Network Design

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

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

### Overview

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

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

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

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

### CDS with Vaults and Streamers

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

**CDS with ISVs**

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

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

**TV CDS Topologies**

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

---

**Caution**

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

---

**Note**

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

**Centralized Topology**

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

Decentralized Topology

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

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

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

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

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

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

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

Streamer Workflow

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

- Setup server
- Control server
- Play server

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

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

The Setup and Control server IP addresses are configurable. For an ISA environment, the Setup IP address is the same as the Stream Master IP address. The Stream Service selects a Streamer in the Stream Group to be the Setup server, and another Streamer (sometimes the same Streamer) to be the Control server.
Chapter 2      Network Design

BMS Considerations

Setup Server

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

Control Server

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

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

Play Server

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

BMS Considerations

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

OpenStream ISA Integration

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

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

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

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

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

**nABLE Integration**

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

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

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

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

Table 2-1  CDS Interfaces

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

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

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

Figure 2-8 ISV Network Connections
Ingest Interface

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

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

Management Interface

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

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

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

Cache Interfaces

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

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

Note

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

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

Cache/Stream Interfaces

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

**Streaming Interface**

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

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