are unable to access this file folder, you must change your web browser compatibility settings. In the Internet Explorer (IE) web browser, choose **Tools > Internet Options > Advanced,** and check the **Use Passive FTP** check box.

---

**Enabling System Logs**

Use the System Logs page to set specific parameters for the system log file (syslog). This file contains authentication entries, privilege level settings, and administrative details. System logging is always enabled. By default, the system log file is stored as `/local1/syslog.txt`.

To enable system logging, do the following:

---

**Step 1**
Choose **Devices > Devices > General Settings > Notification and Tracking > System Logs.** The System Log Settings page is displayed.

**Step 2**
Enter the settings as appropriate. See Table 5-34 for a description of the fields.
### Table 5-34  System Logs Settings Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Logs</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Enables system logs.</td>
</tr>
<tr>
<td>Facility</td>
<td>Facility where the system log is sent.</td>
</tr>
<tr>
<td><strong>Console Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Enable sending the system log to the console.</td>
</tr>
<tr>
<td>Priority</td>
<td>Severity level of the message that should be sent to the specified remote syslog host. The default priority is warning. The priorities are: Emergency—System is unusable. Alert—Immediate action needed. Critical—Critical condition. Error—Error conditions. Warning—Warning conditions. Notice—Normal but significant conditions. Information—Informational messages. Debug—Debugging messages.</td>
</tr>
<tr>
<td><strong>Disk Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Enables saving the system logs to disk.</td>
</tr>
<tr>
<td>File Name</td>
<td>Path and filename where the system log file is stored on the disk. The default is /local1/syslog.txt.</td>
</tr>
<tr>
<td>Priority</td>
<td>Severity level of the message that should be sent to the specified remote syslog host.</td>
</tr>
<tr>
<td>Recycle</td>
<td>The maximum size of the system log file before it is recycled. The default is 10000000 bytes.</td>
</tr>
<tr>
<td><strong>Host Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Enables sending the system log file to a host. You can configure up to four hosts.</td>
</tr>
<tr>
<td>Hostname</td>
<td>A hostname or IP address of a remote syslog host.</td>
</tr>
<tr>
<td>Priority</td>
<td>Severity level of the message that should be sent to the specified remote syslog host.</td>
</tr>
<tr>
<td>Port</td>
<td>The destination port on the remote host. The default is 514.</td>
</tr>
<tr>
<td>Rate Limit</td>
<td>The message rate per second. To limit bandwidth and other resource consumption, messages can be rate limited. If this limit is exceeded, the remote host drops the messages. There is no default rate limit, and by default all system log messages are sent to all syslog hosts.</td>
</tr>
</tbody>
</table>

**Step 3**  Click **Submit** to save the settings.
Multiple Hosts for System Logging

Each syslog host can receive different priority levels of syslog messages. Therefore, you can configure different syslog hosts with a different syslog message priority code to enable the device to send varying levels of syslog messages to the four external syslog hosts.

However, if you want to achieve syslog host redundancy or failover to a different syslog host, you must configure multiple syslog hosts on the device and assign the same priority code to each configured syslog host.

Configuring Troubleshooting

The Kernel Debugger troubleshooting page allows you to enable or disable access to the kernel debugger. Once enabled, the kernel debugger is automatically activated when kernel problems occur.

**Note**

The “hardware watchdog” is enabled by default and automatically reboots a device that has stopped responding for over ten minutes. Enabling the kernel debugger disables the “hardware watchdog.”

If the device runs out of memory and kernel debugger (KDB) is enabled, the KDB is activated and dump information. If the KDB is disabled and the device runs out of memory, the syslog reports only dump information and reboots the device.

Enabling the Kernel Debugger

To enable the kernel debugger, do the following:

**Step 1** Choose Devices > Devices > General Settings > Troubleshooting > Kernel Debugger. The Kernel Debugger window appears.

**Step 2** To enable the kernel debugger, check the Enable check box, and click Submit.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.

For information about monitoring the SEs, see the “Device Monitoring” section on page 8-8.

Configuring Service Router Settings

The keepalive interval is used by the SE to send keepalive messages to the SR. If the SE is configured with more than one streaming interface, the keepalives are sent for each streaming interface.

Keepalive interval the SE uses for messages to this SR, do the following:

**Step 1** Choose Devices > Devices > General Settings > Service Routing Settings. The Service Routing Settings page is displayed.

**Step 2** In the Keepalive-Interval field, enter the number of seconds the messages from the SR should be kept alive on this SE. The range is from 1 to 120. The default is 2.
Configuring the Service Router

Configuring a Service Router (SR) consists of the following procedures:

- Activating a Service Router
- Configuring Routing Settings
- Configuring Load Monitoring
- Configuring Transaction Logs for the Service Router

For information on configuring the general settings, except last-resort routing and transaction logging, see the “General Settings” section on page 5-19.

Activating a Service Router

**Step 1**  Devices > Devices. The Devices Table page is displayed.

**Step 2**  Click the Edit icon next to the SR you want to configure. The Devices home page is displayed.

**Step 3**  Click Show All to display the top-level menu options, and choose Device Activation. The Device Activation page is displayed.

**Step 4**  Enter the settings as appropriate. See Table 5-35 for a description of the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Location</td>
<td>The Location drop-down list lists all the location configured for the VDS-OS.</td>
</tr>
<tr>
<td>Activate</td>
<td>To activate or deactivate the device, check or uncheck the Activate check box. Alternatively, you can click the Deactivate Device icon in the task bar. When you uncheck the Activate check box and click Submit, the Replaceable check box is displayed. Check the Replaceable check box when you need to replace the device or recover lost registration information. For more information, see the “Recovering VDS-OS Network Device Registration Information” section on page 9-24.</td>
</tr>
</tbody>
</table>
Server Offload

To offload this device for maintenance or a software upgrade, check the Server Offload check box. When checked, the Service Router stops processing client requests.

When the SR is marked as inactive or is marked with server offload on the VOSM it stops responding to DNS queries. Instead, the SR sends a SERVFAIL error as the DNS response, and for RTSP/HTTP requests, the SR sends a 503 Service Unavailable message.

To monitor the current activity on an SR during the Server Offload state, use the show interface command. If the packets received or packets sent is increasing then the SR is processing client requests.

Note We recommend separating the management traffic from the client request traffic by using the port channel configuration, see the “Configuring Port Channel” section on page D-1 for more information.

- If management and client request traffic are separated, the show interface command for the client request port channel displays information on active sessions.

- If management and streaming traffic are not separated, the show interface command shows very low traffic; the packets received and packets sent are lower than a client request session.

Once the SR has finished processing client requests, you can perform maintenance or upgrade the software on the device. For information about upgrading the software, see the “Upgrading the Software” section on page 9-4.

The Status field on the Device Activation page and the Devices Table page displays “offloading” when Server Offload is checked.

Once the software upgrade or maintenance is complete, you need to uncheck the Server Offload check box so that the device can again participate in the system.

Coverage Zone File

To have a local Coverage Zone file overwrite the VDS-OS network-wide Coverage Zone file, choose a file from the Coverage Zone drop-down list. See the “Coverage Zone File Registration” section on page 7-10 for information about creating and registering a Coverage Zone file. Otherwise, choose None.

---

Table 5-35 Service Router Activation Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Offload</td>
<td>To offload this device for maintenance or a software upgrade, check the Server Offload check box. When checked, the Service Router stops processing client requests. When the SR is marked as inactive or is marked with server offload on the VOSM it stops responding to DNS queries. Instead, the SR sends a SERVFAIL error as the DNS response, and for RTSP/HTTP requests, the SR sends a 503 Service Unavailable message. To monitor the current activity on an SR during the Server Offload state, use the show interface command. If the packets received or packets sent is increasing then the SR is processing client requests. Note We recommend separating the management traffic from the client request traffic by using the port channel configuration, see the “Configuring Port Channel” section on page D-1 for more information. • If management and client request traffic are separated, the show interface command for the client request port channel displays information on active sessions. • If management and streaming traffic are not separated, the show interface command shows very low traffic; the packets received and packets sent are lower than a client request session. Once the SR has finished processing client requests, you can perform maintenance or upgrade the software on the device. For information about upgrading the software, see the “Upgrading the Software” section on page 9-4. The Status field on the Device Activation page and the Devices Table page displays “offloading” when Server Offload is checked. Once the software upgrade or maintenance is complete, you need to uncheck the Server Offload check box so that the device can again participate in the system.</td>
</tr>
<tr>
<td>Coverage Zone File</td>
<td>To have a local Coverage Zone file overwrite the VDS-OS network-wide Coverage Zone file, choose a file from the Coverage Zone drop-down list. See the “Coverage Zone File Registration” section on page 7-10 for information about creating and registering a Coverage Zone file. Otherwise, choose None.</td>
</tr>
</tbody>
</table>
Chapter 5  Configuring Devices

Configuring Devices

Configuring the Service Router

Note
To make sure the SR is binding to the primary interface (or management IP address if configured) as the source IP address when sending management traffic to the VOSM, create a static route from the SR to the VOSM. To configure a static IPv4 route from the SR, see the “Configuring Static IPv4 Routes” section on page 5-49 section. Alternatively, you can use the ip route command on the VDS-OS device.

Step 5
Click Submit to save the settings.

Configuring Routing Settings

Configuring Redirect Burst Control

Keepalive messages between the SEs and the SR. The keepalive messages occur every two seconds. If a burst of client requests occurs between two keepalive messages, the SR may not know about the current state of the SE, and might route a request to an already overloaded SE.
The Redirect Burst Control page allows you to configure how many requests (transactions per second [TPS]) the SR should redirect to an SE during a burst.

To configure the redirect burst control, do the following:

**Step 1** Choose Devices > Devices > Routing Settings > Request Routing Settings > Redirect Burst Control. The Redirect Burst Control page is displayed.

**Step 2** Check the Enable Redirect Burst Control check box. The Redirect Burst Control is disabled by default.

**Step 3** In the Rate field, enter the maximum TPS the SR can send to an SE. The default is 100000. The range is from 1 to 100000.

**Step 4** Click Submit.

To apply the factory default settings for the device, click the Apply Defaults icon in the task bar.

To remove the settings from the device, click the Remove Settings icon in the task bar.

### Configuring Load Monitoring

“General Settings” section on page 5-19 “General Settings” section on page 5-19.

Load monitoring provides the following functionality:

- Monitoring and aggregates of the load information of all SEs in the VDS-OS
- Monitoring and aggregates of all SEs assigned to a specific origin service

Minor alarms are raised when the monitored load exceeds the configured average or maximum threshold for all SEs in an origin service or all SEs in the VDS-OS.

To configure load monitoring, do the following:

**Step 1** Choose Devices > Devices. The Devices Table page is displayed.

**Step 2** Click the Edit icon next to the SR you want to configure. The Devices home page is displayed.

**Step 3** Click Show All to display the top-level menu options, and choose General Settings > Notification and Tracking > VOS Monitor > General Settings. The VOS Monitor General Settings page is displayed.

**Step 4** In the Sample Period field, enter the number of seconds between two consecutive samples. The sample period is the time during which the SE and the SR exchange keepalive messages that contain the device information. The default is 2. The range is from 1 to 300.

**Step 5** Check the Enable check box to enable load monitoring. If the Enable check box is not checked, the SE Settings and Domain Settings pages do not take effect.

**Step 6** Click Submit.

**Step 7** To enable the monitoring of all SEs in the VDS-OS and configure the aggregate thresholds for the VDS-OS, choose Devices > Devices (SR) > General Settings > Notification and Tracking > VOS Monitor > SE Settings. The VOS Monitor Settings page is displayed.

**Step 8** Enter the settings as appropriate. See Table 5-36 for a description of the fields.
Step 9 Click Submit.

Step 10 To enable monitoring of specific origin services and configure the aggregate thresholds for each domain, choose Devices > Devices (SR) > General Settings > Notification and Tracking > VOS Monitor > Domain Settings. The Domain Monitor Table page is displayed.

The table is sortable by clicking the column headings.

Step 11 Click the Create New icon.

Click the Edit icon next to the domain name to edit a table entry.

Step 12 Enter the settings as appropriate. See Table 5-37 for a description of the fields.

Table 5-36 VDS-OS Load Monitoring Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Check the Enable check box to enable load monitoring of all SEs in the VDS-OS.</td>
</tr>
<tr>
<td>Note</td>
<td>If the Enable check box is not checked on the VOS Monitor General Settings page, the SE Settings do not take effect.</td>
</tr>
<tr>
<td>Device Average Threshold</td>
<td>Aggregate load value (as a percentage) of the average of all SEs in the VDS-OS. This threshold defines the average device load of all the SEs in the VDS-OS. If the threshold is exceeded, an alarm is raised. The default is 80. The range is from 1 to 100.</td>
</tr>
<tr>
<td>Device Maximum Threshold</td>
<td>Aggregate load value (as a percentage) of the maximum of all SEs in the VDS-OS. This threshold defines the maximum device load of all the SEs in the VDS-OS. If the threshold is exceeded, an alarm is raised. The default is 80. The range is from 1 to 100.</td>
</tr>
</tbody>
</table>

Step 13 Click Submit. The entry is added to the Domain Monitor Table.

To delete a load monitoring configuration for a domain, click the Edit icon for the domain, then click the Delete icon in the task bar.

Table 5-37 Domain Load Monitoring Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>The service routing fully-qualified domain name (RFQDN) (for example, srfqdn.cisco.com) configured for the origin service.</td>
</tr>
<tr>
<td>Enable</td>
<td>Check the Enable check box to enable load monitoring of this domain.</td>
</tr>
<tr>
<td>Note</td>
<td>If the Enable check box is not checked on the VOS Monitor General Settings page, the Domain Settings do not take effect.</td>
</tr>
<tr>
<td>Device Average Threshold</td>
<td>Aggregate load value (as a percentage) of the average of all SEs in the VDS-OS. This threshold defines the average device load of all the SEs in the VDS-OS. If the threshold is exceeded, an alarm is raised. The default is 80. The range is from 1 to 100.</td>
</tr>
<tr>
<td>Device Maximum Threshold</td>
<td>Aggregate load value (as a percentage) of the maximum of all SEs in the VDS-OS. This threshold defines the maximum device load of all the SEs in the VDS-OS. If the threshold is exceeded, an alarm is raised. The default is 80. The range is from 1 to 100.</td>
</tr>
</tbody>
</table>
## Configuring Transaction Logs for the Service Router

To enable transaction logging for the SR, do the following:

### Step 1
Choose Devices > Devices > General Settings > Notification and Tracking > Transaction Logging. The Transaction Log Settings page is displayed.

### Step 2
Enter the settings as appropriate. See *Table 5-38* for a description of the fields.

### Table 5-38 Transaction Log Settings Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td></td>
</tr>
<tr>
<td>Transaction Log Enable</td>
<td>Enables transaction logging.</td>
</tr>
<tr>
<td>Compress Files before Export</td>
<td>When this check box is checked, archived log files are compressed into gzip format before being exported to external FTP servers</td>
</tr>
<tr>
<td>Archive Settings</td>
<td></td>
</tr>
<tr>
<td>Max size of Archive File</td>
<td>Maximum size (in kilobytes) of the archive file to be maintained on the local disk. The range is from 1,000 to 2,000,000. The default is 500,000.</td>
</tr>
<tr>
<td>Max number of files to be archived</td>
<td>Maximum number of files to be maintained on the local disk. The range is from 1 to 10,000. The default is 10.</td>
</tr>
<tr>
<td>Archive occurs</td>
<td>How often the working log is archived and the data is cleared from the working log. Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Choose <em>every</em> to archive every so many seconds, and enter the number of seconds for the interval. The range is from 120 to 604800.</td>
</tr>
<tr>
<td></td>
<td>• Choose <em>every hour</em> to archive using intervals of one hour or less, and choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>– <em>at</em>—Specifies the minute in which each hourly archive occurs</td>
</tr>
<tr>
<td></td>
<td>– <em>every</em>—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30)</td>
</tr>
<tr>
<td></td>
<td>• Choose <em>every day</em> to archive using intervals of one day or less, and choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>– <em>at</em>—Specifies the hour in which each daily archive occurs</td>
</tr>
<tr>
<td></td>
<td>– <em>every</em>—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24)</td>
</tr>
<tr>
<td></td>
<td>• Choose <em>every week on</em> to archive at intervals of one or more times a week, choose the days of the week, and choose what time each day.</td>
</tr>
<tr>
<td>Export Settings</td>
<td></td>
</tr>
<tr>
<td>Enable Export</td>
<td>Enables exporting of the transaction log to an FTP server.</td>
</tr>
</tbody>
</table>
Table 5-38  Transaction Log Settings Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export occurs</td>
<td>How often the working log is sent to the FTP server and the data is cleared from the working log. Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>every</strong> to export every so many minutes, and enter the number of minutes for the interval. The range is from 1 to 100800.</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>every hour</strong> to export using intervals of one hour or less, and choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>– <strong>at</strong>—Specifies the minute in which each hourly export occurs</td>
</tr>
<tr>
<td></td>
<td>– <strong>every</strong>—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30)</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>every day</strong> to export using intervals of one day or less, and choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>– <strong>at</strong>—Specifies the hour in which each daily export occurs</td>
</tr>
<tr>
<td></td>
<td>– <strong>every</strong>—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24)</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>every week on</strong> to export using intervals of one or more times a week, choose the days of the week, and what time each day.</td>
</tr>
<tr>
<td>FTP Export Server</td>
<td>IP address or hostname of the FTP server.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the user.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirms the password for the user.</td>
</tr>
<tr>
<td>Directory</td>
<td>Name of the directory used to store the transaction logs on the FTP server.</td>
</tr>
<tr>
<td>SFTP</td>
<td>Check the SFTP check box, if you are using an SFTP server.</td>
</tr>
</tbody>
</table>

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

---

**Configuring the VOSM**

Configuring a VOSM consists of the General Settings menu items. For information on configuring general settings, see the “**General Settings**” section on page 5-19.

Device activation is accomplished during installation and initialization of the VDS-OS devices.

The Device Activation page for the VOSM displays information about the management IP address and the role of the VOSM. To change the name of the VOSM, enter a new name in the **Name** field and click **Submit**.
For information about primary and standby VOSMs, see the “Configuring Primary and Standby VOSMs” section on page 4-11.
Creating Origin Services and Live Channels

This chapter provides information on configuring the VDS-OS.

- Configuring Origin Services, page 6-1
- Creating Live Channels, page 6-7

Configuring Origin Services

Origin services are configured for capture and playout of linear (live), ODE, and shared copy time-shifted content. Each origin service consists of the workflows that are required to originate the requested resources for downstream CDN nodes.

Configuring an origin service consists of defining the following:

- Creating an Origin Service
- Creating Live Channels

Creating an Origin Service

An origin service is a configuration used to define how content is acquired, distributed, and stored in advance of a client request. For more information about origin services, see the “Origin Services” section on page 1-29.

Before creating origin services, make sure the devices that participate in the origin service are configured.

An origin service configuration consists of the following required and optional settings:

- Service Definition (required)
- General Settings (default or custom settings required)
- SE Assignment (required)
- Assign Network Storage Shares (required)
- Asset Resolver Settings (required)
- Cross-Domain Settings (default or custom settings required)
- Content Protection Settings (required for encryption)
- View Assigned Live Channels
Service Definition

Step 1  Choose Services > Virtual Origin Services > Service Definition. The Virtual Origin Services Table page is displayed (Figure 6-1).

Figure 6-1  Virtual Origin Services Table

Step 2  Click the Create New icon in the task bar. The Virtual Origin Services Definition page is displayed (Figure 6-2).

To edit an origin service, click the Edit icon next to the origin service name.

Figure 6-2  Virtual Origin Service Definition Page

Step 3  Enter the settings as appropriate. See Table 6-1 for a description of the fields.
Table 6-1  Virtual Origin Service Definition Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the origin service. <strong>Note</strong> Spaces are not allowed in the origin service name. The origin service name can consist of alphanumeric characters and the underscore (_) and hyphen (-). The maximum length is 256 characters. Make sure the origin service name does not match any origin service name or live channel name that has already been configured.</td>
</tr>
<tr>
<td>Service Routing Domain Name</td>
<td>The FQDN to route client requests. The SE translates the service routing FQDN, known as the Service Routing Domain Name (SRDN) to the origin service whenever it needs to retrieve content from the origin service. <strong>Note</strong> The string “.se.” cannot be used in the SRDN. The SRDN configured for the origin service should also be configured in the DNS servers, so client requests can get redirected to a Service Router for request mediation and redirection. There is a 255 character limit per FQDN including the dots. There is a 63 character limit per domain label (name between dots). Names can only contain alphanumeric characters and the dash (-). The URLs that are published to the clients have the service routing domain names as the prefix.</td>
</tr>
<tr>
<td>Comments</td>
<td>Information about the origin service.</td>
</tr>
</tbody>
</table>

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

To delete an origin service, from the Virtual Origin Service Table page, click the **Edit** icon next to the origin service you want to delete, and click the **Delete** icon in the task bar.

---

**General Settings**

**Step 1**  From the left-panel menu, click **General Settings**. The General Settings page is displayed.

**Step 2**  Enter the settings as appropriate. See Table 6-2 for a description of the fields.
Table 6-2  General Settings Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum bitrate limit per session for HTTP</td>
<td>Maximum rate, in Kbps, at which a client can receive content. The default is 1000. This bit rate applies to content that is stored locally, specifically, prefetched, hybrid, or cached. For a cache miss, content is delivered at the rate the origin service sends it.</td>
</tr>
<tr>
<td></td>
<td>To configure an origin service for non-paced HTTP sessions, set the Maximum bitrate limit per session for HTTP field to 0. This setting provides best-effort behavior and sessions use the available bandwidth. When the content file is smaller than the chunk size, UKSE sends the entire file immediately. In this case, UKSE does not check pacing; therefore, the bit rate for files smaller than the chunk size is not honored.</td>
</tr>
<tr>
<td>QoS value for content delivery</td>
<td>Configures a Differentiated Services Code Point (DSCP) value for the QoS on a per-origin service basis. Content delivery refers to the traffic the SEs serve to clients. If you choose Other, enter a decimal value in the corresponding field. Note If an SE is configured with the ip dscp all command, this setting overrides both the system-wide QoS setting and any origin service QoS setting.</td>
</tr>
<tr>
<td>Content Expiry</td>
<td>Content expiration time, in hours. The valid range is 0 to 1464 (61 days). The default setting is 1464 hours. For cache-control headers, the Content Expiry is also used as the max-age setting. Setting the Content Expiry to 0 means no cache-control header is set.</td>
</tr>
</tbody>
</table>

Step 3  Click Submit to save the settings.
To remove the settings from the origin service, click the Remove Settings icon in the task bar.

SE Assignment

Note  If a mount option profile is assigned to an SE, it is used for all Network Storage Share mounts assigned to this origin service.

Step 1  Choose Services > Virtual Origin Services > Service Definition. The Virtual Origin Services Table page is displayed.
Step 2  From the left-panel menu, click Assign Service Engines. The Service Engine Assignment page is displayed (Figure 6-3).
Chapter 6  Creating Origin Services and Live Channels

Configuring Origin Services

Figure 6-3  Service Engine Assignment Page

Step 3  Click the Assign icon (blue cross mark) next to the SE you want to assign to this origin service. Alternatively, in the task bar, click Assign All Service Engines. The SE assignment states are described in Figure 6-4.

Figure 6-4  SE Assignment State

Step 4  Click Submit to save the SE assignments.

Assign Network Storage Shares

Note  At least one Service Engine must be assigned to the Origin Service first, before assigning Network Storage Shares. The SEs assigned to the origin service are associated with a location; only Network Storage Shares associated with the same location can be assigned to the origin service. Only one location is allowed; therefore, all SEs and Network Storage Shares have the same location.

If there is a mount option profile assigned to the SE, it is used for all NSS mounts on that SE.

At least one Network Storage Share must be assigned to an origin service.
Step 5: To assign a Network Storage Share to an origin service, click **Assign Network Storage Shares** from the left-panel menu. The Network Storage Shares Table page displays the Network Storage Shares configured in the VDS-OS system.

Step 6: Click the **Assign** icon (blue cross mark) next to each Network Storage Share you want to assign to this origin service. Alternatively, in the task bar, click **Assign All Network Storage Shares**. The Network Storage Share assignment states are similar to the SE assignment states, which are described in Figure 6-4.

Step 7: Click **Submit** to save the Network Storage Share assignments.

---

## Asset Resolver Settings

**Step 1**: Choose **Services > Virtual Origin Services > Service Definition**. The Virtual Origin Services Table page is displayed.

**Step 2**: Select the origin service to which you want to apply the Asset Resolver file.

**Step 3**: From the left-panel menu, click **Asset Resolver Settings**. The Asset Resolver File Assignment page is displayed.

**Step 4**: Select the Asset Resolver file and click **Submit** to save the Asset Resolver file assignment.

The new Asset Resolver file is assigned to all Service Engines that are assigned to the selected origin service.

For information about registering Asset Resolver files, see the “Asset Resolver File Registration” section on page 7-12.

For sample Asset Resolver files, see the “Creating Asset Resolver Files” appendix.

---

## Cross-Domain Settings

**Step 1**: From the left-panel menu, click **Cross-Domain Settings**. The Cross-Domain Files page is displayed.

**Step 2**: Enter the settings as appropriate, then Click **Submit** to save the settings.

To remove the settings from the origin service, click the **Remove Settings** icon in the task bar.

---

## Content Protection Settings

If you plan to use encryption in your network, you must configure Content Protection Settings for the origin service.

**Note**: The following procedure shows how to configure Content Protection Settings for Verimatrix, but the procedure is similar for other supported key profile types.
You must also use an Asset Resolver file that references the content protection key profile name that you configure. In the following procedure, the key profile name is `verimatrix`, so the Asset Resolver file must contain the following line:

```xml
<ContentProtectionProfileName>verimatrix</ContentProtectionProfileName>
```

---

**Step 1** From the left-panel menu, click **Content Protection Settings**. The Content Protection Settings page is displayed.

**Step 2** Click the **Create New Content Protection Key Profile** icon.

Enter a Profile Name for the content protection key profile, such as `verimatrix`, and select Profile Type **Verimatrix**.

For all other fields, enter or select appropriate values.

**Step 3** Click **Submit** to save the content protection key file.

**Step 4** Verify that you have set the DNS addresses correctly on the origin service.

**Step 5** On the client, configure the DNS server to enable it to reach the Verimatrix server.

---

**View Assigned Live Channels**

Click the **Edit** icon next to the live channel you want to edit. The Live Channel Definition page is displayed.

---

**Creating Live Channels**

Each origin service can support the playout of one or more live channels. Input feeds for the origin service (capture resources), as well as the outputs from the origin service (publish resources), are defined as resources. Resources are configured for each live channel. For more information, see the “Origin Services” section on page 1-29.

Live channels are assigned to one origin service. The origin service defines the SRDN, the SEs, and Network Storage Shares available to the live channel. Additionally, the virtual origin service can have an Asset Resolver file associated. Before creating live channels, create the origin service that will be assigned to it. For more information, see the “Creating an Origin Service” section on page 6-1.

If a live channel is started, the following rules apply:

- Cannot delete the started live channel nor change its configuration
- Can create new capture resources and publish resources when a channel is started.
- To modify a capture resource setting, stop the capture resource and all associated publish resources first.
- Can modify the stop time of a publish resource without stopping it, any other changes to the publish resource require stopping it.
- Cannot modify or delete an origin service associated with a live channel that has been started.
- Can assign new Service Engines and unassign Service Engines that are not acting as Acquisition nodes, but you cannot unassign a Service Engine that is assigned to a started live channel.
• Can assign new NSSs to an origin service and unassign NSSs that are not assigned to a started live channel, but you cannot unassign an NSS that is assigned to a started live channel.

• Cannot modify or delete an NSS that is assigned to a started live channel.

Channel Definition

Step 1
Choose Services > Virtual Origin Services > Live Channels. The Live Channels Table page is displayed (Figure 6-5) listing all the live channels defined.

Figure 6-5 Live Channels Table

Step 2
Click the Create New icon in the task bar. The Channel Definition page is displayed (Figure 6-6). To edit a live channel, click the Edit icon next to the live channel name.

Figure 6-6 Channel Definition Page

Step 3
Enter the settings as appropriate. See Table 6-1 for a description of the fields.
Chapter 6  Creating Origin Services and Live Channels

Creating Live Channels

Table 6-3  Channel Definition Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the live channel. This name is part of the Live Channel URI, which has the format: <a href="http://SRDN/live">http://SRDN/live</a> channel name/</td>
</tr>
<tr>
<td>Note</td>
<td>Spaces are not allowed in the live channel name. Make sure the live channel name does not match any live channel name or origin service name that has already been configured.</td>
</tr>
<tr>
<td>Live Channel URI</td>
<td>The Live Channel URI (not initially displayed) is created automatically from the SRDN of the origin service and the live channel name. The Live Channel URI is populated after an origin service is selected.</td>
</tr>
<tr>
<td>Time Shift Window</td>
<td>Amount of time (in minutes) to provide for the default time-shift window for all publish resources. The range is from 0 to 10080.</td>
</tr>
<tr>
<td>Note</td>
<td>There is a Time-Shift Window setting for each Publish Resource, which overrides this default live channel setting.</td>
</tr>
<tr>
<td>Comments</td>
<td>Information about the live channel.</td>
</tr>
</tbody>
</table>

Step 4  Click Submit to save the settings.

