Product Overview

This chapter provides a brief introduction to the Cisco Videoscape Distribution Suite (VDS) video content delivery system for a Real Time Streaming Protocol (RTSP) environment.

This chapter covers the following major topics:

Overview

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

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

The VDS functionality can be separated into five areas:

- Ingest
- Storage
- Caching
- Streaming
- Management

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

Table 1-1 CDA Mapping to Functionality and CDSM

CDA Name	Functionalities	CDSM Device Name
Vault	Ingest and storage	Vault
Content Cache	Content distribution between Vaults and Streamers	Caching Node
TV Streamer	Content caching, personalization, and streaming to STBs	Streamer

Table 1-1 CDA Mapping to Functionality and CDSM (continued)

CDA Name	Functionalities	CDSM Device Name
TV MediaX Suite	Aids content ingest workflow and scheduling tasks for both asset-based and real-time content	CDSM
TV Content Delivery System Manager	Management	CDSM

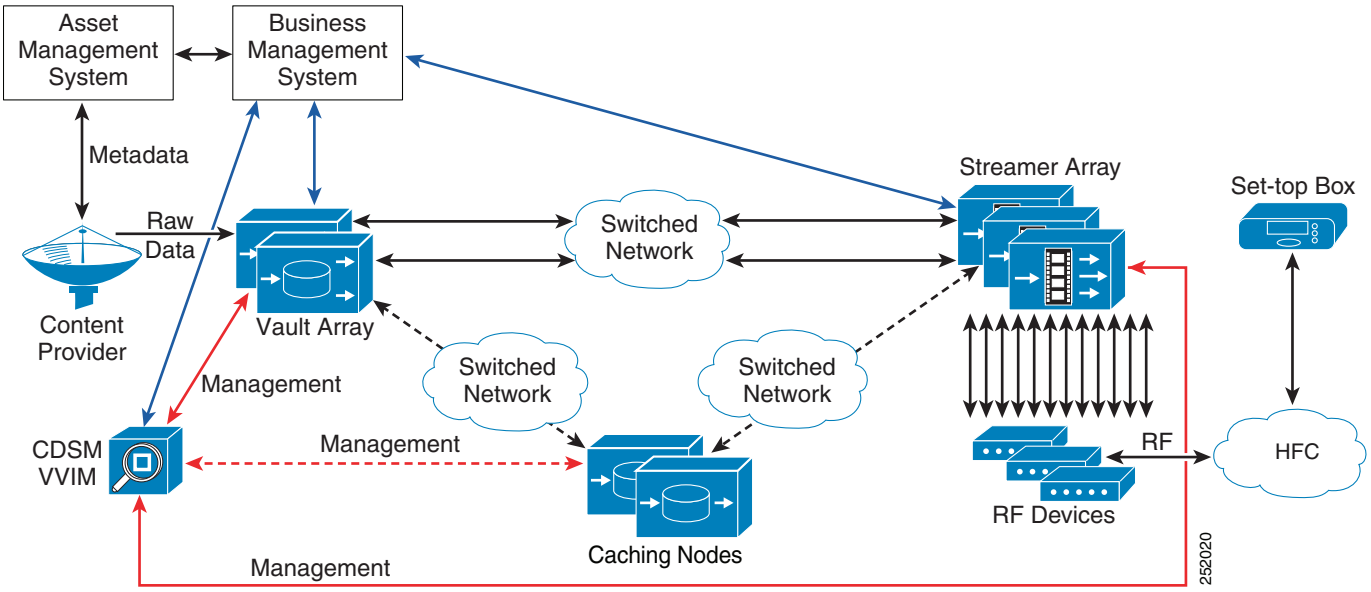
Figure 1-1 illustrates how a VDS network can be deployed. A business management system (BMS), commonly called a backoffice, enables service providers to deploy on-demand services using video on demand (VOD) servers, networks, billing systems and other system components. The asset management system (AMS) manages the content on headend and node servers, while the BMS handles functions related to pitching and catching. Sometimes there is some overlap of functionality between the BMS and the AMS.

There are two types of systems available with the VDS:

- A VDS with an array of Vaults and Streamers
- A Virtual Video Infrastructure (VVI) with an array of Vaults, Caching Nodes, and Streamers

The CDSM manages the Vaults and Streamers in a VDS. The VVIM manages the Vaults, Caching Nodes, and Streamers in a VVI with centralized management. For more information about network design and VVI management, see VDS and VVI Topologies, page 2-2. Figure 1-1 shows a high-level view of both a VDS and a VVI.

Figure 1-1 High-Level System View of VDS and VVI



The VDS solution has three major elements:

- A Vault array consisting of one or more Vault servers. The Vault array is responsible for ingest and reliable storage of video on demand (VOD) content. The number of Vault servers in the Vault array is driven by the amount of content that the system offers and the degree of redundancy.
- One or more Streamer arrays each consisting of one or more Streamer servers. The Streamer array is responsible for the personalization and streaming of content in response to user requests. The number of Streamer servers and Streamer arrays is determined by the number of streams deployed and by the topology that best suits your individual network and redundancy requirements.
- A CDSM server. The Content Delivery System Manager is used to manage the Vault and Streamer servers, collect event logs, and provide reporting tools.

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

The VVI solution has four major elements:

- One or more Vault Groups consisting of one or more Vaults. The Vaults are responsible for ingest and reliable storage of VOD content. The number of Vaults in the Vault Group, and the number of Vault Groups is driven by the amount of content that the system offers and the degree of redundancy.
- One or more Cache Groups, consisting of one or more Caching Nodes. The Caching Nodes provide more flexibility in designing a multi-tiered VVI by acting as a tier between the Vaults and the Streamers. The Caching Nodes facilitate content distribution and remove distribution traffic from the network backbone.
- One or more Stream Groups each consisting of one or more Streamers. The Stream Group is responsible for the personalization and streaming of content in response to user requests. The number of Streamers and Stream Groups is determined by the number of streams deployed and by the topology that best suits your individual network and redundancy requirements.
- The CDSM is used to manage the Vaults, Streamers, and Caching Nodes in the same array, collect event logs, and provide reporting tools. In a split-domain management system configuration, there is a Stream Manager that manages all the Streamers, and a VVI Manager (VVIM) that manages all the Vaults and Caching Nodes.

VDS Software

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

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

Content is delivered across the network in response to cache-fill calls from the Streamers in an opportunistic manner, depending on the availability of bandwidth; delivery can be faster than real-time delivery where bandwidth allows. The VDS software that ensures content on the Streamer servers is

always the most popular content; that is, the content requested by the largest number of subscribers. User requests are generally served from the cache on the Streamer. Requests for content that are not already in the local cache on the Streamer are pulled from the Vault, cached on the Streamer, and streamed to the subscriber. Wherever the content is stored relative to the point of playout, all content appears as if it is local to the Streamer and the streaming of any content is nearly instantaneous.

Caching Nodes

A Caching Node is an intermediary fill source for the Streamers. Caching Nodes are deployed in VVIs. The VVI is a deployment type of the VDS. In a VDS, servers cannot communicate with servers in other groups. In a VVI, servers in other groups can communicate with each other on an as needed basis. Streamers and Caching Nodes dynamically discover fill sources within other groups. Streamers send cache-fill calls to remote servers (Streamers in other Stream Groups and Caching Nodes) for content that is not found locally (DRAM, disk cache, or peer Streamers). In a VVI, the Caching Nodes can communicate with the Streamers by using CCP or HTTP. For more information on how a Caching Node interfaces with a CCP Streamer and an HTTP Streamer, see Caching Node Workflow, page 2-12.

Streamer Load Balancing

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

CServer Functionality

The CServer is responsible for the following:

- Storing content
- Streaming content
- Managing bandwidth usage for ingests
- Managing bandwidth usage for streaming
- Mirroring content among Vault servers
- Making decisions on content retention on Streamer servers

Streamer Content Delivery Applications

On top of the CServer, and taking advantage of the services it offers, a variety of applications deliver individual personalized entertainment services. Cisco currently offers the following applications:

- TV Streamer delivering VOD and network personal video recorder (nPVR) services
- TV MediaX Suite for simplifying ingest and workflow scheduling tasks for asset-based and real-time content

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

TV Streamer CDA

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

TV MediaX Suite CDA

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

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

Content Delivery

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

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

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

The key content delivery capabilities include the following:

- Supports multiple content formats (high-definition and standard-definition content, multiple video codec formats, multiple media file types, and so on)
- Supports ingest and streaming of real-time video services, VOD services, and Internet video
- Supports advertising content distribution and streaming
- Supports nPVR capabilities to provide a digital video recorder (DVR)-like experience with the network
- Provides a single content delivery network for serving set-top boxes (STBs), PCs, and mobile devices
- Supports content security and encryption
- Supports narrowcast service such as VOD, time-shifted TV, and switched digital video (SDV) sharing the same infrastructure
- Supports both traditional and next-generation STBs and headends

Content Chunking

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

Note The Content Chunking feature is disabled by default. All the VDS servers in a deployment must be upgraded before enabling this feature. To enable, the following line must be added to the setupfile of each VDS server and the server must be rebooted: **content id type 2**

Playlist Enhancements

Beginning with VDS-VR (formerly TV VDS) Release 3.0, the following playlist enhancements are available:

- Skip Missing Playlist Element
- Mid-Roll Advertisement Placement Accuracy
- Trick-Mode Restriction
- Relax Forward Trick-Mode Restriction After Initial Playback
- Enforce Trick-Mode Restriction for Jump Play Commands

Skip Missing Playlist Element

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

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

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

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

Mid-Roll Advertisement Placement Accuracy

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

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

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

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

Configuring Conversion Mode for Playlist Ranges

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

Trick-Mode Restriction

Restriction of trick-mode controls (pause, rewind, fast-forward) per playlist segment is supported.

If a client issues a trick-mode command for a locked-out playlist segment or attempts to bypass a trick-mode restricted segment by jumping to the next segment, an RTSP/1.0 403 Forbidden response is sent to the set-top box.

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

Relax Forward Trick-Mode Restriction After Initial Playback

Previously, if trick-mode restriction is configured on a playlist element and a fast-forward command is issued, the restricted element ignores the fast-forward command and plays the content at normal speed.

Beginning with VDS-VR (formerly TV VDS) Release 3.0, if the restricted element has been played once from beginning to end at normal speed in a specific session, then the fast-forward trick-mode restriction is relaxed for that element in that session and any further fast-forward commands on the restricted element are honored. This relaxation only applies for that session. Other sessions using the same playlist must play the restricted playlist element at least once at normal speed before the fast-forward command is honored for the restricted element.

Enforce Trick-Mode Restriction for Jump Play Commands

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

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

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

Digital Video Watermarking

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

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

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

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

Enabling Digital Watermarking

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

```
isa 6983 1  0 Sep20 ? 00:01:56 /home/isa/bss/bin/VDSWaterMarkSvr --serverid 188 --groupid
66 --dbpath /tmp/isadb --logfile /arroyo/log/wmsvr.log --loglevel LOW
```

To enable Digital Watermarking, run the **cdsconfig** script on each Streamer and answer yes (y) to the question “Do you want to enable Watermark Server?”

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

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

HTTP Ingest

This feature enables the Recorder to ingest Common Index Format (CIF) based Adaptive Transport Streams (ATS) using HTTP GET operations. Typically, MPEG transport streams are packaged into CIF ATS with Media Presentation Description (MPD) for MPEG Dynamic Adaptive Streaming over HTTP (DASH).

The Recorder interacts with the Media Capture Engine (MCE+) of the Cisco Media Origination System (MOS) to ingest the streams. Both the Recorder and the MCE+ are installed on the same CServer.

The HTTP ingest proceeds as follows:

- The Recorder, on detecting the need to ingest a CIF ATS, interacts with the MCE+ and provides recording details such as the channel MPD URL and ingest interface.
- MCE+ parses the MPD and downloads the CIF ATS segments for each profile listed in the description.
- MCE+ passes on the downloaded segments as a continuous stream through a Unix Domain Socket (UDS) to the CServer, enabling the recording and ingesting of the CIF ATS by the Recorder.