To delete a live channel, from the Live Channel Table page, click the Edit icon next to the live channel you want to delete, and click the Delete icon in the task bar.

Assign Origin Service

Step 1  Assign Origin Service. The Assign Origin Service Table page is displayed.

The Assign Origin Service Table is populated from the origin services that have been created.

Step 2  Select the origin service you want to assign to this live channel and click Submit.

After you have selected an origin service for the live channel, the Live Channel URI is populated on the Channel Definition page, the Assign Acquisition Nodes page is populated with the available SEs, and the Assign Network Storage Shares page is populated with the available Network Storage Shares.

Assign Acquisition Node

Step 1  Assign Acquisition Nodes. The Assign Acquisition Nodes Table page is displayed.

Step 2  Click the Assign icon (blue cross mark) next to the SEs you want to assign as Acquisition nodes. Alternatively, in the task bar, click Assign All Service Engines. The SE assignment states are described in Figure 6-7.

At least two SEs must be assigned as Acquisition nodes to provide redundancy. All other SEs displayed from the assigned origin service are Playout nodes. An Acquisition node acquires and registers content for the channel, and can act as a Playout node.
Assign Network Storage Shares

**Step 1**  
Assign Network Storage Shares. The Network Storage Shares Table page displays all the Network Storage Shares assigned to the origin service that is associated with this live channel.

**Note**  
At least one Network Storage Share must be assigned to a live channel.

**Step 2**  
Select the Network Storage Share you want to assign to this live channel and click **Submit**.

Capture Resources

**Step 1**  
From the left-panel menu, click **Capture Resources**. The Capture Resources Table page is displayed listing all the capture resources defined. Each capture resource entry in the table lists the Base URI, the Resource Type, and the Resource Control (either the **Stop** icon or the **Start** icon).

**Step 2**  
Click the **Create New** icon in the task bar. The Capture Resources page is displayed.

To edit a capture resource, click the **Edit** icon next to the capture resource name.

**Step 3**  
Enter the settings as appropriate. See Table 6-4 for a description of the fields.

**Table 6-4 Capture Resource Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base URI</td>
<td>Base URI is composed of the capture directory and the capture resource type (HLS). The capture resource type is added automatically when a Capture Resource Type is selected.</td>
</tr>
<tr>
<td>Capture Resource URI</td>
<td>Capture Resource URI is created automatically by combining the Live Channel URI and the Base URI.</td>
</tr>
</tbody>
</table>
Chapter 6  Creating Origin Services and Live Channels

Creating Live Channels

Table 6-4  Capture Resource Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Resource Type</td>
<td>Select DASH or HLS.</td>
</tr>
<tr>
<td>Arrival Rate</td>
<td>Rate (in seconds) at which the feed is received from the encapsulator. This maps to the segment duration. The range is from 0 to 100. The default is 2.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about this capture resource.</td>
</tr>
</tbody>
</table>

Step 4  In the Stream Name and Bitrate fields, enter the capture stream name and bit rate (in Kbps) for each capture stream, and click Add. The stream name is displayed in the Capture Resource Streams section with an Edit icon.

To edit a stream, click the Edit icon next to the Stream Name, enter the edits in the Stream Name and Bitrate fields, and click Update. To delete a stream, first remove any associated streams in the Publish Resource page, then click the Edit icon next to the Stream Name and click Delete.

The Capture Resource URI and the stream name are used in the manifest and fragment URLs that are pushed from the external encapsulator. For example, if the Capture Resource URI was the following:

http://vos.abr.net/golf/golf-abr/hls

and the stream name was “high” with a bit rate of 1200 Kbps, the URL would be as follows:

http://vos.abr.net/golf/golf-abr/hls/high.m3u8

This URL is made up of the following fields:

- SRDN—vos.abr.net
- Live Channel Name—golf
- Capture Resource Base URI—golf-abr
- Capture Resource Type—hls
- Stream Name—high
- HLS Playlist Extension—m3u8

Step 5  Click Submit. to save the settings.

Publish Resources

Step 1  From the left-panel menu, click Publish Resources. The Publish Resources Table page is displayed listing all the publish resources defined. Each publish resource entry in the table lists the Publish URI, the Resource Type, the Capture Resource, the Resource Status of the Playout nodes, and the Resource Control (either the Stop icon or the Start icon).

Step 2  Click the Create New icon in the task bar. The Publish Resources page is displayed.

To edit a publish resource, click the Edit icon next to the publish resource name.

Step 3  Enter the settings as appropriate. See Table 6-5 for a description of the fields.
After a Capture Resource has been selected, the associated streams are displayed. Check the check box next to each stream name you want to associated with this publish resource, or check the check box in the column heading to select all streams.
Step 5  Click Submit to save the settings.

Capture Schedule

Step 1  To specify a Capture Schedule file, click Capture Schedule in the left-panel menu. The Capture Schedule Table page is displayed and lists the Capture Schedule file associated with this live channel.

Step 2  Click the Edit icon to import or upload a new Capture Schedule file.

Step 3  From the File Import Method drop-down list, select either Import or Upload.
- Upload—Uploads a file from any location that is accessible from your PC using the browse feature.
- Import—Imports a file from an external HTTP, HTTPS, or FTP server.

Step 4  Enter the fields as appropriate. Table 6-6 describes the upload method fields. Table 6-7 describes the import field methods.

<table>
<thead>
<tr>
<th>Table 6-6  Upload Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
</tr>
<tr>
<td>Source File Upload</td>
</tr>
<tr>
<td>Destination Filename</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 6-7  Import Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
</tr>
<tr>
<td>File URL</td>
</tr>
<tr>
<td>Destination File Name</td>
</tr>
<tr>
<td>Update Interval</td>
</tr>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

Step 5  To save the settings, click Submit.
Configuring the System

This chapter provides information on configuring the system parameters of the VDS-OS. This chapter has the following major topics:

- Configuring AAA, page 7-1
- Changing a Password, page 7-7
- Configuring System Settings, page 7-8
- Viewing or Downloading XML Schema Files, page 7-15

For information on logs, see the “System Audit Logs” section on page 8-6.

For information on upgrading the VDS-OS software, see the “Software Upgrade” section on page 9-1.

For information on the ports used by the VDS-OS, see the “System Port Numbers” section on page 8-7.

Configuring AAA

Authentication determines who the user is and whether that user should be allowed access to the network or a particular device. It allows network administrators to bar intruders from their networks. It may use a simple database of users and passwords. It can also use one-time passwords.

Authorization determines what the user is allowed to do. It allows network managers to limit which network services are available to different users.

Accounting tracks what users did and when they did it. It can be used for an audit trail or for billing for connection time or resources used (bytes transferred).

Collectively, authentication, authorization, and accounting are sometimes referred to as AAA. Central management of AAA means the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices.

In the VDS-OS network, login authentication and authorization are used to control user access and configuration rights to the SEs, SRs, and VOSM. There are two levels of login authentication and authorization:

- Device
- VOSM

In a VDS-OS network, user accounts can be created for access to the VOSM and, independently, for access to the SEs and SRs that are registered to the VOSM.
This section covers login authentication and authorization for the VOSM. For information about device login authentication and authorization, see the “Login Access Control” section on page 5-19 and the “Authentication” section on page 5-27.

Login authentication is the process by which VOSM verifies whether the person who is attempting to log in has a valid username and password. The person logging in must have a user account registered with the device. User account information serves to authorize the user for login and configuration privileges. The user account information is stored in the AAA database. When the user attempts to log in, the VOSM compares the person’s username, password, and privilege level to the user account information that is stored in the database.

Each user account can be assigned to a role and a domain. A role defines which VOSM configuration pages the user can access and which services the user has authority to configure or modify. A domain defines which entities in the network the user can access and configure or modify. You can assign a user account to zero or more roles, and to zero or more domains.

Creating, Editing, and Deleting Users

Note

This section is addressed to users with administrator-level privileges (admin users) only.

Two default user accounts are preconfigured in the VOSM. The first account, called admin, is assigned the administrator role that allows access to all services and access to all entities in the system. This account cannot be deleted from the system, but it can be modified. Only the username and the role for this account are unchangeable. To change the password for this account, use the username admin password password command through the CLI.

The second preconfigured user account is called default. Any user account that is authenticated but has not been registered in the VOSM gets the access rights (role and domains) assigned to the default account. This account is configurable, but it cannot be deleted nor can its username be changed.

When you create a new user account in the VOSM, you have the option to create the user account in the CLI for the VOSM device at the same time. Using this option to create the new account in the CLI provides the following benefits:

- User account is created in the primary and standby VOSM management databases and in the VOSM CLI from one central point.
- Users can change their passwords, and the password changes are propagated to a standby VOSM.

If you choose to create the user account from the VOSM without creating the user account in the VOSM CLI at the same time, the following results apply:

- User account is created in the primary and standby VOSM management databases.
- No user account is created in the VOSM CLI, and the user cannot log in to the VOSM until an account is created from the CLI.
- Local users cannot change their passwords using the VOSM.
- Local users can change their passwords using the CLI; however, the password changes are not propagated from the CLI to the VOSM databases when the CLI user option is enabled in the VOSM.

If a user account has been created from the CLI only, when you log in to the VOSM for the first time, the Centralized Management System (CMS) database automatically creates a user account (with the same username as configured in the CLI) with default authorization and access control. However, to change the password in this scenario, the user account must be explicitly configured from the VOSM with the CLI user option enabled.
To create or edit a user account, do the following:

**Step 1**  
Choose **System > AAA > Users**. The User Table page is displayed.  
*Table 7-1* describes the icons for the User Table page.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Creates a new entry.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Edits an entry.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Creates a filtered table. Filter the table based on the field values.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Views all table entries. Click this icon to view all entries after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Prints the current window.</td>
</tr>
</tbody>
</table>

**Table 7-1 User Table Icons**

**Step 2**  
Click the **Create New** icon in the task bar. The User Account page is displayed.  
To edit an account, click the **Edit** icon next to the username.  
*Note* The User Account page can only be accessed by users with administrator-level privileges.

**Step 3**  
In the **Username** field, enter the user account name. The username must be between 4 and 32 characters in length, and begin with a letter.  
The following characters are not permitted in a username: ? . / ; [ ] { } “ @ = |.

**Step 4**  
If you want to create a local user account with a password and privilege level from the VOSM, check the **Create CLI User** check box. The user account is created automatically in the CLI. To prevent the creation of a CLI user account from the GUI, leave the check box unchecked.

**Step 5**  
In the **Password** field, enter a password for the CLI user account, and re-enter the same password in the **Confirm Password** field.  
The password strength must be a combination of alphabetic character, at least one number, at least one special character, and at least one uppercase character.  
The following characters are not allowed: ? . /[ ] { } “ @ = |.

**Step 6**  
From the Privilege Level drop-down list, choose a privilege level for the CLI user account. The choices are 0 (zero) (normal user) or 15 (superuser). The default value is 0.  
*Note* A superuser can use privileged-level EXEC commands, whereas a normal user can use only user-level EXEC commands.
Step 7  In the Username Information area, enter the following information about the user: First Name, Last Name, Phone Number, Email Address, Job Title, and Department.

Step 8  In the **Branding String** field, enter a name or phrase that you want to appear in the CDSM banner, when this user logs in.

Step 9  In the **Comments** field, enter any additional information about this account.

Step 10  Click **Submit** to save the settings.

Step 11  From the left-panel menu, click **Role Management**. The Role Management Table page is displayed. Table 7-1 describes the icons for the Role Management page.

### Table 7-2  Role Management Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Creates a new entry.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>Edits an entry.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>Creates a filtered table. Filter the table based on the field values.</td>
</tr>
<tr>
<td><img src="image4" alt="Icon" /></td>
<td>Views all table entries. Click this icon to view all entries after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image5" alt="Icon" /></td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td><img src="image6" alt="Icon" /></td>
<td>Assigns all roles.</td>
</tr>
<tr>
<td><img src="image7" alt="Icon" /></td>
<td>Removes all roles.</td>
</tr>
<tr>
<td><img src="image8" alt="Icon" /></td>
<td>Views read-only items.</td>
</tr>
<tr>
<td><img src="image9" alt="Icon" /></td>
<td>Indicates that the current transaction was successfully completed.</td>
</tr>
</tbody>
</table>

To add roles, see the “Creating, Editing, and Deleting Roles” section on page 7-5.

To view the setting for the role, click the **View** (eyeglasses) icon next to the role.

Step 12  Click the **Assign** icon (blue cross mark) next to each role name you want to assign to the user account. To remove the role from the user account, click the **Assign** icon again.

To assign all roles, click the **Assign all Roles** icon in the task bar. To unassign all roles, click the **Remove all Roles** icon in the task bar.

Step 13  Click **Submit** to save the settings.

A green arrow wrapped around the blue cross mark indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

Step 14  From the left-panel menu, click **Domain Management**. The Domain Management Table page is displayed.
To add domains, see the “Creating, Editing, and Deleting Domains” section on page 7-6.

To view the setting for the domain, click the View (eyeglasses) icon next to the domain.

**Step 15**

Click the Assign icon next to each domain name you want to assign to the user account.

To remove the domain from the user account, click the Assign icon again.

To assign all domains, click the Assign All icon in the task bar. To unassign all domains, click the Remove All icon in the task bar.

**Step 16**

Click Submit to save the settings.

To delete a user, in the User Table page, click the Edit icon next to the username, and from the User Account page, click the Delete icon in the task bar.

**Note**

Deleting a user account from the CLI does not delete the corresponding account in the VOSM database. User accounts created in the VOSM should always be deleted from within the VOSM.

### Creating, Editing, and Deleting Roles

Although the VOSM provides many types of services, not all users have access to all services. Users are assigned a role, which indicates the services to which they have access. A role is a set of enabled services.

Each user account can be assigned zero or more roles. Roles are not inherited or embedded. The VOSM provides one predefined role, known as the admin role. The admin role has access to all services and all VDS-OS network entities.

**Note**

The admin user account, by default, is assigned to the role that allows access to all domains and all entities in the system. It is not possible to change the role for this user account.

To create or edit a role, do the following:

**Step 1**

Choose System > AAA > Roles. The Roles Table page is displayed.

Table 7-1 describes the icons for the Role Management page.

<table>
<thead>
<tr>
<th>Table 7-3 Role Management Icons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Icon</strong></td>
</tr>
<tr>
<td>![ creates a new entry. ]</td>
</tr>
<tr>
<td>![ edits an entry. ]</td>
</tr>
<tr>
<td>![ creates a filtered table. Filter the table based on the field values. ]</td>
</tr>
</tbody>
</table>
Configuring AAA

Step 2  Click the Create New icon in the task bar. The Role page is displayed.

To edit a role, click the Edit icon next to the role name.

Step 3  In the Name field, enter the name of the role.

Step 4  To enable read-only access for this role, check the Read-Only check box. Users assigned to this role are only be able to view the VOSM pages. They are not able to make any changes.

Step 5  To expand a listing of services under a category, click the folder, and then check the check box next to the service or services you want to enable for this role. To choose all the services under one category simultaneously, check the check box for the top-level folder.

Step 6  In the Comments field, enter any comments about this role.

Step 7  Click Submit to save the settings.

Table 7-3  Role Management Icons (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Views all table entries. Click this icon to view all entries after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Assigns all roles.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Removes all roles.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Views read-only items.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Indicates that the current transaction was successfully completed.</td>
</tr>
</tbody>
</table>

Creating, Editing, and Deleting Domains

A domain is a set of VDS-OS network entities or objects that make up the VDS-OS network. Whereas a role defines which services a user can perform in the VDS-OS network, a domain defines the entities to which the user has access. An entity can be a Service Engine, a device group, or an origin service. These predefined entities are treated like services and can be enabled or disabled when you set up user roles.

When you configure a domain, you can choose to include Service Engines, device groups, or origin services in the domain.
To create or edit a domain, do the following:

**Step 1** Choose **System > AAA > Domains**. The Domains Table page is displayed.

**Step 2** Click the **Create New** icon in the task bar. The Domain page is displayed.

To edit a domain, click the **Edit** icon next to the domain name.

**Step 3** In the **Name** field, enter the name of the domain.

**Step 4** From the **Entity Type** drop-down list, choose Service Engines, Device Groups, or Origin Services.

**Step 5** In the **Comments** field, enter any comments about this domain.

**Step 6** Click **Submit** to save the settings. If the entity type you chose has not already been assigned to the domain, then a message displays indicating that the entity type has not been assigned.

**Step 7** From the left-panel menu, click **Entity Management**. The Entity Management page is displayed.

**Step 8** Click the **Assign** icon (blue cross mark) next to each entity name you want to include. A green arrow wrapped around the blue cross mark indicates an entity is assigned.

To assign all entities in the domain, click the **Assign All** icon in the task bar.

To remove an entity from the domain, click the **Assign** icon again.

To remove all entities from the domain, click the **Remove All** icon in the task bar.

**Step 9** Click **Submit** to save the settings.

To delete a domain, in the Domain Table page click the **Edit** icon next to the domain name. Once the Domain page is displayed, click the **Delete** icon in the task bar.

### Changing a Password

If you are a user *without* admin privileges and you are logged in to the VOSM, you can change your own VOSM and CLI user password if you meet the following requirements:

- Your CLI user account and password were created in the VOSM and not in the CLI.
- You are authorized to access the Password page.

⚠️ **Caution**

We do not recommend changing the CLI user password from the CLI. Any changes to CLI user passwords from the CLI are *not* updated in the management database and are not propagated to the standby VOSM. Therefore, passwords in the management database do not match a new password configured in the CLI.

The advantage of initially setting passwords from the VOSM is that both the primary and the standby VOSMs are synchronized, and VOSM users do not have to access the CLI to change their passwords.

To change the VOSM and CLI user password for the user account that is currently logged in to the VOSM, do the following:

**Step 1** Choose **System > Password**. The Password page is displayed.

**Step 2** In the **New Password** field, enter the changed password.

The following characters are not allowed: ?./|}”@=|
Configuring System Settings

This section covers the following topics:

- System Properties
- Configuring Device Offline Detection
- Configuring Service Routing
- Asset Resolver File Registration
- Defining Network Storage Shares
  Creating Mount Option Profiles for Network Storage Shares

System Properties

To modify the system properties, do the following:

**Step 1** Choose **System > Configuration > System Properties**. The System Properties page is displayed.

**Step 2** Click the **Edit** icon next to the system property you want to change. The Modify Config Property page is displayed.

**Step 3** For true or false values, choose a setting from the **Value** drop-down list. For other values, enter a new value. The range is displayed for each numeric value.

Table 7-4 describes the system properties.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOSM.gui.rowCount</td>
<td>Default row count for all pages containing a table. The default setting is 10.</td>
</tr>
<tr>
<td>VOSM.session.timeout</td>
<td>Length of a Content Distribution Manager session (in minutes). The default is 10. The range is from 5 to 120.</td>
</tr>
<tr>
<td>DeviceGroup.overlap</td>
<td>SE feature overlapping (enable or disable).</td>
</tr>
<tr>
<td>System.CmsUnsProgram Sync.Interval</td>
<td>Interval by which CMS synchronizes program import UNS objects (in minutes). The default is 1440 minutes. The range is from 1 to 43200.</td>
</tr>
<tr>
<td>System.datafeed.pollRate</td>
<td>Poll rate between the SE or the SR and the VOSM (in seconds). The default is 300. The range is from 30 to 1800.</td>
</tr>
<tr>
<td>System.device.recovery.key</td>
<td>Device identity recovery key. This property enables a device to be replaced by another node in the VDS-OS network.</td>
</tr>
<tr>
<td>System.healthmonitor.collect Rate</td>
<td>Sets the collect and send rate in seconds for the CMS device health (or status) monitor. The default is 120. The range is from 5 to 3600.</td>
</tr>
</tbody>
</table>
Configuring System Settings

Step 4

Click **Submit** to save the settings.

---

### Configuring Device Offline Detection

Communication between all devices and the VOSM use User Datagram Protocol (UDP), which allows for fast detection of devices that have gone offline. UDP heartbeat packets are sent at a specified interval from each SE to the primary VOSM in a VDS-OS network. The primary VOSM tracks the last time it received a UDP heartbeat packet from each SE. If the VOSM has not received the specified number of UDP packets, it displays the status of the nonresponsive SEs as offline.

**Note**

In VDS-OS networks with heavy traffic, dropped UDP packets can cause the VOSM to incorrectly report the status of SEs as offline. To avoid this problem, configure a higher value for dropped UDP heartbeat packets.

To configure Device Offline Detection, do the following:

**Step 1**

Choose **System > Configuration > Device Offline Detection**. The Configure Device Offline Detection page is displayed.

**Note**

The Device Offline Detection feature is in effect only when the VOSM receives the first UDP heartbeat packet from an SE. UDP port of the heartbeat on the VOSM must be reachable for all devices; otherwise, the device shows as offline.
Configuring System Settings

Step 2 In the **Heartbeat Rate** field, specify how often, in seconds, the SEs should transmit a UDP heartbeat packet to the VOSM. The default is 10. The range is from 5 to 3600.

Step 3 In the **Heartbeat Fail Count** field, specify the number of UDP heartbeat packets that can be dropped during transmission from SEs to the VOSM before an SE is declared offline. The default is 3. The range is from 1 to 100.

**Note** Decreasing the heartbeat interval (Heartbeat Rate * Heartbeat Fail Count) may take twice the original configured time to take effect. During this time, the online device status is not changed to “Offline” or “Online [Waiting for datafeed].”

Step 4 In the **Heartbeat UDP Port** field, specify the VOSM port number that the SEs use to send UDP heartbeat packets. The default is 2000. The range is from 1000 to 10000.

The **Maximum Offline Detection Time** field displays the product of the failed heartbeat count and heartbeat rate, where:

\[
\text{Maximum Offline Detection Time} = \text{Heartbeat Rate} \times \text{Heartbeat Fail Count}
\]

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

Configuring Service Routing

- Coverage Zone File Registration
- Configuring Global Routing

Coverage Zone File Registration

See Appendix B, “Creating Coverage Zone Files,” for information about creating a Coverage Zone file. The system administrator places a Coverage Zone file where the VOSM or individual devices can access the URL. The administrator then registers the Coverage Zone file URL in the VOSM. Coverage Zone files can be applied globally to the entire VDS-OS network, or locally to a specific SR. If a Coverage Zone file is made global, then it is read and parsed by each SR that does not have a Coverage Zone file assigned. If the coverage zone is specified in an individual SR configuration, it is only applied to that particular SR.

You have the choice of using two types of coverage zones:

- Default coverage zones
- User-defined coverage zones

A default coverage zone consists of all the SEs that reside in the same local network segment, or subnet. The VOSM provides a check box to specify whether the default coverage zone is to be used.

A user-defined coverage zone consists of all the SEs that are specified in a Coverage Zone file. This file defines the network segments to be covered in the routing process. The Coverage Zone file is registered with the VOSM and then applied to an SR for routing definitions.
To apply a custom coverage zone to an SR, you first need to register a Coverage Zone file URL in the VOSM. After you have registered the Coverage Zone file URL with the VOSM, you can apply the Coverage Zone file in one of two ways:

- Globally—Deploy the Coverage Zone file across the entire VDS-OS network
- Locally—Deploy the Coverage Zone file on a specific SR

**Note**
If you apply a Coverage Zone file locally for a device, this file overwrites the global Coverage Zone file for that device.

To register a Coverage Zone file, do the following:

**Step 1** Choose **System > Configuration > Service Routing > Coverage Zone File Registration**. The Coverage Zone File Table page is displayed.

**Step 2** Click the **Create New** icon in the task bar. The Registering Coverage Zone File page is displayed. To edit a Coverage Zone file registration, click the **Edit** icon next to the registration you want to edit.

**Step 3** Choose a file import method from the **File Import Method** drop-down list:

- **Upload**—The upload method allows you to upload a Coverage Zone file from any location that is accessible from your PC by using the browse feature.
- **Import**—The import method allows you to import the Coverage Zone file from an external HTTP, HTTPS, or FTP server.

When you choose a method, the page refreshes and displays the configuration fields that are associated with the method that you chose.

**Step 4** Enter the fields as appropriate. Table 7-5 describes the upload method fields. Table 7-6 describes the import method fields.

<table>
<thead>
<tr>
<th>Table 7-5</th>
<th>Upload Method for Coverage Zone Files</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Coverage Zone File Upload</td>
<td>Local directory path to the Coverage Zone file. To locate the file, use the <strong>Browse</strong> button. Click the <strong>Validate</strong> button to validate the Coverage Zone file.</td>
</tr>
<tr>
<td>Destination Filename</td>
<td>Name of the Coverage Zone file. This field is filled in automatically with the filename from the local directory path.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 7-6</th>
<th>Import Method for Coverage Zone Files</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Coverage Zone File URL</td>
<td>The URL where the Coverage Zone file is located, including path and filename. Click the <strong>Validate</strong> button to validate the Coverage Zone file.</td>
</tr>
<tr>
<td>Destination File Name</td>
<td>Name of the Coverage Zone file.</td>
</tr>
<tr>
<td>Update Interval (minutes)</td>
<td>Frequency with which the VOSM looks for changes to the Coverage Zone file. The default value is 10 minutes.</td>
</tr>
</tbody>
</table>
Configuring System Settings

Configuring Global Routing

Step 1  System > Configuration > Service Routing > Global Routing Config. The Set Global Coverage Zone File page is displayed.

Step 2  From the Coverage Zone File drop-down list, choose a Coverage Zone file.

Step 3  In the DNS TTL field, configure the time period (in seconds) for caching DNS replies. Enter a number from 0 to 60. The default is 60 seconds.

Step 4  Click Submit to save settings.

To apply a Coverage Zone file to an individual SR for local coverage zone configuration, see the “Configuring the Service Router” section on page 5-66.

Asset Resolver File Registration

Step 1  Create the Asset Resolver file. Make sure it contains both the HDS or HLS rule and the DASH rule. For sample Asset Resolver files, see the “Creating Asset Resolver Files” appendix.

Step 2  Choose System > Configuration. The Configuration Properties page is displayed.

Step 3  From the left-panel menu, click Asset Resolver File Registration. The Asset Resolver Files Registration page is displayed.

Step 4  Click the Create New Asset Resolver File icon.

   a.  Select Upload as the File Import Method and Asset Resolver File as the File Type.

   b.  Source File Upload is the Asset Resolver file that you are uploading.

   c.  Enter the Destination File Name, if different from the source file name.

   d.  Click Validate.

   e.  Verify that the File Validation Result shows no errors, then click Submit.

The Asset Resolver file is registered with VOSM.

For information about assigning the new Asset Resolver file to Service Engines assigned to origin services, see the “Asset Resolver Settings” section on page 6-6.

Table 7-6 Import Method for Coverage Zone Files

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Name of the user to be authenticated when fetching the Coverage Zone file.</td>
</tr>
<tr>
<td>Password</td>
<td>User password for fetching the Coverage Zone file.</td>
</tr>
</tbody>
</table>
Defining Network Storage Shares

“Assign Network Storage Shares” section on page 6-5 “Assign Network Storage Shares” section on page 6-5. For information about Network Storage Shares, see the “External Storage Devices—NAS” section on page 1-25. To assign a Network Storage Share to an origin service, you first need to define it.

Network traffic performance can be impacted by too small a value for the TCP parameter: net.inet.tcp.rexmit_slop. If it is determined that network throughput performance is impacted, the net.inet.tcp.rexmit_slop value on the NSS server should be reviewed.

To define a Network Storage Share, do the following:

**Step 1** Choose **System > Configuration > Network Storage Shares**. The Network Storage Share Table page is displayed.

**Step 2** Click the **Create New** icon in the task bar. The Network Storage Share page is displayed.

To edit a Network Storage Share, click the **Edit** icon next to the Network Storage Share you want to edit.

**Step 3** Enter the settings as appropriate. See Table 7-7 for a description of the fields.

<table>
<thead>
<tr>
<th>Table 7-7</th>
<th>Network Storage Shares Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Name</td>
<td>Unique name for the Network Storage Share.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Spaces are not allowed in the Network Storage Share name. The Network Storage Share name can consist of alphanumeric characters and the underscore (_) and hyphen (-). The maximum length is 15 characters.</td>
</tr>
<tr>
<td>Storage Type</td>
<td>From the <strong>Storage Type</strong> drop-down list, select the storage type.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Only NFS is supported.</td>
</tr>
<tr>
<td>Location</td>
<td>From the <strong>Location</strong> drop-down list, select a location.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Only one location is supported.</td>
</tr>
<tr>
<td>Shared Directory</td>
<td>Shared directory on the Network Storage Share.</td>
</tr>
<tr>
<td>Mount Path</td>
<td>Local path on the Service Engine to mount the Network Storage Share.</td>
</tr>
<tr>
<td>Number of Mounts</td>
<td>Enter the number of servers that are to be mounted from the cluster pool.</td>
</tr>
<tr>
<td>IP Range &lt;1–4)</td>
<td>IP address ranges that the Network Storage Share can be mounted on. Up to four IP address ranges can be specified.</td>
</tr>
</tbody>
</table>

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

To delete a Network Storage Share, first unassign it from the live channels and origin services, then from the Network Storage Share Table page, click the **Edit** icon next to the Network Storage Share you want to delete, and click the **Delete** icon in the task bar.

The following guidelines should be considered when defining NSSs:

- NSS should be network accessible
Chapter 7  Configuring the System

Configuring System Settings

- Shared directory is the NFS exported file system that needs read (ro) access for VOD content and read write (rw) access for live and Live-to-VOD content
- File system exported should have sufficient file-mode access to read, or read and write
- For read/write access the mount option profile must be defined with Read-Write access

Creating Mount Option Profiles for Network Storage Shares

“Activating a Service Engine” section on page 5-9 “Activating a Service Engine” section on page 5-9.

Note

The mount option change takes effect on a SE reload, and only affects new mounts, not existing mounts.

To create a mount option profile, do the following:

Step 1
Choose System > Configuration > Mount Option Profiles. The Mount Option Profiles Table page is displayed.

Step 2
Click the Create New icon in the task bar. The Mount Option Profiles page is displayed.
To edit a Mount Option Profile, click the Edit icon next to the Mount Option Profile you want to edit.

Step 3
Enter the settings as appropriate. See Table 7-8 for a description of the fields.

Table 7-8 Mount Option Profiles Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the Mount Option Profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Spaces are not allowed in the Mount Option Profile name. The Mount Option Profile name can consist of alphanumeric characters and the underscore (_) and hyphen (-). The maximum length is 256 characters.</td>
</tr>
<tr>
<td>NFS Access Mode</td>
<td>Select either Read-Only or Read-Write.</td>
</tr>
<tr>
<td>NFS Read Block Size</td>
<td>Read block size (in bytes) for NFS. The range is from 32768 to 524288.</td>
</tr>
<tr>
<td>NFS Write Block Size</td>
<td>Write block size (in bytes) for NFS. The range is from 32768 to 524288.</td>
</tr>
<tr>
<td>NFS Timeout</td>
<td>Time interval (in deciseconds) in which the SE has to respond to the Network Storage Share. After which the message is retransmitted. The range is from 1 to 6000. The default is 600.</td>
</tr>
<tr>
<td>NFS Retrans</td>
<td>Number of times to retransmit a message after a timeout has been reached. The range is from 1 to 60. The default is 3.</td>
</tr>
<tr>
<td>NFS Retry</td>
<td>Time (in minutes) to wait between retransmissions. The range is from 0 to 60. The default is 2.</td>
</tr>
</tbody>
</table>

Step 4
Click Submit to save the settings.
To delete a Mount Option Profile, from the Mount Option Profile Table page, click the Edit icon next to the mount option profile you want to delete, and click the Delete icon in the task bar.
Viewing or Downloading XML Schema Files

The XML Schema Files page provides links to the XML schema files for viewing or downloading. All XML files can be validated through the VOSM by clicking the Validate button on the associated VOSM page. However, if you want to use an external XML validation program, you can save the XML schema file to use for that purpose.

The following XML schema files are available:

- VOSCoverageZone.xsd—Coverage Zone file is used to customize the networks and geographic regions each SE services. VDS-OS uses the VOSCoverageZone.xsd XML schema file to customize the networks and geographic regions that are serviced by each SE.

- VOSCaptureSchedule.xsd—Capture Schedule file used to convert live content to VOD content (such as catch-up-to-live and start over)

To open or save an XML schema file, do the following:

**Step 1** Choose System > Files > XML Schema Files. The VOS-IS XML Schema page is displayed with a link to each XSD (schema) file.

**Step 2** Click the link for the file. Depending on the browser program used, one of the following or something similar happens:

- File is displayed in a new window and the File Download dialog box is also displayed
- Opening dialog box is displayed
- File is displayed in a text editor program.
Monitoring the VDS-OS

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

- System Monitoring, page 8-1
- Device Monitoring, page 8-8
- Origin Service Monitoring, page 8-18
- Viewing Statistics, page 8-20
- Log Files, page 8-22
- Transaction Logs, page 8-23

System Monitoring

System monitoring consists of the following:

- System Status
- System Home Page
- System Audit Logs
- System Port Numbers

System Status

The VOSM displays the system status in the System Status bar that is located above the navigation tabs in every window. The System Status bar presents the overall device and service health of the system. You can use this feature to monitor devices and services in your VDS-OS network. The System Status bar helps you immediately identify any problems on the network, allowing you to act and respond to problems quickly.

The system status reporting mechanism uses four alarm lights to identify problems that need to be resolved. Each light represents a different alarm level, as follows:

- Green—No alarms (the system is in excellent health)
- Yellow—Minor alarms
- Orange—Major alarms
- Red—Critical alarms
When you roll your mouse over an alarm light in the System Status bar, a pop-up message provides further details about the device, origin service, or license status. See Figure 8-1.

The icon next to the System Status either displays a yellow triangle with an exclamation mark or a green circle with a check mark. The yellow triangle indicates the alarms and alerts count includes only the unacknowledged alarms and alerts. The green circle with a check mark indicates all alarms and alerts are counted, whether they are acknowledged or unacknowledged.

**Figure 8-1 System Status Bar**

![System Status Bar](image)

When you click the alarm light or the link next to the alarm light, a new window opens (Troubleshooting Devices or Troubleshooting Services), listing the individual devices or origin services that need attention.

**Figure 8-2 Troubleshooting Device Window**

![Troubleshooting Device Window](image)

**Troubleshooting Window Pop-Up Menus**

When you roll your mouse over an item under the Alarm Information column in the Troubleshooting window, the Troubleshooting Tools menu is displayed. The Troubleshooting Tools menu provides links to all the diagnostic tools, troubleshooting tools, and monitoring applications for troubleshooting and resolving the problem. Figure 8-2 shows the Troubleshooting Tools menu for device alarms.
- Table 8-1 describes the icons for the Troubleshooting window.

**Table 8-1 Troubleshooting Window Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Create a filtered table. Filter the alarms by severity or device type." /></td>
<td>Create a filtered table. Filter the alarms by severity or device type.</td>
</tr>
<tr>
<td><img src="image" alt="View all alarms. Click this icon to view all alarms after you have created a filtered table." /></td>
<td>View all alarms. Click this icon to view all alarms after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh the table" /></td>
<td>Refresh the table</td>
</tr>
<tr>
<td><img src="image" alt="Print the current window." /></td>
<td>Print the current window.</td>
</tr>
<tr>
<td><img src="image" alt="View acknowledged alarms." /></td>
<td>View acknowledged alarms.</td>
</tr>
</tbody>
</table>

You can sort the Troubleshooting table by clicking any column heading displayed in blue. The first time the column heading is clicked, the table is sorted by that column in increasing order. If the column heading is clicked again, the table is sorted by that column in decreasing order.

**Note**

If there is more than one alarm for a device, and the Troubleshooting window is sorted by device, then the device is only listed once for multiple alarms associated with it. The same is true for service alarms.

**Troubleshooting Window Acknowledge and Unacknowledge Alarms Function**

The following procedure describes acknowledging and unacknowledging an alarm:

**Step 1**

To remove an alarm from the Troubleshooting window, check the check box for the alarm. The alarm is moved to the Acknowledged Alarm window.

**Step 2**

To view the acknowledged alarms, click the **View acknowledged alarms** icon. The Acknowledged Alarm window is displayed (Figure 8-3).

**Figure 8-3 Acknowledged Alarms Window**

**Step 3**

To unacknowledge an alarm, check the check box for the alarm. The alarm is returned to the Troubleshooting window.
Step 4 To view the Troubleshooting window again, click the **Back** (blue left arrow) icon.

**Device Alarms**

Device alarms are associated with device objects and pertain to applications and services running on SEs, SRs, and VOSMs. Device alarms are defined by the reporting application or service. For example, the SR raises an alarm for an SE (the keepalive time-out alarm) if the SE has a Layer 3 failure. Device alarms can also reflect reporting problems between the device and the VOSM. (See Table 8-2.)

Alarm thresholds are configured for each device. For more information, see the “Setting Service Monitor Thresholds” section on page 5-52.

**Table 8-2 Device Alarms for Reporting Problems**

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Alarm Severity</th>
<th>Device Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device is offline</td>
<td>Critical</td>
<td>Offline</td>
<td>The device has failed to communicate with the VOSM.</td>
</tr>
<tr>
<td>Device is pending</td>
<td>Major</td>
<td>Pending</td>
<td>The device status cannot be determined.</td>
</tr>
<tr>
<td>Device is inactive</td>
<td>Minor</td>
<td>Inactive</td>
<td>The device has not yet been activated or accepted by the VOSM.</td>
</tr>
<tr>
<td>Device has lower software version</td>
<td>Minor</td>
<td>Online</td>
<td>The device is not interoperable with the VOSM because it has an earlier software version.</td>
</tr>
</tbody>
</table>

To troubleshoot a device from the System Status bar, do the following:

**Step 1** In the System Status bar, click the **Devices** alarm light or click the **Device** link. The Troubleshooting Devices window is displayed.

**Step 2** In the Alarm Information column, hold your mouse over the alarm message until the Troubleshooting Tools menu is displayed. See **Figure 8-2**.

**Step 3** Click the troubleshooting tool you want to use. The link takes you to the corresponding page in the VOSM. **Table 8-3** describes the tools available for all device alarms.
Remote Storage Alarms

Storage alarms have two levels: major and minor. A minor alarm transits to a major alarm if it persists for more than 60 seconds. All alarms are viewable by using the `show alarm` command and through the Device alarms in the System Status bar.

Storage alarms are generated at two levels from each SE:
- Storage server—Single alarm is generated for each storage server, and indicates that the SE could not connect to the storage server within the timeout period (that is, the mount command timed out).
- Origin service—Alarm is generated when an origin service fails to access one or more shares. A different alarm is generated for each share. The storage server alarms also trigger origin service alarms.

Service Alarms

Service alarms pertain to content problems and are associated with origin services. Service alarms are raised by the VOSM based on content status reports, or by the SE health manager based on acquisition and distribution errors.

If the same fault is reported by the content status and by the SE health manager, the VOSM reports both; one appears as the true alarm and the other as an error. The VOSM does not correlate nor attempt to consolidate the errors generated by the content status and by the SE health manager.

To troubleshoot service content issues from the System Status bar, do the following:

| Step 1 | In the System Status bar, click the Services alarm light or click the Service link. The Troubleshooting Services window is displayed. |
| Step 2 | In the Alarm Information column, hold your mouse over the alarm message until the Troubleshooting Tools menu is displayed. |
| Step 3 | Click the troubleshooting tool that you want to use. The link takes you to the corresponding page in the VOSM. |
System Home Page

The System Home page (Figure 8-4) provides overall system information on configuration and software versions running on the VDS-OS devices. Clicking the links for devices and origin services and live channels takes you to the corresponding table pages.

Note

The number of devices that have a lower version of software than the VOSM only compares the major and minor release numbers (X.Y) of the software release number. The software release number consists of X.Y.Z-b#, where X is the major release number, Y is the minor release number, Z is the maintenance release number, and b# is the build number. Devices with a lower X.Y version than the VOSM do not interoperate with the VOSM, and the VOSM does not send configuration updates to those devices. A minor alarm is generated for the devices with a lower version of software.

Figure 8-4  System Home Page

System Audit Logs

The VOSM logs user activity in the system. The only activities that are logged are those that change the VDS-OS network. This feature provides accountability for users actions (for example, which user did what and when). Logged activities include the following:

- Creation of VDS-OS network entities
- Modification and deletion of VDS-OS network entities
- System configurations

To view audit trail logs, do the following:

Step 1  Choose System > Logs > Audit Trail Logs. The Audit Log page is displayed. All logged transactions in the VOSM are listed by date and time, user, actual transaction that was logged, and the IP address of the machine that was used.
**Step 2**

To determine the number of rows that you want to display, choose a number from the Rows drop-down list.

---

**System Port Numbers**

Information on all the protocols and ports used by the VDS-OS can be viewed on the Well Known Ports page.

To view ports used by the VDS-OS, choose **System > Well Known Ports**. The Well Known Ports page is displayed. **Table 8-4** lists all ports listed on the Well Known Ports page.

To view all ports on one page, from the **Rows** drop-down list, choose **All**.

**Table 8-4 Well Known Ports**

<table>
<thead>
<tr>
<th>Source Group</th>
<th>Destination Group</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator (PC)</td>
<td>VOSM</td>
<td>TCP</td>
<td>ANY</td>
<td>8443</td>
<td>Access to VOSM GUI from administrator PC</td>
</tr>
<tr>
<td>All Devices</td>
<td>All Devices</td>
<td>TCP</td>
<td>ANY</td>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>All Devices</td>
<td>All Devices</td>
<td>TCP</td>
<td>ANY</td>
<td>23</td>
<td>Telnet (disabled by default)</td>
</tr>
<tr>
<td>All Devices</td>
<td>NTP Servers</td>
<td>UDP</td>
<td>ANY</td>
<td>123</td>
<td>Query time servers</td>
</tr>
<tr>
<td>All Devices</td>
<td>NMS Servers</td>
<td>TCP</td>
<td>ANY</td>
<td>161</td>
<td>SNMP query or polling</td>
</tr>
<tr>
<td>All Devices</td>
<td>NMS Servers</td>
<td>UDP</td>
<td>ANY</td>
<td>162</td>
<td>SNMP trap</td>
</tr>
<tr>
<td>All Devices</td>
<td>Syslog Server</td>
<td>UDP</td>
<td>ANY</td>
<td>514</td>
<td>Syslog</td>
</tr>
<tr>
<td>Client</td>
<td>DNS Server/Proxy</td>
<td>UDP</td>
<td>ANY</td>
<td>53</td>
<td>DNS query for Service Router Fully-Qualified Domain Name (SRFQDN) from client</td>
</tr>
<tr>
<td>Client</td>
<td>SR</td>
<td>TCP</td>
<td>ANY</td>
<td>80</td>
<td>HTTP request to Service Router from client</td>
</tr>
<tr>
<td>Client</td>
<td>SE</td>
<td>TCP</td>
<td>ANY</td>
<td>80</td>
<td>HTTP request to Service Engine from client</td>
</tr>
<tr>
<td>DNS Server/Proxy</td>
<td>SR</td>
<td>UDP</td>
<td>ANY</td>
<td>53</td>
<td>DNS query for RRFQDN from DNS server/proxy used by client</td>
</tr>
<tr>
<td>DNS Server/Proxy</td>
<td>All Devices</td>
<td>UDP</td>
<td>ANY</td>
<td>1023-65535</td>
<td>DNS server responses to DNS query requests</td>
</tr>
<tr>
<td>SE</td>
<td>VOSM</td>
<td>TCP</td>
<td>ANY</td>
<td>443</td>
<td>VDS-OS management (notifications, updates, queries)</td>
</tr>
<tr>
<td>SE</td>
<td>SE</td>
<td>TCP</td>
<td>ANY</td>
<td>80</td>
<td>HTTP request between Service Engines</td>
</tr>
<tr>
<td>SE</td>
<td>VOSM</td>
<td>UDP</td>
<td>ANY</td>
<td>2000</td>
<td>Service Engine to VOSM keepalives</td>
</tr>
<tr>
<td>SE</td>
<td>SR</td>
<td>UDP</td>
<td>ANY</td>
<td>2323</td>
<td>Service Engine to Service Router keepalives</td>
</tr>
<tr>
<td>SE</td>
<td>NFS NAS Server</td>
<td>TCP</td>
<td>ANY</td>
<td>2049</td>
<td>Mounting NFS shares</td>
</tr>
<tr>
<td>SR</td>
<td>VOSM</td>
<td>TCP</td>
<td>ANY</td>
<td>443</td>
<td>VDS-OS management (notifications, updates, queries)</td>
</tr>
<tr>
<td>SR</td>
<td>VOSM</td>
<td>UDP</td>
<td>ANY</td>
<td>2000</td>
<td>Service Router to VOSM keepalives</td>
</tr>
<tr>
<td>VOSM</td>
<td>SE</td>
<td>TCP</td>
<td>ANY</td>
<td>443</td>
<td>VDS-OS management (notifications, updates, queries)</td>
</tr>
</tbody>
</table>
The Destination Ports that have a port range indicate the possible ports that the Source Group could be expecting to send traffic to and receive traffic from. The specific ports required to be open to receive and send data depends on the Source Group configuration.

### Device Monitoring

This section covers the following topics:

- Devices Table
- Devices Home Page
- Using show, clear, and alarm Commands
- Core Dump Files
- CPU Utilization

For more detailed statistics on HTTP traffic, see the “Viewing Statistics” section on page 8-20.
Devices Table

The Devices Table page displays all devices registered in the VDS-OS network (Figure 8-5).

Figure 8-5 Devices Table Page

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Host name of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>Device type: SE, SR, VOSM (Primary), VOSM (Secondary).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Primary IP address of the device.</td>
</tr>
</tbody>
</table>
Table 8-5  Device Table Columns (continued)

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Online—Device has been activated through the VOSM and is able to send and receive data and control traffic.</td>
</tr>
<tr>
<td></td>
<td>• Offline—Device has failed to communicate with the VOSM.</td>
</tr>
<tr>
<td></td>
<td>• Pending—Device status cannot be determined. The device could be in the process of being activated by the VOSM</td>
</tr>
<tr>
<td></td>
<td>• Offloading—Device is in the Server Offload state. See the Server Offload field in Table 5-6 on page 5-10 for more information. To monitor the current traffic on an SE during the Server Offload state, view the statistics for HTTP (see Table 8-15 on page 8-21). After all HTTP traffic has finished, you can perform maintenance or upgrade the software on the device. For information about upgrading the software, see the “Upgrading the Software” section on page 9-4.</td>
</tr>
<tr>
<td></td>
<td>• Online [Waiting for datafeed]—In some situations, the VOSM may receive regular heartbeat messages, but not receive a datafeed message for a long time. The Online [Waiting for datafeed] state indicates that the VOSM has not received a datafeed message from this online device in the last 2.25 * polling rate seconds. When the datafeed message is received, the state changes to Online.</td>
</tr>
<tr>
<td>Location</td>
<td>Location the device is assigned to.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Device software version.</td>
</tr>
</tbody>
</table>

Table 8-6 describes the icons for the device table. To view or modify the configuration of a device, click the Edit icon next to the device name.

Table 8-6  Device Table Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Activate all inactive Service Engines." /></td>
<td>Activate all inactive Service Engines.</td>
</tr>
<tr>
<td><img src="image" alt="Edit the device." /></td>
<td>Edit the device.</td>
</tr>
<tr>
<td><img src="image" alt="Export a table to a comma-separated value (CSV) file." /></td>
<td>Export a table to a comma-separated value (CSV) file.</td>
</tr>
<tr>
<td><img src="image" alt="Create a filtered table. Filter the devices by the device name, device type, and device status." /></td>
<td>Create a filtered table. Filter the devices by the device name, device type, and device status.</td>
</tr>
<tr>
<td><img src="image" alt="View all devices. Click this icon to view all devices after you have created a filtered table." /></td>
<td>View all devices. Click this icon to view all devices after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh the table" /></td>
<td>Refresh the table</td>
</tr>
<tr>
<td><img src="image" alt="Print the current window." /></td>
<td>Print the current window.</td>
</tr>
</tbody>
</table>
For more information, see the “Devices, Services, and Other Tables” section on page 4-7.

Devices Home Page

The Devices home page (Figure 8-6) provides alarm status and information on the device. Only basic information is displayed for the SR and VOSM.

By clicking the Origin Services and Device Groups links in the Assignments area on the home page for an SE a table is displayed listing all the origin services or device groups in the VDS-OS, and which ones the SE is assigned to. Through this page, you can assign the device to additional origin services or device groups by clicking the icon next to the applicable origin services or device groups and submitting your selection.

You can update the device software, and telnet to the device from the Devices home page. For more information about updating the software, see the “Software Upgrade” section on page 9-1.

Figure 8-6     SE Devices Home Page

The Devices home page for an SE or an SR provides several icons. Table 8-7 describes these icons. The VOSM home page has a subset of the icons.
Device Monitoring

Chapter 8  Monitoring the VDS-OS

Table 8-7  SE Devices Home Page Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Displays all devices. Clicking this icon displays a list of the Service Engines. To view or configure another Service Engine, click the Service Engine name. The configuration page for that device is displayed and the left-panel menu displays. This feature allows you to compare the configuration on different Service Engines. To return to the left-panel menu, click the Display Menu icon.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Displays the left-panel menu for the device.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Refreshes the page.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Deletes the device. See the “Deleting a Device” section on page 9-9.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Updates application statistics. The device statistics are updated at a configurable time interval, which is set in the System Configuration page (System.monitoring.collectRate). See the “Configuring System Settings” section on page 7-8. To see the latest statistics immediately, without waiting for the time interval to elapse, click this icon.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Forces a full database update from the VOSM to the SE. If the VOSM and SE databases are not synchronized because of network errors or other errors, you can synchronize them by clicking this icon.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Reboots the device. See the “Rebooting Devices” section on page 9-8.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Prints the home page.</td>
</tr>
</tbody>
</table>

For more information about the Devices home page, see the “Devices Home Page” section on page 4-8.

Using show, clear, and alarm Commands

The show, clear, and alarm commands offer more detailed monitoring of the device.

- Table 8-8 lists only the show command parameters where arguments are required or are optional.
- Table 8-9 lists only the clear command parameters where arguments are required.
- Table 8-10 lists only the alarm command parameters where arguments are required.

A full list of the show, clear, and alarm commands is available from the drop-down list on the respective page.
Using the VOSM show, clear, or alarm Command Tool

To use the VOSM show, clear, or alarm command tool, do the following:

Step 1  Choose Devices > Devices > Monitoring > Show/Clear/Alarm Commands and then click either Show Commands, Clear Commands, or Alarm Commands.

Step 2  From the drop-down list, choose a command.

Step 3  Enter arguments for the command, if any.

Step 4  Click Submit to display the command output. The results of the command are displayed in a new window.

Table 8-8       show Command Arguments

<table>
<thead>
<tr>
<th>show Command</th>
<th>Arguments</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>{300}</td>
<td>SE</td>
</tr>
<tr>
<td>alarms</td>
<td>[critical</td>
<td>detail</td>
</tr>
<tr>
<td>authentication</td>
<td>{user}</td>
<td>SE, SR, VOSM</td>
</tr>
<tr>
<td>cdn-statistics</td>
<td>http [service-engines</td>
<td>device-group-name groupname</td>
</tr>
<tr>
<td>cdnfs</td>
<td>{usage</td>
<td>volumes}</td>
</tr>
<tr>
<td>clock</td>
<td>[detail</td>
<td>standard-timezones {all</td>
</tr>
<tr>
<td>cms</td>
<td>{database {content {dump filename</td>
<td>text</td>
</tr>
<tr>
<td>content</td>
<td>{all</td>
<td>diskpath diskpath</td>
</tr>
<tr>
<td>content-origin</td>
<td>{request-fqdn domain_name}</td>
<td>SE</td>
</tr>
<tr>
<td>device-mode</td>
<td>{configured</td>
<td>current}</td>
</tr>
<tr>
<td>disks</td>
<td>{current</td>
<td>details</td>
</tr>
<tr>
<td>interface</td>
<td>{GigabitEthernet slot/port</td>
<td>PortChannel port-num</td>
</tr>
</tbody>
</table>
### Chapter 8  Monitoring the VDS-OS

#### Device Monitoring

```
ip
On SE or VOSM: {access-list [acl-name | acl-num] | routes}
| border-routers | database [adv-router
| ip-address-advertising-router | asbr-summary
| ip-address-link-state-id | database-summary | detail | external [ip-address-link-state-id | detail] | network
| ip-address-link-state-id | detail] | nssa-external
| ip-address-link-state-id | detail] | router
| ip-address-link-state-id | detail] | self-originated [detail] | summary [ip-address-link-state-id | detail]] | interface
| memory | neighbor [ip-address-neighbor [detail] | detail | summary | request-list ip-address-neighbor-router
| {GigabitEthernet slot/port | PortChannel channel-number} | retransmission-list [GigabitEthernet slot/port | PortChannel channel-number] | route [single-ip-route] | rsfp route
| {ip-address-advertising-router} | traffic | proximity
| {algorithm | server} | rib {clients [single-client] | memory | recursive-next-hop [ip-address-next-virtual-hop] | route
| {ip-address-single-route | bgp | direct | isis | ospf | summary] | unresolved-next-hop [ip-address-unresolved-next-hop] | route
| static route

lacp
{counters | internal} SE, SR, VOSM

cmp
{status} SE, SR, VOSM

processes
{cpu | debug pid | memory | system [delay 1-60 | count 1-100]} SE, SR, VOSM

service-registry
{process | service} SR

service-router
On SE: {keepalive-interval | service-monitor}
On SR: {vos-monitor | lastresort [domain domain-name] | load
| all | surname surname | memory | redirect-burst-control | routes | service-monitor | services [all | surname surname] | summary] | unified-routing-table}
On VOSM: {service-monitor}

services
{ports [port-num] | summary} SE, SR, VOSM

snmp
{alarm-history | engine ID | group | stats | user} SE, SR, VOSM
```
### Table 8-8  show Command Arguments (continued)

<table>
<thead>
<tr>
<th>show Command</th>
<th>Arguments</th>
<th>Device</th>
</tr>
</thead>
</table>
Note

The clear statistics web-engine and clear statistics all commands only clear normal statistics, not the Web Engine statistics details. To clear all Web Engine statistics, use the clear statistics web-engine force command. We do not recommend using the clear statistics web-engine force command, but if it is used, restart the Web Engine service by entering the web-engine stop and web-engine start commands.

Core Dump Files

The Core Dump Files page lists any core dump files for the device. To view a list of core dump files for the device, choose Devices > Devices > Monitoring > Core Dump Files. The Core Dump File page is displayed and lists any core dump files that have occurred on the device.

To delete a core dump file, check the check box next to the filename and click the Delete icon in the task bar.

To delete all core dump files, check the check box in the heading of the check box column, and click the Delete icon in the task bar.

To refresh the table, click the Refresh Table icon in the task bar.

To print the table, click the Print icon in the task bar.

The core dump files are located in the /local1/local1/core_dir directory.
**CPU Utilization**

The CPU Utilization report displays the CPU usage for the SE.

To view the CPU Utilization report for an SE, do the following:

**Step 1** Choose Devices > Devices > Monitoring > Statistics > CPU Utilization. The CPU Utilization Report page is displayed.

**Step 2** Enter the settings as appropriate. Table 8-11 describes the report settings.

**Table 8-11 CPU Utilization Report Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chart Size</td>
<td>The chart display size choices are small, medium, or large.</td>
</tr>
</tbody>
</table>
| Time Frame        | The time frame options are last hour, last day, last week, last month, or custom. There is a difference in the meaning of the graphs based on the time frame chosen:  
   • Last Hour—Shows raw data collected from the SEs. Real-time values are reported.  
   • Last Day—Shows hourly data, which consolidates the raw data. Consolidation is done by averaging the raw data for each hour. So the value reported in the Last Day graph are average values per hour.  
   • Last Week, Last Month, and Custom—Shows daily data, which consolidates hourly data. Consolidation is done by averaging the hourly data for each day. So these are average values per day. |
| Time Zone         | The time zone choices are SE local time, VOSM local time, or UTC. |
| Custom Date Range | The custom date range is used when Time Frame is set to custom. Enter the dates, beginning and end, for the chart in the mm/dd/yyyy format, or choose the dates by using the calendar icons. |

**Step 3** Click Update to see the report.

To export the report to a CSV (comma-separated value) file, click the Export icon in the task bar. A dialog box is displayed. Choose either Open or Save.

If you choose Open, the tabular report is displayed in the same browser window or a new browser window, depending on your browser.

If you choose Save, you are prompted to choose a location where to save the file. The file can be opened with any spreadsheet program.

To print the report, click the Print icon in the task bar.
Origin Service Monitoring

This section covers the Virtual Origin Service Table.

Virtual Origin Services Table

The Virtual Origin Services Table page lists all origin services on the system and displays the Service Routing Domain Name (SRDN) for each origin service.

Table 8-12 describes the icons for the Virtual Origin Services Table. To view or modify the configuration of an origin service, click the Edit icon next to the origin service name. To create a new origin service, click the Create New icon in the task bar.

Table 8-12 Virtual Origin Service Table Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon1.png" alt="New" /></td>
<td>Creates a new origin service.</td>
</tr>
<tr>
<td><img src="icon2.png" alt="Edit" /></td>
<td>Edits an origin service.</td>
</tr>
<tr>
<td><img src="icon3.png" alt="Filter" /></td>
<td>Creates a filtered table. Filter the origin service by the origin service name and content origin.</td>
</tr>
<tr>
<td><img src="icon4.png" alt="View" /></td>
<td>Views all origin services. Click this icon to view all origin services after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="icon5.png" alt="Refresh" /></td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td><img src="icon6.png" alt="Print" /></td>
<td>Prints the current window.</td>
</tr>
</tbody>
</table>

For more information, see the “Devices, Services, and Other Tables” section on page 4-7.