HTTP Live Streaming

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

- Catch-Up to Live
- Play While Ingesting the Same Content

Catch-Up to Live

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

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

Play While Ingesting the Same Content

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

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

H.264/AVC Ingest

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

VOD Error Repair

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

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

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

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

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

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

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

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

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

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

Following is an example of the first SETUP message:

```
SETUP rtsp://192.0.2.100/movie.mpg RTSP/1.0<CRLF>
CSeq: 2 <CRLF>
Transport: RTP/AVPF/UDP; unicast; destination=54.0.1.1; client_port=8998-7123,
           MP2T/DVBC/UDP; unicast; destination=54.0.1.1; client_port=8998<CRLF>

RTSP/1.0 200 OK<CRLF>
CSeq: 2<CRLF>
Session: 12345678<CRLF>
Transport: RTP/AVPF/UDP; unicast; destination=54.0.1.1; client_port=8998-7123;
                          source=101.1.2.3; server_port=50236-50237<CRLF>
```

Following is an example of the second SETUP message:

```
SETUP rtsp://192.0.2.100/movie.mpg/rtx RTSP/1.0<CRLF>
Session: 12345678 <CRLF>
CSeq: 2 <CRLF>
Transport: RTP/AVPF/UDP; unicast; destination=54.0.1.1; client_port=8999-7124<CRLF>
<CRLF>

RTSP/1.0 200 OK<CRLF>
CSeq: 2<CRLF>
```

```
Session: 12345678<CRLF>
Transport: RTP/AVPF/UDP; unicast; destination=54.0.1.1; client_port=8999-7124;
                         source=101.1.2.3; server_port=50238-50239<CRLF>
<CRLF>
```

Note Retransmission-based Error Repair is only available with RTP streaming.

Background

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

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

Error Repair Client on STB

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

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

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

Monitoring

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

AMT

Application Monitoring Tool (AMT) runs a web application on each Streamer and provides several troubleshooting tools. For more information, see Using the VDS Streamer Application Monitoring Tool, page E-1

Validating Recordings

This feature allows the Recorder to specify a list of COIDs for the Recorder Manager to verify. If there are discrepancies, the Recorder Manager takes appropriate action.

To trigger the Recorder to send this list to the Recorder Manager, send an HTTP GET request to the following Recorder URL:

http://recorder ip:port/rec/record/ValidateRequest

A COID is included in the list based on the age of the recording. COIDs of recordings older than the number of days specified in the ValidateRecordingInDays parameter are included in this list. The ValidateRecordingInDays parameter is saved in /home/isa/bss/etc/recsvr.conf.

To set the validation age for the recordings by using the CDSM, see Configuring Shared Recorder Settings, page 4-19 and Configuring Individual Recorder Settings, page 4-75.

Integrated Streamer Recorder (ISR)

Beginning with VDS-VR (formerly TV VDS) Release 3.4, VDS supports an Integrated Streamer/Recorder platform, a new server type based on VDS architecture. ISR has multiple control interfaces that interacts with external systems to provide recording, streaming, and delivery functionalities. It also has both high throughput ingress and egress data interfaces.

The ISR also supports the separation of configuration management and login network traffic from the control traffic with external systems using a separate configuration interface. By default, the configuration management traffic shares the control (management) interface with the control traffic.

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

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

ISR Monitoring via GUI	Description
System Level Monitoring	
System Health	Monitoring of ISR Server health
Server Level Monitoring	
Disk Monitor	Monitoring of Disk Statistics
NIC Monitor	Monitoring of NIC on ISR Server
Server Vitals	Configuration of Individual Recorder settings
Services Monitor	Monitoring of Services on ISR Server

Media Origination Suite (MOS) 2.x VOD Support

MOS Release 2.0 introduces the following new features:

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

Beginning with VDS-VR (formerly TV VDS) Release 3.4, VDS-TV supports IP delivery to ABR clients on VOD application from VDS Vault cluster via ATIS C2. Multi-Bitrate Adaptive Transport Stream (ATS) files generated from VOD Transcoder (ex: CTM) are ingested onto Vault and this workflow is controlled by CMS/VMS. CMS/VMS controls ingestion of ATS files as well as all associated metadata files and vault serves those files to VOS via ATIS C2 using HTTP 1.1 interface.

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

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

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

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

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

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

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

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

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

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

For detailed information on MOS 2.x architecture, refer the following documents:

- *Cisco Media Origination Suite Release 2.x Software Installation and Configuration Guide*
- *Cisco Media Origination Suite Release 2.x API Guide*
- *Cisco Media Origination Suite Release 2.x Command Reference*
- *Cisco Media Origination Suite Release 2.x Alarms and Error Messages Guide*
- *Release Notes for Cisco Media Origination Suite Release 2.x*

Content Delivery System Architecture

Vaults and Streamers have different but important functions that are required for the VDS software to run efficiently. The Integrated Streamer-Vault (ISV) server combines the functionality of both the Vault and Streamer for smaller networks. The Content Delivery System Manager (CDSM) provides a browser-based user interface for configuration, monitoring, maintenance, and reports of the VDS solution. In a VVI, the Caching Nodes provide a pure caching layer for a multi-tiered VVI. Figure 1-2 shows the different elements of the VDS and VVI with the addition of the Caching Nodes.