Monitoring Live Channels

Live channels can be managed through the Live Channel, Capture Resource, and Publish Resource tables. The Control Command column in each table provides a way to start and stop each channel and resource. The operational state of the channels and resources are displayed as well. This section describes the control and status monitoring functions of the following tables:

- Live Channel Table
- Capture Resource Table
- Publish Resource Table
Live Channel Table

Table 8-13 for more information. To view or modify the configuration of a live channel, click the Edit icon next to the live channel name. To create a new live channel, click the Create New icon in the task bar.

Channel States

- Table 8-13 for more information.
- Stopped—Channel is not capturing content; therefore, content is not being published
- Not Available—Channel configuration is incomplete (for example, there are no Acquisition nodes assigned, or the resources have not been defined)

Table 8-13 describes the state of a live channel based on the states of the Acquisition nodes. The Aggregated Channel State column shows the state that is displayed for the Live Channel Status based on the state of the Acquisition nodes assigned to the channel.

<table>
<thead>
<tr>
<th>Aggregated Channel State</th>
<th>State of Acquisition node 1</th>
<th>State of Acquisition node 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>Ready</td>
<td>Ready</td>
</tr>
<tr>
<td>Ready</td>
<td>Ready</td>
<td>Stopped</td>
</tr>
<tr>
<td>Ready</td>
<td>Ready</td>
<td>Updating</td>
</tr>
<tr>
<td>Partial Failure</td>
<td>Ready</td>
<td>Failed</td>
</tr>
<tr>
<td>Partial Failure</td>
<td>Partial Failure</td>
<td>Partial Failure</td>
</tr>
<tr>
<td>Partial Failure</td>
<td>Partial Failure</td>
<td>Partial Failure</td>
</tr>
<tr>
<td>Partial Failure</td>
<td>Partial Failure</td>
<td>Partial Failure</td>
</tr>
<tr>
<td>Partial Failure</td>
<td>Partial Failure</td>
<td>Stopped</td>
</tr>
<tr>
<td>Failed</td>
<td>Failed</td>
<td>Failed</td>
</tr>
<tr>
<td>Failed</td>
<td>Failed</td>
<td>Stopped</td>
</tr>
<tr>
<td>Failed</td>
<td>Failed</td>
<td>Updating</td>
</tr>
</tbody>
</table>

Channel Control

Stop icon displayed in the Control column. All channels that are currently stopped have the Start icon displayed. To start or stop a live channel, click the Stop or Start icon.

Capture Resource Table

Table 8-12 for more information. To view or modify the configuration of a capture resource, click the Edit icon next to the capture resource, name. To create a new capture resource, click the Create New icon in the task bar.

The Capture Resources Status includes the state of each Acquisition node. Following are the possible states of the Acquisition node Resource Status column:

- Ready—Acquisition node is ready to capture resources
Chapter 8: Monitoring the VDS-OS

Viewing Statistics

- Failed—Acquisition node has a failure in the capturing of resources
- Partial Failure—Acquisition node has a partial failure means that the capture resource is still functional, but there is a partial failure.
- Stopped—Acquisition node is not capturing content; therefore, content is not being published
- Not Available—Acquisition node configuration is incomplete (for example, the encapsulator is not pushing content)

The Capture Resources Table provides a way to start or stop a capture with the Control column. All capture resources that are currently started have the Stop icon displayed in the Control column. All capture resources that are currently stopped have the Start icon displayed. To start or stop a capture resources, click the Stop or Start icon.

Publish Resource Table

Table 6-11 for more information. To view or modify the configuration of a publish resource, click the Edit icon next to the publish resource name. To create a new publish resource, click the Create New icon in the task bar.

The Publish Resources Status includes the state of each Acquisition node. Following are the possible states of the Acquisition node Resource Status column:
- Ready—SE is ready to publish resources
- Failed—SE has a failure in the publishing of resources
- Partial Failure—SE has a partial failure means that the publish resource is still functional, but there is a partial failure.
- Stopped—SE is not publishing content
- Not Available—SE configuration is incomplete (for example, the encapsulator is not pushing content)
- Init—SE has not scheduled the resource yet, one reason could be there is an issue with setting up the channel

The Capture Resources Table provides a way to start or stop a capture with the Control column. All capture resources that are currently started have the Stop icon displayed in the Control column. All capture resources that are currently stopped have the Start icon displayed. To start or stop a capture resources, click the Stop or Start icon.

Viewing Statistics

The Statistics pages track system-wide playout and routing traffic in the VDS-OS. You can view statistics on playout traffic listed by SE or device group. The Routing Statistics page lists client requests and redirects.

This section contains the following procedures:
- Viewing Service Engines and Device Group Statistics
- Viewing Routing Statistics
Viewing Service Engines and Device Group Statistics

To view the statistics for all SEs or all device groups, do the following:

**Step 1**  
Choose **Devices > Statistics**. The Statistics page is displayed.

**Step 2**  
Choose **Service Engines** or **Device Groups**, and then choose **HTTP**.

Table 8-14 describes the icons provided on the Statistics pages.

### Table 8-14 Statistics Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Update application statistics. The statistics are updated at a configurable time interval, which is set in the System Configuration page (System.monitoring.collectRate). See the “Configuring System Settings” section on page 7-8. To see the latest statistics immediately, without waiting for the time interval to elapse, click this icon.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>Export a table to a comma-separated value (CSV) file.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>Refresh the table</td>
</tr>
<tr>
<td><img src="image4" alt="Icon" /></td>
<td>Print the current window.</td>
</tr>
</tbody>
</table>

Table 8-15 describes the statistic for HTTP.

### Table 8-15 Service Engine and Device Group Statistics

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP</strong></td>
<td></td>
</tr>
<tr>
<td>Requests/Sec</td>
<td>Number of requests per second.</td>
</tr>
<tr>
<td>Bytes/Sec</td>
<td>Number of bytes per second.</td>
</tr>
<tr>
<td>Hit Rate</td>
<td>Average number (as a percentage) of content items successfully served per minute from the cache of the SE or from all the SEs in the device group.</td>
</tr>
<tr>
<td>Updated</td>
<td>Timestamp indicating when the statistics were updated.</td>
</tr>
</tbody>
</table>
Viewing Routing Statistics

Step 1: Devices > Statistics > Routing Statistics.
Step 2: Choose one of the following options:
- Routing Requests
- Routing Redirects

See Table 8-14 for descriptions of the icons provided on the Routing Statistics pages. Table 8-16 describes each routing statistic.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Requests</td>
<td></td>
</tr>
<tr>
<td>Total Requests</td>
<td>Total number of content requests received from clients.</td>
</tr>
<tr>
<td>HTTP Requests</td>
<td>Number of ASX and traditional HTTP web requests received.</td>
</tr>
<tr>
<td>Updated</td>
<td>Timestamp indicating when the statistics were updated.</td>
</tr>
<tr>
<td>Routing Redirects</td>
<td></td>
</tr>
<tr>
<td>Total Requests</td>
<td>Total number of content requests received from clients.</td>
</tr>
<tr>
<td>Reqs Redirected</td>
<td>Total number of redirected client requests.</td>
</tr>
<tr>
<td>Reqs Not Redirected</td>
<td>Total number of client requests not redirected.</td>
</tr>
<tr>
<td>Updated</td>
<td>Timestamp indicating when the statistics were updated.</td>
</tr>
</tbody>
</table>

Log Files

Log files can be generally categorized in three main classes:
1. Transaction logs
2. Error and debug logs
3. General system logs and core files

Transaction Logs
Transaction logs are stored under the /local/local1/logs/ directory. They are disabled by default; to enable transaction logging either enter the transaction-logs enable command or check the Transaction Log Enable check box on the Transaction Log Settings page. See the “Configuring Transaction Logs” section on page 5-15 for more information.

Transaction log archiving is configured by using the transaction-logs archive command or by entering the settings on the Transaction Log Settings page.

To allow the Service Monitor module to collect threshold information enter the service-router service-monitor transaction-log enable command or check the Enable check box for each setting on the Service Monitor page. See the “Setting Service Monitor Thresholds” section on page 5-52 for more information. To configure the Service Monitor thresholds, use the Service Monitor page.
For more information about transaction logs, see the “Transaction Logs” section.

**Error and Debug Logs**

Error and debug logs are stored under the `/local/local1/errorlog/` directory. By default, all software modules only log error related information. Debug logging levels can be controlled (on a per software module basis) through the `debug` command.

There is a background cron job that periodically (every hour) monitors and trims the overall size of SYSFS (including the `errorlog/` directory).

**General System Logs and Core Files**

General system logs primarily consist of `/local/local1/syslog.txt`. In addition, any core files generated are stored to the `/local/local1/core_dir/` directory. The same background cron job used for the error and debug logs also monitors and trims the growth of `syslog.txt` and `core_dir/` directory. If the overall space usage of SYSFS exceeds 80 percent, this cron job raises an alarm indicating that.

When the overall SYSFS space usage exceeds 90 percent, this cron job starts freeing up space by removing the oldest files first. The algorithm used basically removes files based on their age. Initially, all files that are older than 30 days are removed (from the `core_dir/`, `errorlog/`, and `logs/` directories). If this does not free up enough space (that is less than 90 percent of capacity), then all files having an age of 10 days are removed.

---

**Transaction Logs**

Transaction logs allow administrators to view the traffic that has passed through the SE. Typical fields in the transaction log are the date and time when a request was made, the URL that was requested, whether it was a cache hit or a cache miss, the type of request, the number of bytes transferred, and the source IP address. For more information about configuring transaction log settings for SEs, see the “Configuring Transaction Logs” section on page 5-15.

This section discusses the following topics:

- Transaction Log Formats for Web Engine
- Usage Guidelines for Log Files
- Service Router Transaction Log Fields
- Service Monitor Transaction Logs
- Content Manager Transaction Log Fields
- Capture Controller Transaction Log Fields

**Note**

Each transaction log includes a header line that provides the VDS-OS software version and a summary line as the last line in the transaction log, which includes a summary of all the requests that appear in the transaction log.

---

**Transaction Log Formats for Web Engine**

The transaction logs for Web Engine consist of the following:

- Extended Squid
- Apache
Custom Format

Note
Changing the time zone on an SE does not affect the log entry nor the log filename. Both the log entries and the log filename always use UTC.

Note
The timestamp for Web Engine transaction log entry has no space between the date and the time. An example follows:


Extended Squid

The Extended Squid format logs the same fields logged by the Squid-1.1 access log file format. The Extended Squid transaction logs are located in the logs/webengine_extsquid/ directory.

For details on the Squid-1.1 native log file format, see the Squid documentation “Frequently Asked Questions,” “Squid Log” section, access.log heading at:

http://wiki.squid-cache.org/SquidFaq/FaqIndex

The Extended Squid-style log file format is as follows:

Current-Time Time-to-Serve Client-IP Request-Desc/Status-Returned Bytes-Xferred Method URL MIME-Type

An Extended Squid-style log format example looks like this:

[21/May/2009:00:29:12 +0530] 952195 171.71.50.197 TCP_REFRESH_MISS/200 11120239 GET http://7.9.0.3/1mbs_ai/1mbs1-100.wmv video/x-ms-wmv

Table 8-17 describes the fields for the Extended-Squid transaction log.

Table 8-17  Extended-Squid Transaction Log Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current-Time</td>
<td>Time (milliseconds), in common log time format, the request was received.</td>
</tr>
<tr>
<td>Time-to-Serve</td>
<td>Time, in microseconds, taken to complete the request.</td>
</tr>
<tr>
<td></td>
<td>This field could be zero if the transaction complete time is greater than</td>
</tr>
<tr>
<td></td>
<td>the transaction start time, which could occur if NTP is not synchronized.</td>
</tr>
<tr>
<td>Client-IP</td>
<td>IP address of the requesting client.</td>
</tr>
<tr>
<td>Request-Desc/Status-Returned</td>
<td>Combination of Squid result codes and the response code returned to the</td>
</tr>
<tr>
<td></td>
<td>client. The Request-Desc/Status-Returned field includes the error status</td>
</tr>
<tr>
<td></td>
<td>code for both TCP_MISS and TCP_HIT. A TCP_HIT with an error status code</td>
</tr>
<tr>
<td></td>
<td>means the HTTP response was served from cache. The meaning of a TCP_MISS</td>
</tr>
<tr>
<td></td>
<td>with an error status code has not changed.</td>
</tr>
<tr>
<td>Bytes-Xferred</td>
<td>Bytes sent to the client, including the headers.</td>
</tr>
</tbody>
</table>
Table 8-17  Extended-Squid Transaction Log Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>Request method.</td>
</tr>
<tr>
<td>URL</td>
<td>Requested URL, including the query string.</td>
</tr>
<tr>
<td>MIME-Type</td>
<td>MIME type.</td>
</tr>
</tbody>
</table>

Table 8-18 describes the Squid codes currently supported. The TCP_ codes refer to the cache status of the object when the request was handled by the Web Engine. In addition to the cache statistics listed in Table 8-18, the client or server error statistics could get incremented as well depending on the response code.

Table 8-18  Squid Code Request Descriptions

<table>
<thead>
<tr>
<th>Squid Result Code</th>
<th>Description</th>
<th>Valid Response (Status) Code</th>
<th>Mapping to Cache Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP_MISS</td>
<td>Requested object was not in cache.</td>
<td>0–5xx</td>
<td>Cache miss</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cache bypass</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Partial hit</td>
</tr>
<tr>
<td>TCP_MEM_HIT</td>
<td>Valid copy of the requested object was in memory.</td>
<td>Currently supports only 2xx response code</td>
<td>Cache hit and memory hit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(show statistics web-engine detail)</td>
</tr>
<tr>
<td>TCP_HIT</td>
<td>Valid copy of the requested object was in cache.</td>
<td>0, 2xx, 3xx, 406, 412, 416, 500</td>
<td>Cache hit</td>
</tr>
<tr>
<td>TCP_REFRESH_MISS</td>
<td>Requested object was cached but is stale. The query returned the new content.</td>
<td>0—5xx</td>
<td>Cache miss</td>
</tr>
<tr>
<td>TCP_REFRESH_HIT</td>
<td>Requested object was cached, but expired. The query for the object resulted in a “304 not modified” message.</td>
<td>0, 2xx, 406, 412, 416, 500</td>
<td>Cache hit</td>
</tr>
<tr>
<td>TCP_IMS_HIT</td>
<td>Client issued an IMS request for an object, which was in cache and was not stale.</td>
<td>0, 2xx, 3xx, 500</td>
<td>Cache hit</td>
</tr>
<tr>
<td>TCP_DENIED</td>
<td>Access was denied for this request.</td>
<td>403</td>
<td>—</td>
</tr>
<tr>
<td>NONE</td>
<td>See Request Description—None and None_Aborted, for the description.</td>
<td>000</td>
<td>—</td>
</tr>
<tr>
<td>NONE_ABORTED</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Request Description—None and None_Aborted

Normally, when a transaction completes, if the cache status is unknown (before the content lookup completes, the cache status is unknown), and the request was not denied by the Authorization Server, the request description that is written to the transaction log is “NONE.”
If a transaction completes because the client aborted the connection, “_ABORTED” is appended to “NONE.”

If a transaction completes because of an internal Web Engine failure, and there are no more transactions waiting for the process within the session, then the transaction was not aborted; therefore, the “_ABORTED” is not appended to “NONE.”

Under the conditions described above, because this occurs before the origin service is contacted and there is no Authorization Server failure or redirect, the response status code that is written to the transaction log is 000.

**Apache**

The Apache format is the Common Log File (CLF) format defined by the World Wide Web Consortium (W3C) working group. This format is compatible with many industry-standard log tools. The Apache-style transaction log files are located in the /webengine_apache/ directory.

The Apache-style log file format is as follows:

client-IP-address URI bytes-sent object-size bytes-received method status time-received time-to-serve

An Apache-style log file format example looks like this:

```
171.71.50.197 http://spcdn-se612-5.sanity.spcdn.net/gmedia-0.4gb.wmv 363704065 137
363710748 GET 200 [06/Nov/2007:00:25:32 +0530] 325033158
```

Table 8-19 describes the fields for the Apache-style transaction log.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-IP-address</td>
<td>IP address of the requesting client</td>
</tr>
<tr>
<td>URI</td>
<td>Requested URL, including the query string</td>
</tr>
<tr>
<td>bytes-sent</td>
<td>Bytes sent to client, including the headers</td>
</tr>
<tr>
<td>object-size</td>
<td>Bytes sent to client, excluding the HTTP headers</td>
</tr>
<tr>
<td>bytes-received</td>
<td>Bytes received from client</td>
</tr>
<tr>
<td>method</td>
<td>Request method</td>
</tr>
<tr>
<td>status</td>
<td>HTTP response code for the request</td>
</tr>
<tr>
<td>time-received</td>
<td>Time, in common log time format, the request was received</td>
</tr>
<tr>
<td>time-to-serve</td>
<td>Time, in microseconds, taken to complete the request</td>
</tr>
</tbody>
</table>

**Custom Format**

The transaction-logs format custom command allows you to use a log format string to log additional fields that are not included in the predefined Extended Squid format or Apache CLF format. The log format string is a string that can contain the tokens listed in Table 8-20 and that mimics the Apache log format string.

The log format string can contain literal characters that are copied into the log file. Double backslashes (\) can be used to represent a literal backslash, and a backslash followed by a single quote (\') can be used to represent a literal single quote. A literal double quote cannot be represented as part of the log format string. The control characters \t and \n can be used to represent a tab and a new line character, respectively. The custom transaction logs are located in the /webengine_clf/ directory.
The following command can be entered to generate the well-known Apache Combined Log Format:

```
transaction-logs format custom "%t %r %>s %b"
```

The following transaction log entry example is configured by using the preceding custom format string:

```
```

Apache and Squid can be represented by the following custom log format patterns:

Apache-style logging with custom patterns:

```
%a %U %O %b I %m %>s %t %D
```

Squid-style logging with custom patterns:

```
%Z %D %a %R/%>s %O %m %U %M
```

### Table 8-20 Custom Log Format String Values

<table>
<thead>
<tr>
<th>Format Token</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>%a</td>
<td>IP address of the requesting client.</td>
</tr>
<tr>
<td>%A</td>
<td>IP address of the SE.</td>
</tr>
<tr>
<td>%b</td>
<td>Bytes sent, excluding HTTP headers.</td>
</tr>
<tr>
<td>%B</td>
<td>Bit rate in bits per second (bps). Only for HSS session tracking.</td>
</tr>
<tr>
<td>%c</td>
<td>Time, in common log time format, that the log entry was generated.</td>
</tr>
<tr>
<td>%C</td>
<td>Records AuthLOOKupTime</td>
</tr>
<tr>
<td></td>
<td>CacheRouterTime displays only on the revalidation scenario. In normal cache-miss use case, the CALLOOKuptime includes the time taken by cache route lookup as well.</td>
</tr>
<tr>
<td>%D</td>
<td>Time consumed to serve the request in microseconds</td>
</tr>
<tr>
<td>%h</td>
<td>Remote host (IP address of the requesting client is logged).</td>
</tr>
<tr>
<td>%H</td>
<td>Request protocol.</td>
</tr>
<tr>
<td>%I</td>
<td>Bytes received from the client.</td>
</tr>
<tr>
<td>%k</td>
<td>Method of session tracking (cookie, URL query)</td>
</tr>
<tr>
<td>%m</td>
<td>Request method.</td>
</tr>
<tr>
<td>%M</td>
<td>MIME type of the requested asset.</td>
</tr>
<tr>
<td>%O</td>
<td>Bytes sent to client, including the headers.</td>
</tr>
<tr>
<td>%p</td>
<td>Client that set up the transport session for the request. The value is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Local—Request is from this SE.</td>
</tr>
<tr>
<td></td>
<td>• Internal—Request is from other SE</td>
</tr>
<tr>
<td></td>
<td>• External—Request is from end user</td>
</tr>
<tr>
<td>%q</td>
<td>Query string (which is preceded by a question mark (?) if a query string exists; otherwise, it is an empty string).</td>
</tr>
<tr>
<td>%r</td>
<td>First line of the request. The space in the first line of the request is replaced with a vertical bar (!) delimiter (for example, Get!/index.html!HTTP/1.1)</td>
</tr>
<tr>
<td>%R</td>
<td>Request description (Squid description codes).</td>
</tr>
<tr>
<td>%&gt;s</td>
<td>Status. The translog code always returns the HTTP response code for the request.</td>
</tr>
</tbody>
</table>
Usage Guidelines for Log Files

This section provides some guidelines for working with log files, and includes the following topics:

- Working Logs
- Archive Working Log
- Exporting Log Files

**Note**
The time stamp in the filename is always in UTC, but the time stamp for the log entries in the transaction logs depends on the transaction log.

Working Logs

Transaction logs are located in the `/local/local1/logs` directory. Each component has one or more directories, depending on its configuration.

There is a working log file in each directory, which is a symbol link, linking to the current working log file.

The log files are logged to a working log on the local disk as follows:

- Service Router logs are logged to a working log on the local disk in the `/local1/logs/service_router/working.log`
Chapter 8 Monitoring the VDS-OS

Transaction Logs

- Web Engine client transaction logs are located in the /local1/logs/webengine_apache, the /local1/logs/webengine_clf, and the /local1/logs/webengine_extsquid directories.
- Service Router transaction logs are located in the /local1/logs/service_router directory.
- Service Monitor transaction logs are located in the /local1/logs/service_monitor directory.
- Content Manager transaction logs are located in the /local1/logs/content_mgr directory.

Archive Working Log

You can specify the interval at which the working log should be cleared, when the interval occurs the data is moved to an archive log. The archive log files are located on the local disk in the /local1/logs/ directory.

The archiving of working logs can be configured to occur at a specified time interval and when the working log file reaches a specified size. If one of the criteria is met and at least one new message has been written to the working log, a log rotation occurs. If one of the criteria is met and no new messages have been written to the working log, a log rotation does not occur. You can specify the maximum number of old logs kept on disk.

Because multiple archive files are saved, the filename includes the timestamp when the file was created. The time stamp in the filename is always in UTC, but the time stamp for the log entries in the transaction logs depends on the transaction log. Because the files can be exported to an FTP/SFTP server, the filename also contains the IP address of the SE.

The archive filenames use this format:
`modulename_IPADDRESS_YYYYMMDD_HHMMSS_file-generation-number`.

**Note**
The IP address used in the archived filename is not necessarily the primary interface of the SE. The transaction log function decides on which IP address to use in creating the archive name.

Exporting Log Files

To facilitate the post-processing of cache log files, you can export transaction logs to an external host. This feature allows log files to be automatically exported by FTP to an external host at configurable intervals. The username and password used for FTP are configurable, as is the directory to which the log files are uploaded.

The log files automatically have a filename that uses the `<type>_<ipaddr>_yyyyymmdd_hhmss_<file_generation_number>` format, where:

- `<type>` represents the type of log file, with `selog` for cache logs such as HTTP, HTTPS, and FTP.
- `<ipaddr>` represents the SE IP address.
- `yyyyymmdd_hhmss` represents the date and time when the log was archived for export.
- `<file_generation_number>` represents the File Generation Number, which has a range from 00001 to 99999.

Exporting Transaction Logs to External FTP Servers

To export transaction logs to an FTP server, you must first enable exporting of transaction logs and then configure the FTP or secure FTP (SFTP) server parameters. This feature can support up to four FTP servers. The following information is required for each target FTP server:

- Server IP address or the hostname
The SE translates the hostname with a DNS lookup and then stores the IP address in the configuration.

- FTP user login and user password
- Path of the directory where transferred files are written

Use a fully qualified path or a relative path for the user login. The user must have write permission to the directory.

You can also compress archived log files into gzip format before exporting them to external FTP servers. The compressed filename has a .gz extension. This compression feature uses less disk space than that required for uncompressed archived files on both the SE and the FTP export server and also requires less bandwidth during export because of the smaller size of the files to be exported.

For more information about exporting and archiving transaction logs, see the “Configuring Transaction Logs” section on page 5-15 for SEs, and the “Configuring Transaction Logs for the Service Router” section on page 5-71 for SRs.

To immediately have the transaction logs archived and exported following the next transaction, use the following commands:

```
SE# transaction-log force archive
SE# transaction-log force export
```

The `transaction-log force archive` command causes the transaction log to be archived to the SE hard disk following the next transaction. The `transaction-log force export` command causes the transaction log to be exported to the configured FTP server. The `transaction-log force` commands do not change the configured or default schedule for an archive or export of the transaction logs. The archive or export interval is restarted after the forced operation. If a scheduled archive or export job is in progress when the `transaction-log force` command is entered, the command has no effect.

### Restoring Export After Receiving a Permanent Error from the External FTP Server

When an FTP server returns a permanent error to the SE, the export is retried at 10-minute intervals or sooner if the configured export interval is sooner. If the error is a result of a misconfiguration, the archive transaction logs are no longer exported to that server. You must re-enter the SE transaction log export parameters for the misconfigured server to clear the error condition.

A permanent error (Permanent Negative Completion Reply, RFC 959) occurs when the FTP command to the server cannot be accepted, and the action does not take place. Permanent errors can be caused by invalid user logins, invalid user passwords, and attempts to access directories with insufficient permissions or directories that do not exist.

### Exporting Transaction Logs to External SFTP Servers

You can also export transaction logs to a Secure File Transfer Protocol (SFTP) server. You must first enable the feature and configure the SFTP server parameters. The following information is required for each target SFTP server:

- SFTP server IP address or the hostname
  
  The SE translates the hostname with a DNS lookup and then stores the IP address in the configuration.

- SFTP user login and user password

- Path of the directory where transferred files are written

Use a fully qualified path or a relative path for the user login. The user must have write permission to the directory.
To enable this feature, enter the `sshd allow-non-admin-users` command on the SE. If this feature is enabled, the output of the `show running-config` EXEC command shows that this feature is enabled on the SE.

**Service Router Transaction Log Fields**

Table 8-21 describes the fields for the Service Router transaction log.

**Table 8-21  Service Router Transaction Log Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c-ip</td>
<td>Source Internet Protocol (IP) address of the connected socket. This may be the IP address of a proxy server or firewall.</td>
</tr>
<tr>
<td>user-agent</td>
<td>Browser type used if the player was embedded in a browser. If the player was not embedded, this field refers to the user agent of the client that generated the log. The user-agent value is enclosed in double quotes (“ “).</td>
</tr>
<tr>
<td>date</td>
<td>Date, in international date format, when a client is connected.</td>
</tr>
<tr>
<td>time</td>
<td>Time when the client is connected. The time format is either in Coordinated Universal Time (UTC) or local time, depending on how the logging plug-in is configured.</td>
</tr>
<tr>
<td>url</td>
<td>URL requested by the client.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol used to access the content.</td>
</tr>
<tr>
<td>server-picked</td>
<td>Service Engine selected by the Service Router.</td>
</tr>
<tr>
<td>routed-path</td>
<td>Path of the redirected URL that is used for last-resort error-domain redirects and last-resort translator API requests.</td>
</tr>
<tr>
<td>status</td>
<td>Status code.</td>
</tr>
<tr>
<td>routing-method</td>
<td>Routing method chosen. The routing-method field has the following possible values:</td>
</tr>
<tr>
<td></td>
<td>• Last-Resort</td>
</tr>
<tr>
<td></td>
<td>• Network</td>
</tr>
<tr>
<td></td>
<td>• Proximity</td>
</tr>
<tr>
<td></td>
<td>• Zero-Network</td>
</tr>
<tr>
<td></td>
<td>• Geo-Location</td>
</tr>
</tbody>
</table>

**Service Monitor Transaction Logs**

Service Monitor transaction logs provide a tool for analyzing the health history of a device to ensure the device is within the configured capacity limits.

The device and service health information are periodically logged on the device in transaction log files. Transaction logs provide a useful mechanism to monitor and debug the system. The transaction log fields include device information applicable to Service Engines and Service Routers that are useful for capacity monitoring. Additionally, when a device threshold is exceeded, detailed information is sent to a file (threshold_exceeded.log) to capture the processes that triggered the threshold alarm. To configure threshold settings, see the “Setting Service Monitor Thresholds” section on page 5-52.
Chapter 8  Monitoring the VDS-OS

Transaction Logs

The Service Monitor transaction log filename has the following format:
```
service_monitor_<ipaddr>_yyyymmdd_hhnmmss_<>
```
where:
- `<ipaddr>` represents the IP address of the SE, SR, or VOSM.
- `yyyymmdd_hhnmmss` represents the date and time when the log was created.

For example, `service_monitor_192.168.1.52_20110630_230001_00336` is the filename for the log file on the device with the IP address of 192.168.1.52 and a time stamp of June 30, 2011 at 3:36 AM.

The Service Monitor transaction log file is located in the `/local1/logs/service_monitor` directory.

An entry to the Service Monitor transaction log is made every two seconds.

**Note**

The following rules apply to Service Monitor transaction logs:
- A transaction log value is only logged if the Service Monitor is enabled for that component on the device. For example if CPU monitoring is not enabled, the transaction log value “–” is displayed.
- If a log field can have more than one value, the values are delimited by the pipe (|) character.
- If a value can have sub-values, the sub-values are delimited by the carrot (^) character.
- Some of the fields display aggregate values. If the statistics are cleared using the `clear statistics` command, the value after clearing the statistics may be less than the previous values, or may be zero (0).

**Table 8-22** describes the fields for the Service Monitor transaction log on an SE.

<table>
<thead>
<tr>
<th>Field</th>
<th>Sample Output</th>
<th>Description</th>
<th>Corresponding CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>2011-06-30</td>
<td>Date of log.</td>
<td><code>show service-router service-monitor</code></td>
</tr>
<tr>
<td>time</td>
<td>22:52:02</td>
<td>Time of log.</td>
<td><code>show service-router service-monitor</code></td>
</tr>
<tr>
<td>cpu_avg</td>
<td>21</td>
<td>Moving average value in percentage of CPU usage.</td>
<td><code>show service-router service-monitor</code></td>
</tr>
<tr>
<td>mem_avg</td>
<td>44</td>
<td>Moving average value in percentage of memory usage.</td>
<td><code>show service-router service-monitor</code></td>
</tr>
<tr>
<td>kernel-mem-avg</td>
<td>11</td>
<td>Moving average value in percentage of kernel memory.</td>
<td><code>show service-router service-monitor</code></td>
</tr>
<tr>
<td>disk_avg</td>
<td>2</td>
<td>Moving average value in percentage of disk usage.</td>
<td><code>show service-router service-monitor</code></td>
</tr>
<tr>
<td>disk_fail_count_threshold</td>
<td>Y</td>
<td>Boolean value to indicate if disk fail count threshold has been reached.</td>
<td><code>show service-router service-monitor</code></td>
</tr>
<tr>
<td>per_disk_load</td>
<td>disk03-01^2\ disk04-02^5</td>
<td>Current load per disk, as a percentage. The sample output indicates that disk03–partition01 has a 2 percent load and disk04–partition02 have a 5 percent load.</td>
<td><code>show service-router service-monitor</code></td>
</tr>
</tbody>
</table>
### Table 8-22  SE Service Monitor Transaction Log Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Sample Output</th>
<th>Description</th>
<th>Corresponding CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth_avg</td>
<td>Port_Channel_1^2^4&amp;\ Port_Channel_2^0^0</td>
<td>Moving average bandwidth used, as a percentage, of bandwidth in and bandwidth out per interface. The sample output indicates that port channel 1 has an average bandwidth of 2 percent for receiving and 4 percent for transmitting, and port channel 2 average bandwidth usage is 0.</td>
<td>show service-router service-monitor Device status—NIC—Average BW In/Average BW Out</td>
</tr>
<tr>
<td>file-desc-count</td>
<td>1023</td>
<td>Total count of file descriptors open on the device. File descriptors are internal data structures maintained by the Linux kernel for each open file.</td>
<td>show statistics lsof</td>
</tr>
<tr>
<td>tcp_server_connections</td>
<td>35</td>
<td>Number of TCP server connections open.</td>
<td>show statistics tcp TCP Statistics—Server connection openings</td>
</tr>
<tr>
<td>tcp_client_connections</td>
<td>24</td>
<td>Number of TCP client connections open.</td>
<td>show statistics tcp TCP Statistics—Client connection openings</td>
</tr>
<tr>
<td>processes_count</td>
<td>42</td>
<td>Number of processes running on the device.</td>
<td>show processes</td>
</tr>
<tr>
<td>dataserver-cpu-percentage</td>
<td>1</td>
<td>Percentage of the CPU used for the dataserver process.</td>
<td>--</td>
</tr>
<tr>
<td>web_engine_threshold_exceeded</td>
<td>Y</td>
<td>Boolean value to indicate if the Web Engine threshold has been exceeded.</td>
<td>show service-router service-monitor Services status—Web—Threshold</td>
</tr>
<tr>
<td>web-engine-augment-threshold-exceeded</td>
<td>Y</td>
<td>Boolean value to indicate if Web Engine augmentation alarm threshold has been exceeded.</td>
<td>--</td>
</tr>
<tr>
<td>web_engine_stopped</td>
<td>N</td>
<td>Boolean value to indicate if Web Engine has stopped.</td>
<td>show service-router service-monitor Services status—Web—Stopped</td>
</tr>
<tr>
<td>web-engine-cpu-percentage</td>
<td>3</td>
<td>Percentage of the CPU used by the Web Engine.</td>
<td>--</td>
</tr>
<tr>
<td>web_engine_mem</td>
<td>3500</td>
<td>Memory (in bytes) used by the Web Engine.</td>
<td>show web-engine health Total memory usage</td>
</tr>
<tr>
<td>web_engine_get_requests</td>
<td>250</td>
<td>Count of get requests received by the Web Engine (Aggregate value)</td>
<td>show statistics web-engine detail HTTP Request Type Statistics—Get requests</td>
</tr>
<tr>
<td>web_engine_sessions</td>
<td>5</td>
<td>Count of HTTP connections.</td>
<td>show statistics web-engine detail Web-Engine Detail Statistics—Total HTTP Connection + Active Session</td>
</tr>
<tr>
<td>web_engine_upstream_connections</td>
<td>2</td>
<td>Count of HTTP connections to upstream SE or origin service.</td>
<td>show statistics web-engine detail Web-Engine Detail Statistics—Total HTTP Connection</td>
</tr>
</tbody>
</table>
Table 8-22  
**SE Service Monitor Transaction Log Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Sample Output</th>
<th>Description</th>
<th>Corresponding CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>uns-cpu-percentage</td>
<td>3</td>
<td>Percentage of CPU used by the Unified Namespace (UNS) process.</td>
<td>–</td>
</tr>
<tr>
<td>uns_mem</td>
<td>3500</td>
<td>Memory used by the UNS process.</td>
<td>–</td>
</tr>
</tbody>
</table>

Table 8-23 describes the fields for the Service Monitor transaction log on a SR.

Table 8-23  
**SR Service Monitor Transaction Log Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Sample Output</th>
<th>Description</th>
<th>Corresponding CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>2011-06-30</td>
<td>Date of log.</td>
<td>–</td>
</tr>
<tr>
<td>time</td>
<td>22:52:02</td>
<td>Time of log.</td>
<td>–</td>
</tr>
<tr>
<td>cpu_avg</td>
<td>21</td>
<td>Moving average value in percentage of CPU usage.</td>
<td><code>show service-router service-monitor</code> <code>Device status—CPU—Average load</code></td>
</tr>
<tr>
<td>mem_avg</td>
<td>44</td>
<td>Moving average value in percentage of memory usage.</td>
<td><code>show service-router service-monitor</code> <code>Device status—Mem—Average used memory</code></td>
</tr>
<tr>
<td>kernel-mem-avg</td>
<td>11</td>
<td>Moving average value in percentage of kernel memory.</td>
<td><code>show service-router service-monitor</code> <code>Device status—KMEM—Average kernel memory</code></td>
</tr>
<tr>
<td>disk_avg</td>
<td>2</td>
<td>Moving average value in percentage of disk usage.</td>
<td><code>show service-router service-monitor</code> <code>Device status—Disk—Average load</code></td>
</tr>
<tr>
<td>disk_fail_count_threshold</td>
<td>Y</td>
<td>Boolean value to indicate if disk fail count threshold has been reached.</td>
<td><code>show service-router service-monitor</code> <code>Device status—Device Status—Disk—Status</code></td>
</tr>
<tr>
<td>file-desc-count</td>
<td>1023</td>
<td>Total count of file descriptors open on the device.</td>
<td>–</td>
</tr>
<tr>
<td>tcp_server_connections</td>
<td>35</td>
<td>Number of TCP server connections open.</td>
<td><code>show statistics tcp</code> <code>TCP Statistics—Server connection openings</code></td>
</tr>
<tr>
<td>tcp_client_connections</td>
<td>24</td>
<td>Number of TCP client connections open.</td>
<td><code>show statistics tcp</code> <code>TCP Statistics—Client connection openings</code></td>
</tr>
<tr>
<td>processes_count</td>
<td>42</td>
<td>Number of processes running on the device.</td>
<td><code>show processes</code></td>
</tr>
<tr>
<td>dataserver-cpu-percentage</td>
<td>1</td>
<td>Percentage of the CPU used for the dataserver process.</td>
<td>–</td>
</tr>
<tr>
<td>sr-cpu-percentage</td>
<td>12</td>
<td>Cpu percentage used by SR.</td>
<td>–</td>
</tr>
<tr>
<td>sr_mem</td>
<td>750000</td>
<td>Memory (in bytes) used by SR.</td>
<td><code>show processes memory</code> and search for service_router</td>
</tr>
</tbody>
</table>
**Content Manager Transaction Log Fields**

The Content Manager transaction log filename has the following format:

```
content_mgr__<ipaddr>__yyyymmdd_hhmmss__>
```

- `<ipaddr>` represents the IP address of the SE, SR, or VOSM.
- `yyyymmdd_hhmmss` represents the date and time when the log was created.

The Content Manager transaction log file is located in the `/local1/logs/content_mgr` directory. Table 8-24 describes the fields for the Content Manager transaction log on an SE.

### Table 8-24 Content Manager Transaction Log Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Date of log entry.</td>
</tr>
<tr>
<td>Time</td>
<td>Time of log entry.</td>
</tr>
<tr>
<td>ContentType</td>
<td>Type of content, which is either cached or prepos-content (prefetched).</td>
</tr>
<tr>
<td>Operation</td>
<td>Content Manager operation, which is addition, deletion, update, or eviction.</td>
</tr>
<tr>
<td>Priority</td>
<td>Prefetched content always has a priority of 0, which means ignore. The lower the number, the lower the priority.</td>
</tr>
<tr>
<td>CreationDate</td>
<td>Date the content object was created.</td>
</tr>
<tr>
<td>CreationTime</td>
<td>Time the content object was created.</td>
</tr>
<tr>
<td>FileSize</td>
<td>File size, in bytes, of the content object.</td>
</tr>
<tr>
<td>HitCount</td>
<td>Number of times the content object was accessed.</td>
</tr>
<tr>
<td>URL</td>
<td>URL of the content object. If Content Manager cannot retrieve the URL by using the FastCAL lookup of the disk path, then the ContentType field has a value of “unknown-content” and the URL field displays “-.”</td>
</tr>
<tr>
<td>Path</td>
<td>Disk path of the content object.</td>
</tr>
</tbody>
</table>

Table 8-23 SR Service Monitor Transaction Log Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Sample Output</th>
<th>Description</th>
<th>Corresponding CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>requests_received</td>
<td>34</td>
<td>Total count of requests received by SR (aggregate value)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>show statistics service-router summary Requests Received</td>
<td></td>
</tr>
<tr>
<td>http_normal_requests_received</td>
<td>5</td>
<td>Not applicable in VDS-OS.</td>
<td></td>
</tr>
<tr>
<td>http_asx_requests_received</td>
<td>5</td>
<td>Not applicable in VDS-OS.</td>
<td></td>
</tr>
<tr>
<td>rtsp_requests_received</td>
<td>5</td>
<td>Not applicable in VDS-OS.</td>
<td></td>
</tr>
<tr>
<td>rtmp_requests_received</td>
<td>5</td>
<td>Not applicable in VDS-OS.</td>
<td></td>
</tr>
<tr>
<td>dns_requests_received</td>
<td>6</td>
<td>Total count of DNS requests received by SR (aggregate value).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>show statistics service-router dns Total DNS queries</td>
<td></td>
</tr>
</tbody>
</table>
Capture Controller Transaction Log Fields

\(<ipaddr>_yyyymmdd_hhmmss_<>\), where:

- \(<ipaddr>\) represents the IP address of the SE or SR.
- \(yyyymmdd_hhmmss\) represents the date and time when the log was created.

The Capture Controller transaction log file is located in the `/local1/logs/capturecontroller` directory.

Table 8-25 describes the fields for the Capture Controller transaction log on an SE or SR.

**Table 8-25  Capture Controller Transaction Log Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Time (in UTC) this particular record is logged.</td>
</tr>
<tr>
<td>PublishURI</td>
<td>URI used to publish the recorded asset to the client. This is the live channel URI followed by the publish resource base URI configured on the VOSM; for example, <a href="http://vos.demo.net/abchd_west/live/hls/index.m3u8">http://vos.demo.net/abchd_west/live/hls/index.m3u8</a>.</td>
</tr>
<tr>
<td>Channel URI</td>
<td>Uniquely identifies the channel across the system. It is a combination of the origin service and the live channel name; for example, <a href="http://vos.demo.net/abchd_west">http://vos.demo.net/abchd_west</a>.</td>
</tr>
<tr>
<td>Event</td>
<td>Event has the following values:</td>
</tr>
<tr>
<td></td>
<td>- Linear—Live publish resource</td>
</tr>
<tr>
<td></td>
<td>- Scheduled—Live-to-VOD publish resource configured using the Capture Schedule XML or through the Recorder Manager.</td>
</tr>
<tr>
<td>MediaType</td>
<td>Indicates the Media Encapsulation Format (hss/smooth/hls/dash/c2)</td>
</tr>
<tr>
<td>StartTime</td>
<td>Time the recording started for the publish resource. This is the configured start time.</td>
</tr>
<tr>
<td>StopTime</td>
<td>Time the recording stopped/completed for the publish resource. this is the configured stop time.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the publish resource when it completed or stopped. Status has the following values:</td>
</tr>
<tr>
<td></td>
<td>- Complete,</td>
</tr>
<tr>
<td></td>
<td>- Partial Complete</td>
</tr>
<tr>
<td></td>
<td>- Failed</td>
</tr>
<tr>
<td></td>
<td>- Partial Failed</td>
</tr>
<tr>
<td></td>
<td>- Stopped</td>
</tr>
<tr>
<td></td>
<td>- Playout Only</td>
</tr>
<tr>
<td>CaptureResource</td>
<td>Capture resource is a collection of source profiles defined on the Cisco Media Encapsulator (CME). A live channel can have multiple capture resources. This field (relative to the Channel ID) indicates which of the configured capture resources is used by this publish resource.</td>
</tr>
<tr>
<td>TimeShiftDuration</td>
<td>Time (in minutes) the user can seek back to while playing a live stream.</td>
</tr>
<tr>
<td>StartOverURI</td>
<td>Currently not supported.</td>
</tr>
</tbody>
</table>
### Table 8-25 Capture Controller Transaction Log Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActionOnCompletion</td>
<td>The VDS-OS provides an option to notify an external entity, by using the Capture Schedule XML file, after the recording of a VOD publish resource is complete. This field indicates the action as “Notify” if configured and the Notify URL.</td>
</tr>
<tr>
<td>PublishStreamInfo (Stream</td>
<td>BitRate</td>
</tr>
</tbody>
</table>
CHAPTER 9

Maintaining the VDS-OS

This chapter explains how to perform common administrative tasks including updating system software, hard disk drive maintenance, rebooting and deleting devices, and troubleshooting.

- Software Upgrade, page 9-1
- Rebooting Devices, page 9-8
- Deleting a Device, page 9-9
- Replacing a Device, page 9-12
- Backup and Recovery Procedures, page 9-14
- Troubleshooting, page 9-25

For information about database maintenance, see the “Scheduling Database Maintenance” section on page 5-31.

Software Upgrade

The software upgrade section covers the following topics:

- Getting a Software File from Cisco.com
- Finding the Software Version of the Devices
- Configuring the Software Image Settings
- Upgrading the Software
- Upgrading an SE, SR, or VOSM
- Upgrading a Virtual Machine (VM)

Getting a Software File from Cisco.com

To get a software file from Cisco.com, do the following:

**Step 1**
Launch your web browser and enter the following URL:
http://www.cisco.com/cisco/software/navigator.html
The Select a Product page is displayed if you have recently logged in; otherwise, the Log In page is displayed.
Step 2 Log in to Cisco.com using your designated username and password.

Step 3 Choose Products > Video > Videoscape > Cisco Videoscape Distribution Suite > Cisco Videoscape Distribution Suite Origin Server. The Downloads page is displayed.

Step 4 Click the software release you want. The page refreshes and the software image files are displayed.

Step 5 Click the link for the software image file you want.

- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click Accept.
- If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.

The Download page is displayed with the information about the software image file and a Download link.

Step 6 Click Download Now to download the file, or click Add to cart to select more image files before downloading them. The Download Cart page is displayed.

Step 7 Click Proceed With Download. The Cisco End User Software License Agreement is displayed.

Step 8 Read the agreement and click Agree. The Download Software page is displayed.

Step 9 Choose a download option, either Download Manager Option or Non Java Download Option. A new window displays the filename of the ISO image file.

Step 10 Click Download. The File Download dialog box is displayed.

Step 11 Click Save. The Save As dialog box is displayed.

Step 12 Navigate to the location where you want to save the file and click Save. The file downloads.

Finding the Software Version of the Devices

The VOSM Home page gives a brief summary of the software versions in use on all the devices in the VDS-OS network.

To view the software version running on a particular device, choose Devices > Devices. The Devices Table page displays the software version for each device listed.

Clicking the Edit icon next to the device name in the Devices Table page displays the Devices home page, which shows the software version for that device.

Note The software version is not upgraded until a software upgrade has been successfully completed. If a software upgrade is in progress, the version number displayed is the base version, not the upgraded version number.

Configuring the Software Image Settings

To upgrade your VDS-OS software release, you must first configure the software image settings.

To configure the software image settings, do the following:
**Step 1** Choose **System > Software Image Management**. The Software Files Table page is displayed.

**Step 2** Click the **Create New** icon in the task bar. The Software Image page is displayed (Figure 9-1).

**Figure 9-1 Software Image Page**

```
Creating New Software Image

Software Image Settings

Software Image URL: [http or ftp]
Username: [Enter username]
Password: [Enter password]
Confirm Password: [Enter password]
Software Version: [Enter valid version]
File Size: [Enter size in bytes]

Advanced Settings

Auto Reloc: [Specify whether to automatically relocate after install]
Download Method: [Default, Direct Download Only]
VOS IP Address: [Enter IP address]

Comments

Submit Cancel
```

**Step 3** In the **Software Image URL** field, enter the URL for the .bin software file that you downloaded from Cisco.com.

a. Choose a protocol (http or ftp) from the drop-down list.

b. Enter the URL of the software file; for example, a valid URL might look like this:

   `http://internal.mysite.com/vos/VDS-OS-2.x.x-K9.bin`

   In this URL, `VDS-OS-2.x.x-K9` is the name of the software upgrade file. (The filename might include the version number.)

**Step 4** If your server requires user login authentication, enter your username in the **Username** field and enter your login password in the **Password** field. Enter the same password in the **Confirm Password** field.

**Step 5** Enter the software version number in the **Software Version** field. You can copy this number from the version portion of the software filename in the software file URL.
Software Upgrade

Chapter 9 Maintaining the VDS-OS

Specify the version in one of two formats: X.Y.Z-bB or X.Y.Z.b.B, where X = major version, Y = minor version, Z = maintenance version, b = build letter, and B = build number.

Step 6 If you want the size of the software file considered during validation, enter a file size (in bytes) in the File Size field. If you leave this field blank, the URL is checked without regard to the software file size.

Step 7 To validate the Software Image URL, Username, and Password fields, click the Validate Software Image Settings button.

When you click the Validate Software Image Settings button, the following occurs:

- Software file URL is resolved.
- Connection to the software file URL is established using the username and password, if specified.
- If a file size is specified, the actual size of the software file is obtained and compared against the value in the File Size field.
- Message is returned, indicating success or errors encountered.

Step 8 In the Advanced Settings section, check the Auto Reload check box to automatically reload a device when you upgrade the software.

Step 9 If you want, you can choose one of three download methods:

- Default—Uses pre-positioned content but always falls back to direct download.
- Direct Download Only—Directly downloads the file using the software file URL.

Step 10 For downgrades only, specify the VOSM IP address to be used for device registration in the VOSM IP Address field.

The VOSM IP Address field is the IP address of a VOSM after the software is downgraded. (This field is optional and only applies for downgrades.) After the downgrade, the SE registers with the VOSM with the IP address specified in this field.

Step 11 Click Submit.

To delete a software file, click the Delete icon in the task bar.

Caution

If your browser is configured to save the username and password for the VOSM, the browser auto-populates the Username and Password fields in the Software Image page. You must clear these fields before you click Submit.

The software file that you want to use is now registered with the VOSM. When you perform the software upgrade or downgrade, the URL that you just registered becomes one of the choices available in the Update Software page. (See the “Upgrading the Software” section on page 9-4.)

Upgrading the Software

When upgrading software in your VDS-OS network, begin with Service Engines and Service Routers before upgrading the VOSM. The VOSM reboots at the conclusion of the upgrade procedure, causing you to temporarily lose contact with the device and the user interface. After the VOSM has upgraded its software and rebooted, it may be unable to communicate with devices running different versions of the VDS-OS software.
Caution

Primary and standby VOSMs must be running the same version of VDS-OS software. If they are not, the standby VOSM detects this and does not process any configuration updates it receives from the primary VOSM. You need to upgrade your standby VOSM first, and then upgrade your primary VOSM. We also recommend that you create a database backup for the primary VOSM and copy the database backup file to a safe place before you upgrade the software.

To upgrade the software image on a server, you first need to offload a server for maintenance. Once the server has been fully offloaded, you can upgrade the software. After updating the software, uncheck the Server Offload check box to allow the server to receive client requests from the Service Router. See the Server Offload field in Table 5-6 on page 5-10 for more information.

Downgrading the Software

For software downgrades of systems with primary and standby VOSMs, you need to do the following:

1. If you are using the VOSM GUI, downgrade the standby VOSM first, followed by the primary VOSM.
   
   If you are using the CLI, downgrade the primary VOSM first, followed by the standby VOSM.

2. After downgrading the primary and standby VOSMs, using the CLI, log in to each VOSM and run the following commands:
   
   ```
   cms database downgrade
   cms enable
   ```

3. Downgrade the software on the Service Routers.

4. Downgrade the Acquisition Nodes.

5. Downgrade the middle-tier Service Engines.

6. Downgrade the edge Service Engines.

Interoperability Considerations

In general, a VDS-OS network is upgraded gradually, so that your network might consist of nodes with different software versions for the duration of time it takes to upgrade all nodes. Dissimilar software versions are not supported in the long term, and only the interoperability considerations listed below are supported until all devices are running the same software version. You can expect the following behavior during an upgrade or downgrade of your network:

- VDS-OS network continues to operate with mixed versions up to one major or minor version difference in a deployed solution.

- New features that depend on device cooperation might not be fully functional until the VDS-OS network upgrade is complete, but no existing features are affected.

- While being upgraded, a node is unavailable for a short time.

- All nodes, other than the node being upgraded, continue to operate at full capacity. The availability of other nodes is not affected during an upgrade.

- Content is preserved during an upgrade or downgrade unless you remove an origin service.

- All logs are preserved during an upgrade or downgrade, unless you change the disk configuration. Anytime disk space is reconfigured, the logs are automatically removed.
We strongly recommend that you upgrade your VDS-OS network devices in the following order:

1. Edge Service Engines
2. Middle-tier Service Engines
3. Acquisition Nodes

**Note** When upgrading the Acquisition Node in an origin service, to avoid having a critical alarm generated while the Acquisition Node is being upgraded, temporarily set the System.datafeed.pollRate field to 200 seconds or higher. When the upgrade is complete, reset the field to the original value. See the “System Properties” section on page 7-8 for more information.

4. Service Routers
5. Standby VOSMs (Upgrade before primary when using the GUI only.)
6. Primary VOSM

**Note** When you upgrade VOSMs using the CLI, we recommend that you upgrade your primary VOSM first, and then upgrade your standby VOSM. Primary and standby VOSMs must be operating with exactly the same software release as each other for failover to be successful.

### Upgrading Software by Device Groups

**Note** This procedure is for Service Engines only. Service Routers and VOSMs cannot be associated with device groups.

To upgrade your software on multiple Service Engines, do the following:

**Step 1** Choose Devices > Device Groups. The Device Groups Table page is displayed.

**Step 2** Click the Edit icon next to the name of the device group that you want to upgrade. The Device Group page is displayed.

**Step 3** From the left-panel menu, choose Software Update. The Software Update for Device Group page is displayed.

**Step 4** Choose the software file URL from the Software File URL list by clicking the radio button next to the filename.

**Step 5** Click Submit.

To view progress on an upgrade, go to the Devices Table page (Devices > Devices). Software upgrade status messages are displayed in the Software Version column. These intermediate messages are also written to the system log on the Service Engines. See Table 9-1 for a description of upgrade status messages.
### Table 9-1 Upgrade Status Messages

<table>
<thead>
<tr>
<th>Upgrade Status Message</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>The request has yet to be sent from the VOSM to the device, or receipt of the request has yet to be acknowledged by the device.</td>
</tr>
<tr>
<td>Downloading</td>
<td>The download method for the software file is being determined.</td>
</tr>
<tr>
<td>Proceeding with Pre-positioned Download</td>
<td>The download method for the software file is detected as pre-positioned. Proceeding with download of a pre-positioned software file.</td>
</tr>
<tr>
<td>Proceeding with Download</td>
<td>The download method for the software file is detected as direct download. Proceeding with the request for direct download of the software file.</td>
</tr>
<tr>
<td>Download in Progress (Completed …)</td>
<td>Direct download of the software file is being processed. “Completed” indicates the number of megabytes processed.</td>
</tr>
<tr>
<td>Download Successful</td>
<td>The direct download of the software file has been successful.</td>
</tr>
<tr>
<td>Download Failed</td>
<td>The direct download of the software file cannot be processed. Further troubleshooting is required; see the device system message log.</td>
</tr>
<tr>
<td>Proceeding with Flash Write</td>
<td>A request has been made to write the software file to the device flash memory.</td>
</tr>
<tr>
<td>Flash Write in Progress (Completed …)</td>
<td>The write of the device flash memory is being processed. “Completed” indicates the number of megabytes processed.</td>
</tr>
<tr>
<td>Flash Write Successful</td>
<td>The flash write of the software file has been successful.</td>
</tr>
<tr>
<td>Reloading</td>
<td>A request to reload the device has been made to complete the software upgrade. The device may be offline for several minutes.</td>
</tr>
<tr>
<td>Reload Needed</td>
<td>A request to reload the device has not been made. The device must be reloaded manually to complete the software upgrade.</td>
</tr>
<tr>
<td>Canceled</td>
<td>The software upgrade request was interrupted, or a previous software upgrade request was bypassed from the CLI.</td>
</tr>
<tr>
<td>Update Failed</td>
<td>The software upgrade could not be completed. Troubleshooting is required; see the device system message log.</td>
</tr>
</tbody>
</table>
Upgrading an SE, SR, or VOSM

Use this upgrade procedure for Service Routers and VOSMs. You can also use this upgrade procedure to upgrade Service Engines one at a time.

To upgrade your software on a single device, do the following:

---

**Step 1** Choose Devices > Devices. The Devices Table page is displayed.

**Step 2** Click the Edit icon of the device that you want to upgrade. The Devices home page is displayed.

**Step 3** Verify that the device is not already running the version that you plan to upgrade to, and that the current version has an upgrade path to the version that you plan to upgrade to.

**Step 4** Click Update Software. The Software Update page is displayed.

**Step 5** Choose the software file URL from the Software Files list by clicking the radio button next to the filename.

**Step 6** Click Submit, and then click OK to confirm your decision.

The Devices Table page is displayed again. You can monitor the progress of your upgrade from this page. Software upgrade status messages are displayed in the Software Version column. These intermediate messages are also written to the system log on the Service Engines. See Table 9-1 for a description of upgrade status messages.

---

Upgrading a Virtual Machine (VM)

The process used to upgrade a VM is similar to the process used to upgrade a real machine for a minor release. To upgrade a VM, enter the following command in EXEC configuration mode:

```
SE# copy http install <http-server-ip-addr> <dir-name> <filename>
```

However, if a major release includes changes to the Open Virtual Appliance (OVA) definition, you must remove the old VM and deploy a new VM using the OVA.

---

Rebooting Devices

You can reboot a device or device group. The VOSM performs a controlled shutdown of all devices and then restarts the operating system on each device.

To reboot an individual device, do the following:

---

**Step 1** Choose Devices > Devices.

**Step 2** Click the Edit icon next to the device name that you want to reboot. The Devices home page is displayed.

**Step 3** In the task bar, click the Reload icon. You are prompted to confirm your decision.

**Step 4** To begin rebooting the device, click OK.
To reboot an entire device group, do the following:

**Step 1** Choose Devices > Device Groups.
**Step 2** Click the Edit icon next to the name of the device group that you want to reboot. The Device Group page is displayed.
**Step 3** In the task bar, click the Reboot All Devices in Device Group icon. You are prompted to confirm your decision.
**Step 4** To begin rebooting each SE in the device group, click OK.

## Deleting a Device

You can delete a device if the device is experiencing problems that cannot be resolved, or when its network address or configuration has changed and you need to add the device back to the VDS-OS network using its new address and configuration information.

⚠️ **Caution**

If you delete the only SR in your VDS-OS network, you are removing the ability of your VDS-OS network to serve requests.

When you delete an SE from the VDS-OS network, you are removing that device and the content it contains from the routing scheme that the VDS-OS uses to serve requests. Although the VDS-OS routes requests around SEs that are busy, offline, or missing, removing an SE may affect the speed at which the VDS-OS network can serve requests.