Figure 1-2 High-Level View of the VDS and VVI

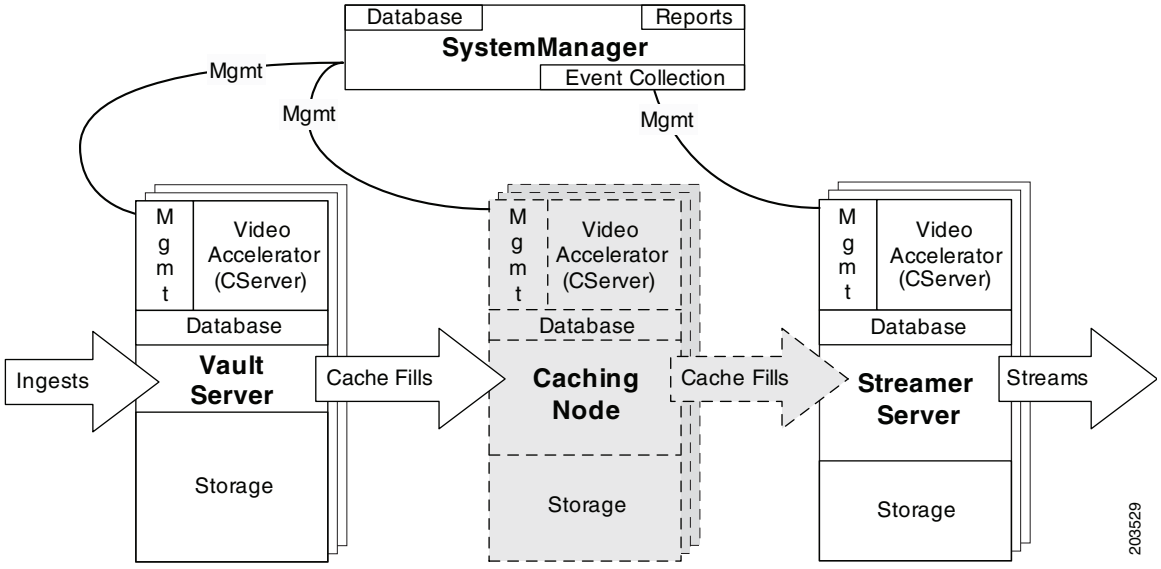


Table 1-2 describes the system elements shown in Figure 1-2.

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

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

Vault

The Vault ingests content delivered over a standard interface (for example, using FTP to receive content from a catcher), performs whatever processing is required (for example, generating trick-play files), and stores the processed content reliably on disk. A Vault Group consists of a scalable number of Vaults that divide the responsibility for ingest and storage among the members of the group. Vault servers can be colocated or distributed to multiple locations across an IP or Ethernet network. Each Vault can simultaneously ingest up to 160 channels of MPEG-2 transport stream (TS) content and store up to 6000 hours of MPEG-2 TS standard definition content with two mirrored copies of the content and one or two trick files.

VDS-VR (formerly TV VDS) Release 3.0 and later support 600,000 assets for RTSP environments. This support has the following limitations:

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

- Maximum number of assets per Vault is 65,000.

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

Streamer

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

Caching Node

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

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

Integrated Streamer-Vault

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

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

CDSM and VVIM

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

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

The VVIM provides centralized management function for the VVI, including configuration, monitoring, troubleshooting, reporting, and maintenance. The VVIM in a centralized domain management configuration manages the Vaults, Caching Nodes, and Streamers, The VVIM in a split-domain management configuration manages the Vaults and Caching Nodes, while the Streamers are managed by the Stream Manager. For more information about split-domain management, see VVI Management, page 2-6.