**Note**

You cannot delete an SE if it is the only device assigned to a location that is designated as the root location for an origin service and there are other SEs associated with the origin service. You can delete the SE for an origin service if it is the only SE associated with that origin service. However, deleting the only SE in an origin service makes the origin service unable to deliver content. If you receive an error message referencing the SE for an origin service, add more SEs to that location before attempting to delete the SE again.

Removing the device from the VDS-OS network involves using the CLI to shut down VDS-OS network services and deregister the node. If you are removing the device because of hardware failure and it cannot be accessed through its CLI, you can remove the device by using the VOSM; however, the device continues to store its registration information until you deregister it by using the CLI.

Before a device can be removed from the VDS-OS network, the following conditions must be met:

- Device must have been activated in the VOSM.
- VOSM must be operating.
- Device must have the correct VOSM IP address or hostname configured.
- VOSM IP address or hostname must be that of the primary VOSM.
- Device must not be the Acquisition Node for any origin service.

Deleting a device from the VDS-OS network involves using the CLI to remove the registration information from the device itself and removing the registration record from the VOSM.
Deleting a Device

Note
Do not use the VOSM to delete a device while the device is still active and registered. The VOSM delete feature removes only the device’s registration record from the VOSM; it does not deregister the device. The device retains its registration information and continues to contact the VOSM; however, the VOSM no longer recognizes the device.

If for some reason the VOSM loses the registration record of a device, use the `cms deregister force` command on the device to remove all its registration information. Then use the `cms enable` command to reregister the device with the VOSM as though it were a new node in the VDS-OS network.

To remove and deregister a device, do the following:

**Step 1**
Open an SSH session to the device CLI.

**Step 2**
In global configuration mode, enter the `no cms enable` command.

```
SE# configure
SE(config)# no cms enable
```

Note
Issuing the `no cms enable` command does not disable acquisition and distribution services on the device; however, issuing the `cms deregister` command does. The `cms deregister` command disables the CMS, all acquisition and distribution services, and all routing communications to and from this device.

**Step 3**
In EXEC mode, enter the `cms deregister` command.

```
SE(config)# exit
SE# cms deregister
```

Note
The `cms deregister` command cleans up the database automatically. You do not need to use the `cms database delete` command.

If the deregistration fails, the best practice is to resolve any issues that caused the deregistration failure. For example, the Service Engine is the Acquisition Node of an origin service and cannot be deleted or deactivated. In this case, assign a different SE as the Acquisition Node in each origin service where this SE is assigned as the Acquisition Node and try the `cms deregister` command again.

**Step 4**
If for some reason the deregistration fails, you can force the deregistration by using the `cms deregister force` command.

```
SE# cms deregister force
```

Note
Take note of any messages stating that the deregistration failed and make sure to resolve them before reregistering the device with the same VOSM or registering the device to another VOSM. The `cms deregister force` command forces the deregistration to continue.

**Step 5**
To add the device back into the VDS-OS network, reregister the device with the VOSM by using the `cms enable` command in global configuration mode.

```
SE# configure
```
Deleting a Device

In case of a hardware failure, you might need to remove the device from the VDS-OS network routing scheme by using the VOSM.

Before a device can be removed from the VDS-OS network through the VOSM, the following conditions must be met:

- Device must have been activated in the VOSM.
- VOSM must be running.
- Device must have the correct VOSM IP address or hostname configured.
- VOSM IP address or hostname must point to the primary VOSM.
- Device must not be the Acquisition Node for any origin service.

To delete a device using the VOSM, do the following:

**Step 1** Choose Devices > Devices. The Devices Table page is displayed. The online status of the device is listed in the Status column.

**Step 2** Click the Edit icon next to the device name you want to delete. The Devices home page is displayed.

**Step 3** In the task bar, click the Delete Device icon. You are prompted to confirm your decision.

**Step 4** To execute your request, click OK. The device is removed from the VOSM.

**Step 5** If possible, access the device CLI to deregister the device.

**Step 6** In the CLI, enter the `cms deregister force` command.

**Note** You must use the `cms deregister force` command after deleting a device in the VOSM. This is because once the device has been deleted, the VOSM no longer has a record of the device.

**Step 7** To add the device back in to the VDS-OS network, reregister the device with the VOSM by using the `cms enable` command in global configuration mode.

Deleting a Warm Standby VOSM

You can delete a warm standby VOSM from the VDS-OS network at any point after you have registered the device and before the device has come online as the primary VOSM. Once the device has been called into use as the primary VOSM, however, you cannot delete it by using the VOSM.

Delete a warm standby VOSM when the device is experiencing problems that cannot be resolved, or when its network address or configuration has changed and you need to add the device back to the VDS-OS network by using its new address and configuration information.

To delete a warm standby VOSM, do the following:

**Step 1** Log in directly to the VOSM CLI, and enter the `cms deregister` command.

If for some reason the deregistration fails, you can force the deregistration by using the `cms deregister force` command.
Replacing a Device

The procedure to replace a device in the VDS-OS is different depending on the type of the device being replaced. This section covers the following procedures:

- Replacing a VOSM
- Replacing an SE, SR, or VDS-OS
- Replacing a VM across OVA Releases

Replacing a VOSM

To replace a VOSM in a VDS-OS you must first add the new VOSM into the network as a standby VOSM. For procedural information, see the “Configuring Primary and Standby VOSMs” section on page 4-11.

The primary and standby VOSMs must be running the same version of software. You must first add the new VOSM with the same version as the existing VOSM. Once the standby VOSM has been added, you must wait at least two polling intervals (10 minutes) for the databases to synchronize before you can begin the upgrade procedure.

After you have activated the standby VOSM using the primary VOSM web interface and the device shows as online in the Devices Table page, wait at least two polling intervals (10 minutes) before changing roles to ensure that the standby VOSM has a record of the most recent configuration changes.

To promote the standby VOSM to primary, first stop the primary VOSM using the `VOSM role standby` command. For procedural information, see the “Changing a Standby to a Primary VOSM” section on page 4-12.

After the primary VOSM has been stopped, and the standby VOSM has taken the role of primary, wait at least two polling intervals (10 minutes) before logging in to the new primary VOSM. The new primary VOSM is accessible by entering the IP address of the VOSM with port 8443 in a web browser. For example, if the IP address of your VOSM is 192.168.0.236, enter `https://192.168.0.236:8443`.

It is now safe to deactivate the old primary VOSM in the VOSM web interface and remove it from the VDS-OS network.

---

Step 2  From the VOSM GUI, choose Devices > Devices.
The browser refreshes, listing the VOSMs on your VDS-OS network. The warm standby VOSM is identified as Standby.

Step 3  Click the Edit icon next to the name of the warm standby VOSM. The Devices home page is displayed.

Step 4  From the left-pane menu, choose Device Activation. The Activation page is displayed.

Step 5  In the task bar, click the Delete icon. You are prompted to confirm your decision.

Step 6  To execute your request, click OK.
Replacing a Device

Note Do not try to take a back up of the old VOSM database and restore it on the new VOSM. This can cause problems.

Replacing an SE, SR, or VDS-OS

Note If you replace an Acquisition Node with an SE that was not previously assigned to the origin service, all content is reacquired and old content is deleted.

To prevent the reacquisition of content when replacing an Acquisition Node, make one of the receiver SEs in the same origin service the replacement Acquisition Node. Add the new SE as a receiver SE, wait until replication is complete for the newly added SE, and then designate it as the Acquisition Node. When you replace an Acquisition Node in this manner, the SEs in the origin service synchronize with the new Acquisition Node through the metadata poll. Content is not redistributed to the other SEs in the origin service unless the content has changed since the last metadata poll.

To replace an SE, SR, or VDS-OS, do the following:

Step 1 Open an SSH session to the device being replaced.
Step 2 In global configuration mode, enter the no cms enable command to disable CMS on the device that needs to be replaced.

```
SE# configure
SE(config)# no cms enable
```
Step 3 From the VOSM, choose Devices > Devices > Device Activation. The Device Activation page is displayed.
Step 4 Uncheck the Activate check box and click Submit. The page refreshes and displays a Replaceable check box.
Step 5 Check the Replaceable check box and click Submit.
Step 6 Choose System > Configuration > System Properties. The System Properties page is displayed.
Step 7 Click the edit icon next to the System.deivce.recovery.key property. The Modify Config Property page is displayed.
Step 8 In the Value field, enter a key and click Submit. The default value is default.
Step 9 Follow the instructions for configuring a device using the setup utility. For detailed instructions, see the Cisco Content Delivery Engine Hardware Installation Guide that applies to your device.

Note The replacement device must be the same hardware model as that of the device being replaced.

When prompted by the setup utility, configure the basic network settings.

a. When prompted for the hostname of the new device, use the same hostname of the device being replaced. For example, if the old device has a hostname of “SE1,” the new device must have a hostname of “SE1.”

b. When prompted for the IP address of the VOSM, enter the IP address of the VOSM.

Step 10 Open an SSH session to the new device.
Step 11  In EXEC mode, enter the `cms recover identity` command with the key parameter you set in Step 8.

```
SE# cms recover identity <key>
```

On successful registration to the VOSM, a message similar to the following is displayed:

```
DT-7326-4#cms recover identity sr
Registering this node as Service Router...
Sending identity recovery request with key sr
Node successfully registered with id CrConfig_291
Registration complete.
```

Step 12  Register the device with the VOSM by using the `cms enable` command in global configuration mode.

```
SE# configure
SE(config)# cms enable
```

Step 13  From the VOSM, choose Devices > Devices > Device Activation. The Device Activation page is displayed.

Step 14  Check the Activate check box and click Submit.

After a few minutes, approximately two polling intervals, the device status shows online and all configurations (origin service assignments, programs, and so on) are the same as those on the device that was replaced.

Step 15  Once the new device is up and running, as noted by the online status, the old device can be removed from the VDS-OS network.

---

**Replacing a VM across OVA Releases**

The OVA file contains the hardware definition of the VM. Under rare circumstances, the hardware definition might change from one software release to another. For example, the pre-beta OVA might define two hard disks where the beta OVA defines four hard drives.

For new releases, software is provided in both OVA and image (ruby.bin) formats.

- To deploy a new VM, use the OVA.
- To upgrade an existing VM, use the image.

However, if the OVA’s hardware definition has changed and you want to move to the newer definition, you must remove the old VM and deploy a new VM using the OVA.

**Backup and Recovery Procedures**

This section provides VOSM database backup and VDS-OS software recovery procedures. This section contains the following sections:

- Performing Backup and Restore on the VOSM Database, page 9-15
- Using the VDS-OS Software Recovery CD-ROM, page 9-16
- Recovering the System Software, page 9-17
- Recovering a Lost Administrator Password, page 9-20
- Recovering from Missing Disk-Based Software, page 9-21
- Recovering VDS-OS Network Device Registration Information, page 9-24
Performing Backup and Restore on the VOSM Database

The VOSM stores VDS-OS network-wide device configuration information in its Centralized Management System (CMS) database. You can manually back up the CMS embedded database contents for greater system reliability.

To back up the CMS database for the VOSM, use the `cms database backup` EXEC command.

**Note**
The naming convention for backup files includes the timestamp.

To back up and restore the CMS database on the VOSM, do the following:

**Step 1**  Back up the CMS database to a file.

```
SE# cms database backup
creating backup file backup-db-11-06-2007-13-10.dump
backup file local1/backup-db-11-06-2007-13-10.dump is ready.
Please use 'copy' commands to move the backup file to a remote host.
```

**Step 2**  Save the file to a remote server by using the `copy disk ftp` command. This command copies the file from the local disk to a remote FTP server, as shown in the following example:

```
SE# cd /local1
SE# copy disk ftp 10.86.32.82 /incoming vos-db-9-22-2002-17-36.dump
vos-db-9-22-2002-17-36.dump

Enter username for remote ftp server: ftp
Enter password for remote ftp server: ********
Initiating FTP upload...
Sending:USER ftp
10.86.32.82 FTP server (Version wu-3.0.1-18) ready.
Password required for ftp.
Sending:PASS ********
User ftp logged in.
Sending:TYPE I
Type set to I.
Sending: PASV
Entering Passive Mode (10,86,32,82,203,135)
Sending: CWD /incoming
CWD command successful.
Sending: PASV
Entering Passive Mode (10,86,32,82,112,221)
Sending: CWD /incoming
CWD command successful.
Sending: STOR vos-db-9-22-2002-17-36.dump
Opening BINARY mode data connection for vos-db-9-22-2002-17-36.dump.
Transfer complete.
Sent 18155 bytes
```

**Step 3**  Delete the existing CMS database.

```
SE# cms database delete
```

**Step 4**  Restore the CMS database contents from the backup file.

```
SE# cms database restore vos-db-9-22-2002-17-36
```

**Step 5**  Enable CMS.

```
SE# cms enable
```
Using the VDS-OS Software Recovery CD-ROM

A software recovery CD-ROM image (.iso file) is available for each software release. The recovery CD-ROM can be used to recover system software that must be completely reimaged. The recovery CD-ROM image contains the system software for a single software release and a single application software.

This section presents instructions for creating and using the software recovery CD-ROM to reinstall your system software if for some reason the software that is installed has failed.

⚠️ Caution

If you upgraded your software with a later release than the software recovery CD-ROM image file you downloaded, using the CD-ROM software recovery images may downgrade your system.

System Software Components

VDS-OS software consists of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All these components must be correctly installed for the VDS-OS software to work properly.

The software is contained in two types of software images provided by Cisco:

- A .bin image containing disk and flash memory components
  
  An installation containing only the VDS-OS flash memory-based software, without the corresponding disk-based software, boots and operates in a limited mode, allowing for further disk configuration before completing a full installation.

- A .sysimg image containing a flash memory component only
  
  The .sysimg component is provided for recovery purposes, and allows for repair of flash memory only, without modifying the disk contents.

Getting the VDS-OS Software Recovery File from Cisco.com

To get a software file from Cisco.com, do the following:

**Step 1**
Launch your web browser and enter the following URL:

http://www.cisco.com/cisco/software/navigator.html

The Select a Product page is displayed if you have recently logged in; otherwise, the Log In page is displayed.

**Step 2**
Log in to Cisco.com using your designated username and password.

**Step 3**
Choose Products > Video > Videoscope > Cisco Videoscope Distribution Suite > Cisco Videoscope Distribution Suite Origin Server. The Downloads page is displayed.

**Step 4**
Click the link for the software recovery file you want to download.

- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click Accept.
If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.

The Download page is displayed with the information about the software image file and a Download link.

Step 5 Click **Download**. The Cisco End User Software License Agreement is displayed.

Step 6 Read the agreement and click **Agree**. The File Download dialog box is displayed.

Step 7 Click **Save**. The Save As dialog box is displayed.

Step 8 Navigate to the location where you want to save the file and click **Save**. The file downloads.

Step 9 Burn the software recovery image file onto a CD-ROM.

### Installing the Software Using the Recovery CD-ROM

To install the system software by using the recovery CD-ROM, perform the following steps:

---

**Step 1** Plug a USB CD-ROM drive into a USB port on the device.

**Step 2** Insert the recovery software CD-ROM into the USB CD-ROM drive, and boot the device.

**Step 3** When the installer menu appears, choose **2 Install all Software**.

**Step 4** Wait for the process to complete.

**Step 5** Before you reboot the device, remove the USB CD-ROM drive from the USB port so that the device boots from flash memory.

**Step 6** Reboot the device.

### Recovering the System Software

The Service Engine, Service Router, and VOSM have a resident rescue system image that is invoked should the image in flash memory be corrupted. A corrupted system image can result from a power failure that occurs while a system image is being written to flash memory. The rescue image can download a system image to the main memory of the device and write it to flash memory.

*Note* The .sysimg file is located under the images folder on the Recovery CD-ROM. If you have upgraded the VDS-OS software, download the corresponding rescue CD iso image, copy to a CD and use the rescue iso image.

To install a new system image using the rescue image, do the following:

---

**Step 1** Download the system image file (*.sysimg) to a host that is running an FTP server.

**Step 2** Establish a console connection to the device and open a terminal session.

**Step 3** Reboot the device by toggling the power switch.
The rescue image dialog appears. The following example demonstrates how to interact with the rescue
dialog and use a port channel for the network connection (user input is denoted by entries in bold
typeface).

This is the rescue image. The purpose of this software is to let
you download and install a new system image onto your system's
boot flash device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.

To download an image, this software will request the following
information from you:
- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- FTP server IP address
- username/password on FTP server
- path to system image on server

System Recovery Menu:
1. Configure Network
2. Download and install system image
3. Exit (and reboot)
Choice [1]: 1

Network Configuration Menu:
1. Configure ethernet interface
2. Configure portchannel interface
3. Exit to main menu
Choice [1]: 2

Please enter an interface from the following list:
0. GigabitEthernet 1/0
1. GigabitEthernet 2/0
2. GigabitEthernet 3/0
3. GigabitEthernet 4/0
4. GigabitEthernet 5/0
5. GigabitEthernet 6/0
6. GigabitEthernet 7/0
7. GigabitEthernet 8/0
8. GigabitEthernet 9/0
9. GigabitEthernet 10/0
10. Done
0
Please select an interface from the list below:
0. GigabitEthernet 1/0 [Use]
1. GigabitEthernet 2/0
2. GigabitEthernet 3/0
3. GigabitEthernet 4/0
4. GigabitEthernet 5/0
5. GigabitEthernet 6/0
6. GigabitEthernet 7/0
7. GigabitEthernet 8/0
8. GigabitEthernet 9/0
9. GigabitEthernet 10/0
10. Done
Choice [1]: 1

Please select an interface from the list below:
0. GigabitEthernet 1/0 [Use]
1. GigabitEthernet 2/0 [Use]
2. GigabitEthernet 3/0
3. GigabitEthernet 4/0
4. GigabitEthernet 5/0
5. GigabitEthernet 6/0
6. GigabitEthernet 7/0
7. GigabitEthernet 8/0
8. GigabitEthernet 9/0
9. GigabitEthernet 10/0
10. Done

Choice [2]: 10

Please enter the local IP address to use for this interface:
[Enter IP Address]: 172.16.22.22

Please enter the netmask for this interface:
[Enter Netmask]: 255.255.255.224

Please enter the IP address for the default gateway:
[Enter Gateway IP Address]: 172.16.22.1

Network Configuration Menu:
1. Configure ethernet interface
2. Configure portchannel interface (done)
3. Exit to main menu

Choice [3]: 3

System Recovery Menu:
1. Configure Network (done)
2. Download and install system image
3. Exit (and reboot)

Choice [2]: 2

Please enter the IP address for the FTP server where you wish to obtain the new system image:
[Enter Server IP Address]: 172.16.10.10

Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: anonymous

Please enter the password for username 'anonymous' on FTP server (an email address): 

Please enter the directory containing the system image file on the FTP server:
[Enter Directory on server (e.g. /)]: /

Please enter the file name of the system image file on the FTP server:
[Enter Filename on server]: VDS-OS10.sysimg

Here is the configuration you have entered:
Current config:
IP Address: 172.16.22.22
Netmask: 255.255.255.224
Gateway Address: 172.16.22.1
Server Address: 172.16.10.10
Username: anonymous
Password:
Image directory: /
Image filename: VDS-OS-24.sysimg

Attempting download...
Downloaded 34234368 byte image file
A new system image has been downloaded.
You should write it to flash at this time.

Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no'))]: yes

Ok, writing new image to flash
Chapter 9  Maintaining the VDS-OS

Backup and Recovery Procedures

Step 4  Log in to the device as username admin. Verify that you are running the correct version by entering the show version command.

Username: admin
Password:

Console> enable
Console# show version
Content Videoscape Distribution Suite Origin Server Software (VDS-OS)
Copyright (c) 2013 by Cisco Systems, Inc.
Content Videoscape Distribution Suite Origin Server Software Release 2.1.1 (build b460 June 5 2013)
Version: se507-2.4.0

System was restarted on Thu June 15 16:03:51 2013.
The system has been up for 4 weeks, 1 day, 6 hours, 7 minutes, 23 seconds.

Recovering a Lost Administrator Password

If an administrator password is forgotten, lost, or misconfigured, you need to reset the password on the device.

Note  There is no way to restore a lost administrator password. You must reset the password to a new one, as described in this procedure.

To reset the password, do the following:

Step 1  Establish a console connection to the device and open a terminal session.

Step 2  Reboot the device.

While the device is rebooting, watch for the following prompt and press Enter when you see it:

Cisco VDS-OS boot:hit RETURN to set boot flags:0009

Step 3  When prompted to enter bootflags, enter the 0x800 value.

Available boot flags (enter the sum of the desired flags):
0x0000 - exit this menu and continue booting normally
0x2000 - ignore Carrier Detect on console
0x4000 - bypass nvram config
0x8000 - disable login security
[SE boot - enter bootflags]: 0x8000
You have entered boot flags = 0x8000
Boot with these flags? [yes]: yes

[Display output omitted]
Setting the configuration flags to 0x8000 lets you into the system, bypassing all security. Setting the configuration flags field to 0x4000 lets you bypass the NVRAM configuration.

**Step 4**  When the device completes the boot sequence, you are prompted to enter the username to access the CLI. Enter the default administrator username (**admin**).

Cisco Service Engine Console

Username: admin

**Step 5**  When you see the CLI prompt, set the password for the user using the `username password` command in global configuration mode.

```
ServiceEngine(config)# configure
ServiceEngine(config)# username admin password 0 password
```

You can specify that the password be either clear text or encrypted. Zero (0) means the password is displayed as a plain word; one (1) means the password is encrypted. The password strength must be a combination of alphabetic character, at least one number, at least one special character, and at least one uppercase character.

**Note**  Do not set the user ID (uid).

**Step 6**  Save the configuration change by using the `write memory` command in EXEC mode.

```
ServiceEngine(config)# exit
ServiceEngine# write memory
```

**Step 7**  Optionally, reboot your device by using the `reload` command.

```
ServiceEngine# reload
```

Rebooting is optional; however, you might want to reboot to ensure that the boot flags are reset, and to ensure that subsequent console administrator logins do not bypass the password check.

**Note**  In VDS-OS software, the bootflags are reset to 0x0 on every reboot.

---

**Recovering from Missing Disk-Based Software**

This section describes the recovery procedures to use if for some reason the software installation on both system disks is corrupt or missing.

There are two types of disk volumes in the VDS-OS: system disk volumes (which contain all of the system volumes plus the sysfs volume) and cdnfs disk volumes. A disk is either allocated as a system disk or a cdnfs disk (on some hardware models, a system disk might contain a cdnfs volume). The system volumes, contain data and applications that are critical to the system’s basic functionality.
The system volumes are stored in a two-disk RAID-1 (mirrored) array. RAID-1 duplicates data between each of the disks in the array. The two-disk scheme allows for either of the drives in the system volumes array to fail without sustaining data loss or incurring system errors.

The status of the volumes can be seen through the `show disk raid-state` command, and can be in any of the following states:

- **Normal**—Both drives are attached, and data is mirrored between them.
- **Syncing**—Data is being copied between the drives to restore the volumes to a normal state. This typically happens when a new drive is added to repair degraded volumes.
- **Degraded**—One of the disks has failed. It is highly recommended that a new disk is added to repair the volumes.
- **Bad**—Both disks have failed. The system has likely lost all but basic functionality.

The VDS-OS state of “missing disk-based software” is most likely to occur if you replaced both system disks in your Service Engine, Service Router, or VOSM. By design, the software installation on the system disks cannot be corrupted by a system failure or a power failure. If both system disks fail or are missing, the software continues to run. However, it runs in a basic functionality mode in which HTTP proxy and related HTTP features still work, but most other features fail.

The compact flash functionality is merged on to the system disk in some hardware models (non-Content Delivery Engine models [non-CDE]). If both system disks fail or are missing on a non-CDE platform, the non-CDE device can not function and needs to have the VDS-OS software reinstalled by using the Recovery CD-ROM. For more information, see the “Using the VDS-OS Software Recovery CD-ROM” section on page 9-16.

---

**Caution**

This procedure should only be used as a last-resort method to recover the system software on a unit. Typically, the system automatically repairs itself across a reboot if any new disks are detected. If the volumes are degraded and a new disk is present at reboot, the new disk is added to the existing array (sync starts). If the volumes are “bad” and a new disk is present at reboot, the initial system volume is built on the disk.

To recover from this condition, do the following:

---

**Step 1**

Remove the Service Engine record from the VOSM.

a. Choose **Devices > Devices**.

b. Click the **Edit** icon next to the name of the Service Engine that you want to delete. The Devices home page is displayed.

c. Click the **Delete** icon. You are prompted to confirm your decision.

d. Click **OK** to execute your request. The Service Engine is removed from the VOSM.

**Note**

The Service Engine registration record needs to be deleted from the VOSM for the Service Engine to complete reregistration after it comes back online. The VOSM does not register a device if the device already appears in the record as registered.

---

**Step 2**

Power down the device and replace the failed or missing system disks with new, blank disks.

**Step 3**

After the new disks are installed, power up the device.
**Step 4** From a console or through an SSH session, check the startup messages that appear on your screen.

If there is a problem with the system disk or the disk-based software, a message similar to the following appears:

```
ruby_disk:Your first disk is not in standard configuration.
ruby_disk:Run 'disk recover-system-volumes' from the CLI
```

**Step 5** Log in as admin.

Cisco Service Engine Console

Username: admin
Password:
System Initialization Finished.
SE-507 con now available
Press RETURN to get started!

**Step 6** After logging in to a console or SSH session, enter the `copy ftp install` or `copy http install` EXEC command to download and install a new system image.

```
ServiceEngine# copy ftp install ftp-server remotefiledir remotefilename
```

For example:

```
SE# copy ftp install vista /VDS-OS/upgrades VDS-OS-2.0.0.2-K9.bin
Enter username for remote ftp server: biff
Enter password for remote ftp server:
Initiating FTP download...
printing one # per 1MB downloaded
Reclaiming unused safe state sectors...
############################################################################
###########
############################################################################
Installing phase3 bootloader...
Installing system image to flash: done
The new software will run after you reload.
#
ServiceEngine# show flash
VDS-OS software version (disk-based code): VDS-OS-2.0.1-b130
```

**Step 7** Reboot the software with the new disk and new system image by entering the `reload` EXEC command.

```
SE# reload
```

**Step 8** Register the device with the VOSM by using the `cms enable` command in global configuration mode.
Recovering VDS-OS Network Device Registration Information

Device registration information is stored both on the device itself and on the VOSM. If a device loses its registration identity or needs to be replaced because of hardware failure, the VDS-OS network administrator can issue a CLI command to recover the lost information or, in the case of adding a new device, assume the identity of the failed device.

To recover lost registration information, or to replace a failed node with a new one having the same registration information, do the following:

**Step 1** Mark the failed device as “Inactive” and “Replaceable” in the VOSM.

a. Choose Devices > Devices.

b. Click the Edit icon next to the name of the Service Engine you want to deactivate. The Devices home page is displayed.

c. From the left-panel menu, choose Device Activation.

d. Uncheck the Activate check box. The page refreshes, displaying a check box for marking the device as replaceable.

e. Check the Replaceable check box and click Submit.

Note This check box only displays when the device is inactive.

**Step 2** Configure a system device recovery key.

a. Choose System > Configuration.

b. Click the Edit icon next to the System.device.recovery.key property. The Modifying Config Property page is displayed.

c. Enter a password in the Value field and click Submit. The default password is default.

**Step 3** Configure the basic network settings for the new device.

**Step 4** Open an SSH session to the device CLI and enter the cms recover identity keyword EXEC command, where keyword is the device recovery key that you configured in the VOSM.

When the VOSM receives the recovery request from the Service Engine, it searches its database for the Service Engine record that meets the following criteria:

- Record is inactive and replaceable.
- Record has the same hostname as given in the recovery request.
- Device is the same hardware model as the device in the existing record.
- File system allocations for the device are the same as or greater than the device in the existing record.

SE# configure
SE(config)# cms enable
If the recovery request matches the Service Engine record, then the VOSM updates the existing record and sends the requesting Service Engine a registration response. The replaceable state is cleared so that no other device can assume the same identity. When the Service Engine receives its recovered registration information, it writes it to file, initializes its database tables, and starts.

**Step 5** Return to the VOSM and activate the device.

a. Choose **Devices > Devices**.

b. Click the **Edit** icon next to the name of the Service Engine you want to activate. The Devices home page is displayed.

c. From the left-panel menu, choose **Device Activation**. The Service Engine status should be Online.

d. Check the **Activate** check box and click **Submit**.

**Note**

If you are replacing an old device with a different hardware model, check the following hardware-related settings and adjust them according to your needs, after the new device is online in VOSM GUI:

- IP Access List settings associated with network interfaces
- Disk quota settings of origin services
- Service Monitor Disk Failure Percent Settings

---

**Troubleshooting**

- Check the Ingest Log, page 9-25
- Check the DASH and ODE Statistics on the Service Engine, page 9-25
- Enable Debug Trace for the Web-Engine, page 9-26
- Check the Web-Engine Statistics, page 9-26
- Troubleshoot 404, 500, and 504 Errors, page 9-27
  - Check the Translog, page 9-27
  - Check the Web-Engine Error Logs, page 9-27

**Check the Ingest Log**

```
/local/local1/logs/webengine_ingestlog_clf
debugshell# tail -f working.log
#Software: (VDS-OS 1.1.1 b5)
Time URL FailOverSvrList ServerIP BytesRead BytesToRead AssetSize %DownloadComplete DownloadTime(Seconds) ReadCall1Back Status-Returned MIME-Type Revalidation-Request CDSDomain ConnectionInfo(LocalPort|Protocol|ConnectTime|Retry|Reuse) IngestStatus RedirectedUr
```

**Check the DASH and ODE Statistics on the Service Engine**

```
X7-UCS4-Blad4# sho stat web-engine detail
```
X7-UCS4-Blad4#sho stat web-engine abr dash-media-app
X7-UCS4-Blad4#sho stat web-engine abr hls-media-app
X7-UCS4-Blad4#sho stat web-engine abr hss-media-app

Note
All sessions should be zero after playback in detail statistics.

X7-UCS4-Blad4#sho stat web-engine abr dash-media-app detail
Media Detail Statistics
-----------------------
Active Assets               :                    0
Active Manifest Files       :                    0
Active Media Files          :                    0
Active Server Manifest Files:                    0
Active Representation Index Files:                    0
Request Sent To Default App:                    0
X7-UCS4-Blad4#

Enable Debug Trace for the Web-Engine

X7-UCS4-Blad4#debu web-engine trace
Errorlog path:
local/local1/errorlog
debugshell# tail -f webengine_log.current

Check the Web-Engine Statistics

X7-UCS4-BLADE4#sho stat web-engine error summary
Error Summary
-----------------------
Client Error Summary
-----------------------
Client Errors :               8
Bad Request (400) :          0
Forbidden (403) :            0
Not Found (404) :           8
Method Not Allowed (405) :   0
Not Acceptable (406) :      0
Precondition Failed (412) : 0
Range Not Satisfiable (416): 0
Unknown Client Error (Other 4xx) : 0
Server Error Summary
-----------------------
Server Errors :            0
Internal Server Error (500): 0
Not Implemented (501) :    0
Bad Gateway (502) :        0
Service Unavailable (503) : 0
Gateway Timeout (504) :    0
Version Not Supported (505) : 0
Unknown Server Error (Other 5xx) : 0
Troubleshoot 404, 500, and 504 Errors

Check the Translog

If client playback failed with a 404, 500, or 504 error on the Service Engine, check the translog.

debugshell# cd webengine_extsquid/
debugshell# tail -f working.log

#Software: (VDS-OS 1.1.1 b5)
Current-Time Time-to-Serve Client-IP Request-Desc/Status-Returned Bytes-Xferred Method URL MIME-Type

404 Translog

04/09/2013 09:19:47.245(Local)(27942)ERRO:DashProviderCtxt.cpp:263->
 DashProviderCtxt OnHTTPHeaders return Error :404

500 or 504 Translog

debugshell# more webengine_log.* | grep "Error :500"
03/27/2013 21:09:00.181(Local)(11028)ERRO:DashProviderCtxt.cpp:263->
 DashProviderCtxt OnHTTPHeaders return Error :500
03/27/2013 21:29:03.572(Local)(11028)ERRO:DashProviderCtxt.cpp:263->
 DashProviderCtxt OnHTTPHeaders return Error :500

VDS-OS (ODE) to Client Translog

#Software: (VDS-OS 1.2.0 b81)
Current-Time Time-to-Serve Client-IP Request-Desc/Status-Returned Bytes-Xferred Method URL MIME-Type
[09/Apr/2013:09:18:44.850+0000] 42652 64.103.183.22 TCP_MISS/404 217 GET
http://vos.ipndvr1.com/115/ndvr/ip/34.0.116.246/hls/index.m3u8 application/x-mpegURL

Check the Web-Engine Error Logs

If a 404, 500, or 504 error occurred on the Service Engine, or if the statistics indicate that any active sessions are hanging, check the corresponding Web-Engine error logs.
Creating Asset Resolver Files

A virtual origin service uses an Asset Resolver XML file to specify the asset resolvers for all of the SEs in the service. The Asset Resolver file maps incoming requests to stored assets, enabling you to reduce the number of stored copies of the same asset segment for ABR content. The Asset Resolver file resolves incoming fragments, manifest, and other types of requests to the publish resource that can deliver the request.

The Asset Resolver file allows you to specify a set of rules, each clearly identified by an action and a pattern, for all of the SEs in a virtual origin service. Subsequently, for every incoming request, if a pattern for a rule matches the given request, the corresponding action for that rule is taken.

**Note**
The Asset Resolver performs CPU-intensive regular expression (regex) operations. Therefore, the number of rules and their order in the Asset Resolver file is critical. For better performance, we recommend that you use as few rules as possible, and make sure that the DASH rule is the first rule in the file.

You can create Asset Resolver files using any ASCII text-editing tool. The Asset Resolver files are registered to the VDS-OS by using the Asset Resolver File Registration page. For more information see the “Asset Resolver File Registration” section on page 7-12. When the file has been registered, you can assign it to a virtual origin service through the Asset Resolver Settings page. For more information, see the “Asset Resolver Settings” section on page 6-6.

- Asset Resolver File Structure and Syntax, page A-2
  - Pattern Matching, page A-5
- Asset Resolver File Examples, page A-6
  - Default Asset Resolver File, page A-6
  - Asset Resolver Rule for HLS Live Service, page A-8
  - Asset Resolver Rules for CF VOD—Unique ContentID in the URL, page A-8
  - Asset Resolver Rules for CF VOD—ContentID as the Manifest File Name, page A-9
  - Asset Resolver Rule for Content Protection, page A-11
  - Setting the HTTP Response Cache-Control Header, page A-11
- Troubleshooting the Asset Resolver, page A-12
Asset Resolver File Structure and Syntax

The XML Schema file describes and dictates the content of the XML file. The VOSAssetResolver.xsd file contains the XML schema. To view or download a copy of the VOSAssetResolver.xsd file, see the “Viewing or Downloading XML Schema Files” section on page 7-15.

Table A-1 describes the Asset Resolver file elements.

Table A-1  Asset Resolver File Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Subelements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssetResolverRules</td>
<td>Revision</td>
<td>Optional. Revision number to specify the version of this file.</td>
<td></td>
</tr>
<tr>
<td>CustomerName</td>
<td></td>
<td>Optional. Customer name associated with this file.</td>
<td></td>
</tr>
<tr>
<td>ApplyAllTier</td>
<td></td>
<td>Optional.</td>
<td></td>
</tr>
<tr>
<td>Rule_Patterns</td>
<td></td>
<td>Patterns to match for a specified action. There can be only one Rule_Patterns element for an Asset Resolver file.</td>
<td></td>
</tr>
<tr>
<td>Rule_Actions</td>
<td></td>
<td>Action to take when a pattern is matched. There can be only one Rule_Actions element for an Asset Resolver file.</td>
<td></td>
</tr>
<tr>
<td>ApplyAllTier</td>
<td></td>
<td>Valid values for the ApplyAllTier element are yes or no.</td>
<td></td>
</tr>
<tr>
<td>Rule_Patterns</td>
<td>PatternListGrp</td>
<td></td>
<td>Marks the beginning and ending of all the defined patterns in this file.</td>
</tr>
<tr>
<td>PatternListGrp</td>
<td></td>
<td>PatternListGrp id attribute is used to identify the pattern list group and can be up to 128 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td></td>
<td>Domain element is used to match the domain name in the URL or the host header against a regular expression.</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix A  Creating Asset Resolver Files

#### Asset Resolver File Structure and Syntax

<table>
<thead>
<tr>
<th>Element</th>
<th>Subelements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcIp</td>
<td></td>
<td></td>
<td>Matches the source IP address of the request. The SrcIP pattern requires the IP address be specified in the classless inter-domain routing (CIDR) format. The Asset Resolver XML file validation fails if the IP address is not in CIDR format.</td>
</tr>
<tr>
<td>UrlRegex</td>
<td></td>
<td></td>
<td>Matches the URL against a regular expression. The match is case sensitive. The following example covers both uppercase and lowercase expressions of MP4 files: http://(.<em>.)vosis.com/(.</em>.)[mM][pP]4(.*&lt;UrlRegex&gt;</td>
</tr>
<tr>
<td>Rule.Actions</td>
<td>Rule_AssetResolve</td>
<td></td>
<td>Marks the beginning and ending of all the defined actions in this file.</td>
</tr>
<tr>
<td>Rule_AssetResolve</td>
<td>SetTransformResource</td>
<td>nametag</td>
<td>nametag (optional) is a name for the Asset Resolve rule. matchGroup (required) value is the list of PatternListGrp id attributes. protocol (required) value must be http.</td>
</tr>
<tr>
<td>SetTransformResource</td>
<td></td>
<td>matchRegex</td>
<td>matchRegex (required) value is the regular expression the request URL must match to be transformed.</td>
</tr>
<tr>
<td>SourceInfo</td>
<td></td>
<td>matchRegex</td>
<td>SourceInfo PublishInfo DASHAdaptiveTSSource</td>
</tr>
<tr>
<td>DASHAdaptiveTSSource</td>
<td></td>
<td>mpdUrl</td>
<td>mpdUrl (required) is the DASH MPD file used as the source from which to create the transformed asset.</td>
</tr>
<tr>
<td>PublishInfo</td>
<td></td>
<td></td>
<td>PublishInfo HLSPublishInfo HSSPublishInfo</td>
</tr>
<tr>
<td>HLSPublishInfo</td>
<td></td>
<td>mediaManifestUrl</td>
<td>mediaManifestUrl (required) is the corresponding Manifest file for the matching URL (for HLS, the Variant Manifest file) mediaDescriptionUrl (optional) value is assetUrl (required) uniquely identifies the asset mediaDataSourceUrl (optional) value is indexDataSourceUrl (optional) value is</td>
</tr>
<tr>
<td>HSS PublishInfo</td>
<td></td>
<td>mediaFileUrl</td>
<td>mediaFileUrl (optional) value is mediaDataSourceUrl (optional) value is indexDataSourceUrl (optional) value is</td>
</tr>
<tr>
<td>(Both have the following subelements and attributes) ContentProtectionProfile Name MatchSubResource</td>
<td></td>
<td>mediaDescriptionUrl assetUrl indexDataSourceUrl</td>
<td>mediaDescriptionUrl (optional) value is assetUrl (required) uniquely identifies the asset mediaDataSourceUrl (optional) value is indexDataSourceUrl (optional) value is</td>
</tr>
</tbody>
</table>

### Table A-1  Asset Resolver File Elements (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Subelements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Table A-1  Asset Resolver File Elements (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Subelements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Cisco Media Origination System Release 2.0.0 Installation and Configuration Guide

OL-30508-01
### Table A-1  Asset Resolver File Elements (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Subelements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeliveryHeader</td>
<td>SetGenericHeader</td>
<td>name (required) value is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SetDynamicHeader</td>
<td>value (required) value is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SetETagHeader</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SetCachingHeader</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SetGenericHeader</td>
<td></td>
<td>name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>value (required) value is</td>
<td></td>
</tr>
<tr>
<td>SetDynamicHeader</td>
<td></td>
<td>regsub (required) value is</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>generatedName (required)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>generatedValue (required)</td>
<td></td>
</tr>
<tr>
<td>SetETagHeader</td>
<td></td>
<td>inputParams (required)</td>
<td></td>
</tr>
<tr>
<td>SetCachingHeader</td>
<td>Expires</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cache-Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expires</td>
<td></td>
<td>RelativeTime (required)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AbsoluteTime (required)</td>
<td></td>
</tr>
<tr>
<td>Cache-Control</td>
<td></td>
<td>No-Cache</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max-Age</td>
<td></td>
</tr>
<tr>
<td>SetCaptureResource</td>
<td>matchRegex</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>channelId</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>profileId</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>captureId</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mediaType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SetPublishResource</td>
<td>PublishInfo</td>
<td>matchRegex (required)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>value is the regular</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>expression the request URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>must match for the content</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>to be captured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>channelId (required) value</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>profileId (optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>captureId (optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>mediaType (optional)</td>
<td></td>
</tr>
<tr>
<td>NetworkDVR</td>
<td>AssetDescriptionURL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RecorderDiscoveryInfo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AssetDescriptionURL</td>
<td>regsub</td>
<td>regsub (required) value is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>targetUrl</td>
<td>targetUrl (required)</td>
<td></td>
</tr>
<tr>
<td>RecorderDiscoveryInfoType</td>
<td>regsub</td>
<td>regsub (required) value is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>apiType</td>
<td>apiType (required) value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>discoveryUrl</td>
<td>discoveryUrl (required)</td>
<td></td>
</tr>
</tbody>
</table>

The SetTransformResource and SetPublishResource use the PublishInfo subelement to define the HLS and HSS content by setting the MatchSubResource subelement (DeliveryHeader) and attributes. The DeliveryHeader is used to set the HTTP header fields.

When the initial request comes into the Delivery Media Application, the Asset Resolver is used to determine the SetTransformResource.
Pattern Matching

Before any pattern matches are checked, the protocol is checked. If the protocol of the incoming request does not match the protocols specified for the rule action, the action is not taken. If a pattern for a rule matches the given request, the corresponding action for that rule is taken.

**Note**

Asset Resolver only needs to make one successful match before stopping the rule lookup.

Boolean AND Function

When a PatternListGrp is specified for an action, it implies an AND of all the patterns within the group. All patterns specified in that group must be matched for the action to take place. In the following example, both patterns in grp1 must be matched for the action to be taken.

```xml
<Rule_Patterns>
  <PatternListGrp id="grp1">
    <Domain>livevod.com</Domain>
    <UrlRegex>clouds</UrlRegex>
  </PatternListGrp>
</Rule_Patterns>
```

Boolean OR Function

When the matchGroup id attributes are separated by a comma, it implies an OR of all the patterns. The action is taken when either of the patternListGrp elements are matched. In the following example, the pattern of either grp1 or grp2 is considered a match.

```xml
<Rule_Patterns>
  <PatternListGrp id="grp1">
    <Domain>livevod.com</Domain>
  </PatternListGrp>
</Rule_Patterns>
<Rule_Patterns>
  <PatternListGrp id="grp2">
    <UrlRegex>clouds</UrlRegex>
  </PatternListGrp>
</Rule_Patterns>
```

Rule Action Processing

The rules are processed in the same order they are listed in the Rule_Actions element. Multiple Rule_AssetResolve rule actions can be configured. The Rule_assetResolve rule actions can be in any order and the processing of the rules is determined by the order they are listed in the Asset Resolver XML file.

**Note**

Asset Resolver only needs to make one successful match before stopping the rule lookup.

The maximum number of rule actions allows is 100. If the number of rule actions exceeds 100, then the Asset Resolver XML file validation fails.
Asset Resolver File Examples

- Default Asset Resolver File, page A-6
- Asset Resolver Rule for HLS Live Service, page A-8
- Asset Resolver Rules for CF VOD—Unique ContentID in the URL, page A-8
- Asset Resolver Rules for CF VOD—ContentID as the Manifest File Name, page A-9
- Asset Resolver Rule for Content Protection, page A-11
- Setting the HTTP Response Cache-Control Header, page A-11

Default Asset Resolver File

```xml
<?xml version="1.0"?>
<AssetResolverRules
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:noNamespaceSchemaLocation="schema/VOSAssetResolver.xsd">
 <Revision>1.0</Revision>
 <CustomerName>Customer_name</CustomerName>
 <Rule_Patterns>
  <PatternListGrp id="grp1">
   <UrlRegex>(.*)</UrlRegex>
  </PatternListGrp>
 </Rule_Patterns>
 <Rule_Actions>
  <Rule_AgentRule nametag="native_hls_keyword" matchGroup="grp1" protocol="http">
   <SetPublishResource matchRegex="(.+)/hls/(.*)">
    <PublishInfo>
     <HLSPublishInfo assetUrl="$1/hls" mediaManifestUrl="$1">
      <!--above is not used, but schema requires it -->
     </HLSPublishInfo>
    </PublishInfo>
   </SetPublishResource>
  </Rule_AgentRule>
  <!-- ODE VOD GENERIC RULES -->
  <!-- hls -->
  <Rule_AgentRule protocol="http" matchGroup="grp1" nametag="rule_for_hls_stream_manifest">
   <SetTransformResource matchRegex="(.*//.*)/(.*)/(.*)\.m3u8">
    <SourceInfo>
     <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD" />
    </SourceInfo>
   </SetTransformResource>
  </Rule_AgentRule>
  <!---- ODE VOD GENERICA RULES -->
  <!-- hls -->
  <Rule_AgentRule protocol="http" matchGroup="grp1" nametag="rule_for_hls_stream_manifest">
   <SetTransformResource matchRegex="(.*//.*)/(.*)/(.*)\.m3u8">
    <SourceInfo>
     <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD" />
    </SourceInfo>
   </SetTransformResource>
  </Rule_AgentRule>
  <!-- Uncomment the below line and change the name to use DRM-->
  <!---<ContentProtectionProfileName>drm-name</ContentProtectionProfileName>-->
  <HLSPublishInfo>
   <HLSPublishInfo mediaManifestUrl="$1/$2/$2.m3u8" assetUrl="$1/$2" contentID="$2">
    <!-- Uncomment the below line and change the name to use DRM-->
    </HLSPublishInfo>
  </HLSPublishInfo>
 </Rule_AgentRule>
</SetTransformResource>
</Rule_AgentRule>
</Rule_Actions>
</AssetResolverRules>
```
<Rule_AssetResolve>
  protocol="http" matchGroup="grp1" nametag="rule_for_hls_variant_manifest">
  <SetTransformResource matchRegex="(.*)/(.*)\.m3u8">
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD"/>
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo>
        mediaManifestUrl="$1/$2.m3u8" assetUrl="$1/$2" contentID="$2">
        <!-- Uncomment the below line and change the name to use DRM-->
        <!-- <ContentProtectionProfileName>drm-name</ContentProtectionProfileName> -->
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>

<Rule_AssetResolve>
  protocol="http" matchGroup="grp1" nametag="rule_for_hls_ts">
  <SetTransformResource matchRegex="(.*)/(.*)/(.*)/(.*)\.ts">
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD"/>
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo>
        mediaManifestUrl="$1/$2/$2.m3u8" assetUrl="$1/$2" contentID="$2">
        <!-- Uncomment the below line and change the name to use DRM-->
        <!-- <ContentProtectionProfileName>drm-name</ContentProtectionProfileName> -->
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>

<!-- hds -->
<Rule_AssetResolve>
  protocol="http" matchGroup="grp1" nametag="rule_for_hds_manifest">
  <SetTransformResource matchRegex="(.*)/(.*)\.f4m">
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD"/>
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo>
        mediaManifestUrl="$1/$2.f4m" assetUrl="$1/$2" contentID="$2">
        <!-- Uncomment the below line and change the name to use DRM-->
        <!-- <ContentProtectionProfileName>drm-name</ContentProtectionProfileName> -->
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>

<!-- hds -->
<Rule_AssetResolve>
  protocol="http" matchGroup="grp1" nametag="rule1_for_hds_frag">
  <SetTransformResource matchRegex="(.*)/(.*)/(.*)*-Frag.*">
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD"/>
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo>
        mediaManifestUrl="$1/$2.f4m" assetUrl="$1/$2" contentID="$2">
        <!-- Uncomment the below line and change the name to use DRM-->
        <!-- <ContentProtectionProfileName>drm-name</ContentProtectionProfileName> -->
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>
Asset Resolver File Examples

Asset Resolver Rule for HLS Live Service

Asset Resolver Rules for CF VOD—Unique ContentID in the URL
Asset Resolver Rules for CF VOD—ContentID as the Manifest File Name

```xml
<Rule_AssetResolve nametag="rule_for_hls_stream_manifest" matchGroup="grp1" protocol="http">
  <SetTransformResource matchRegex="(.*)/(.*)/(.*)\.
      m3u8">
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2.dash/MPD" />
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo
        mediaManifestUrl="$1/$2.m3u8" assetUrl="$1/$2" contentID="$2">
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>

<Rule_AssetResolve nametag="rule_for_hls_variant_manifest" matchGroup="grp1" protocol="http">
  <SetTransformResource matchRegex="(.*)/(.*)\.
      m3u8">
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2.dash/MPD" />
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo
        mediaManifestUrl="$1/$2.m3u8" assetUrl="$1/$2" contentID="$2">
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>
```
Appendix A  Creating Asset Resolver Files

Asset Resolver File Examples

```xml
<Rule_AssetResolve nametag="rule_for_hls_ts" matchGroup="grp1" protocol="http">
  <SetTransformResource matchRegex="(.*/.*/.*/.*/.*)\.(ts)">
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2.dash/MPD" />
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo
        mediaManifestUrl="$1/$2.m3u8" assetUrl="$1/$2" contentID="$2">
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>

<Rule_AssetResolve nametag="rule_for_hls" matchGroup="grp1" protocol="http">
  <SetTransformResource matchRegex="(.*/.*/.*)\.(ism)" />
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD" />
    </SourceInfo>
    <PublishInfo>
      <HSSPublishInfo
        mediaManifestUrl="$1/$2.ism" contentID="$2" assetUrl="$1/$2">
        <!-- Uncomment the below line and change the name to use DRM-->
        <!-- <ContentProtectionProfileName>drm_name</ContentProtectionProfileName> -->
      </HSSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>

<Rule_AssetResolve nametag="rule_for_hds_manifest" matchGroup="grp1" protocol="http">
  <SetTransformResource matchRegex="(.*)/(.*)\.(f4m)" />
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD" />
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo
        mediaManifestUrl="$1/$2.f4m" contentID="$2" assetUrl="$1/$2">
        <!-- Uncomment the below line and change the name to use DRM-->
        <!-- <ContentProtectionProfileName>name-here</ContentProtectionProfileName> -->
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>

<Rule_AssetResolve nametag="rule1_for_hds_frag" matchGroup="grp1" protocol="http">
  <SetTransformResource matchRegex="(.*)/(.*)/(.*)-Frag.*" />
    <SourceInfo>
      <DASHAdaptiveTSSource mpdUrl="$1/$2/$2.dash/MPD" />
    </SourceInfo>
    <PublishInfo>
      <HLSPublishInfo
        mediaManifestUrl="$1/$2.f4m" contentID="$2" assetUrl="$1/$2">
        <!-- Uncomment the below line and change the name to use DRM-->
        <!-- <ContentProtectionProfileName> -->
      </HLSPublishInfo>
    </PublishInfo>
  </SetTransformResource>
</Rule_AssetResolve>
```

</SourceInfo>
</PublishInfo>
```
Asset Resolver Rule for Content Protection

If you are using DRM to encrypt content, you can provide the content protection details in the Asset Resolver to enable the VDS-OS to retrieve the key from the key server for each DRM format.

The content protection profile name, defined using the ContentProtectionProfileName tag, must match the one provisioned in VOSM for the origin service.

The contentId field specifies the identifier for any video content. We recommend that you create a key for each unique contentId, so that whenever a key request is sent for a particular contentId, the same key is received from the server.

Setting the HTTP Response Cache-Control Header

You can use the Asset Resolver rules to set different response headers on the URLs. You can use this capability to set cache control headers for ODE VOD requests. For example, defining the max-age attribute in the Asset Resolver overrides the default content expiry value in the origin service general settings page. You can define the value globally or for a particular ODE VOD asset.

- Global Cache-Control Configuration for an Origin Service, page A-11
- Cache-Control Configuration for a Specific HLS .m3u8 or .ts File URL, page A-12
- Generic HTTP Response Header, page A-12

Global Cache-Control Configuration for an Origin Service

```xml
<Rule_AssetResolve
  nametag="global_caching_headers_rule" matchGroup="grp1, grp2" protocol="http">
  <SetMetaData>
    <DeliveryHeader>
      <SetCachingHeader>
        <Cache-Control>
          <Max-Age>300000</Max-Age>
        </Cache-Control>
      </SetCachingHeader>
    </DeliveryHeader>
  </SetMetaData>
</Rule_AssetResolve>
```
Troubleshooting the Asset Resolver

If an ODE VOD fails to play, and there are HTTP 404 responses in the HTTP transaction logs (/local/local/logs/webengine_extsquid/working.log), the Asset Resolver rules might be failing to translate the incoming HDS, HLS, or HSS URL into the corresponding DASH URL. If that is the case, the following procedure can help you determine the problem:

**Step 1** Verify that the rules in the Asset Resolver are correct.
Troubleshooting the Asset Resolver

**Step 2**  Verify that the order of the rules in the file is correct.

**Step 3**  Verify that the input URL matches any rule or the expected rule.

**Step 4**  Verify that you are using the correct Asset Resolver, either the default file or a customized file.

**Step 5**  If you are using the default Asset Resolver, verify that it is meeting your needs.

**Step 6**  For HLS Live requests, determine whether the master manifest rule correctly matches for the stream manifest file requests, and vice versa.
Creating Coverage Zone Files

This appendix describes the Coverage Zone file and provides several Coverage Zone file examples.

Introduction

A Coverage Zone file is an XML file used to specify a user-defined coverage zone. The Coverage Zone file supports different tags to support different types of proximity configurations.

- Network and subnet—Specify the IP address range
- Geographical location—Specify the longitude and latitude of the data center

In addition to the coverage zone information, two optional elements are created for documentation purposes: a revision value to specify the version of the Coverage Zone file and a customer name.

For information about importing or uploading a Coverage Zone file, see the “Coverage Zone File Registration” section on page 7-10.

For more information about Coverage Zone files, see the “Coverage Zone File” section on page 1-38.

Coverage Zone files can be created using any ASCII text-editing tool. You can use a single coverage zone text-format file to define all the coverage zones for your VDS-OS network.

The XML Schema file describes and dictates the content of the XML file. The VOSCoverageZone.xsd file contains the XML schema. To view or download a copy of the VOSCoverageZone.xsd, see the “Viewing or Downloading XML Schema Files” section on page 7-15.

Note

When DNS-based redirection is enabled, the Coverage Zone file needs to have entries with respect to the IP address of the DNS proxies instead of the client IP address.

Table B-1 defines the Coverage Zone file elements.
Introduction

Note

The metric value of a default coverage zone is set to 20. If a particular SE is preferred for a user-defined coverage zone, the metric value in the Coverage Zone file should be set to a value less than 20. If a default coverage zone is preferred, then the metric value in the Coverage Zone file should be set to a value greater than 20.

Zero-IP Based Configuration

The zero-ip based configuration is a catch-all condition for routing. It can be used in combination with proximity-based routing and location-based routing. If an SE cannot be found through location-based routing or proximity-based routing, the zero-ip based configuration is taken into account for selecting an SE.

The zero-ip based configuration is a network entry in the Coverage Zone file defined as 0.0.0.0/0. It matches all client subnets. If the client subnet does not match any of the other network entries in the Coverage Zone file and a 0.0.0.0/0 network entry exists, then the SEs listed for that entry are considered for serving the client request.

Following is an example of the zero-ip based configuration.