In both the VDS and VVI, all Vaults and Streamers are identified by an array ID, a group ID, and a server ID. In the CDSM GUI, the array ID identifies servers that are part of the same system, the group ID identifies servers that are part of the same group (Vault Group or Stream Group), and the server ID is a unique number that identifies the server. Table 1-3 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

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

CDSM GUI ID Name	CServer Files ID Name
Array ID on the Array Name page	groupid
Group ID on the Server-Level pages	groupid
Stream Group ID on the Server Setup page	arrayid
Cache Group ID on the Server Setup page	arrayid
Vault Group ID on the Server Setup page	arrayid
Stream Group ID on the Configuration Generator page	arrayid

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

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

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

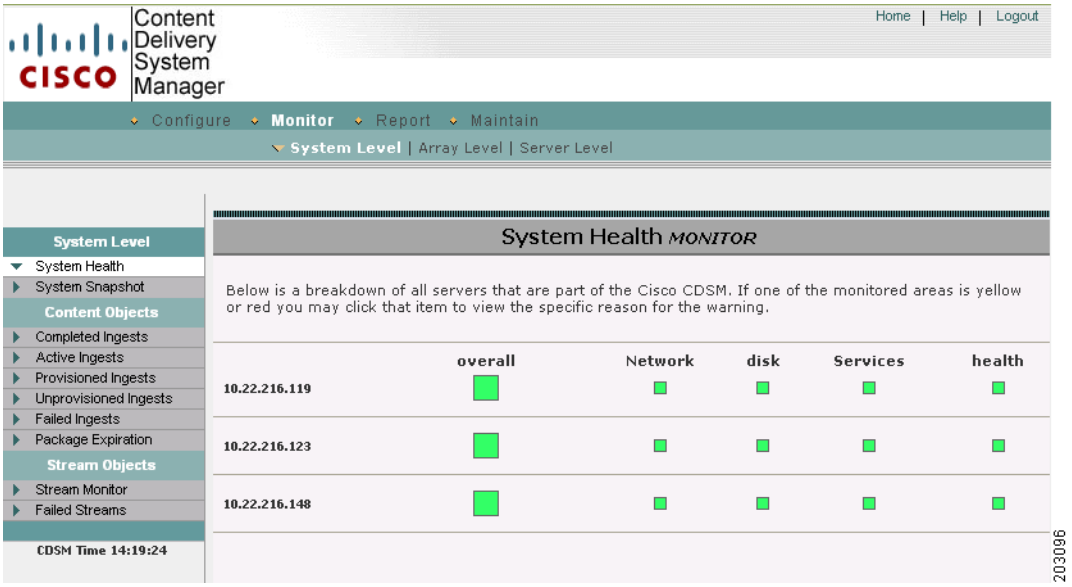
The CDSM and VVIM offer a drill-down approach to show the status of any stream or ingest point, or the physical status of any piece of hardware.

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

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

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

Figure 1-3 Content Delivery System Manager User Interface



Resiliency and Redundancy

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

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

Vault Disk Redundancy

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

Mirroring

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

There are three types of mirroring:

- Local mirroring
- Mirroring within an array
- Array mirroring (from Vault Group to Vault Group)

Local Mirroring

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

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

Mirroring within an Array

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

Array Mirroring

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

Note Array Mirroring is part of the Vault Groups feature and is only available if Vault Groups is enabled on the CDSM Setup page. For more information, see Vault Groups, page F-6.

Vault Server Resiliency

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

Vault Master

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

Vault Group Redundancy

In addition to the Vault server redundancy, the VDS offers redundancy for Vault Groups. When the VDS is configured with Vault Group redundancy and at least two Vault Groups are configured, the system handles the loss of an entire Vault Group without impacting the subscriber experience. Content is mirrored among as many as four Vault Groups (one Vault Group ingests the content and up to three Vault Groups mirror the content), which may be in different geographic regions. If the primary Vault Group becomes unavailable, because of network, power, or other catastrophic problems, any Streamer or Caching Node that was requesting content from that Vault Group would fail over to the other Vault Group until the primary Vault Group came back online and could again respond to cache-fill requests for content.

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

Note The maximum number of Vault Groups is 20.

Streamer Disk Redundancy

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

Streamer Server Resiliency

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

Caching Node Disk Redundancy

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

Caching Node Resiliency

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

CDSM Redundancy

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

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

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

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

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

Ethernet Link Resiliency

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

Scalability

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