```xml
<?xml version="1.0"?>
<CDNNetwork>
<revision>1.0</revision>
<coverageZone>
    <network>3.1.2.18/32</network>
    <SE>U8-UCS200-1</SE>
    <metric>5</metric>
</coverageZone>
</CDNNetwork>
```

Table B-1 Coverage Zone File Elements

<table>
<thead>
<tr>
<th>Tag</th>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>latitude</td>
<td>float</td>
<td>Value indicating the geographical coordinate (latitude) of the data center.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td></td>
<td>Not supported.</td>
</tr>
<tr>
<td></td>
<td>longitude</td>
<td>float</td>
<td>Value indicating the geographical coordinate (longitude) of the data center.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td></td>
<td>Not supported.</td>
</tr>
<tr>
<td>coverageZone</td>
<td>network</td>
<td>IP address</td>
<td>Coverage zone IP address range.</td>
</tr>
<tr>
<td></td>
<td>SE</td>
<td>Service Engine name (string)</td>
<td>Specifies the Service Engines serving the coverage zone specified in the network element. This can have one or more elements.</td>
</tr>
<tr>
<td></td>
<td>metric</td>
<td>integer</td>
<td>Value indicating the proximity of the Service Engine to the end user. The lower the value, the closer the Service Engine is to the end user.</td>
</tr>
<tr>
<td></td>
<td>location</td>
<td>—</td>
<td>Value indicating the geographical coordinates (latitude and longitude) of the data center.</td>
</tr>
<tr>
<td>CDNNetwork</td>
<td>revision</td>
<td>1.0</td>
<td>Not used in this VDS-OS release.</td>
</tr>
<tr>
<td></td>
<td>customerName</td>
<td>customer name</td>
<td>Not used in this VDS-OS release.</td>
</tr>
<tr>
<td></td>
<td>coverageZone</td>
<td>—</td>
<td>This can have one or more coverage zones.</td>
</tr>
</tbody>
</table>
Appendix B      Creating Coverage Zone Files

Coverage Zone File Example

<coverageZone>
  <network>3.1.13.10/32</network>
  <SE>U8-UCS200-2</SE>
  <metric>5</metric>
</coverageZone>

<coverageZone>
  <network>0.0.0.0/0</network>
  <SE>U8-UCS200-3</SE>
  <metric>20</metric>
</coverageZone>

Invalid IPv4 Addresses in Coverage Zone File

The following IPv4 addresses are considered invalid in the Coverage Zone file:

- Limited broadcast address (255.255.255.255)
- Class A (0.x.x.x)—These addresses are reserved.
  
  **Note**  The exception is 0.0.0.0/0, which is used for zero-IP based configuration.

- Class A (127.x.x.x)—These addresses are reserved. They are used as internal host loopback addresses, internal host loopback.
- Class B (191.255.x.x)—These addresses are reserved.
- Class C (223.255.255.x)—These addresses are reserved.
- Class D (224.x.x.x - 239.x.x.x)—Entire class is reserved for multicast addresses (the low order 24 bits represent the multicast group ID).
- Class E (240.x.x.x - 255.x.x.x)—Entire class is reserved for future use.

In addition, the following broadcast IPv4 addresses are not valid, and are not likely to be used in the Coverage Zone file:

- Class A (y.255.255.255, y = 1 to 127)—Directed broadcast to specified network.
- Class B (y.x.255.255, y = 128 to 191)—Directed broadcast to specified network.
- Class C (y.x.x.255, y = 192 to 223)—Directed broadcast to specified network.

Coverage Zone File Example

The following sections show different Coverage Zone file examples in the following scenarios:

- Coverage Zone with Client Network Only
- Coverage Zone for Same Client Network with Different Weighted SEs

For a proximity-based routing include list, the <coverageZone> tag just includes the <SE> and <metric> elements, as follows:

<!-- For proximity based routing include list -->
<coverageZone>
  <SE>W13-UCS200-1</SE>
  <metric>10</metric>
</coverageZone>
Coverage Zone with Client Network Only

<?xml version="1.0" ?>
<!-- Coverage Zone data in XML -->
<CDNNetwork>
  <revision>1.0</revision>
  <customerName> Cisco Systems </customerName>
  <!-- San Jose Datacenter -->
  <coverageZone>
    <network>192.1.2.0/16</network>
    <SE>UCS-200-SE1</SE>
    <SE>UCS-200-SE2</SE>
    <metric>10</metric>
  </coverageZone>
  <!-- Chicago Datacenter -->
  <coverageZone>
    <network>192.1.3.0/24</network>
    <SE>UCS-200-SE3</SE>
    <SE>UCS-200-SE4</SE>
    <metric>10</metric>
  </coverageZone>
  <!-- New York Datacenter -->
  <coverageZone>
    <network>192.1.4.0/24</network>
    <SE>UCS-200-SE5</SE>
    <SE>UCS-200-SE6</SE>
    <metric>10</metric>
  </coverageZone>
</CDNNetwork>

Coverage Zone for Same Client Network with Different Weighted SEs

<?xml version="1.0" ?>
<!-- Coverage Zone data in XML -->
<CDNNetwork>
  <revision>1.0</revision>
  <customerName>Cisco Systems</customerName>
  <coverageZone>
    <network>172.31.10.0/12</network>
    <SE>dmz2-roam</SE>
    <metric>10</metric>
  </coverageZone>
  <coverageZone>
    <network>172.31.10.0/12</network>
    <SE>dmz2-is</SE>
    <metric>20</metric>
  </coverageZone>
</CDNNetwork>
Creating Capture Schedule Files

This appendix describes the Capture Schedule file used by a live channel to specify the live and live-to-VOD events. This appendix consists of the following topics:

- Introduction, page C-1
- Capture Schedule File Structure and Syntax, page C-2
- Capture Schedule File Example, page C-3

Introduction

The Capture Schedule file is an XML file that can be used to specify live and live-to-VOD events for a live channel.

The Capture Schedule file contains the following information:

- Name of the live channel
- Capture events described with the following information:
  - Publish URI—Base URI used by the VDS-OS system for publishing content. The URI always ends with the resource format (hls, hss, hds, or dash), followed by a valid manifest filename and extension (for example, index.m3u8 for an HLS resource).
  - Capture streams (belonging to one Capture Resource)—Must match the configuration that is configured in the VOSM for the live channel.
  - Action on completion—Describes the action the VDS-OS performs on completing the recording. VDS-OS supports the Notify action, which posts a notification to an external entity.

Capture Schedule Based on Live Channel Resources

The live channels configured on the VOSM defines the list of capture resources to be sourced for each channel and the publish resources for each channel.

The Capture Schedule XML file defines a list of publish resources that are treated as live-to-VOD recording requests. The live-to-VOD publish resources defined in the Capture Schedule XML file reference a capture resource defined in the live channel and can consist of all the stream profiles or a subset of the stream profiles defined for the specified capture resource.

If a publish resource references a non-existent capture resource, or if all the streams are undefined, that publish resource is marked failed and is not scheduled.
If a publish resource references an existing capture resource and a few streams are undefined for the capture resource, the publish resource is scheduled to record only the specified streams that are defined for the capture resource.

**Adding a Capture Schedule File to the VDS-OS**

The Capture Schedule files can be created using any ASCII text-editing tool. The Capture Schedule files are uploaded or imported for a live channel by way of the Capture Schedule page.

### Capture Schedule File Structure and Syntax

The XML Schema file describes and dictates the content of the XML file. The VOSCaptureSchedule.xsd file contains the XML schema. To view or download a copy of the VOSCaptureSchedule.xsd file, see the “Viewing or Downloading XML Schema Files” section on page 7-15.

Table C-1 describes the Capture Schedule file elements.

<table>
<thead>
<tr>
<th>Table C-1</th>
<th>Capture Schedule File Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element</td>
<td>Subelements</td>
</tr>
<tr>
<td>VOSCaptureSchedule</td>
<td>Version</td>
</tr>
<tr>
<td>ChannelID</td>
<td></td>
</tr>
<tr>
<td>HLSCaptureEvent</td>
<td></td>
</tr>
<tr>
<td>HSSCaptureEvent</td>
<td></td>
</tr>
<tr>
<td>HLSCaptureEvent</td>
<td>PublishInfo</td>
</tr>
<tr>
<td></td>
<td>SourceInfo</td>
</tr>
<tr>
<td></td>
<td>ActionOnCompletion</td>
</tr>
<tr>
<td>PublishInfo</td>
<td>PublishURI</td>
</tr>
</tbody>
</table>
### Table C-1: Capture Schedule File Elements (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Subelements</th>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SourceInfo</td>
<td>HLSCaptureResourceInput HSSCaptureResourceInput</td>
<td></td>
<td>SourceInfo specifies the capture resource the Capture Event is tied to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• HLSCaptureResourceInput is used with the HLSCaptureEvent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• HSSCaptureResourceInput is used with the HSSCaptureEvent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>There can only be one CaptureResource per CaptureEvent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong> DASHAdaptiveTSCaptureResourceInput is not supported.</td>
</tr>
<tr>
<td>HLSCaptureResourceInput</td>
<td>HLSCaptureStreamInput HSSCaptureStreamInput</td>
<td>baseURI</td>
<td>HLSCaptureStreamInput is used with the HLSCaptureResourceInput.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HSSCaptureStreamInput is used with the HSSCaptureResourceInput.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The CaptureStreamInput element is a stream associated with the Capture Resource element.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong> baseURI (required) is the baseURI used for the capture resource of the live channel.</td>
</tr>
<tr>
<td>ActionOnCompletion</td>
<td>Notify</td>
<td></td>
<td>ActionOnCompletion element specifies the action to be taken after the event is completed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong> The Copy, Delete, and Archive subelements are not supported.</td>
</tr>
<tr>
<td>Notify</td>
<td></td>
<td>Location</td>
<td>Location attribute (required) specifies the location to send the notification. The format is http://&lt;server&gt;</td>
</tr>
</tbody>
</table>

### Capture Schedule File Example

The following is an example of a Capture Schedule file:

```xml
<VOSCaptureSchedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="VOSCaptureSchedule.xsd">
  <Version>1.0</Version>
  <ChannelID>http://vos.tstv.net/tsw</ChannelID>
  <HLSCaptureEvent StartTime="2013-06-19T13:54:00" EndTime="2013-06-19T13:56:00">
    <PublishInfo>
      <PublishURI>live-vod/hls/master.m3u8</PublishURI>
    </PublishInfo>
    <SourceInfo>
      <HLSCaptureResourceInput baseURI="cr/hls">
        <HLSCaptureStreamInput>wifi1980</HLSCaptureStreamInput>
      </HLSCaptureResourceInput>
    </SourceInfo>
  </HLSCaptureEvent>
</VOSCaptureSchedule>
```
<ActionOnCompletion>
  <Notify Location="http://vos.tstv.net/cdvr/RecorderManager/RecordingEvent/" />
</ActionOnCompletion>

</HLSCaptureEvent>

</VOSCaptureSchedule>
CLI Commands

This appendix covers the following topics:

- Configuring Port Channel, page D-1
- Configuring Standby Interfaces, page D-6

Configuring Port Channel

To configure an EtherChannel, you use the `PortChannel` interface configuration command. Port Channel, also known as EtherChannel, supports the grouping of up to eight same-speed network interfaces into one virtual interface. EtherChannel also provides interoperability with Cisco routers, switches, and other networking devices or hosts supporting EtherChannel; load balancing; and automatic failure detection and recovery based on each interface’s current link status.

To achieve the best throughput, we recommend you configure a port channel for the eight gigabit Ethernet ports on the line card. Up to eight gigabit Ethernet interfaces can be put into the same port channel.

Redundant Dedicated Management Ports

All the ports on a hardware platform can be used for playout traffic, as well as system management traffic to communicate with other VDS-OS devices such as the VOSM. To prevent all the bandwidth being used by playout traffic, a dedicated management port setup is often recommended.

In case of physical failure on a single port, channel bonding configuration of multiple gigabit Ethernet ports is also recommended for both playout traffic and management traffic.

A port channel configured with a default gateway is only for playout traffic. Playout traffic places highest bandwidth demand on the VDS-OS network. A port channel configured as the primary interface carries playout traffic.

If an EtherChannel (also known as port channel) is used between the upstream router or switch and the SE for streaming real-time data, the EtherChannel load balance algorithms on the upstream switch or router and the SE should be configured as “src-ip” and “dst-ip” respectively. Using this configuration
ensures session stickiness and general balanced load-distribution based on clients’ IP addresses. Also, distribute your client IP address space across multiple subnets so that the load-balancing algorithm is effective in spreading the traffic among multiple ports.

On a hardware platform with two gigabit Ethernet ports on the motherboard (GigabitEthernet 1/0 and 2/0) and eight gigabit Ethernet ports (GigabitEthernet 3/0 to 10/0) on the NICs, the motherboard Ethernet ports can be bundled for the management port channel and the NIC Ethernet ports can be bundled for the traffic port channel for maximum throughput. For more redundancy, you can configure two channel groups of four interfaces each (3/0 to 6/0 and 7/0 to 10/0) that are standbys for each other.

Configuring Redundant Management Ports

Following is an example of configuring redundant dedicated management ports on a hardware platform with two motherboard Ethernet ports and four NIC ethernet ports using the CLI:

**Step 1** Configure two port channels with different subnets for each one.

```
SE(config)# interface PortChannel 1
SE(config-if)# ip address 3.1.7.73 255.255.255.0
SE(config-if)# exit
SE(config)# interface PortChannel 2
SE(config-if)# ip address 3.1.8.200 255.255.255.0
SE(config-if)# exit
```

**Step 2** Assign the interfaces to the two port channels. PortChannel 1 has four gigabit Ethernet interfaces for application traffic, and PortChannel 2 has two gigabit Ethernet interfaces for management traffic.

```
SE(config)# interface GigabitEthernet 1/0
SE(config-if)# channel-group 2
SE(config-if)# exit
SE(config)# interface GigabitEthernet 2/0
SE(config-if)# channel-group 2
SE(config-if)# exit
SE(config)# interface GigabitEthernet 3/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 4/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 5/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 6/0
SE(config-if)# channel-group 1
SE(config-if)# exit
```

**Note** The port channel carrying playout traffic should always be configured as channel-group 1 and set as the primary interface.

Whenever the IP address of the primary interface is changed, you must restart the DNS server.

**Step 3** Configure the playout port channel as the primary interface.

```
SE(config)# primary-interface PortChannel 1
```

**Step 4** Configure a default gateway for the playout traffic.
SE(config)# ip default-gateway 3.1.7.1

Step 5  Set the load balancing algorithm to the destination IP address.
SE(config)# port-channel load-balance dst-ip

Step 6  Configure a static route to the VOSM (4.0.5.5) to specify that all management traffic goes through this interface.
SE(config)# ip route 4.0.5.5 255.255.255.255 3.1.8.1

Step 7  Configure the port channel and VLANs on the switch that the SE is directly connected to.
SW3750(config)# interface Port-channel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# exit
SW3750(config)# interface Port-channel2
SW3750(config-if)# switchport access vlan 202
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/1
SW3750(config-if)# description Connected to portchannel1
SW3750(config-if)# switchport access vlan 202
SW3750(config-if)# channel-group 2 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/2
SW3750(config-if)# description Connected to portchannel1
SW3750(config-if)# switchport access vlan 202
SW3750(config-if)# channel-group 2 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/3
SW3750(config-if)# description connected to portchannel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# channel-group 1 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/4
SW3750(config-if)# description connected to portchannel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# channel-group 1 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/5
SW3750(config-if)# description connected to portchannel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# channel-group 1 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/6
SW3750(config-if)# description connected to portchannel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# channel-group 1 mode on
SW3750(config-if)# exit
SW3750(config)# interface Vlan201
SW3750(config-if)# ip address 3.1.7.1 255.255.255.0
SW3750(config-if)# exit
SW3750(config)# interface Vlan202
SW3750(config-if)# ip address 3.1.8.1 255.255.255.0
SW3750(config-if)# exit

Step 8  Set the load balancing algorithm to the source IP address.
SW3750(config)# port-channel load-balance src-ip
Note

The optimal load-balance setting on the switch for traffic between the Acquisition Node and the edge Service Engine is **dst-port**, which is not available on the 3750, but is available on the Catalyst 6000 series.

---

### Switch Port-Channel Configuration for Acquisition Node and Edge Service Engine

The Cisco Catalyst 6500 Series Switch supports more port-channel load-balance options than the Cisco Catalyst 3750 Series Switch. The Cisco Catalyst 6500 Series Switch allows for full utilization of all eight port-channels grouped together between the Acquisition Node and the edge SE when dst-port is selected as the port-channel load-balance option. When the Cisco Catalyst 3750 Series Switch is used, the content is fetched by way of a single gigabit Ethernet interface because there is no dst-port load-balance option.

The following configuration recommendation for the switch port-channel load-balance option, and Acquisition Node and edge SE load-balance options, fully use all eight ports when the edge SE is fetching content from the Acquisition Node:

- Acquisition Node port-channel load-balance option is set to **round-robin**
- Edge SE port-channel load-balance option is set to **dst-ip**
- Cisco Catalyst 6500 Series Switch instead of Cisco Catalyst 3750 Series Switch to use the dst-port option
- Cisco Catalyst 6500 Series Switch port-channel load-balance option is set to **dst-port**

### Verifying Port Channel Configuration

To verify the setup before application traffic is sent, use the following commands:

```
SE# clear statistics all
SE# show interface portChannel 1
```

#### Interface PortChannel 1 (2 physical interface(s)):

- GigabitEthernet 3/0 (active)
- GigabitEthernet 4/0 (active)
- GigabitEthernet 5/0 (active)
- GigabitEthernet 6/0 (active)

----------

- Type: Ethernet
- Ethernet address: 00:04:23:D8:86:02
- Internet address: 3.1.7.73
- Broadcast address: 3.1.7.255
- Netmask: 255.255.255.0
- Maximum Transfer Unit Size: 1500
- Metric: 1
- Packets Received: 28
- Input Errors: 0
- Input Packets Dropped: 0
- Input Packets Overruns: 0
- Input Packets Frames: 0
- Packet Sent: 40
- Output Errors: 0
- Output Packets Dropped: 0
- Output Packets Overruns: 0
- Output Packets Carrier: 0
- Output Queue Length: 0
- Collisions: 0
Flags: UP BROADCAST RUNNING MASTER MULTICAST

SE# show interface portChannel 2
Interface PortChannel 2 (4 physical interface(s)):
GigabitEthernet 1/0 (active)
GigabitEthernet 2/0 (active)
---------------------
Type: Ethernet
Ethernet address: 00:30:48:33:01:26
Internet address: 3.1.8.200
Broadcast address: 3.1.8.255
Netmask: 255.255.255.0
Maximum Transfer Unit Size: 1500
Metric: 1
Packets Received: 6
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 0
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length: 0
Collisions: 0
Flags: UP BROADCAST RUNNING MASTER MULTICAST

To verify the setup after application traffic is sent, use the following:

SE# show interface portChannel 1
Interface PortChannel 1 (4 physical interface(s)):
GigabitEthernet 3/0 (active)
GigabitEthernet 4/0 (active)
GigabitEthernet 5/0 (active)
GigabitEthernet 6/0 (active)
---------------------
Type: Ethernet
Ethernet address: 00:04:23:D8:86:02
Internet address: 3.1.7.73
Broadcast address: 3.1.7.255
Netmask: 255.255.255.0
Maximum Transfer Unit Size: 1500
Metric: 1
Packets Received: 1875
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 5221
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length: 0
Collisions: 0
Flags: UP BROADCAST RUNNING MASTER MULTICAST

SE# show interface portChannel 2
Interface PortChannel 2 (2 physical interface(s)):
GigabitEthernet 1/0 (active)
GigabitEthernet 2/0 (active)
---------------------
Type: Ethernet
Ethernet address:00:30:48:33:01:26
Internet address:3.1.8.200
Broadcast address:3.1.8.255
Netmask:255.255.255.0
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 21
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 0
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:0
Collisions: 0
Flags: UP BROADCAST RUNNING MASTER MULTICAST

In the Devices Table page on the VOSM (Devices > Devices), the SE or SR status should be “Online.” The IP address for the device always shows the IP address of the port channel’s primary interface.

Configuring Standby Interfaces

You can configure one or more interfaces to act as a backup interface (a standby interface) for another interface on a Service Engine. This feature is called **standby interface support**. Standby groups, which are logical groups of interfaces, are used to implement this feature. When an active network interface fails (because of cable trouble, Layer 2 switch failure, high error count, or other failures) and the interface is part of a standby group, a standby interface can become active and take the load off the failed interface.

A standby group must have at least two interfaces. Interfaces that are part of a standby group are called member interfaces. After you create a standby group, you define which interfaces should be assigned to this logical group. As part of defining the member interfaces, you specify the priority of each member interface in a standby group. The member interface with the highest assigned priority is the active interface for that particular standby group. If the active interface fails, the operational member interface with the next highest priority in the standby group comes up, and so forth. If all member interfaces of a particular standby group are down and then one of the member interfaces comes up, the VDS-OS software detects this situation and brings up the standby group on the member interface that just came up.

The failure or failover of member interfaces within a standby group triggers alarms and traps (if alarms and traps are enabled on the Service Engine). Alarms are sent out when failover occurs between member interfaces in a standby group. Specifically, minor alarms are sent out when member interfaces fail, and these alarms are cleared automatically when the interface failover has been successfully completed. Major alarms are sent out if the standby group goes down (no member interface in a standby group can be brought up).

---

**Note**

A physical interface can belong to more than one standby group, and a single interface can act as a standby interface for more than one standby group.

To configure standby interfaces, interfaces are logically assigned to standby groups. The following rules define the standby group relationships:
Each standby group is assigned a unique standby IP address, shared by all member interfaces of the standby group. The IP address of the standby group is shared among the member interfaces; however, only the active interface of the standby group uses this shared IP address at any one time. This shared IP address is configured as an alias on the active interface.

Duplex and speed settings of the member interfaces can be configured for better reliability.

If a physical interface is a member of a port-channel group, it cannot join a standby group. If a physical interface is a member of a standby group, it cannot join a port-channel group.

Maximum number of standby groups on a Service Engine is four.

**Note**

Interface IP addresses and standby group IP addresses must be on different subnets to ensure reliable operation. You can use dummy IP addresses in the private address space to serve as interface primary IP addresses, and use the real Service Engine IP address to serve as the standby group IP address in a different subnet to satisfy this requirement. When dummy IP addresses are used, these interface IP addresses serve only as substitutes to bring up the interface. For example, the Service Engine interface requires an IP address on an interface for initialization. Make sure to configure the interface default gateway using the `ip default-gateway` global configuration command instead of the `ip route` command.

Each interface in a standby group is assigned a priority. The operational interface with the highest priority in a standby group is the active interface. Only the active interface uses the group IP address.

Priority of an interface in a standby group can be changed at run time. The member interface that has the highest priority after this change becomes the new active interface (the default action is to preempt the currently active interface if an interface with higher priority exists).

Maximum number of errors allowed on the active interface before the interface is shut down and the standby is brought up is configured with the `errors` option, which is disabled by default.

**Tip**

If an interface belongs to more than one standby group, you can configure the interface with a different priority in each standby group for better load balancing. For example, interfaces gigabit Ethernet 0/0 and gigabit Ethernet 0/1 are both in Standby Group 1 and in Standby Group 2. If you configure gigabit Ethernet 0/0 with the highest priority in Standby Group 1 and configure gigabit Ethernet 0/1 with the highest priority in Standby Group 2, Standby Group 1 uses gigabit Ethernet 0/0 as the active interface, while Standby Group 2 uses gigabit Ethernet 0/1 as the active interface. This configuration allows each interface to back up the other one, if one of them fails.

Use the `interface standby` global configuration command to create standby groups on Service Engines.

**Note**

Unlike port channels, standby groups do not support IP ACLs at a group level. However, you can configure a member interface of a standby group to support an IP ACL at the interface level. For example, you can individually configure the two member interfaces of Standby Group 1 (the gigabit Ethernet 0/0 interface and the gigabit Ethernet 0/1 interface) to support an IP ACL named ACL1 but you cannot configure the Standby Group 1 to support ACL1.

To configure an interface to be a backup for another interface, use the `standby` interface configuration command. To restore the default configuration of the interface, use the `no` form of this command.

```
standby group_number { description text | errors max-errors | ip ip-address netmask | priority priority_level | shutdown }

no standby group_number { description text | errors max-errors | ip ip-address netmask | priority priority_level | shutdown }
```
### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group_number</strong></td>
<td>Standby group number (1–4).</td>
</tr>
<tr>
<td><strong>description</strong></td>
<td>(Optional) Sets the description for the specified interface.</td>
</tr>
<tr>
<td><strong>text</strong></td>
<td>Description for the specified interface. The maximum length of the description text is 240 characters.</td>
</tr>
<tr>
<td><strong>errors</strong></td>
<td>Sets the maximum number of errors allowed on the active interface before the interface is shut down and the standby interface is brought up. This option is disabled by default.</td>
</tr>
<tr>
<td><strong>max-errors</strong></td>
<td>Maximum number of errors (1–2147483647).</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>Sets the IP address for the specified standby group (Standby Group 1, 2, 3, or 4).</td>
</tr>
<tr>
<td><strong>ip-address</strong></td>
<td>IP address of the specified standby group (Standby Group 1, 2, 3, or 4). The group IP address and netmask of a standby group must be configured on all the member interfaces.</td>
</tr>
<tr>
<td><strong>netmask</strong></td>
<td>Netmask of the specified standby group (Standby Group 1, 2, 3, or 4).</td>
</tr>
<tr>
<td><strong>priority</strong></td>
<td>Sets the priority of the member interface within a standby group. The priority of a member interface can be changed at run time. The member interface that has the highest priority after this change becomes the new active interface (the default action is to preempt the currently active interface if an interface with higher priority exists).</td>
</tr>
<tr>
<td><strong>priority_level</strong></td>
<td>Each member interface is assigned a priority number. The member interface with the highest priority number is the active interface for that standby group. Only the active interface uses the group IP address. If the <strong>priority</strong> option is specified without a priority number, the default value of 100 is used.</td>
</tr>
<tr>
<td><strong>shutdown</strong></td>
<td>(Optional) Shuts down the specified standby group (Standby Group 1, 2, 3, or 4). You can shut down a standby group even if you have not configured a group IP address of the standby group.</td>
</tr>
</tbody>
</table>

#### Examples

The following example configures three gigabit Ethernet interfaces to be part of the same standby group, with interface 1/0 as the active interface:

```plaintext
Console(config-if)# interface GigabitEthernet 1/0 standby 2 priority 300
Console(config-if)# interface GigabitEthernet 2/0 standby 2 priority 200
Console(config-if)# interface GigabitEthernet 3/0 standby 2 priority 100
Console(config-if)# interface standby 2 errors 1000
```

The following example displays information about the standby group configuration by entering the `show standby` EXEC command. In the following sample command output, one standby group (Standby Group 1) is configured on this Service Engine. The command output also shows which member interface is the active interface. In this case, the active interface is the gigabit Ethernet slot 3/port 0 interface.

```plaintext
ServiceEngine# show standby
Standby Group:1
IP address: 172.16.10.10, netmask: 255.255.254.0
Maximum errors allowed on the active interface: 10000
Member interfaces:
  GigabitEthernet 3/0 priority: 300
  GigabitEthernet 3/1 priority: 200
  GigabitEthernet 3/2 priority: 100
```
Active interface: GigabitEthernet 3/0

Note

To display information about a specific standby group configuration, enter the `show interface standby group_number` EXEC command.

The following example creates a standby group, Standby Group 1:

```
ServiceEngine# configure
ServiceEngine(config)# interface standby 1
ServiceEngine(config-if)#
```

The following example assigns a group IP address of 10.10.10.10 and a netmask of 255.0.0.0 to Standby Group 1:

```
ServiceEngine(config-if)# ip address 10.10.10.10 255.0.0.0
ServiceEngine(config-if)# errors 500
```

The following example shows how to add two gigabit Ethernet interfaces to Standby Group 1 and then assign each of these member interfaces a priority within the group:

1. Add a gigabit Ethernet interface 0/0 to Standby Group 1 and assign a priority of 150.

```
ServiceEngine(config)# interface GigabitEthernet 0/0
ServiceEngine(config-if)# standby 1 priority 150
```

2. Add a second gigabit Ethernet interface 0/1 to Standby Group 1 with the default priority value of 100.

```
ServiceEngine(config)# interface GigabitEthernet 0/1
ServiceEngine(config-if)# standby 1
ServiceEngine(config-if)# exit
ServiceEngine(config)#
```

Because gigabit Ethernet 0/0 is assigned the highest priority (a priority number of 150) of all the member interfaces in the group, it is chosen as the active interface for the group if it can be brought up.

The following example removes the gigabit Ethernet 0/1 interface from Standby Group 1 using the `no` form of the `standby` command:

```
ServiceEngine(config)# interface FastEthernet 0/1
ServiceEngine(config-if)# no standby 1
ServiceEngine(config-if)# exit
ServiceEngine(config)#
```

The following example shows how to shut down Standby Group 1. When a standby group is shut down, all the alarms previously raised by this standby group are cleared.

```
ServiceEngine(config)# interface standby 1
ServiceEngine(config-if)# shutdown
ServiceEngine(config-if)# exit
```

The following example shows how to tear down Standby Group 1:

```
ServiceEngine(config)# interface standby 1
ServiceEngine(config-if)# no ip address 10.10.10.10 255.0.0.0
Please remove member interface(s) from this standby group first.
ServiceEngine(config)# interface GigabitEthernet 2/0
ServiceEngine(config-if)# no standby 1
ServiceEngine(config-if)# exit
ServiceEngine(config)#
```

```
ServiceEngine(config)# no interface standby 1
```
Standby Interface with Switch Failover Configuration Procedure

This procedure describes how to configure a standby interface for two port channels and a standby interface for two management interfaces on a device with a total of six interfaces.

To configure a standby interface with two port channels, do the following:

**Step 1** Configure gigabit Ethernet 1/0 and gigabit Ethernet 2/0 as management interfaces and create one standby interface for redundancy.

```
SE(config)# interface GigabitEthernet 1/0
SE(config-if)# standby 2 priority 200
SE(config-if)# exit
SE(config)# interface GigabitEthernet 2/0
SE(config-if)# standby 2
SE(config-if)# exit
SE(config-if)# interface Standby 2
SE(config-if)# description for management
SE(config-if)# ip address 4.0.7.127 255.255.255.0
SE(config-if)# exit
```

**Step 2** Add gigabit Ethernet 3/0 and gigabit Ethernet 4/0 to port channel 1, add gigabit Ethernet 5/0 and gigabit Ethernet 6/0 to port channel 2, and create a standby interface for these two port channels for redundancy.

```
SE(config)# interface GigabitEthernet 3/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 4/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 5/0
SE(config-if)# channel-group 2
SE(config-if)# exit
SE(config)# interface GigabitEthernet 6/0
SE(config-if)# channel-group 2
SE(config-if)# exit
SE(config)# interface PortChannel 1
SE(config-if)# standby 1 priority 120
SE(config-if)# exit
SE(config)# interface PortChannel 2
SE(config-if)# standby 1 priority 200
SE(config-if)# exit
SE(config)# interface Standby 1
SE(config-if)# description for traffic
SE(config-if)# ip address 7.35.0.7 255.255.0.0
SE(config-if)# exit
SE(config)# primary-interface Standby 1
```
Software Licensing Information

This appendix provides software license information related to the VDS-OS.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.


4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

   The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].